Produto 2

Roadmap tecnológico

Versão 2.0

2017

BNDES O banco nacional do desenvolvimento

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL

Esclarecimentos sobre o *roadmap* tecnológico

"O documento referente ao *roadmap* tecnológico registrou as iniciativas desenvolvidas em âmbito global no tema de Internet das Coisas, não levando em consideração questões específicas de qualquer país. Os dados descritos neste documento foram encontrados em diversas fontes públicas, entre o período de dezembro de 2016 a fevereiro de 2017, dentre elas a Consulta Pública intitulada *Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil*.

Foram também consideradas informações coletadas por meio de entrevistas com especialistas de diversos setores relevantes para a implantação da Internet das Coisas no Brasil, bem como aquelas obtidas durante uma oficina realizada em fevereiro de 2017, com a participação de dezenove Instituições Científicas e Tecnológicas (ICTs). Esse esforço de colaboração envolvendo vários atores constituiu, assim, o sólido alicerce sobre o qual repousam os resultados apresentados.

Cabe ressaltar que as tendências tecnológicas relacionadas a IoT descritas no presente documento não representam a opinião ou o juízo de valor do Ministério da Ciência, Tecnologia, Inovações e Comunicações, do Banco Nacional de Desenvolvimento Econômico e Social ou dos membros do Consórcio. "

Lista de Acrônimos

3GPP	3rd Generation Partnership Project
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
API	Application Program Interface
BI	Business Intelligence
BLE	Bluetooth Low Energy
BOM	Bill Of Materials
CI	Circuito Integrado
CMOS	Complementary Metal-Oxide-Semiconductor
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
DEX	HIP Diet Exchange
DTLS	Datagram Transport Layer Security
ERP	Enterprise Resource Planning
GSM	Global System for Mobile communication
IEEE	Institute of Electrical and Electronics Engineers
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
LPWAN	Low-Power Wide-Area Network
LoRa	Long Range Radio
LoRaWAN	Long Range Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MCU	MicroController Unit
MEMS	Micro-Electro-Mechanical Systems
MPU	MicroProcessor Unit
MPW	Multi-Project Wafer
MQTT	Message Queuing Telemetry Transport
MTC	Machine Type Communication
MVNO	Mobile Virtual Network
NAN	Neighborhood Area Network
NB-IoT	NarrowBand IoT
NFV	Network Function Virtualization
PAN	Personal Area Network
SDN	Software Defined Network
SO	Sistema Operacional
SoC	System-on-a-Chip
TLS	Transport Layer Security
UIT	União Internacional das Telecomunicações
WLAN	Wireless Local Area Network

Índice

1. Contexto

O presente documento "*Relatório de Roadmap Tecnológico*" é um dos produtos do estudo "Internet das Coisas: um plano de ação para o Brasil", liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O estudo, que tem por objetivo propor um plano de ação estratégico para o País em Internet das Coisas (em inglês, *Internet of Things* - IoT), está dividido em quatro grandes fases:

- **Diagnóstico Geral e aspiração para o Brasil:** Desenvolver *benchmark* de projetos e políticas de IoT, mapear o *roadmap* tecnológico de IoT no mundo e analisar a demanda e a oferta de IoT no Brasil;
- **Seleção de verticais e horizontais:** Definição de critérios-chave para seleção e priorização de verticais e horizontais;
- **Aprofundamento e elaboração de plano de ação (2017 - 2022):** Aprofundamento nas verticais escolhidas, elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2017-22;
- **Suporte à implementação:** Apoio à execução do Plano de Ação 2017-22**.**

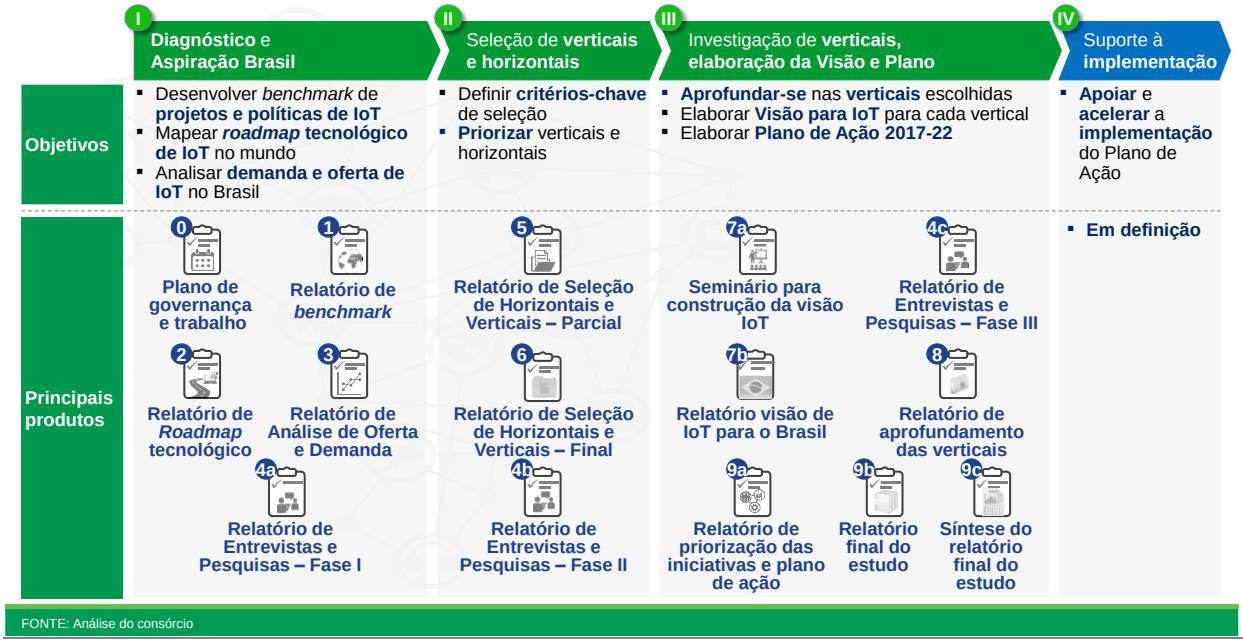
As 3 primeiras fases são compostas de 9 produtos principais, como descrito no QUADRO 1 a seguir. O presente documento representa o Produto 2 e está inserido na Fase 1 do estudo. Os principais objetivos do documento são:

- Descrever as tendências tecnológicas que podem potencializar o florescimento de IoT;
- Identificar atores que estão na fronteira do conhecimento sobre o tema.

Os resultados desse levantamento devem permitir identificar e descrever, ainda que sinteticamente, as principais tendências tecnológicas no mundo de IoT, bem como fazer uma antevisão de sua possível evolução. Outrossim, devem permitir mapear os principais *atores* atuando nos diversos elos da cadeia de valor de IoT, as principais alianças (comerciais ou não), além dos movimentos mais representativos desses atores.

QUADRO 1

Fases e principais produtos do estudo "Internet das Coisas: um plano de ação para o Brasil"



FONTE: Análise do consórcio

Todavia, há que se ressaltar que estas tendências tecnológicas são incertas, não apenas pela evolução imprevisível da tecnologia, sempre com surpresas decorrentes de inovações, mas pelo impacto que as forças de mercado, políticas e regulatórias têm na adoção de uma dada tecnologia. Sendo assim, o presente documento condensa a visão de hoje[1], devendo este trabalho ser atualizado frequentemente a fim de se capturar as esperadas evoluções tecnológicas que possam advir.

Em face da diversidade que o assunto abarca, para endereçar esse desafio o Consórcio se valeu de várias fontes de informação que se mostraram importantes e complementares:

[1] Primeiro semestre de 2017.

- Consulta Pública intitulada "Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil", de dezembro de 2016[2];
- Workshop com Instituições Científicas e Tecnológicas (ICTs)[3];
- Entrevistas com especialistas de diversos setores relevantes à implantação da Internet das Coisas no Brasil[4;]
- Conhecimento tácito do conjunto de participantes do consórcio.[5]

Esse esforço de colaboração envolvendo vários atores constituiu, assim, o sólido alicerce sobre o qual repousam agora os resultados apresentados.

[2] A Consulta Pública, lançada em 12 de dezembro de 2016, recebeu contribuições durante oito semanas, por meio da plataforma digital Participa.br, e foi encerrada em 6 de fevereiro de 2017. Nesse período, foram recebidas 2.288 contribuições, feitas por atores públicos e privados, representantes de associações interessadas na temática de IoT, membros da academia, de ICTs, representantes da indústria e da sociedade civil. Cobrindo 13 categorias de perguntas, a Consulta Pública forneceu subsídios importantes para a construção deste documento, pois trouxe insights relevantes sobre aspectos regulatórios, de P&D, de oferta tecnológica e de capital humano, de demanda (pública e privada), de composição de ecossistemas de investimento e financiamento e, não menos importante, das aspirações do país e do papel do Estado como órgão fomentador de IoT.

[3] O Workshop de Tendências Tecnológicas de IoT e suas implicações para o Brasil foi realizado em 16 de fevereiro de 2017, nas dependências da Universidade Metodista Mackenzie, contando com a participação ativa de 19 ICTs, convidados em função da relevância de sua atuação em IoT no Brasil. Ao longo de todo o evento os participantes tiveram a oportunidade de contribuir com suas visões acerca da evolução das tecnologias habilitadoras da IoT, promovendo assim uma profunda reflexão sobre as principais oportunidades para o Brasil e as barreiras que o país precisa eliminar a fim de lançar bases sólidas para o desenvolvimento de um ecossistema profícuo para a IoT.

[4] Durante os dois primeiros meses de 2017, as equipes do consórcio conduziram entrevistas em profundidade com especialistas de diversos setores, e com atuação em vários ramos de tecnologia, no Brasil e no exterior, com vistas a colher suas contribuições para a elaboração deste Relatório.

[5] O quadro de colaboradores das instituições consorciadas promoveu um levantamento de informações extenso e profundo que, apoiado em seus conhecimentos tácitos, possibilitou enriquecer as análises ora realizadas.

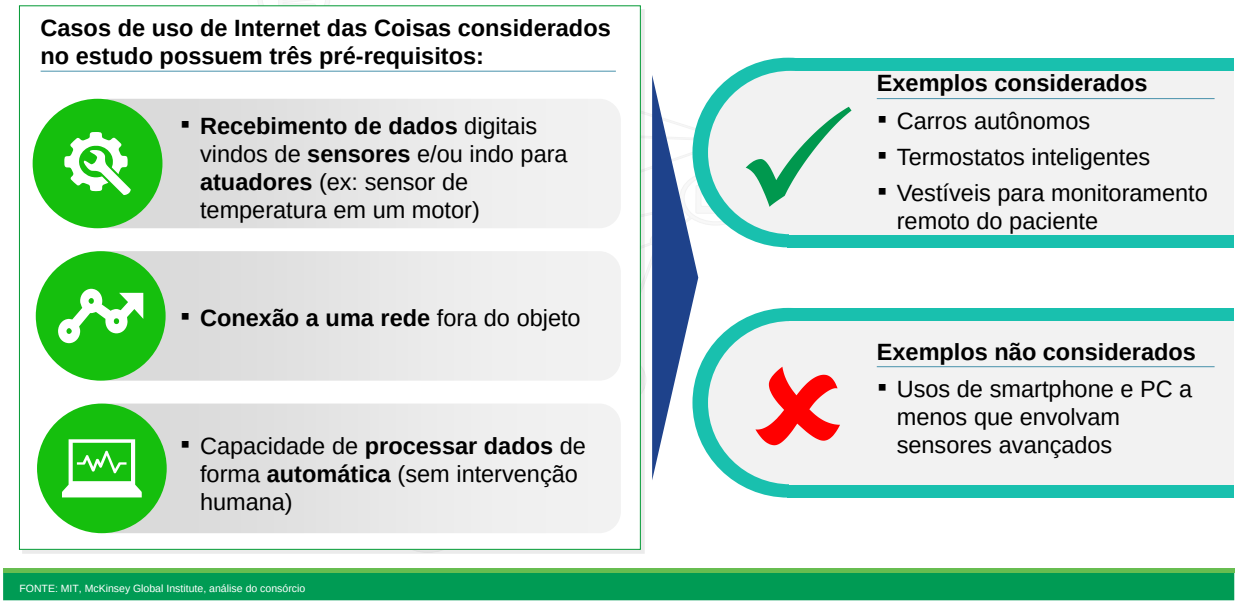
2. Alinhamento conceitual

De acordo com a União Internacional das Telecomunicações (UIT)[6], Internet das Coisas é uma **infraestrutura global** para a sociedade da informação, que **habilita serviços avançados por meio da interconexão entre coisas** (físicas e virtuais), com base nas **tecnologias de informação e comunicação (TIC)**. Em sentido amplo, trata-se não apenas de conectar coisas, mas também de dotá-las do poder de processar dados, tornando-as "inteligentes".

Neste sentido, a Internet das Coisas vem ganhando visibilidade não só devido ao surgimento de **tecnologias disruptivas**, mas também por conta da **evolução de um conjunto de tecnologias já disponíveis**, que estão se tornando mais **acessíveis**, possibilitando sua **adoção em massa**. De forma geral, o estudo utilizou três requisitos básicos para que um caso de uso seja considerado IoT, como descrito no QUADRO 2 a seguir.

QUADRO 2

Pré-requisitos utilizados pelo estudo para que casos de uso sejam considerados IoT



FONTE: MIT, McKinsey Global Institute, análise do consórcio

Ao utilizar tais critérios é possível perceber vários exemplos, tais como: o trator que passa não só a arar a terra, mas também a coletar uma extraordinária quantidade de dados, que serão posteriormente analisados por uma aplicação hospedada em um *data center*, produzindo relatórios que permitem que um agricultor tome decisões sobre onde e quando plantar; uma linha de montagem, que com uso de sensores fornecem dados que são analisados e alertam sobre o melhor momento para se realizar uma parada para manutenção; dispositivos vestíveis (*wearables*) que fornecem informações ao médico sobre

[6] União Internacional das Telecomunicações: agência das Nações Unidas para as tecnologias da informação e da comunicação (TIC).

indicadores relacionados à saúde de um paciente, e; veículos autônomos que conseguem se comunicar de modo a evitar acidentes, dentre outros.

Um importante conceito a ser utilizado nesse estudo são os espaços físicos onde a "Internet das Coisas' opera, denominados "Ambientes de aplicação", tais como residências, cidades e fábricas. A lente de Ambientes é relevante, uma vez que o impacto dos casos de uso normalmente transcende setores específicos. Outra razão para se utilizar a lente de Ambientes reside no fato de que a interoperabilidade e a interação entre diversos atores, pontos cruciais para o desenvolvimento de IoT, normalmente ocorrem dentro de um mesmo Ambiente. O QUADRO 3 exemplifica os principais ambientes de aplicação de IoT.

QUADRO 3

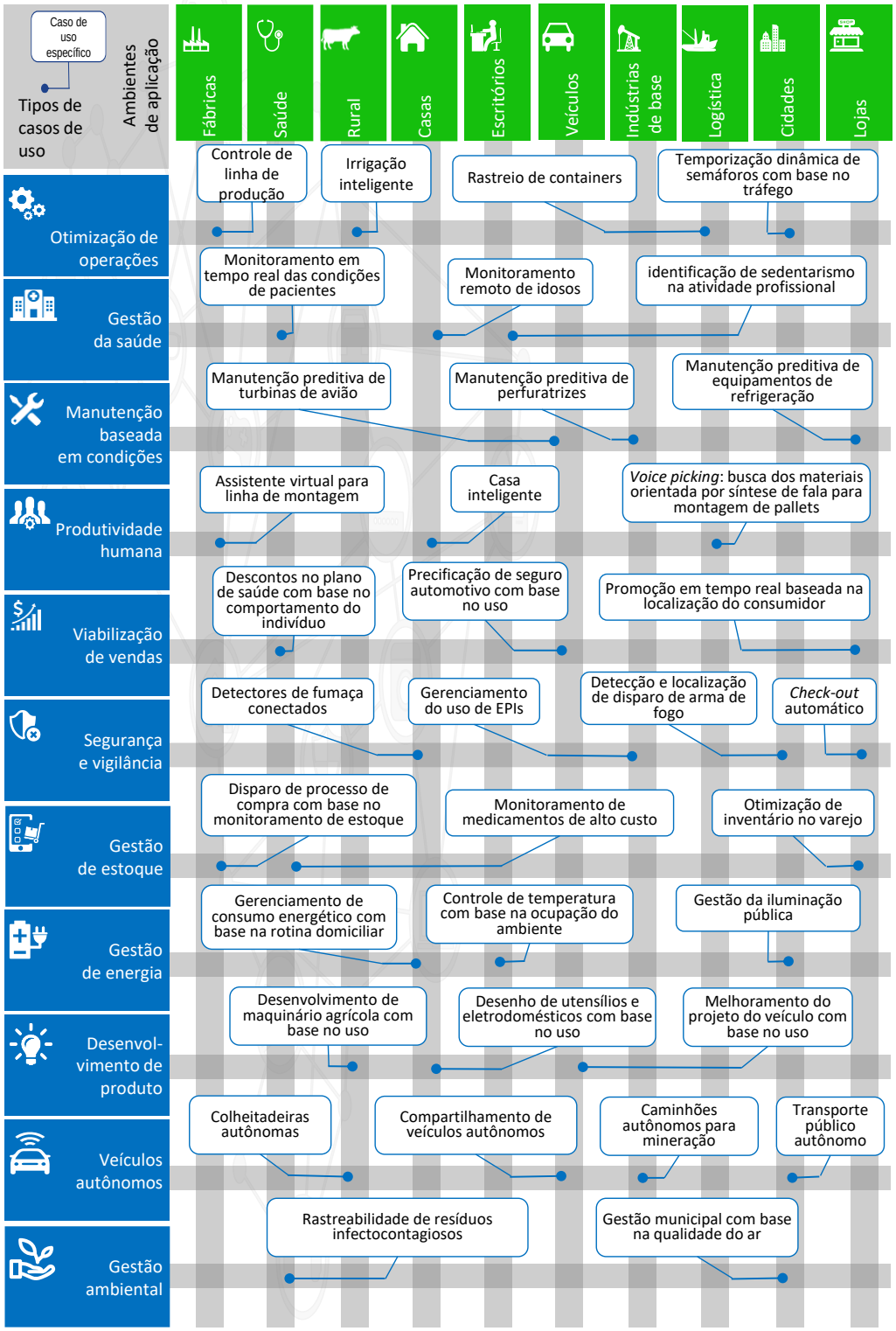
A Internet das Coisas é a rede de todos os objetos que se comunicam e se regulam de forma autônoma via internet

FONTE: Análise do consórcio

Verifica-se então que a Internet das Coisas já é uma realidade e tem gerado oportunidades tangíveis de geração de valor em diversos ambientes de aplicação de IoT. O QUADRO 4 descreve, de forma não exaustiva, exemplos de casos de uso de IoT aplicáveis aos principais ambientes, com base no relatório *Unlocking the potential of the Internet of Things*, elaborado pelo McKinsey Global Institute.

QUADRO 4

Exemplos de casos de uso nos principais ambientes de aplicação de IoT



Visto isto, o presente documento sintetiza a análise realizada no que se refere às tendências nas camadas tecnológicas de IoT, bem como o posicionamento de atores na cadeia de valor de IoT.

As definições de "camadas tecnológicas" e "cadeia de valor" serão apresentadas a seguir.

2.1 Camadas tecnológicas

A diversidade de aplicações da IoT requer o desenvolvimento de inúmeras tecnologias, abrangendo desde o componente semicondutor, que permite a um sensor medir uma determinada grandeza física, passando por um *chip*, que transmite esse dado via radiofrequência, até um servidor que trata a informação, transformando-a em conhecimento e agregando-lhe valor.

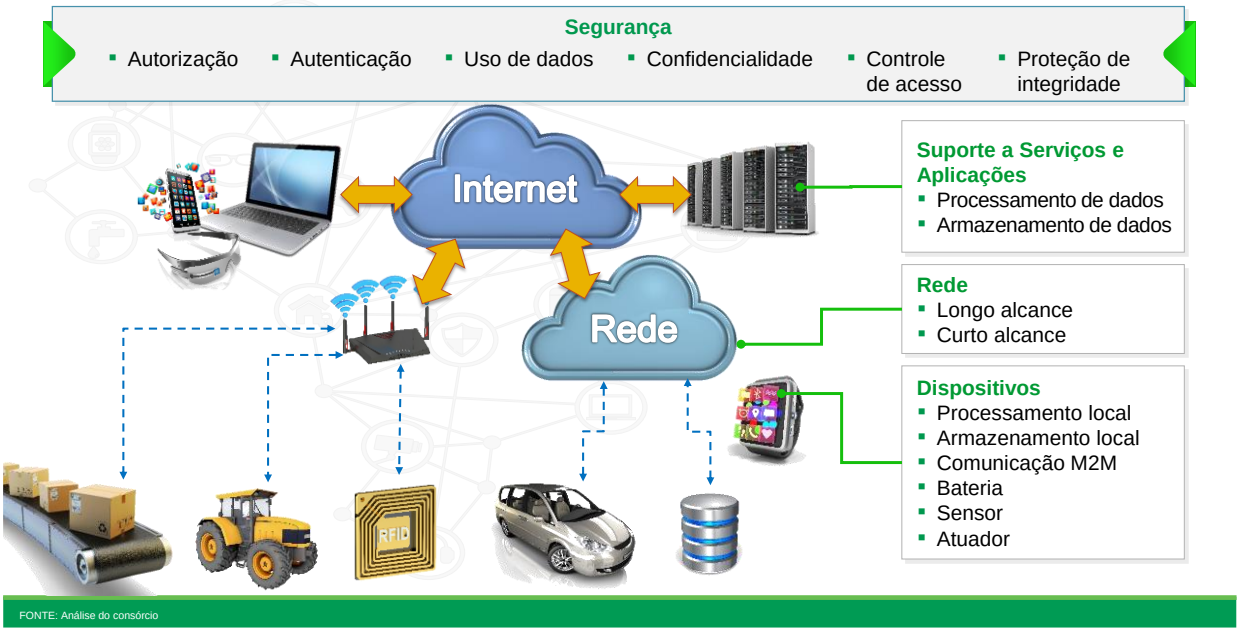
Nesse contexto, a IoT é impulsionada por tecnologias capacitadoras, cuja arquitetura é organizada em camadas, formando uma rede globalmente acessível de coisas, provedores e consumidores. No presente documento, foi utilizada a arquitetura de IoT definida pela União Internacional das Telecomunicações (UIT), baseada em 4 camadas tecnológicas:

- **Dispositivos:** Engloba os levantamentos referentes à evolução dos chips, sensores, atuadores e estruturas de armazenamento e captação de energia**;**
- **Rede:** Fornece funções de conectividade e controle de acesso e mobilidade para serviços de IoT;
- **Suporte a Serviços e Aplicações:** Provêm capacidades de suporte, como processamento ou armazenamento de dados, que podem ser utilizadas por diferentes aplicações de IoT, além de capacidades de suporte de escopo mais específico;
- **Segurança da Informação:** Apresenta tecnologias utilizadas para garantir privacidade e confiabilidade no envio de dados, que permearão todas as demais camadas;

As quatro camadas tecnológicas, assim como exemplos de soluções em cada camada, estão ilustradas no QUADRO 5 a seguir.

QUADRO 5

Principais camadas tecnológicas definidas pela União Internacional das Telecomunicações (UIT)



FONTE: Análise do consórcio

2.2 Cadeia de valor

A cadeia de valor de IoT é definida como o conjunto de oportunidades de geração de valor (por exemplo, novos negócios, conteúdo e serviços) desenvolvidas pelos atores do ecossistema de IoT. A cadeia de valor de IoT é formada por elos que representam grupos de atividades desempenhadas para a entrega de valor aos clientes e usuários.

Foram identificados seis elos da cadeia de valor de IoT (módulos inteligentes, objetos inteligentes, conectividade, habilitador, integrador e provedor de serviço), com base em análises da literatura especializada, validadas por especialistas. As descrições, principais atividades e exemplos de atores em cada elo da cadeia estão detalhados na tabela abaixo.

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Descrição	Compreendem os elementos constitutivos dos objetos inteligentes, contemplando desde componentes básicos, tais como processadores, sensores, atuadores, memórias, *modems* e baterias, até dispositivos mais complexos. Em algumas situações, podem atuar como *gateways* de dispositivos com limitada capacidade de processamento e comunicação.	Consiste nos elementos tangíveis com os quais interagimos no universo da IoT.	Contempla fornecedores de equipamentos e provedores de serviços, que garantem a comunicação entre os elementos que compõem as soluções de IoT.	Oferece os sistemas de suporte para coleta, armazenamento, transformação, análise, visualização dos dados e gerenciamento dos objetos inteligentes	Combina diferentes sistemas, processos e objetos para atuarem conforme as regras de negócios do cliente. Na maioria dos casos, a integração é realizada através de interfaces padronizadas de programação de aplicativo (APIs)[7].	Presta serviços com base em solução fim-a-fim composta por hardware, software e conectividade[8].

[7] API: Application program interface; conjunto de rotinas, protocolos e ferramentas para a construção de aplicativos de software. Especifica como os componentes de software devem interagir, e são usadas ao programar componentes de interface gráfica do usuário.

[8] Soluções fim-a-fim: soluções desempenhadas em todos os elos da cadeia de valor de IoT.

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Principais atividades	Fabricação de processadores, micro controladores, sensores, atuadores, memórias, *modems*, baterias e funcionalidades de segurança e de gerenciamento de *endpoints*.	Sensoriamento, comunicação, atuação, cognição, gestão remota, processamento e armazenamento de energia.	Fornecimento de equipamentos de infraestrutura e serviços de comunicação de dados.	Desenvolvimento e disponibilização de soluções (produtos e serviços) de armazenagem, tratamento de dados (BI[9], *Analytics*, etc.), virtualização e gerenciamento de dispositivos, e também fornecimento de infraestrutura para tais soluções.	Combinação de diferentes sistemas, processos e objetos, inclusive com vistas a atuarem conforme regras de negócios (privados ou públicos). As atividades são voltadas tanto para a integração entre aplicações e os processos de negócio, como entre a aplicação e os módulos inteligentes.	Empacotamento de serviços de IoT que atendam a necessidades de consumidores ou empresas. Criação de um relacionamento direto com os clientes, abrangendo suporte, precificação, faturamento e o provimento de uma solução fim-a-fim.

[9] BI: Business Intelligence: soluções e tecnologias que permitem que uma empresa ou organização aprenda sobre suas operações através de aplicações de relatórios e ferramentas de análise

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Exemplos de atores	Fabricantes de: - Processadores; - Memórias; - Sensores; - Atuadores; - Agregadores / modems; - SIM cards; - Baterias; - Módulos embarcados; - *Gateways;* - Funcionalidade de segurança para *endpoints;* - Funcionalidade de gerenciamento de *endpoints.*	Fabricantes de: - Eletrodomésticos; - Veículos; - Estações de monitoramento; - Equipamentos de automação.	Provedores de: - Soluções de PAN[10] e NAN[11]; - Operadoras; - MVNO[12]; - Solução de segurança para redes; - Solução de gestão de rede; - Fabricantes de equipamentos de rede.	Provedores de: - Armazenamento de dados; - Orquestração de Dados; - Middleware; - *Analytics;* - Controle dos *endpoints;* - Solução de gerenciamento de *endpoints;* - Solução e funcionalidade de segurança (*endpoints*, armazenamento, aplicativos).	Provedores de: - Interfaces de APIs. - Orquestração de Serviços; - Integração com sistemas *back-end* (ERP[13]).	Provedores de Serviço para: - Consumidores; - Empresas.

[10] PAN: personal area network; rede de computadores utilizada para transmissão de dados entre dispositivos como computadores, telefones, tablets e assistentes digitais pessoais.

[11] NAN: neighborhood area network; ramo de hotspots Wi-Fi e redes locais sem fio (WLAN), que permitem aos usuários se conectar à Internet rapidamente e com menor custo.

[12] MVNO: mobile virtual network operator; provedor de serviços de comunicações sem fio que não possui a infra-estrutura de rede sem fio sobre a qual presta serviços a seus clientes.

[13] ERP: Enterprise resource planning; Software de gerenciamento de processos de negócios que permite que uma organização use um sistema de aplicativos integrados para gerenciar o negócio e automatizar muitas funções de back office relacionadas a tecnologia, serviços e recursos humanos

3. Tendências tecnológicas

BNDES O banco nacional do desenvolvimento
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL PÁTRIA EDUCADORA

Em cada uma das camadas tecnológicas foi possível observar uma série de tendências relativas ao desenvolvimento de tecnologias em IoT. Tais tendências, apresentadas na tabela a seguir, refletem a direção geral das tecnologias, com base nas evidências observadas durante a fase de pesquisa e coletas de insumos. Repise-se que, por sua própria natureza, tais tendências podem ou não se concretizar no horizonte de estudo considerado, dadas as condições de contorno e incertezas associadas com a evolução tecnológica.

Tendências por camada tecnológica

Camada tecnológica	Tendências
Dispositivos	1. *Sensor nodes* de IoT tendem a continuar se valendo de unidades micro controladas (UMCs) como computador principal; a evolução destes pode ser marcada principalmente pela queda de custo em relação ao aumento de capacidade. 2. Alguns casos de uso devem demandar um alto desempenho computacional embarcado em objetos inteligentes. 3. Profissionais para o desenvolvimento de software embarcado devem ser cada vez mais requisitados pelo mercado. O diferencial destes profissionais provavelmente se dará pela proficiência no uso de projetos de código aberto de referência. 4. A grande diversidade de casos de uso de IoT tem o condão de estimular inovações em microeletrônica, como SoC customizado, e mecanismos como o MPW (*Multi-Project Wafer*), com potencial de viabilizar projetos de microeletrônica para IoT, inclusive por meio de *start-ups.* 5. *Gateways* devem ser utilizados para uma grande quantidade de casos de uso, prestando serviços (por exemplo, acesso à rede e segurança) aos dispositivos.
Rede	1. As tecnologias SDN (*Software Defined Network*) e NFV (*Network Function Virtualization*) devem minimizar o impacto da IoT no *core* das redes. 2. Para as tecnologias de conectividade de curto alcance *indoor*, tende a ser maior a adoção dos padrões 802.11 do IEEE[14], dada a hegemonia do WiFi para acesso à internet sem fio tanto no ambiente residencial como no corporativo. 3. Um volume considerável de casos de uso deve utilizar dispositivos móveis pessoais (*smartphones* e *tablets*) como *gateways* para sensores e atuadores sem fio, por meio da tecnologia BLE (*Bluetooth Low Energy*). 4. As diversas tecnologias para conectividade de longo alcance provavelmente coexistirão para atender a diferentes casos de uso, seja em faixa de frequência licenciada (com vantagem em áreas com cobertura adequada de rede celular), seja em faixa de frequência não licenciada (utilizada por atores que explorarem a vantagem de *first movers*).

[14] IEEE: Institute of Electrical and Electronics Engineers: associação profissional de engenheiros elétricos e eletrônicos; busca o avanço educacional e técnico da engenharia elétrica e eletrônica, e disciplinas aliadas.

Camada tecnológica	Tendências
	5. É provável que o principal habilitador para tratar dos elementos conectados à rede continue sendo o IPv6.
Suporte a Serviços e Aplicações	1. É provável que o modelo arquitetural de *Edge Computing* seja necessário para tratar de casos de uso que requerem baixa latência; *data centers* devem ficar cada vez mais automatizados, tendo suas funcionalidades virtualizadas e definidas por software. 2. Diversos protocolos de camada de aplicação possivelmente continuarão a ser utilizados, e é provável que o *middleware* tenha um importante papel na interoperabilidade; é provável a coexistência de algumas soluções de *middleware* por vertical. 3. O desenvolvimento de soluções customizadas tende a ser facilitado na medida em que funcionalidades preexistentes em diversas plataformas em nuvem se tornem disponíveis. 4. Bancos de dados não relacionais tendem a ser comuns em diversos casos de uso, dada a tendência de IoT de gerar grandes quantidades de dados (*Big Data*) processados através de *machine learning* de *batch* ou *stream processing*, de acordo com a necessidade do tempo de resposta. 5. No que diz respeito à experiência do usuário, várias tecnologias tendem a se desenvolver, como realidade aumentada e os assistentes virtuais.
Segurança da Informação	1. Novas soluções de IoT tendem a ser cada vez mais voltadas para o princípio de *security by design*. 2. Os maiores desafios têm sido observados na camada de dispositivos, em particular aqueles restritos em termos de processamento, memória e comunicação, que demandam criptografia leve, com suporte complementar nos *gateways*. 3. A segurança das redes provavelmente se dará pela adoção de variantes de protocolos de segurança IP para IoT já consolidados, tais como DTLS, IPsec, *Advanced Encryption Standard*, dentre outros. 4. Em um primeiro momento de implantação da IoT, a necessidade de segurança faz com que cada fabricante verticalize sua solução de segurança, dificultando o desenvolvimento do ecossistema de IoT. 5. Com o amadurecimento da IoT, a falta de padrões de segurança tem levado organismos de padronização a abordar o assunto de maneira segmentada, tratando grandes áreas temáticas, tais como saúde, cidades e transportes inteligentes. 6. A utilização da tecnologia *blockchain* em IoT pode permitir que as aplicações sejam desenvolvidas e utilizadas com um nível maior de segurança e privacidade, dadas as características intrínsecas desta tecnologia. Contudo, é prematuro afirmar que *blockchain* será escolhida para tratar os diversos desafios das implementações e casos de uso IoT de modo geral.

As tendências apresentadas acima serão detalhadas nos próximos subcapítulos. Com o objetivo de facilitar o entendimento, será utilizado um conjunto de casos de uso para

contextualizar a aplicação das tendências. O QUADRO 6 a seguir descreve estes casos de uso, e suas respectivas necessidades em termos de tecnologias de IoT.

QUADRO 6

Exemplos de casos de uso utilizados para ilustrar as tendências tecnológicas observadas

Rastreio de contêineres	Compartilhamento de veículos autônomos	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
▪ Mensagens enviadas por B*eacon bluetooth low energy* (BLE) identificam o contêiner a que está associado ▪ *Gateways* instalados em alguns pontos do trajeto (ex.: portos) recebem, processam a informação localmente, e a enviam para aplicação de rastreio através de conectividade com a Internet. A aplicação dever ser centralizada e acessível globalmente. ▪ Smartphones podem assumir a função dos *gateways* em áreas sem infraestrutura fixa de *gateways*.	▪ Diversos sensores, incluindo câmeras, são utilizados para detecção do ambiente ao redor do veículo ▪ O veículo deve ser capaz de tomar decisões localmente e de forma rápida para evitar acidentes. ▪ Também deve possuir conectividade para que a aplicação possa enviar as requisições dos usuários.	▪ Dados dos sensores das turbinas armazenados durante o voo devem ser descarregados e processados para indicar ações de manutenção ▪ Processamento dos dados não pode demorar mais que algumas poucas dezenas de minutos para que a aeronave receba o aval para iniciar o próximo voo.	▪ Restrição de espaço e custo demanda por dispositivo otimizado que congregue sensor de umidade, bateria, circuito de *energy harvesting* para painel fotovoltaico, bateria, processamento e módulo *wireless*. ▪ Para viabilizar a implantação em áreas extensas as Informações geradas devem ser captadas por poucas estações rádio base de grande cobertura. ▪ Dada a dificuldade de acesso à Internet os dados devem ser processados localmente.	▪ Através do uso de u *smart speaker* o morador solicita por comando de voz que ventilador do cômod seja acionado ▪ *Smart speaker*, conectado à Internet capta e envia o *strea* de áudio para a nuv para que seja processado, ▪ Ventilador recebe da aplicação em nuvem um comando simple de fácil processame para que inicie o funcionamento.

FONTE: Análise do consórcio

3.1 Dispositivos

Na **Camada de Dispositivos, que inclui os dispositivos de acesso (como smartphones, sensores, dentre outros) e *gateways*,** estão concentradas as maiores restrições não-funcionais inerentes à IoT, em especial: custo, consumo energético e espaço físico. Isso gera alguns desafios, dentre eles:

- **Aumento significativo do custo total de objetos de baixo valor**: Em objetos de baixo valor, a adição de sensoriamento, inteligência e comunicação aumenta significativamente o custo total dos objetos, impactando casos de uso como rastreio de latas de refrigerante e identificação de violação de embalagens de alimentos congelados;
- **Restrições quanto ao consumo de energia**: Em grande parte dos casos de uso de IoT, não é possível conectar os objetos à rede elétrica. Portanto, objetos inteligentes precisam ser alimentados por bateria ou indução eletromagnética-um processo limitado em termos de fornecimento de energia. Desta forma, o consumo de energia deve ser suficientemente baixo. Esse desafio afeta casos de uso com objetos de menor tamanho, como uma pílula que mede a temperatura interna do paciente e transmite os dados para um aplicativo do *smartphone*.

Contudo, a evolução dos processos da integração de microeletrônica, ainda obedientes à lei de Moore[15], tem propiciado a superação desses desafios em um número cada vez maior de aplicações. As principais tendências da camada de dispositivos estão elencadas a seguir.

1. O crescimento nas vendas das **arquiteturas de micro controladores de 32 bits**, que já superam em valor de mercado as arquiteturas de 8 bits, é um efeito da IoT no mercado de semicondutores. Tais arquiteturas de 32bits são mais propícias para o desenvolvimento de objetos inteligentes, uma vez que estes não requerem apenas capacidade de processamento, mas também de comunicação, o que, por sua vez, demanda uma grande quantidade de protocolos e sistemas operacionais embarcados.

   Apesar dessa evolução, é provável que **arquiteturas mais robustas, como a de microprocessadores, não se tornem dominantes em *sensor nodes*** para a maioria dos casos de uso de IoT nos próximos anos[16]. Assim, a massificação da implantação se dará menos pelo aumento na capacidade dos dispositivos (com a adoção de arquiteturas superiores a 32 bits e maior quantidade de memória), e mais pela redução de custos, posto que esta permite atender a um número maior de casos de uso.

[15] Lei de Moore: teoria que prevê que o número de transistores em um processador dobraria, em média, a cada dois anos, mantendo o mesmo (ou menor) custo e espaço

[16] ICInsights, disponível em http://www.icinsights.com/services/mcclean-report/report-contents/, acesso em junho de 2017.

2. Dada a grande amplitude de aplicações de IoT, **alguns objetos devem demandar capacidade computacional bastante elevada**. Para exemplificar, os veículos autônomos terão capacidade computacional local similar à de servidores em *data centers*[17].

3. A massificação de aplicações baseadas em micro controladores tem um impacto na mão de obra. Arquiteturas microcontroladas, mesmo de 32 bits, em geral não permitem de forma satisfatória o uso de linguagens de programação de alto nível, como Java e Python. Nesses ambientes prevalece, o uso de linguagem C/C++. Assim, restringe-se significativamente **o número de profissionais para o desenvolvimento de software embarcado capacitados em linguagens com C/C+**, hoje estimado em cerca de 500 mil em todo o mundo.

   Essa restrição de mão de obra também se configura como uma oportunidade para países que desejam atender a demandas de desenvolvimento de projetos de objetos inteligentes. Para tal, o investimento de recursos para formação de engenheiros de software embarcado pode resultar na criação de um diferencial estratégico. No entanto, a formação desse tipo de profissional pressupõe a capacitação necessária em projetos de código livre de referência, como sistemas operacionais de tempo real, que já implementam diversas funcionalidades necessárias à IoT. Desta forma, a proficiência em linguagens de programação de menor nível e a customização de soluções já desenvolvidas para demandas específicas serão qualidades esperadas do profissional que desenvolve software embarcado para IoT.

4. **Diante do amplo espectro de casos de uso de IoT, abre-se a oportunidade para novos atores no segmento de microeletrônica de propósito específico**. Embora as previsões de crescimento de dispositivos conectados à rede indiquem valores da ordem de dezenas de bilhões implantados nos próximos anos, os inúmeros casos de uso, com necessidades distintas, devem impedir uma predominância de um ou poucos tipos de objetos inteligentes.

   Isso se configura como um desafio para o desenvolvimento de componentes integrados para atender a casos de uso diversos, uma vez que a previsão relativamente baixa de volume não justifica o alto investimento exigido por esses projetos.

   De forma geral, os casos de IoT podem ser agrupados em três blocos, de acordo com o volume de vendas e o número de casos de uso atendidos, como mostram o QUADRO 7 e a descrição a seguir:

   - **SoC específico**: Pequeno número de casos de uso, que demandam um volume de vendas de centenas de milhões de SoCs[18]; nesses casos, é justificado o

[17] Intel, disponível em http://www.intel.com.br/content/www/br/pt/automotive/go-automated-accelerated-product-brief.html, acesso em junho de 2017.

[18] SoC: system-on-a-chip: circuito que integra os componentes de um computador ou de outros sistemas eletrônicos, como *smartphones*

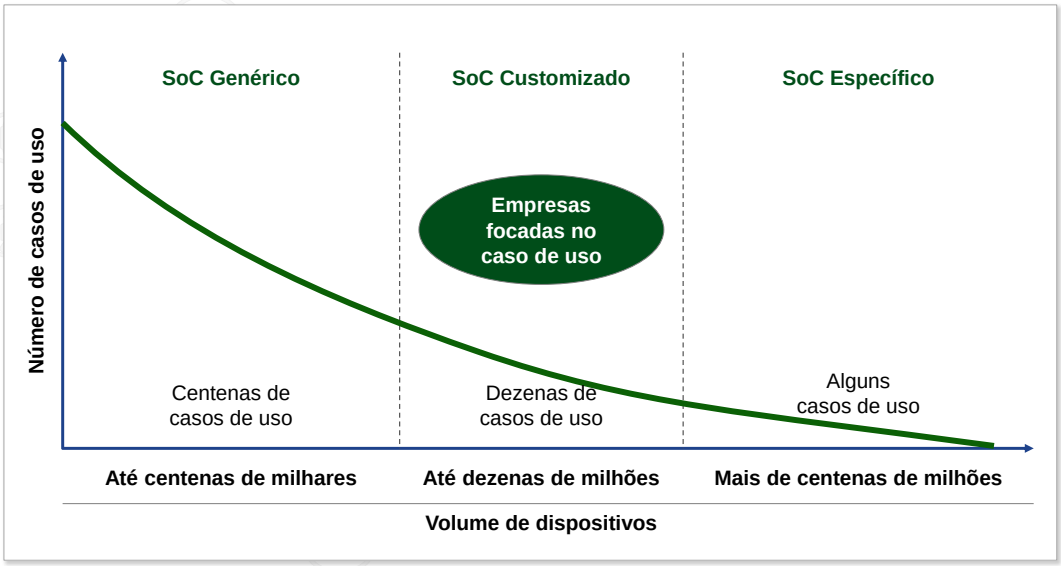
desenvolvimento de semicondutores específicos. Estão bem posicionadas nesse mercado grandes empresas de semicondutores;

- **SoC customizado**: Maior número de casos de usos (dezenas), com volumes de até dezenas de milhões de dispositivos por ano, o que abre espaço para inovações em microeletrônica, como SoCs customizados, que, no contexto de um ecossistema de IP (Intellectual Property), *cores* e técnicas de desenvolvimento ágil, permitem a criação em poucos meses de semicondutores mais competitivos que as soluções especializadas em nível de eletrônica discreta, e com desenvolvimentos que se pagam com volumes a partir da ordem de poucos milhões de unidades. Da mesma forma, técnicas como MPW (Multi Project Wafer)[19] tornam possível a viabilização das primeiras amostras com investimentos moderados. Neste caso, merecem destaque os atores cujo foco recaia na criação de soluções para o atendimento de casos de uso específicos;

- **SoC genérico**: Grande número de casos de uso (centenas), que devem gerar demandas na ordem de até centenas de milhares de unidades por ano. Neste caso, são utilizados SoCs genéricos capazes de tratar de forma não ótima diversos casos de uso por meio da especialização em nível de eletrônica discreta e software embarcado.

QUADRO 7

Casos de uso versus volume de dispositivos



FONTE: Análise do consórcio

5. *Gateways* devem ser utilizados para uma grande quantidade de casos de uso, prestando serviços (por exemplo, acesso à rede e segurança) aos dispositivos. Os ***gateways*** de IoT devem ter por base o uso de processadores similares aos aplicados em microcomputadores, configurando um mercado mais concentrado e com poucas oportunidades locais em semicondutores. Contudo, também em razão da grande

[19] Multi Project Wafer: serviço de protótipo que permite que vários clientes e projetos compartilhem recursos comuns, como wafers de engenharia, reduzindo os custos de design e prototipagem.

diversidade de casos de uso, poderá haver espaço para o desenvolvimento de soluções no âmbito da eletrônica, empacotamento mecânico e software que implementem funções complementares às capacidades, em geral limitadas, dos *sensor nodes*.

A título de ilustração, algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como mostra o QUADRO 8.

QUADRO 8

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de dispositivos

Rastreio de contêineres	Compartilhamento de veículos autônomos	Irrigação inteligente	Casa Inteligente
Tendências 1 e 5	**Tendência 2**	**Tendências 3 e 4**	**Tendências 1, 3, 5**
▪ O módulo inteligente adicionado ao contêiner deve ter custo moderado e baixo consumo para permitir a implantação massiva e não tornar a operação inviável dada a troca frequente de bateria. ▪ Os gateways localizados em pontos importantes ao longo do trajeto auxiliam o objeto inteligente a enviar a sua localização para a aplicação em nuvem.	▪ A grande quantidade de sensores, em especial câmeras, gera uma grande quantidade de informação que requer alto capacidade de processamento local para a tomada de decisão.	▪ A heterogeneidade da IoT aliada a requisitos de baixo consumo energético, custo e restrições de espaço demandará por inovações em microeletrônica, como a criação de SoC customizados, SiP e MPW ▪ O desenvolvimento do software embarcado requer mão de obra especializada dada as especificidades deste componente customizado.	▪ Muitos eletrodomésticos possuem restrição de custo, o que limita a capacidade do processamento embarcado. ▪ Diversidade de eletrodomésticos requer software embarco específico. ▪ *Smart speaker* atua como *gateway* que uniformiza a interface com o usuário e facilita as ações dos objetos.

FONTE: Análise do consórcio

3.2. Rede

Na **Camada de Rede, que inclui os equipamentos que promovem a conectividade entre os dispositivos e a nuvem,** há desafios bastante heterogêneos, uma vez que a IoT abrange inúmeros casos de uso para os quais os requisitos de rede são específicos, tais como:

- Para aplicações de tempo real, como a comunicação entre veículos autônomos, a latência de comunicação, assim como o tempo de resposta, são fatores cruciais que estão diretamente relacionados à rede;
- Aplicações que demandam baixo tráfego de dados e convivem com uma grande dispersão geográfica (por exemplo, agricultura de precisão) impõem um novo paradigma para a evolução das tecnologias, na contramão do que tem sido desenvolvido na última década, onde a maior capacidade de banda era o objetivo predominante.

Devido à diversidade de dispositivos e aplicações, com os mais variados requisitos de qualidade de serviço, a camada de acesso da IoT poderá ser de natureza heterogênea, com **tecnologias de acesso gerais e de nicho compondo um vasto ecossistema**. As principais tendências dessa camada são elencadas a seguir.

1. As tecnologias **SDN (*Software Defined Network*)**[20] e **NFV (*Network Function Virtualization*)**[21], que podem ser empregadas não apenas no *backhaul*, mas também no *core*, devem minimizar o impacto da IoT nas redes. Diferentemente do que ocorre com usuários humanos, a comunicação entre as máquinas tem em geral um caráter periódico e regular, independentemente do período do dia, do dia da semana, do mês ou do ano. Se os dados, que podem ser da ordem de dezenas de bilhões de dispositivos, forem todos para a nuvem, simultaneamente, poderão gerar gargalos de rede. Ambas as tecnologias permitem reconfigurar a rede de maneira rápida e eficiente, reservando recursos e garantindo qualidade de serviço para as aplicações, conforme necessário.
2. Para as tecnologias de **conectividade de curto alcance *indoor*, tende a ser maior a adoção dos padrões 802.11 do IEEE**. Com o aumento expressivo de dispositivos WLAN em IoT, é provável que seja necessário utilizar uma maior quantidade de soluções baseadas em espectro não licenciado, assim como *femtocells*, para complementar os serviços celulares fornecido pelas operadoras por meio de novas tecnologias complementares às coberturas *outdoor*, por exemplo: LTE-U (*Long Term Evolution – LTE in Unlicensed spectrum*).

[20] Software Defined Network: técnica que permite aos administradores de rede gerenciar dinamicamente o comportamento da rede.

[21] Network Function Virtualization: utiliza tecnologias de virtualização de TI para virtualizar classes de funções de nó de rede em blocos de construção que podem se conectar em conjunto para criar serviços de comunicação.

3. Alguns casos de uso devem utilizar **dispositivos móveis pessoais** (*smartphones* e *tablets*) como ***gateways* para sensores e atuadores sem fio**, por meio da tecnologia BLE (*Bluetooth Low Energy*).
4. As **diversas tecnologias para conectividade de longo alcance devem coexistir para atender a diferentes casos de uso**, utilizando faixa de frequência licenciada (com **tecnologias padronizados pelo 3GPP**), ou não licenciada (**tecnologias** proprietárias ou semiproprietárias **em faixas não licenciadas como Sigfox e LoRa**).

   As primeiras implantações dessas redes de longo alcance têm sido baseadas em tecnologias proprietárias ou semiproprietárias. Entretanto, no médio e longo prazos, os padrões baseados no 3GPP, como o Narrowband IoT (NB-IoT), tendem a ganhar espaço onde houver cobertura de rede celular, uma vez que se valerão desta infraestrutura e da operação preexistente.

5. Com respeito aos protocolos, o **principal habilitador para tratar** dos elementos conectados à rede **deve continuar sendo o IPv6**. O IPv6 oferece uma série de vantagens, como o acesso a mão de obra familiarizada, o fato de ser o padrão mais utilizado da indústria, além de proporcionar uma série de melhorias de segurança em relação à versão 4. Para contornar as limitações em dispositivos restritos, têm sido desenvolvidos diversos protocolos, como 6LoWPAN (IPv6 *over Networks of Resource-constrained Nodes*), CoAP (*Constrained Application Protocol*) e MQTT (*Message Queuing Telemetry Transport*).

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 9 a seguir.

QUADRO 9

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de rede

Rastreio de contêineres	Compartilha-mento de veículos autônomos	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
Tendência 3	**Tendências 4 e 5**	**Tendência 1**	**Tendência 4**	**Tendência 2**
▪ Em locais intermediários entre a origem e o destino dos containers, em que seja necessário fazer seu rastreio, o uso de dispositivos móveis como *gateways* será factível por meio da tecnologia BLE	▪ Em ambiente de alta disponibilidade de redes de acesso celulares, a comunicação entre veículos autônomos se valerá da ampla cobertura provida pelas tecnologias baseadas no 3GPP ▪ A necessidade de tratar univocamente de veículo requererá a utilização de tratamento por IPv6	▪ A transferência de grandes quantidades de informação extraídas dos inúmeros sensores das turbinas dos aviões será possível por meio do emprego de técnicas de virtualização de rede que permitem alocar dinamicamente os recursos a fim de evitar gargalos em momentos específicos	▪ Em ambientes com cobertura deficitária de redes de acesso celular as soluções baseadas em tecnologias proprietárias ou semiproprietárias podem ser utilizadas para prover conectividade em áreas amplas	▪ Em ambientes *indoor* as tecnologias baseadas no padrão 802.11 devem ser largamente empregadas, haja vista sua já predominância nesses ambientes, seja em uso residencial ou corporativo

FONTE: Análise do consórcio

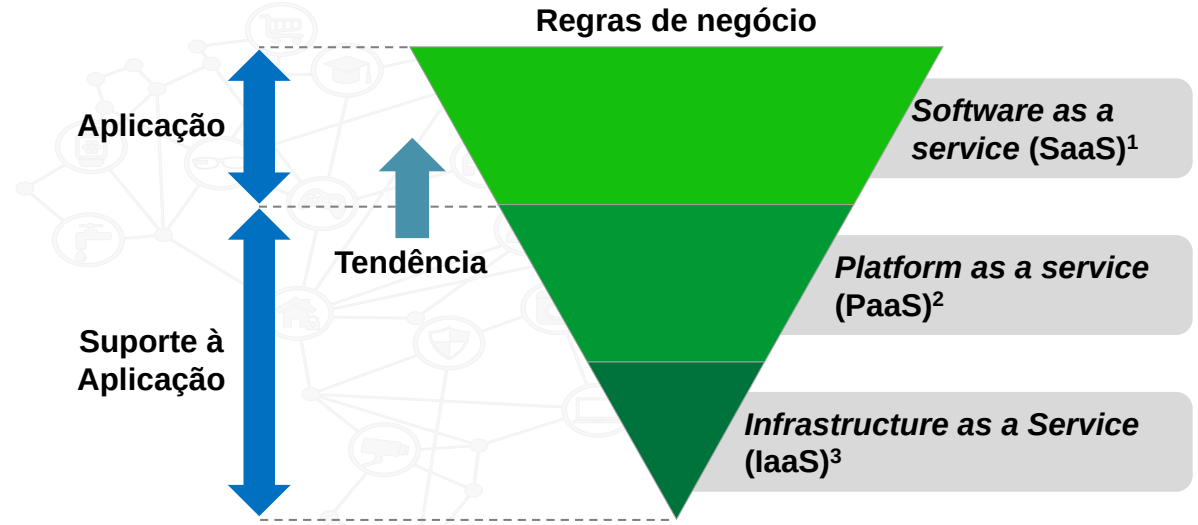
3.3. Suporte a serviços e aplicações

Na **Camada de Suporte a serviços e aplicações,** ocorre a concentração dos dados gerados e transmitidos pelos objetos inteligentes para serem processados e analisados, gerando o valor esperado dos casos de uso. Assim, há o desafio de se armazenar e tratar a imensa quantidade de dados, em especial quando existem rígidos requisitos de tempo de respostas a serem atendidos, por exemplo:

1. A IoT impactará diretamente a infraestrutura de *data centers*, fazendo com que estes evoluam para atender às novas aplicações. Desta forma, espera-se que sejam criados novos **micro *data centers* distribuídos** e mais próximos das bordas (*edge computing*), seguindo um modelo de *cloudlets*, onde ambientes de nuvem reduzidos executam aplicações especializadas no tratamento, filtragem inicial dos dados e resposta a demandas que exigem baixa latência e maior agilidade na resposta.
   Esses *data centers* devem ficar cada vez mais **automatizados,** tendo suas **funcionalidades virtualizadas e definidas por software**. Os modelos de armazenamento de dados devem ser unificados por meio de interfaces centralizadas e bem definidas.
2. Em relação ao ***middleware***, devido à natureza diversa dos casos de uso em IoT, **é provável que algumas arquiteturas coexistam por vertical**. Com o amadurecimento do ecossistema, tende a haver uma consolidação de alguns deles, tornando necessário interoperá-los. Esse fato deve redundar na padronização ou no surgimento de mediadores/orquestradores para facilitar a integração.
   Assim como **devem coexistir várias arquiteturas de *middleware***, também devem coexistir vários protocolos de comunicação, uma vez que cada um tem características específicas que justificam sua aplicabilidade a casos de uso bem definidos. Os produtos de *middleware* devem ser integráveis aos protocolos do seu nicho de aplicação.
3. O **desenvolvimento de soluções customizadas tende a ser facilitado** na medida em que **funcionalidades preexistentes em diversas plataformas em nuvem se tornem disponíveis**. Com isso, o desenvolvimento de aplicações tende a ter um *time-to-market* cada vez menor, dependendo menos de *expertise* em programação e mais de conhecimento dos negócios em si, como pode ser visto no QUADRO 10.

QUADRO 10

Tendência para desenvolvimento de aplicações de IoT



1 Modelo de entrega em que o software é licenciado em uma base de assinatura e é hospedado centralmente
2 Categoria de serviços de computação em nuvem que fornece uma plataforma que permite aos clientes desenvolver, executar e gerenciar aplicativos
3 Tipo de computação em nuvem que fornece recursos de computação virtualizados pela Internet

FONTE: Análise do consórcio

4. O armazenamento de dados em IoT é um problema de *Big Data*, devido ao volume de dados e, consequentemente, **bancos de dados não relacionais tendem a ser utilizados em diversos casos de uso**. Já os **bancos de dados relacionais devem continuar relevantes nos cenários em que os dados são estruturados ou podem ser pré-processados**. Outra forma de tratar o volume de dados vem da adoção do conceito de dados espaço-temporais, por ser uma forma relevante de dividi-los por local e horário de ocorrência. Essa evolução tende a alavancar os dados para diversos usos, como monitoramento de dados para prevenção, dados para valorizar a automação via validação e enriquecimento de dados, além dos mais diversos usos do *analytics*.

   A **Inteligência Artificial (IA)** é atualmente incorporada à própria aplicação, com o suporte de bibliotecas padronizadas. Alguns atores, no entanto, buscam oferecer, em suas plataformas, serviços de IA mais ou menos complexos. A adoção dessas plataformas, porém, tem sido restrita, devido ao fato de que o uso eficiente de IA demanda alto grau de customização para explorar características específicas de cada problema abordado.

   Outro ponto que merece destaque é como conciliar a alta demanda de mecanismos de IA com o **pequeno número de profissionais capacitados na área**. O uso de métodos baseados em *transfer learning* pode acelerar o desenvolvimento de aplicações de IA por meio do reuso de modelos, porém um maior desenvolvimento de técnicas de *meta-learning* pode vir a ser a solução adequada no médio e longo prazos.

Adicionalmente, considerando a necessidade de sistemas mais dinâmicos, provavelmente ganhará relevância o **aprendizado a partir de fluxos de dados** (*stream*), em contraposição ao atual domínio das técnicas baseadas em grandes cargas de dados (*batch*). Formas de **aprendizado contínuo**, como aprendizado *online* e por reforço, tendem a crescer em relevância no médio prazo.

5. No que diz respeito à **experiência do usuário**, várias tecnologias tendem a se desenvolver, como **realidade aumentada**, **realidade virtual** e **assistentes virtuais**.

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 11 a seguir.

QUADRO 11

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de suporte a serviços e aplicações

Rastreio de contêineres	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
Tendência 3 ▪ Aplicação desenvolvida em plataforma em nuvem (PaaS) com cobertura global e que provê diversas funcionalidades que simplificam o seu desenvolvimento	**Tendências 1 e 4** ▪ Havendo indisponibilidade de rede o uso de técnicas como *edge computing* associado a *batch processing* permite atender os rígidos requisitos de tempo de processamento ▪ Por sua vez, o data center deve ser dinâmico para acomodar horários de pico no aeroporto	**Tendência 2** ▪ Dadas as restrições de conectividade com a rede ampla, os dados são armazenados em *middleware* instalado localmente e especializado para casos de uso do ambiente rural, facilitando o desenvolvimento da aplicação que controla os aspersores de água que irrigarão a plantação com maior eficiência	**Tendência 5** ▪ Através do uso de um *smart speaker* o morador solicita por comando de voz que o ventilador do cômodo seja acionado. O *stream* de áudio é enviado para a nuvem para que seja processado pelo sistema de assistente virtual que envia o comando para que o ventilador seja ligado

FONTE: Análise do consórcio

3.4. Segurança da informação

Independentemente da camada tecnológica, em um curto prazo de tempo, os dispositivos inteligentes ou "coisas" devem se tornar participantes ativos no ambiente, onde serão capazes de interagir e comunicar-se entre si, trocar informações coletadas e reagir aos acontecimentos do mundo físico sem intervenção direta do ser humano. Contudo, essa realidade traz inúmeros desafios referentes à segurança de IoT, como aumento da superfície de ataque à rede, restrição dos dispositivos no sentido de suportar técnicas e mecanismos robustos de segurança, mau uso por parte do usuário e até mesmo falhas de projeto do produto. Assim, a segurança pode ser considerada um dos principais desafios tecnológicos de IoT, compreendendo componentes críticos de qualquer solução. Por exemplo, a confidencialidade, a autenticidade e a privacidade dos interessados devem ser asseguradas para permitir a adoção em massa de IoT. As principais tendências dessa camada são elencadas a seguir.

1. Novas **soluções de IoT tendem a ser cada vez mais voltadas para o princípio de *security by design***, considerando desde a arquitetura a ser utilizada, passando pela definição e desenvolvimento da aplicação, da comunicação, do dispositivo, até a conscientização do usuário, seguindo os pilares da segurança em IoT: confidencialidade, integridade, disponibilidade, autenticidade e privacidade.
2. Os **maiores desafios têm sido observados na camada de dispositivos**, em particular dispositivos restritos em termos de processamento, memória e comunicação, que demandarão **criptografia leve** (*lightweight cryptography*). Uma alternativa é contar com **suporte complementar nos *gateways***, para assegurar proteção fim-a-fim.
3. No que diz respeito à **segurança das redes**, a adoção de variantes de protocolo de segurança IP para IoT com primitivas criptográficas de chave pública, tais como DTLS (*Datagram Transport Layer Security*), DEX (HIP *Diet Exchange*) e IKEv2, podem atender aos requisitos da IoT relacionados a escalabilidade e interoperabilidade. Adicionalmente, a **segmentação de rede** tem a funcionalidade de garantir que os dispositivos conectados não prejudiquem a segurança da rede, evitando assim o acesso indevido e a possível propagação de *malware* por seu intermédio. Outra possível abordagem seria a utilização de mecanismos dinâmicos de segregação, como controle para conter um ataque e limitar os danos de um incidente.
4. Em termos de soluções de segurança fim-a-fim (entre o dispositivo e a aplicação), dada a falta de uma padronização amplamente adotada nesta área, observa-se a verticalização por fornecedor, o que desfavorece o amadurecimento de um ecossistema mais robusto, em que o usuário pode adquirir dispositivos e aplicações de fornecedores distintos que interoperem.
5. Com o amadurecimento da IoT, no que diz respeito à **gestão de segurança para IoT**, a falta de padrões tem levado organismos de padronização a **abordar o assunto de maneira segmentada**, tratando de grandes **áreas temáticas**, tais como casas, saúde, cidades e transportes inteligentes.

6. A utilização da tecnologia ***blockchain* em IoT pode permitir** que as aplicações sejam desenvolvidas e utilizadas com **um nível maior de segurança e privacidade**, descentralizando a confiança, **dadas as características intrínsecas da tecnologia**, tais como: segurança, rastreabilidade, imutabilidade e auditoria. Contudo, apesar de iniciativas de empresas e *startups*, considerando a maturidade em que se encontra a tecnologia, **é prematuro afirmar que *blockchain* será escolhida para tratar os diversos desafios** das implementações e casos de uso IoT de modo geral.

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 12 a seguir.

QUADRO 12

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de segurança

Rastreio de contêineres	Manutenção preditiva de turbinas de avião	Casa Inteligente
Tendência 2	**Tendências 1 e 4**	**Tendências 3 e 5**
▪ O uso de mecanismos de criptografia leve, associado a funcionalidades adicionais nos *gateways* provê solução em cenários onde os dispositivos são restritos em termos de processamento	▪ A melhor forma de abordar a segurança em IoT é implementá-la desde a concepção (*security by design*), da arquitetura a ser utilizada, passando pelo desenvolvimento da aplicação, da comunicação, do dispositivo até a conscientização do usuário, seguindo os pilares da segurança em IoT: confidencialidade; integridade; disponibilidade; autenticidade; e privacidade ▪ Dada a falta de um padrão de fato, o fabricante da turbina desenvolve todos os mecanismos de segurança o que obriga o usuário a ter que usar a aplicação de *analytics* deste fornecedor uma vez que este é o único software que consegue se valer dos dados desse hardware	▪ Protocolos existentes como DTLS, IPsec, dentre outros, são capazes de tratar de segurança de rede, ao passo que técnicas de segmentação podem ser usadas de maneira complementar para isolar eventuais ocorrências e impedir a propagação de ataques ▪ Um consórcio de fabricantes de eletrodomésticos foi formado para garantir a interoperabilidade destes através da definição de mecanismos comuns de segurança

FONTE: Análise do consórcio

4. Cadeia de Valor

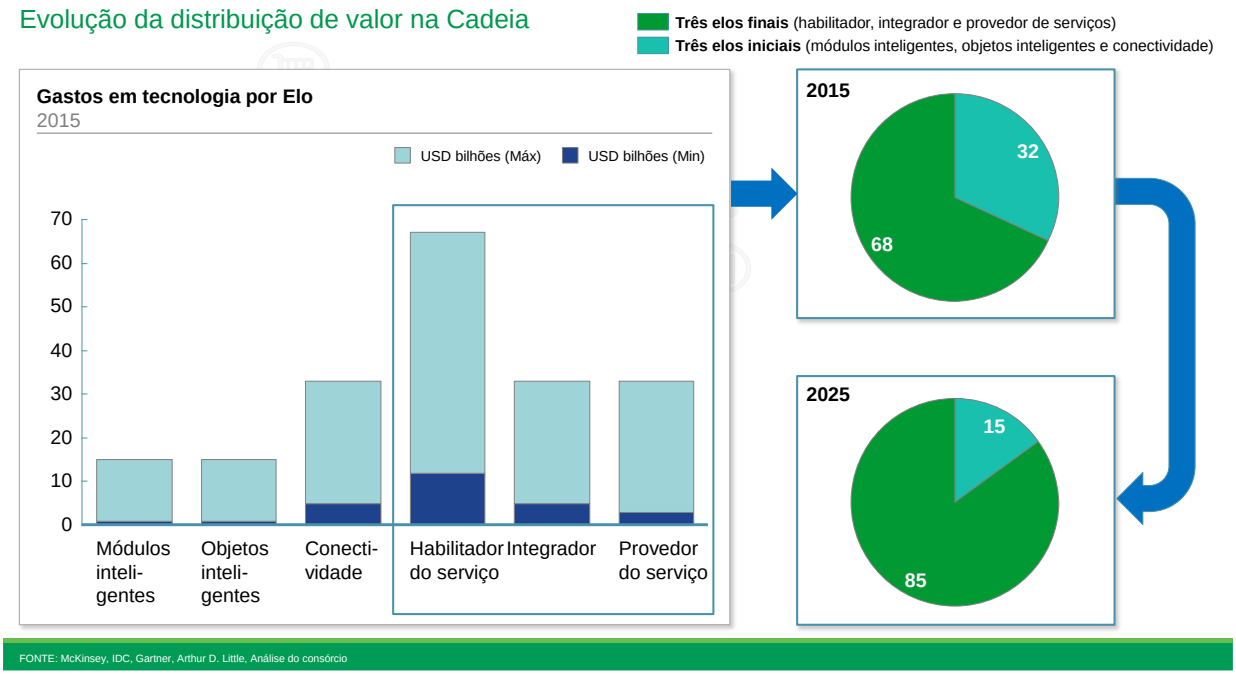
BNDES O banco nacional do desenvolvimento
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL PAÍS RICO É PAÍS SEM POBREZA

De maneira análoga às tendências tecnológicas observadas, o mapeamento dos atores da cadeia de valor de IoT compreende o levantamento dos principais atores operando à época do estudo[22], e não tem por objetivo trazer uma lista exaustiva. Assim, eventualmente, atores mais recentes ou inovadores no ecossistema podem não figurar nas análises realizadas.

Durante o levantamento dos principais atores da cadeia de valor de IoT, foram identificadas as seguintes tendências:

- Foi observada uma maior concentração do valor nos elos finais da cadeia, bem como a previsão da ampliação da relevância dos elos finais nos próximos anos. Por exemplo, os elos Habilitador, Integrador e Provedor de Serviços foram responsáveis por 68% dos USD 45 a 135 bilhões gerados na cadeia tecnológica global de IoT em 2015; em 2025, estima-se que a participação desses elos suba para 85% de um total de USD 273 a 777 bilhões, conforme indica o QUADRO 13 a seguir.

QUADRO 13



- Os grandes atores (mais de mil funcionários) operam, em geral, em mais de uma vertical e camada tecnológica, e estão buscando oportunidades de negócio em outros elos da cadeia. Empresas de menor porte, por outro lado, atuam principalmente em uma vertical específica, e na camada de Suporte a Serviço e Aplicação, ofertando, na maioria dos casos, soluções para análises computacionais, que podem ser

[22] Primeiro semestre de 2017.

customizadas para mercados de nicho. O elo Habilitador é o que apresenta a maior quantidade de novos entrantes. Com o desenvolvimento do mercado de IoT, podem surgir oportunidades para novos entrantes na camada de Suporte a Serviço e Aplicação, dada a presença de um grande número de novos entrantes (pequenos atores).

- A análise de oportunidades de nicho realizada para as iniciativas internacionais de IoT confirma que se trata de um ecossistema emergente. Nota-se que atores têm buscado um posicionamento estratégico, explorando soluções que poderão atingir mercados mais amplos (*mainstream*), seja em verticais específicas ou em um conjunto delas. Dentre os atores analisados, 43% deles atuam no Brasil.
- Verificou-se maior número de alianças para padronização e difusão da IoT na camada de Rede e na camada de Suporte a Serviço e Aplicação. Além disso, grandes atores participam como patrocinadores de alianças em mais de uma camada, inclusive em camadas em que não atuam tradicionalmente.

5. Detalhamento das Tendências

5.1 Dispositivos

5.1.1 Introdução

De acordo com a recomendação ITU-T Y.2060 (06_2012)[23], os dispositivos são equipamentos com capacidades mandatórias de comunicação, além das capacidades opcionais de sensoriamento, atuação, captura, armazenamento e processamento de dados. A camada de dispositivos compreende as competências dos dispositivos propriamente ditos e *gateways*. Os dispositivos devem ter as seguintes competências:

- **Interação direta com a rede de comunicação**: receber comandos, agregar e enviar informações diretamente à rede de comunicação, sem a utilização de *gateways*;
- **Interação indireta com a rede de comunicação**: receber, agregar e enviar informações à rede de comunicação indiretamente, utilizando-se de *gateways*;
- **Capacidade de formar redes *ad-hoc***: compor redes *ad-hoc* em cenários onde é preciso escalabilidade e implantação rápida;
- **Mecanismos de *sleeping* e *waking-up***: possuir mecanismos de desligar as partes do circuito que não estão em uso e religá-las quando for de interesse, como forma de economizar energia.

Os *gateways*, por seu turno, devem ter as seguintes competências:

- Fornecer suporte a outros dispositivos conectados com ou sem fio (*wireless*), tais como: CAN, ZigBee, Bluetooth e Wi-Fi e comunicar por meio de várias tecnologias como redes celulares, Ethernet, dentre outras;

[23] ITU, "Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things". Disponível em https://www.itu.int/rec/T-REC-Y.2060. Acesso em janeiro de 2017

- Realizar a conversão entre protocolos: em casos em que a comunicação utiliza diferentes protocolos, especificamente envolvendo a camada de dispositivos (por exemplo, entre dispositivos utilizando protocolos ZigBee e Bluetooth) ou entre as camadas de dispositivos e rede (por exemplo, ZigBee na camada de dispositivos e 3G na camada de redes).

As próximas subseções tratam dos temas relativos à camada de dispositivos: *hardware* e microeletrônica (processadores, memórias, módulos *wireless* e plataformas de desenvolvimento), *software* embarcado (SOs e linguagens de programação), energia, sensoriamento e questões de segurança.

5.1.2 *Hardware* e microeletrônica

5.1.2.1 Questões relevantes da evolução da microeletrônica

A microeletrônica vem evoluindo e se aperfeiçoando rapidamente. Comparativamente, se evolução similar tivesse ocorrido na indústria automobilística desde 1971, os automóveis teriam alcançado velocidades de até 420 milhões de milhas por hora em 2015[24]. Esta taxa de crescimento em semicondutores foi prevista em 1965, por Gordon E. Moore, e ficou conhecida como Lei de Moore. Ela estimou que o poder de processamento dos computadores dobraria a cada dezoito meses, sendo o computador considerado como qualquer unidade de processamento.

Alguns especialistas não acreditam que a Lei de Moore se torne obsoleta em um futuro próximo e defendem que a tecnologia de fabricação de transistores poderá sofrer inovações contínuas que permitirão a evolução prevista por Moore. Dentre essas inovações, pode-se citar a tecnologia de 5 nm em 2019 através da *Extreme UltraViolet lithography* (EUV)[25]. Outros especialistas, por outro lado, afirmam que, devido aos custos elevados de se manter e atualizar as *foundries* para novos nós de tecnologia, será inviável manter a validade da Lei de Moore nos próximos anos. Para estes, inovações ocorrerão de maneiras não incrementais, como, por exemplo, através do uso da fotônica integrada ou de outros materiais em substituição ao silício.

Para um nó de tecnologia, isto é, 90 nm, 40 nm, 28 nm, etc., geralmente são necessários alguns anos para atingir o estado-da-arte para a posição de principal tecnologia utilizada, como se observa no QUADRO 14[26]. Essa mudança depende do custo de fabricação, que tende a diminuir à medida que se domina a tecnologia, e o surgimento de demandas por dispositivos de menor potência e/ou maior poder de processamento. A tecnologia de

[24] The Guardian, disponível em https://www.theguardian.com/technology/2017/jan/26/vanishing-point-rise-invisible-computer?CMP=Share_iOSApp_Other, acesso em maio de 2017.

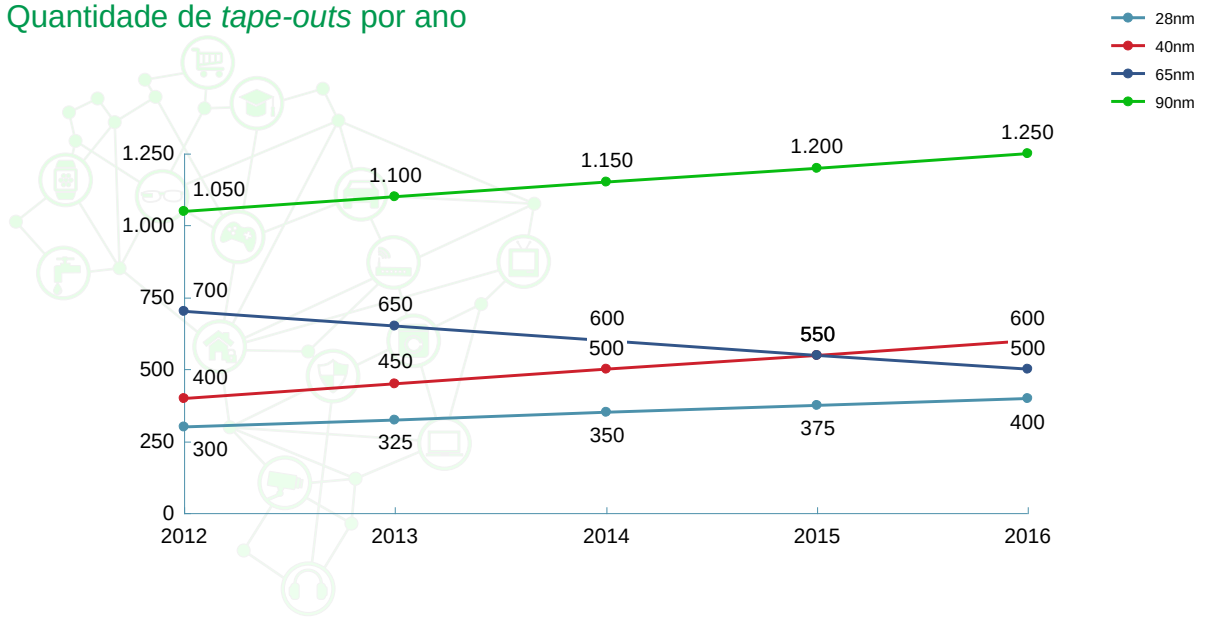
[25] IEEE, disponível em http://spectrum.ieee.org/semiconductors/devices/leading-chipmakers-eye-euv-lithography-to-save-moores-law, acesso em maio de 2017.

[26] Any Silicon, disponível em http://anysilicon.com/semiconductor-technology-nodes/, acesso em maio de 2017.

16nm, que se utiliza de FinFETs, já está disponível em *foundries* como a TSMC[27], e extrapolando-se os resultados das tecnologias anteriores, espera-se que esta esteja entre as mais utilizadas em cinco anos.

QUADRO 14

Quantidade de *tape-outs* por ano



FONTE: Análise do consórcio

Conforme estudo realizado pela McKinsey[28], estima-se que, em 2020, a maior parcela de mercado de semicondutores encontrar-se-á em processadores (31%), seguida pelas baterias (20%), sensores (15%), componentes para comunicação (15%) e memórias (10%). Alguns atores importantes são: ST, Infineon, Broadcom Limited, NXP (ex-Freescale) e Texas Instruments. Ainda de acordo com esse estudo realizado pela McKinsey estima-se que o *Total Available Market* (TAM) para semicondutores represente apenas 2% do total da cadeia de valor, o que corresponde a aproximadamente sete bilhões de dólares em 2020.

O consumo de energia dos componentes de semicondutores é muito relevante na construção de dispositivos. Processadores, em geral, apresentam um consumo relativamente alto e, por isso, é importante escolher processadores eficientes do ponto de vista de consumo de energia (como o modo *idle*) e que realizem somente atividades essenciais. Por sua vez, os módulos *wireless* apresentam, tipicamente, consumo de energia proporcional ao alcance do sinal. Consequentemente, a escolha da tecnologia deve levar

27 TSMC, disponível em http://www.tsmc.com/english/dedicatedFoundry/technology/16nm.htm, acesso em maio de 2017.

28 McKinsey & Company, "Semiconductor 2.0 – The next wave: Where to play? How to play? When to play?", Discussion document 2015 T-30.

em conta os recursos estritamente necessários para a aplicação em análise, sobretudo em dispositivos alimentados por baterias.

5.1.2.2 Processadores para sensor nodes e *gateways*

Em geral, *sensor nodes* são dispositivos com menor poder de processamento. Suas características mais relevantes são: baixo consumo de energia, área e custo reduzidos e possibilidade de acoplamento de sensores, atuadores e módulos de comunicação. Para tanto, o processador destes nós é tão simples quanto possível, de acordo com a aplicação.

Os dispositivos do tipo *gateways*, por sua vez, podem exigir vários níveis de capacidade de processamento, dependendo da aplicação. Duas implementações comuns são: *gateways* simples e *gateways* com controle incorporado. Ambos fornecem conectividade agregando dados de múltiplos *sensor nodes*. Em geral, um *gateway* simples organiza os dados para o transporte na Internet, para transmitir dados dos *sensor nodes* para a nuvem ou vice-versa. Já um *gateway* de controle embutido estende a funcionalidade de um *gateway* simples, fornecendo recursos de processamento e inteligência localmente para as aplicações. Por exemplo, um *gateway* de controle incorporado pode avaliar e filtrar dados de sensores, bem como implementar tarefas de gerenciamento de alto nível. Possuir um *gateway* de controle incorporado pode reduzir a complexidade e o custo dos *sensor nodes*.

Não existe uma separação clara entre os processadores utilizados para diferentes propósitos. O que se busca sempre é que processadores atendam a requisitos de desempenho, com o menor consumo possível de energia, menor custo e a menor área. Estes fatores têm seus pesos determinados pelo caso de uso.

Certos processadores tendem a ser utilizados em *gateways* com controle incorporado, devido à sua alta capacidade de processamento e integração, proporcionando alto nível de segurança, bem como maior poder de processamento de imagens, visando a Indústria 4.0, a indústria de transportes e o varejo.

Já processadores de menor desempenho, menor área e menor custo tendem a ser utilizados em *sensor nodes* em que não há uma demanda elevada por processamento local. Exemplos nesta categoria são adequados, por exemplo, para uso em *wearables*, como relógios inteligentes, ou para o gerenciamento de redes de sensores utilizados em aplicações de *smart cities*, tais como iluminação pública.

5.1.2.3 Processadores *open source*

Na área de *software*, é comum a prática de desenvolvimento colaborativo de código, chamado *open source.* Em *hardware*, o conceito de *open source* se destaca no nível de placas eletrônicas, como o Arduino e o Raspberry Pi. Entretanto, os circuitos integrados que os compõem permanecem proprietários.

A publicação do projeto completo do circuito integrado do processador o classifica como *open source*. Esta prática permite a customização do projeto e a sua prototipagem para testes em *Field Programmable Gate Array* (FPGA), resultando em uma vantagem competitiva para os desenvolvedores de circuitos integrados, cujos gastos de fabricação são bastante elevados. A seguir, encontram-se descritos dois destes processadores.

- **PULPino**[29]: utilizado por pesquisadores do Laboratório de Sistemas Integrados (Integrated Systems Laboratory - IIS) da ETH Zurich. Trata-se de um processador *open source* ideal para aplicações de baixo consumo de energia, como as aplicações de *wearables*. O processador se baseia no projeto PULP (do inglês, *Parallel Ultra Low Power*), que a ETH Zurich mantém em parceria com o grupo de sistemas embarcados eficientes em consumo de energia (*Energy-Efficient Embedded Systems* - EEES) da Universidade de Bolonha, na Itália.

  O PULPino suporta a execução de Sistemas Operacionais de Tempo Real (do inglês, *Real Time Operating System*, RTOS), como o FreeRTOS. Quando o *core* está em modo *idle*, o PULPino pode ser colocado em modo de baixo consumo de energia, na qual somente uma unidade de evento permanece ativa. Uma unidade de tratamento de eventos especial coloca o restante da plataforma em funcionamento quando um evento ou uma interrupção ocorre. O PULPino pode ser utilizado em aplicações como *smartwatches*, *sensor nodes* para monitoramento de sinais fisiológicos e outras aplicações em IoT.

- **RISC-V**[30]**:** novo conjunto de instruções de arquitetura 32, 64 e 128 bits com propósito geral. Produzido pelo *Computer Science Divison* na Universidade da Califórnia, Berkeley, é um *Instruction-Set Architecture* (ISA) *open source* (BSD). Apresenta um conjunto limpo, modular, com várias opções de extensão de instruções como ponto flutuante e multiplicadores de fácil implementação comparado com outras alternativas.

  O projeto possui grande aceitação na indústria de semicondutores, tendo como meta criar um conjunto de instruções universal, livre e aberto para todos os usuários, oferecendo o suporte necessário para projetos comerciais, incluindo *design*, fabricação e venda de *chips* e *software*. RISC-V é modelado para ser utilizado nos dispositivos computacionais mais modernos, que vão desde servidores, celulares *high-end* até

[29] Embarcados, disponível em https://www.embarcados.com.br/pulpino, acesso em maio de 2017.
[30] RISC, disponível em https://riscv.org, acesso em maio de 2017.

projetos embarcados de pequeno porte, como aplicações em IoT. Iniciado em 2010, foi disponibilizado em 2015 e já é utilizado em empresas de grande porte, como Google, Mellanox e Oracle, além de grandes centros acadêmicos. Vários projetos funcionais *online* estão disponíveis, usufruindo da permissão de licença BSD. Um exemplo é o RISC-V Rocket[31,32].

Diferentemente do RISC-V, *chips* da ARM e da MIPS Technologies necessitam de licença para uso de suas patentes e requerem acordos de confidencialidade. O ecossistema RISC-V está nos estágios iniciais de desenvolvimento. Um Linux 4.1 V e um Linux embarcado (baseado em Yocto) foram disponibilizados para o projeto RISC-V. Ferramentas disponíveis do RISC-V incluem compiladores GCC, LLVM e Clang, GDB, uma suíte de verificação e simuladores.

A *RISC-V Foundation*, uma corporação sem fins lucrativos controlada por seus membros, direciona o desenvolvimento futuro e impulsiona a adoção do RISC-V ISA[33].

5.1.2.4 Memórias

5.1.2.4.1 Memórias voláteis x não voláteis para IoT

Do ponto de vista do armazenamento, a memória pode ser categorizada como não volátil e volátil. A memória não volátil (do inglês, *Non-Volatile Memory*, NVM) é capaz de reter dados mesmo depois que a energia é removida e geralmente é mais lenta que a memória volátil. A memória volátil, por outro lado, não retém dados depois que a energia é removida e tem maior custo de armazenamento por bit. Portanto, a memória volátil é usualmente utilizada para armazenamento primário quando a memória interage com um SoC com frequência, enquanto a NVM é usada para armazenamento secundário/de massa. No entanto, essa regra pode mudar, pois a NVM está se tornando mais rápida e, portanto, poderia ser utilizada também como memória de acesso primário dos processadores. Além disso, seu custo por *byte* está caindo, viabilizando sua utilização para o armazenamento primário.

5.1.2.4.2 Memórias não voláteis MTP e OTP

Alguns dispositivos de IoT precisam ter um menor custo e menor tamanho para atrair o mercado de massa. Portanto, a área de silício destes dispositivos torna-se muito importante. Projetistas tem se esforçado para minimizar os custos de fabricação do *wafer*,

31 Rocket, disponível em https://github.com/ucb-bar/rocket, acesso em maio de 2017.

32 Rocket, disponível em https://github.com/ucb-bar/rocket-chip, acesso em maio de 2017.

33 Algumas das empresas que participam da RISC-V Foundation: Google, HP, IBM, Microsoft, Oracle, AMD, Qualcomm, Nvidia, Microsemi, dentre outras.

uma vez que as máscaras ou etapas de processamento elevam o custo. Assim, ao invés de utilizar uma arquitetura generalizada (*one-size-fits-all*), projetistas precisam analisar os modelos de uso exatos de seus produtos para planejar a arquitetura e a memória, de acordo com a necessidade.

Memórias não-voláteis embarcadas no chip oferecem uma vantagem de desempenho para os dispositivos de IoT, pois tornam desnecessário copiar o código da memória externa para a RAM. O mercado de memória do tipo Programável Múltiplas Vezes (do inglês, *Multiple-Time Programmable*, MTP) e as do tipo Programável Uma Única Vez (do inglês, O*ne-Time Programmable,* OTP) tem tido um crescimento considerável, visto que elas se adaptam às aplicações de IoT, tanto em desempenho quanto em tamanho.

Memórias MTP NVM embarcadas oferecem soluções *on-chip* pequenas e reprogramáveis para aplicações que exigem maior duração da bateria, uma vez que a memória externa consome mais energia. O uso de memória *flash* externa não é economicamente viável, pois o custo por bit é alto quando o tamanho é inferior a 1 Mbit, sendo esta a ocasião na qual a MTP NVP embarcada torna-se mais útil. Juntamente com o custo da *flash* externa, há também uma penalidade de energia para aplicativos *Execute-in-Place* (XIP), que são executados diretamente a partir da NVM, sem necessidade da primeira subida na RAM.

Memórias OTP NVM apresentam um custo baixo, devido à facilidade da sua fabricação. Ao mesmo tempo, Memórias OTP NVM permitem que os *chips* armazenem endereços customizados de controlador de acesso de mídia de rede (MAC), chaves de criptografia de dados, ID de rede, códigos de autenticação e *firmware*. A densidade de OTP NVM é comparável à de *arrays* de armazenamento baseados em *flash*, mas não requerem os custos adicionais de máscara da *flash*. Como resultado, a OTP NVM compatível com CMOS representa uma solução econômica.

5.1.2.4.3 Memórias Flash on-Chip

Devido à sua resistência, isto é, à quantidade de programação/apagamento de um bloco de memória antes de a informação deixar de ser confiável, a memória *flash* integrada (eFlash) é altamente desejável em aplicações de IoT que requerem armazenamento crítico de dados e códigos. A capacidade de programação em campo oferece grande flexibilidade para mudanças emergenciais no nível do sistema. O mercado de memória eFlash cresceu exponencialmente e espera-se que aumente ainda mais com a proliferação de tecnologias de IoT, devido ao seu desempenho relativamente alto e alta densidade, capaz de suportar a maioria das aplicações baseadas em micro controladores[34].

[34] Semiconductor Engineering, disponível em http://semiengineering.com/iot-will-force-new-memory-paradigm/, acesso em maio de 2017.

5.1.2.4.4 MEMÓRIAS FLASH EXTERNAS

A memória *flash* tradicional provavelmente continuará a ser utilizada em aplicações de IoT e em produtos de consumo como *smartphones* e leitores eletrônicos (*e-readers*) devido ao seu histórico de confiabilidade, baixo custo (quando maior que 1 Mbit), alta densidade, desempenho XIP, amplo range de suporte a temperatura, arquitetura e flexibilidade.

NOR *Flash* é muito popular entre as aplicações que requerem armazenamento de código, tais como *gateways* domésticos e *set top boxes*, devido à capacidade de suportar aplicações XIP e baixo consumo de energia em espera; o tipo NAND, por sua vez, é mais adequado para aplicações de armazenamento de dados que não requerem suporte XIP. Aplicações de IoT, como *drivers* USB inteligentes e dispositivos *wearable* requerem armazenamento mais econômico e, portanto, tendem a optar por NAND *flash*. A Tabela 1[35] compara as principais características de NAND e NOR *flash*.

TABELA 1 COMPARAÇÃO ENTRE NAND E NOR *FLASH*

	NAND	NOR
Custo por bit	Baixo	Alto
Uso Arquivos Armazenados	Fácil	Difícil
Consumo StandBy	Alto	Baixo
Consumo Ativo	Baixo	Alto
Velocidade de Leitura	Baixo	Alto
Velocidade de Escrita	Alto	Baixo
Capacidade	Alto	Baixo
Execução de Código	Difícil	Fácil

Uma tendência para aplicações de IoT nos *sensor nodes* é o aumento do uso das memórias OTP, que podem ser facilmente implementadas em tecnologias maduras e com processos bem estabelecidos, como a CMOS. Exceto pela desvantagem de poder ser gravada somente uma vez, memórias OTP apresentam benefícios importantes, com destaque para a segurança, pois utilizam um gerador de números aleatórios para criar ID únicos que são permanentemente codificados em parte da memória, o que torna virtualmente impossível de ser *hackeado*. Outras vantagens das memórias OTP são o menor custo e tamanho (um transistor, comparado com as memórias MTP) e a independência de energia para manter o estado de gravação.

[35] Synopsys, disponível em https://www.synopsys.com/designware-ip/newsletters/technical-bulletin/advantages-of-mtv.html, acesso em maio de 2017.

5.1.2.4.5 MEMÓRIAS DRAM (BASEADAS EM DDR/LPDDR)

As DRAMs tradicionais (DDR2/3/4 e LPDRR2/3/4) estão disponíveis como componentes discretos em várias densidades, que variam de 32 MB a 2 GB, enquanto os DIMMs comerciais (múltiplos DRAM juntos) podem prover até 128 GB de armazenamento. A tecnologia 3DS é mais um passo no sentido de aumentar o armazenamento de memória para além dos DIMMs máximos disponíveis e diminuir o consumo de energia.

Acredita-se que a DDR de baixa potência (LPDDR2/3/4) continue dominando o mercado de dispositivos móveis. LPDDR4 extrai 1.2 V de tensão em comparação aos 1.5 V exigidos por LPDDR3, resultando em uma queda de mais de 20% em requisitos de energia. O desempenho do LPDDR3 é capaz de atender à maioria das aplicações de IoT, que requerem baixa potência e maior desempenho. Este tipo de memória é aplicado conjuntamente a processadores de alto desempenho e com IoT baseado em *Edge Computing*, devendo ser bastante utilizada nos *gateways* de IoT. Geralmente são separadas do SoC devido ao custo de fabricação pois utilizam tecnologias diferentes na produção do *wafer*.

5.1.2.4.6 MEMÓRIAS EMMC

O mercado de IoT provavelmente apresentará diversos dispositivos de baixo custo envolvendo sensores, medidores, dispositivos *wearable* e produtos eletrônicos de consumo. Nesse contexto a memória eMMC é adequada para tais aplicações, devido ao seu baixo custo e capacidade de substituir os meios de armazenamento tradicionais.

O padrão eMMC foi desenvolvido para simplificar o projeto da interface do aplicativo, ao mover o controlador da *flash* e interagir com a memória *flash* na própria memória. A maior simplicidade do projeto beneficia os desenvolvedores de memória para IoT, reduzindo o tamanho físico do dispositivo. A especificação eMMC 5.1 permite altas velocidades de transferência, de até 400 MB/s, e capacidades de até 128 GB.

5.1.2.4.7 MEMÓRIAS UFS

O eMMC tem como concorrência o UFS 2.0, que oferece velocidades mais altas de transferência de dados e menor consumo de energia, sendo considerado um sucessor do padrão eMMC. Espera-se que o padrão UFS conduza o armazenamento embutido e removível baseado em memória *flash* em dispositivos de IoT. A evolução de eMMC para UFS oferece benefícios em termos de desempenho e baixa potência. No lado do desempenho, ele oferece 600 MB/s em comparação a 200 MB/s para eMMC, enquanto oferece redução de 30% a 55% no consumo de energia . O maior desempenho da UFS é

também resultado de mudanças arquitetônicas na camada de interconexão. O UFS possui interconexão serial e *full duplex*, enquanto o eMMC possui interface paralela e *half duplex*, o que bloqueia a operação de alta velocidade e execuções eficientes dos comandos.

Por fim, uma vez que os requisitos de consumo de energia e tamanho tendem a ser bastante críticos para os dispositivos em muitos casos de uso de IoT, desenvolvedores devem trabalhar com memórias e processadores que otimizem o desempenho para atender aos requisitos da aplicação, uma vez que isso se traduz em economia de energia. Em outras palavras, ainda que ocorra uma queda nos custos dos componentes de maior desempenho, pode ser mais interessante trabalhar com aqueles de menor capacidade de processamento e armazenamento, dado que seu menor consumo permite uma vida útil maior.

5.1.2.5 Plataformas de desenvolvimento

Arduino, Raspberry Pi e outras são placas com capacidade de processamento e acesso à Internet, na qual sensores e atuadores podem ser acoplados e controlados. Suas capacidades de processamento são variadas e a escolha de plataforma depende das necessidades da aplicação. As plataformas de desenvolvimento são largamente empregadas, sobretudo na construção e na validação de provas de conceito ou mesmo por empresas com um *time-to-market* muito restrito, ou que não têm interesse em desenvolver suas próprias placas. São, ainda, amplamente utilizadas por indivíduos do movimento *maker*[36], que projetam e implementam protótipos ou produtos sem o financiamento de uma empresa.

Essas plataformas de desenvolvimento oferecem a possibilidade de criar protótipos e até produtos rapidamente, sem a necessidade de se trabalhar em uma equipe com vários profissionais. As demandas por processamento, memória, comunicação e disponibilidade de entradas/saídas determinam qual a plataforma mais adequada para cada aplicação/caso de uso. A seguir serão apresentados mais detalhes sobre algumas dessas plataformas.

- **Arduino:** trata-se de um dos mais básicos dispositivos para uso em IoT, sendo composto por uma pequena placa com um processador embarcado e várias portas de entrada e saída, juntamente com uma interface de comunicação USB. Opera em baixa velocidade e, portanto, com baixo consumo de energia. Sua grande vantagem é o baixo custo (10 dólares) aliado a uma vasta gama de possibilidades de expansão e conectividade, além da enorme disponibilidade de suporte pela Internet. Adequa-se

[36] Synopsys, disponível em https://www.synopsys.com/designware-ip/newsletters/technical-bulletin/advantages-of-mtv.html, acesso em maio de 2017.

bem a aplicações de IoT que requerem coleta de dados de vários sensores[37]. Outra iniciativa que merece menção é o Radiuino[38], projeto desenvolvido pelo Prof. Dr. Omar Branquinho, da PUC Campinas, que deriva do Arduino e tem como foco o desenvolvimento de redes sem fio de sensores.

- **Raspberry Pi:** minicomputador de baixo custo (35 dólares) e dimensões comparáveis a de um cartão de crédito. Dispõe de várias portas USB, além de Ethernet, HDMI e interfaces para Câmera e LCD. É baseado em sistema operacional embarcado Linux, armazenado em um cartão de memória SD. Tem boas aplicações em dispositivos de IoT que requerem conectividade direta com a Internet. Sua principal desvantagem em relação ao Arduino é o baixo suporte a sensores e atuadores diversos devido ao mecanismo limitado de interface do processador[39].
- **BeagleBone:** plataforma que apresenta um custo mais elevado (75 dólares), unindo o poder de processamento do Raspberry Pi e a flexibilidade do Arduino. Também utiliza Linux como sistema operacional embarcado e apresenta processamento mais rápido, aliado a inúmeros pinos de entrada e saída para conexão com sensores e atuadores. É amplamente utilizada em aplicações industriais de IoT[40].

A Tabela 2 apresenta uma breve comparação entre as três plataformas citadas.

TABELA 2 COMPARAÇÃO DAS PLATAFORMAS ARDUINO, RAPDBERRY PI E BEAGLE BONE

Nome	Arduino Uno	Raspberry Pi	BeagleBone
Modelo testado	R3	Model B	Rev A5
Preço (USD)	29,95	35	89
Tamanho	2,95”x2,1”	3,37”x2,125”	3,4”x2,1”
Processador	ATMega 328	ARM 11	ARM Cortex A8
Velocidade do Clock	16MHz	700MHz	700MHz
RAM	2KB	256MB	256MB
Flash	32KB	Cartão SD	4GB (microSD)
EEPROM	1KB		
Tensão de alimentação	7-12 V	5 V	5 V

[37] Linkedin, disponível em https://www.linkedin.com/pulse/iot-devices-arduino-vs-raspberry-pi-beaglebone-which-kithion, acesso em maio de 2017.

[38] Fonte: http://radiuino.cc/

[39] Linkedin, disponível em https://www.linkedin.com/pulse/iot-devices-arduino-vs-raspberry-pi-beaglebone-which-kithion, acesso em maio de 2017.

[40] Idem.

Nome	Arduino Uno	Raspberry Pi	BeagleBone
Potência mínima	42 mA (0,3W)	700 mA (3,5W)	170 mA (0,85W)
GPIO Digital	14	8	66
Entrada analógica	6 10-bit	N/A	7 12-bit
PWM	6		8
TWI/I2C	2	1	2
SPI	1	1	1
UART	1	1	5
Dev IDE	Arduino Tool	IDLE, Scratch, Squeak/Linux	Python, Scratch, Squeak, Cloud9/Linux
Ethernet	N/A	10/100	10/100
USB Master	N/A	2 USB 2.0	1 USB 2.0
Saída de vídeo	N/A	HDMI, Composto	N/A
Saída de áudio	N/A	HDMI, Analógico	Analógico

5.1.2.6 Módulos *wireless*

Os dispositivos ou módulos de comunicação *wireless*, compreendem elementos que implementam as subcamadas física e MAC e as demais subcamadas superiores que realizam o controle e processamento das mensagens transmitidas e recebidas. A subcamada física inclui diversos componentes de RF, compreendendo a Banda Base, modulador/demodulador, o DAC e o ADC e o *front end* de RF, na qual estão inseridos os elementos de transmissão e de recepção.

A integração desses elementos pode se dar de diferentes maneiras, dependendo dos requisitos de desempenho, capacidade, disponibilidade e consumo dos dispositivos. Isto resulta em uma ampla gama de opções na oferta de *hardware* e *software* comerciais para os dispositivos ou módulos de comunicação *wireless*. Essas variam desde opções com integração dos componentes de RF em *chip*, possibilitando os *modems* e *transceiver* compactos como, por exemplo, os *modems* com interface USB para integração com estação PC ou com plataformas de desenvolvimento, ou módulos *transceiver* para integração com MCU independentes. Ainda nesta variedade, encontram-se os módulos com todos os componentes de RF e mais o MCU/CPU integrados em um SoC.

Já no lado oposto da integração, tem-se plataformas com *chipsets* em PCBs distintos para Banda Base, modulador/demodulador, ADC, DAC e componentes de *front end* de RF tais como o PA, LNA, filtros e duplexadores. Sendo este último caso a opção de arquitetura de

hardware para Estações Base celular, tal como para a tecnologia LTE/4G/NB-IoT, sendo enquadrado na categoria *carrier grade*, ou seja, uma plataforma de altos desempenho, capacidade e disponibilidade.

Para os *sensor nodes*, a tendência é a maior integração dos componentes de RF em um *transceiver* de pequenas dimensões, como sensores[41] com tecnologia Zigbee que devem ser integrados a um MCU.

Para necessidades de dimensões bem reduzidas e de baixo consumo, tem-se a opção de solução de SoC com *transceiver* integrado com MCU, juntamente com as memórias RAM e *Flash* e até o *hardware* de criptografia. Todos os componentes de RF são projetados para implementar as funcionalidades necessárias da forma mais simples possível e com o menor custo; o MCU recai em opção de baixa capacidade de processamento para atender ao *software* da MAC e das camadas superiores, tal como os produtos IEEE 802.15.4[42].

No caso dos *chipsets* de RF voltados para *gateways* ou concentradores, normalmente os fornecedores apresentam soluções com diferentes interfaces, sendo uma voltada para a rede de *sensor nodes* e a outra voltada para a rede de *backhaul*, esta podendo ser Ethernet, WiFi, IEEE 802.15.4, etc. Exemplos incluem produtos que combinam WiFi e BLE com MCU não integrado[43]. No caso do uso de interface de tecnologia celular, tem-se módulos com diferentes opções de tecnologia (2G, 3G e 4G), como em módulos que possuem tecnologias IEEE 802.15.4, ZigBee e CPU RISC integrada[44].

A integração de diferentes tecnologias de RF ocorre para *chipsets* voltados para os terminais móveis celulares, pois estes trabalham em multibanda e com multitecnologia celular, além de prover WiFi, Bluethoot e NFC. É possível que a integração destas tecnologias aumente ainda mais no futuro, pelo menos para os componentes de RF.

Para a tecnologia LoRa, tem-se a disponibilidade de módulos para camada física de diferentes fornecedores, com licenciamento da Semtech, detentora da patente. A aquisição somente desse módulo implica o desenvolvimento das subcamadas MAC e superiores de forma proprietária. Entre os fornecedores desta tecnologia LoRa estão, por exemplo, a Semtech[45] e a Microchip[46].

[41] Microchip, disponível em Disponível em: http://www.microchip.com/wwwproducts/en/en027752, acesso em maio de 2017.

[42] NXP, disponível em http://www.nxp.com/products/microcontrollers-and-processors/more-processors/application-specific-mcus-mpus/ieee-802.15.4-wireless-mcus:IEEE-802.15.4, acesso em maio de 2017.

[43] TI, disponível em http://www.ti.com/lsds/ti/wireless-connectivity/wi-fi/wilink-wl18xx/products.page, acesso em maio de 2017.

[44] NXP, disponível em http://www.nxp.com/products/microcontrollers-and-processors/more-processors/application-specific-mcus-mpus/ieee-802.15.4-wireless-mcus/zigbee-pro-and-ieee802.15.4-module:JN5168-001-M00#featuresExpand, acesso em maio de 2017.

[45] Semtech, disponível em: http://www.semtech.com/wireless-rf/lora.html, acesso em maio de 2017.

[46] Microchip, disponível em: http://www.microchip.com/wwwproducts/en/RN2483, acesso em maio de 2017.

A tecnologia LoRaWAN inclui as subcamadas física e superiores, que permitem a comunicação em rede dos *end devices*, do LoRa *Gateway*, do *Network Server* e do *Application Server*. Para que não existam desafios de interoperabilidade, os módulos de RF devem ter a certificação da LoRa Alliance. Há diferentes fornecedores para os módulos LoRaWAN, como a Liberium[47].

Para o NFC há opções de módulos com dimensões reduzidas e antena integrada, com a miniaturização ocorrendo principalmente nos *transponders* que podem ser utilizados em *wearables*[48].

No caso do terminal LTE CAT-NB1, a estratégia de desenvolvimento foi atender ao requisito de baixo custo, com a máxima simplificação do *hardware* e do *software*, bem como a redução de componentes de RF de forma a desenvolver uma solução SoC. A operação em modo *idle* deste terminal é um diferencial, tendo melhorias para aumento da eficiência na funcionalidade de DRX desde a Release 8, visando a redução do consumo de energia. Embora a sua especificação tenha ocorrido no final do ano passado, já podem ser encontrados produtos comerciais para algumas bandas de frequência específicas[49]. Para diminuir ainda mais o custo do terminal, vem sendo estudado um novo tipo de SIM Card – o padrão e-SIM na forma integrada, fazendo parte da eletrônica do terminal, permitindo a configuração remota das informações contidas no cartão.

Dispositivos sem fio necessitam de antenas para a comunicação e requerimentos de cobertura da rede de comunicação, bem como sua velocidade, devem ser considerados. Frequências abaixo de 1 GHz permite maiores coberturas, embora com taxas de transferência menores. Em compensação, têm menores consumos de energia, tornando essa faixa de operação sub 1 GHz bastante adequada para comunicação de IoT, ainda que essas antenas sejam maiores que aquelas empregadas para faixas de frequência mais altas. A antena interna, impressa em PCB, representa a principal opção de antena para IoT, por atender aos requisitos de dimensões reduzidas e menor custo dos *sensor nodes*. No entanto, dadas as dimensões cada vez mais reduzidas dos *sensor nodes*, menor tende a ser o espaço disponível para antenas impressas e, consequentemente, menor tende a ser sua eficiência. Outras opções de antena de pequenas dimensões são as *chip antennas*, formadas por condutor sobre cerâmica, que podem ser integradas junto aos demais componentes de RF em SoC.

[47] Libelium, disponível em: http://www.libelium.com/development/waspmote/documentation/waspmote-lorawan-networking-guide/, acesso em maio de 2017.

[48] TI, disponível em: http://www.ti.com/lsds/ti/wireless-connectivity/nfc-rfid/overview.page, acesso em maio de 2017.

[49] U-blox, disponível em: https://www.u-blox.com/en/product/sara-n2-series, acesso em maio de 2017.

5.1.2.7 Eletrônica impressa

Surgida há pouco mais de uma década, a eletrônica impressa une técnicas já empregadas há mais tempo, como impressão gráfica, tecnologias de semicondutores e ciência dos materiais para criar componentes e circuitos sobre variados tipos de substratos[50].

Seu desenvolvimento é balizado pelas aplicações, incluindo sistemas de RFID, etiquetamento de produtos em tempo real (permitindo alteração das informações apresentadas de forma rápida e barata), sistemas de monitoração de qualidade (verificando o estado de conservação dos produtos, violação de lacres, abertura de embalagens, etc.), entre outras.

Suas principais vantagens são:

- Baixo custo por unidade de área;
- Possibilidade de customização de funcionalidades no momento da impressão (no caso de impressão digital por jato de tinta);
- Agregação de novas funcionalidades:
  - Deposição de diferentes materiais no mesmo substrato, possibilitando, por exemplo, a integração de sensores, baterias e componentes ativos/passivos, displays, etc;
  - Uso de materiais flexíveis como o plástico ou até papel para o substrato, viabilizando a construção de produtos leves, robustos e flexíveis.

Ainda há grandes desafios para a combinação das tecnologias de eletrônica e impressão. A fabricação de semicondutores envolve a física da luz, a qual se espalha ao atravessar os padrões geométricos das máscaras fotolitográficas e gera distorções que precisam ser entendidas e compensadas. De forma semelhante, a tecnologia para eletrônica impressa requer o desenvolvimento de uma cadeia de conhecimento em sistemas, *software* e *hardware* que viabilize a concretização dos resultados desejados, desde a concepção até a produção final. A tecnologia para eletrônica impressa enfrenta o desafio da mecânica dos fluidos, na qual se modelam os comportamentos das gotas de tinta depositadas sobre os substratos de forma a se obter aproximações de seu comportamento após a evaporação do solvente, permitindo que formas geométricas mais precisas sejam impressas para a construção de circuitos e componentes semicondutores.

A concepção das tintas, por sua vez, envolve estudos relacionados à ciência dos materiais. Técnicas como o uso de nanopartículas permitem baixar o ponto de fusão de um material para que, após sua deposição (impressão), possa ser aquecido a temperaturas menores (para não danificar o substrato) e fundido, formando um filme eletricamente condutivo.

[50] Vivek Subramanian, disponível em: https://www.youtube.com/watch?v=806JGh4LPSM&feature=youtu.be, acesso em maio de 2017.

Há basicamente duas tecnologias de impressão: jato de tinta e gravura. Na primeira, gotículas de tinta são ejetadas de uma cabeça de impressão e depositadas no substrato. Trata-se de uma tecnologia de impressão "digital", que permite alterações no momento da impressão. Na segunda, os padrões a serem impressos são escavados em uma chapa ou cilindro metálico, criando uma matriz que é prensada contra o substrato para transferência da tinta previamente armazenada em seus sulcos.

A contribuição da eletrônica impressa no desenvolvimento de novos dispositivos para IoT pode viabilizar novas técnicas de sensoriamento, processamento (de baixa velocidade) e exibição de informações para usuários, nas mais variadas situações e aplicações.

5.1.2.8 Tendências

No contexto de *hardware* e microeletrônica para aplicações em IoT, foram cinco as principais tendências observadas:

1. Fabricantes de circuitos integrados passando a prover soluções completas para IoT;
2. SoCs contendo módulos de comunicação (geralmente sem fio) e sensores embarcados;
3. Processadores *open source*;
4. Desenvolvimento de SoCs customizados;
5. Necessidade de investimento em segurança e privacidade.

Essas tendências serão descritas a seguir. Além disso, tendências da tecnologia de módulos *wireless* também são apresentadas no final da seção.

Fabricantes de CIs provendo soluções sistêmicas completas: componentes semicondutores representam uma parcela pequena do TAM, apenas 2% da cadeia de valor[51]. Por isso, provedores de componentes devem evoluir para se tornarem provedores de soluções completas, contendo também *software*, soluções de nuvem, *analytics* e elementos de segurança, focando em alguns casos de uso identificados como promissores do ponto de vista de mercado. De acordo com estudo da McKinsey[52], as áreas que merecem maior atenção da indústria de semicondutores são: dispositivos *wearable*, aplicações em *smart homes*, como aquecedores e iluminação inteligente, eletrônica médica, Indústria 4.0, carros conectados e aplicações em *smart cities*, como controle de tráfego. Diversos fabricantes de semicondutores já vêm atuando desta forma[53]. Vale observar que

[51] McKinsey & Company: "Semiconductor 2.0 – The next wave: Where to play? How to play? When to play?", Discussion document 2015 T-30.

[52] McKinsey & Company, disponível em: http://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies, acesso em maio de 2017.

[53] Intel, disponível em: http://www.intel.com.br/content/www/br/pt/internet-of-things/iot-platform.html, acesso em maio de 2017.

fabricantes tradicionalmente associados a outros níveis da cadeia de valor também estão se adaptando e procurando prover soluções mais completas[54],[55].

Alto grau de integração entre processador, módulo de comunicação e sensores: inovações tecnológicas são esperadas na área de semicondutores, tais como projetos integrados com funções de baixíssimo consumo. Novos processadores utilizam hoje um décimo da potência dos processadores de 16 b mais eficientes de dois anos. Também se espera o desenvolvimento de *chips* com funcionalidades de comunicação e sensoriamento integradas à unidade de processamento, resolvendo, assim, requisitos de potência e área. Ainda em relação à área, é esperado que alguns componentes possam ser usados em *wearables*, isto é, devem ser pequenos e leves o suficiente para que sejam considerados confortáveis pelos usuários[56].

Processadores *open source*: com as possibilidades de prototipagem em FPGA e realização de testes antes da fabricação do ASIC, que é altamente custosa, e a possibilidade de customização do *design*, acredita-se que processadores *open source* tenham sua importância e uso aumentados nos próximos anos, assim como ocorreu anteriormente na área de *software*. Espera-se, ainda, que o desenvolvimento de *hardware* e microeletrônica se aproxime cada vez mais do processo ágil que vem sendo aplicado com sucesso na área de *software*[57].

SoCs customizados: o crescimento da IoT tem gerado uma nova onda de desenvolvimento de SoCs customizados. Apesar de os casos de uso serem distintos, os circuitos integrados que compõem essas soluções de IoT compartilham das mesmas características principais: inteligência embarcada (sob a forma de *software* executando em um processador), sensores analógicos, requisitos de consumo rigorosos, entre outros. O principal motivador para o desenvolvimento de SoCs customizados é adequar os circuitos integrados a um propósito específico. Não se trata apenas da substituição de micro controladores comuns (de prateleira) visando redução de custo, mas sim de construir um dispositivo adequado a um propósito específico que atenda às necessidades funcionais específicas do equipamento a que se destina.

Entre os principais benefícios dessa iniciativa, destacam-se[58]:

- **Redução do custo da BOM** (considerando já uma amortização dos custos de desenvolvimento do *chip*). Exemplo: integração da metrologia analógica com a aplicação digital em um *smart meter*;

[54] Cisco, disponível em: http://www.cisco.com/c/pt_br/services/overview.html, acesso em maio de 2017.

[55] Huawei, disponível em: http://pr.huawei.com/en/news/hw-432402-agilenetwork3.0.htm, acesso em maio de 2017.

[56] McKinsey & Company, disponível em: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity, acesso em maio de 2017.

[57] Embarcados, disponível em: https://www.embarcados.com.br/pulpino, acesso em maio de 2017.

[58] Open Silicon, disponível em: http://www.open-silicon.com/custom-soc-revolutionise-iot-product/, acesso em maio de 2017.

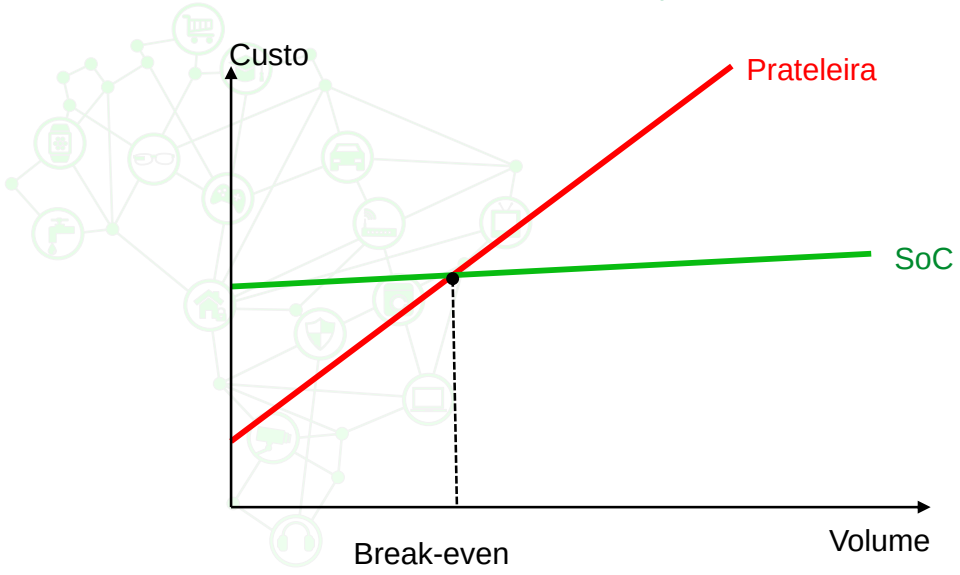
- **Inovação por diferenciação**. Em muitos casos, as funcionalidades desejadas não estão disponíveis em circuitos integrados de prateleira. Por exemplo, o atendimento de normas de segurança ou o surgimento de novos casos de uso podem estimular o desenvolvimento de um SoC customizado;
- **Controle da cadeia de fornecimento**. Na indústria de eletrônica automobilística, por exemplo, os produtos passam por longos e caros processos de certificação, antes que possam ser disponibilizados ao mercado. Nesses casos, o controle completo da cadeia de fornecimento, inclusive do circuito integrado principal, é um importante motivador para o desenvolvimento de um SoC customizado.

Além do custo de desenvolvimento de um SoC, o custo de fabricação de tecnologias de ponta é proibitivo para muitas empresas. No entanto, para tecnologias de processos já maduras, como 180 nm, pode-se obter uma rodada de fabricação em *wafer* compartilhado (*multi-project wafer* – MPW) por um custo inferior, da ordem de 16 mil dólares para 45 amostras de um *chip* de 25 mm[259].

O QUADRO 15[60] mostra que a partir de um certo volume de produção, o qual depende da tecnologia de processo e da complexidade do projeto, o custo total associado à produção de um equipamento utilizando um SoC customizado é menor comparado com CIs de prateleira.

QUADRO 15

Custo baseado em SoC customizado vs. CIs de prateleira



FONTE: Análise do consórcio

59 Idem.

60 Open Silicon, disponível em: http://www.open-silicon.com/custom-soc-revolutionise-iot-product/, acesso em maio de 2017.

Outro fator que contribui para a redução de custo e aceleração do desenvolvimento de um SoC customizado é a disponibilidade de IPs para reuso, fornecidos por fabricantes como a ARM para sua linha de processadores Cortex-M, além de *softwares* e ferramentas disponíveis em seu ecossistema.

Fabricantes sem experiência em microeletrônica podem contar com as chamadas *enablement companies*[61], que oferecem serviços de desenvolvimento em diferentes etapas de um projeto de SoC, ou serviços de cadeia completa de desenvolvimento e fabricação do tipo *turnkey*.

Segurança e privacidade: os maiores riscos associados à IoT são as violações de segurança e de privacidade. A área médica, por exemplo, promissora para a utilização de IoT, é uma das mais impactadas pela necessidade de preservar a segurança dos dados e a privacidade dos pacientes. Empresas de semicondutores podem ter acesso a um mercado de segurança de até 54 bilhões de dólares em 2020 se conseguirem endereçar as questões de privacidade e segurança[62].

Mais especificamente, no contexto de módulo *wireless*, no médio prazo, a tecnologia NB-IoT vai entrar nas operadoras de Telecomunicações e estas devem prover o serviço de comunicação IoT em seus portfólios. Embora o surgimento dos primeiros terminais comerciais CAT NB1 tenha sido previsto para o final de 2017, já existem fabricantes anunciando módulos CAT NB1 em seu portfólio. Paralelamente, já existem operadoras de telecomunicações anunciando serviços de comunicação IoT.

Estudos para a nova geração de rede móvel celular 5G já incluem novas tecnologias de comunicação para IoT, bem como para a comunicação direta entre dispositivos (D2D), uso de espectro não licenciado para transmissão de dados e uso de *white space* (faixas atribuídas a radiodifusão que podem estar vagas em algumas localidades)[63].

5.1.3 *Software* embarcado

Nesta subseção, serão abordados dois dos principais elementos do universo de *software* embarcado: Sistemas Operacionais e Linguagens de Programação. Em seguida, são apresentadas as tendências observadas para a área.

[61] Exemplo de *enablement company*: Open Silicon, disponível em: http://www.open-silicon.com/, acesso em maio de 2017.

[62] McKinsey & Company, disponível em: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity, acesso em maio de 2017.

[63] Communications and Network, disponível em: http://file.scirp.org/pdf/CN_2016022517010096.pdf, acesso em maio de 2017.

5.1.3.1 Sistemas operacionais

Sistemas operacionais utilizados em IoT possuem, basicamente, as mesmas funcionalidades de qualquer SO, mas buscam um consumo menor de recursos, como memória, dadas as restrições das aplicações.

As principais características de sistemas operacionais utilizados em IoT são:

- Baixo *footprint*: consumo de CPU, RAM e *flash*;
- Conectividade, sobretudo sem fio;
- Modular;
- Escalável;
- Seguro;
- Capaz de gerenciar eficientemente o consumo de energia.

Os principais SOs com foco em IoT, seja pela grande comunidade de desenvolvedores, características e funcionalidades, ou mesmo por terem grandes empresas (ou consórcio de empresas) apoiando o projeto são: RIOT-OS, CONTIKI, NUTTX, ZEPHYR, BRILLO, MBED-OS, LiteOS, TinyOS, Ubuntu Core, dentre outros. A seguir, são descritas suas características em mais detalhes[64].

RIOT-OS: desenvolvido de forma colaborativa com o apoio de instituições como a Freie Universität Berlin, INRIA[65], e Universidade de Ciências Aplicadas de Hamburgo. Disponível desde 2013, possui um *footprint* de aproximadamente 1,5 kB de RAM e 5 kB de *flash*, um escalonador de tempo real baseado em prioridades e uma API parcialmente implementada no padrão POSIX. É executado em micro controladores de 8, 16 e 32 bits e possui suporte a gerenciamento de energia. No que concerne à conectividade, apresenta suporte aos padrões e pilhas de protocolo IPv6, 6LoWPAN, RPL, UDP e CoAP. Possui também um porte para Linux, na qual é possível estudar e aprender sobre sua API, e suporta ferramentas comuns de desenvolvimento como GCC e GDB. Foi liberado sob a licença LGPL e possui suporte a diferentes arquiteturas de CPU incluindo x86, AVR, ARM7, ARM Cortex-M e MSP430.

CONTIKI: sistema operacional de código aberto, suportado por uma comunidade de desenvolvedores. Possui um *footprint* de aproximadamente 10 kB de RAM e 30 kB de *flash*, suporte à pilha de protocolos TCP/IP, além dos protocolos IPv6 focados em baixo consumo como 6LoWPAN, RPL e CoAP. Foi projetado de forma a estimar e analisar o consumo de energia da aplicação, sendo executado em sistemas com baixíssimo consumo de energia. Além disso, possui um sistema de arquivos para *flash* chamado Coffee, e um terminal de linha de comandos. Foi liberado sob a licença BSD e pode ser executado em uma grande variedade de arquiteturas de *hardware*, incluindo 8051, AVR, MSP430 e ARM.

64 Sergio Prado, disponível em: https://sergioprado.org/sistemas-operacionais-com-foco-na-internet-das-coisas, acesso em maio de 2017.

65 Instituto nacional francês para ciência da computação de matemática aplicada.

NUTTX: SO de código aberto para micro controladores com ênfase em compatibilidade com padrões de mercado (POSIX e ANSI) e baixo consumo de recursos (CPU, RAM e *flash*). Foi liberado sob a licença BSD e suporta diversas arquiteturas de micro controladores, de 8, 16 e 32 bits, incluindo ARM, AVR, 8051, MIPS e z80. Apresenta funcionalidades comuns em sistemas operacionais de tempo real como determinismo, preempção e herança de prioridade. É um SO bem completo, pois, além do *kernel* de tempo real, possui suporte a sistemas de arquivos, pilha de protocolos TCP/IP, USB *host* e *device*, biblioteca gráfica e um conjunto de aplicações adicionais, como um terminal de linha de comandos.

ZEPHYR: Lançado em 2016 pela Linux Foundation em parceria com grandes empresas como a Intel e a NXP. Trata-se de um RTOS para dispositivos de IoT *multithread* que apresenta funcionalidades para economia de energia, como o modo *tickless idle*. Utiliza um conceito interessante, chamado *fiber*, que consiste em uma tarefa de alta prioridade (comparada às tarefas comuns), escalonada de modo colaborativo. Possui baixo *footprint* (começando em 8 kB de RAM) e suporta diversos protocolos e padrões de mercado como Bluetooth, BLE, WiFi, 6Lowpan, CoAP, IPv4, IPv6, etc. Foi liberado sob a licença Apache e tem suporte às arquiteturas ARM Cortex-M, Intel x86, e ARC, incluindo portes para as placas Arduino 101, Arduino Due, Intel Galileo Gen 2 e a Freedom Board FRDM-K64F da NXP.

BRILLO: SO lançado em 2015 pela Google, o Brillo apresenta uma versão reduzida do Android e um protocolo chamado Weave para conexão entre os dispositivos de IoT. Desenvolvido em parceria com a Nest, possui suporte às arquiteturas ARM, Intel e MIPS. Diferentemente dos SOs apresentados anteriormente, o Brillo não foi feito para micro controladores, já que possui um *footprint* mínimo de 32 MB de RAM e 128 MB de *flash*. Placas como a Intel Edison suportam este SO, que já faz parte de soluções comerciais como um *hub* da Asus[66].

MBED-OS: SO *open source* da ARM que suporta apenas micro controladores ARM Cortex-M. Trata-se de um SO modular, seguro e com foco em conectividade. É capaz de garantir isolamento de memória entre as tarefas através da *Memory Protection Unit* (MPU) existente em micro controladores Cortex M3/M4, e suporta diversos protocolos e padrões de comunicação como Ethernet, WiFi, IPv6, 6LoWPAN, TLS, BLE. Foi lançado sob licença Apache 2.0[67].

LiteOS: Compõe uma solução maior da Huawei, chamada Agile Network 3.0 Architecture[68], que consiste de três componentes: Agile IoT *gateway*, Agile Controller e o LiteOS. A empresa tem por objetivo facilitar o desenvolvimento de aplicações de IoT

[66] ASUS, disponível em: https://www.asus.com/News/uCgzySroxaAEOlam, acesso em maio de 2017.

[67] MBED, disponível em: https://www.mbed.com/en/development/mbed-os, acesso em maio de 2017.

[68] Huwaei, disponível em: http://pr.huawei.com/en/news/hw-432402-agilenetwork3.0.htm, acesso em maio de 2017.

através da padronização da infraestrutura de conectividade. O LiteOS possui as seguintes características: *footprint* de aproximadamente 10 kB, o que torna possível executá-lo em dispositivos com restrições de memória e processamento, *zero configuration*, *auto-discovery* e *auto-networking*. Foi lançado sob a licença GPL v3.

uC-OS: Kernel de tempo-real preemptivo baseado em prioridade para microprocessadores, projetado para sistemas embarcados e, portanto, para IoT. É escalável e portável, escrito em C e pode ser configurado para utilização otimizada de memória. Trata-se de uma solução proprietária, compondo o portfólio da Silicon Labs[69].

Como discutido, existem diversos SOs em desenvolvimento, com características variadas, o que é coerente com o grande número de aplicações de IoT. O desenvolvimento de um novo SO pode ocorrer se não existir um SO adequado para uma aplicação específica ou por motivos de segurança, visto que os já existentes podem conter vulnerabilidades. Além disso, observa-se que o uso de *software open source* auxilia na manutenção da segurança[70], bem como na possibilidade de customização da solução.

5.1.3.2 Linguagens de programação

Nesta subseção, estão listadas as principais linguagens de programação utilizadas em sistemas embarcados e, portanto, adequadas a aplicações de IoT. São elas[71]:

- **C:** linguagem de programação criada em 1972 por Dennis Ritchie. Suas instruções e modelo de gerenciamento de memória são próximos à arquitetura convencional de processadores, o que permite ao programador acessar, diretamente, recursos de *hardware* e do sistema operacional e, portanto, é comumente empregada no desenvolvimento de *sensor nodes* e outros sistemas embarcados.
- **C++**: criada como uma extensão da linguagem C em 1983 por Bjarne Stroustrup; permite o desenvolvimento em um nível de abstração mais alto, com construções orientadas a objetos e de programação genérica. A linguagem mantém compatibilidade com C e todas as construções que permitem o acesso direto aos recursos do *hardware* e do sistema operacional.
- **Java**: criada em 1995 pela Sun Microsystems (adquirida pela Oracle Corporation); possui sintaxe similar às linguagens C e C++, porém com o diferencial de que um programa em Java, uma vez compilado, executa em qualquer plataforma com uma máquina virtual Java disponível, sem necessidade de recompilação. Outro diferencial

69 Micrium, disponível em: https://www.micrium.com/rtos/, acesso em maio de 2017.

70 EBC, disponível em: http://www.ebc.com.br/tecnologia/2015/07/entenda-por-que-*software*-livre-e-mais-seguro-que-*software*-proprietario, acesso em maio de 2017.

71 UBM: "2015 Embedded Markets Study – Changes in Today's Design, Development & Processing Environments", April 2015.

importante de Java é o gerenciamento automático de alocações de memória, o que diminui o risco de erros de programação.

- **Python**: linguagem de alto nível, criada por Guido van Rossum em 1991, com foco em legibilidade do código-fonte. Por ser uma linguagem interpretada, executa em qualquer plataforma que possua um interpretador Python disponível. A linguagem é mantida por uma comunidade *open source*, que desenvolve e disponibiliza diversas de bibliotecas para facilitar o desenvolvimento de novos programas.

O universo de sistemas embarcados e aplicações de IoT é extremamente variado. Em geral, os recursos, como memória e energia, devem ser utilizados com parcimônia. Além disso, é comum que os sistemas sejam de tempo real, o que exige algum poder de processamento. Quando existe a necessidade de acesso direto ao *hardware*, C é a linguagem mais apropriada. Quando as aplicações são de nível mais alto, chegando até a interface com o usuário, Java pode ser utilizada. Alguns sistemas são ainda híbridos, com partes de menor nível implementadas em C e as demais em Python. Acredita-se que a linguagem C continuará sendo a mais utilizada em sistemas embarcados, apesar de haver menos mão-de-obra disponível para ela. De acordo com a Oracle[72], existem aproximadamente 9 milhões de programadores Java no mundo, em contraste com apenas 500 mil programadores para sistemas embarcados[73].

5.1.3.3 Tendências

Assim como em *hardware* e microeletrônica, uma das principais tendências observadas em *software* é o desenvolvimento e a utilização de códigos *open source*. No caso da área de *software* embarcado para IoT, essa tendência responde aos requisitos de interoperabilidade, uma das características mais desejáveis em equipamentos que farão parte de redes, que podem ser altamente heterogêneas.

Dada a grande quantidade de aplicações de IoT, não é provável que tenha uma plataforma única proprietária que seja capaz de atendê-las. Um exemplo é a plataforma Vorto, apoiada pela Open Eclipse Community, que provê um *framework* comum para modelagem das informações, de forma a facilitar a integração entre equipamentos e, portanto, a interoperabilidade. Já existe uma aliança entre PTC e Bosch que utiliza a Vorto[74].

Quanto à tendência de utilização de linguagens de programação, um estudo sobre sistemas embarcados[75], válido também para IoT, mostra a porcentagem de utilização de

[72] Oracle, disponível em: http://www.oracle.com/technetwork/articles/java/afterglow2013-2030343.html, acesso em maio de 2017.

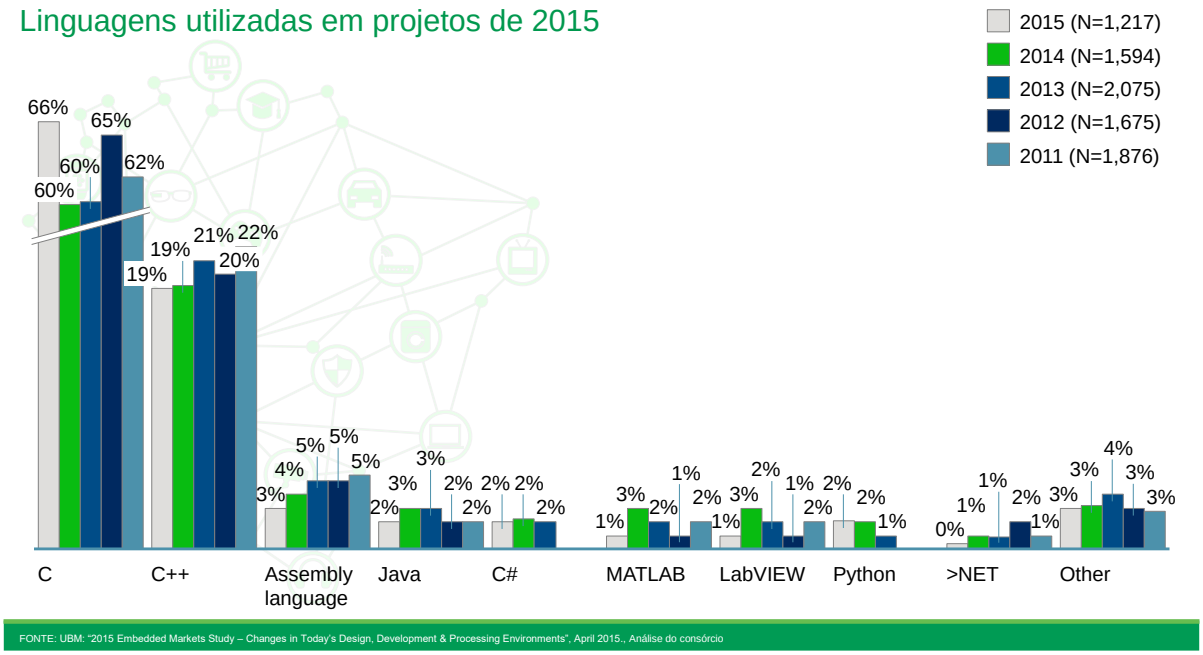
[73] VDC Research, disponível em: http://www.slideshare.net/vdcresearch/searching-for-the-total-size-of-the-embedded-software-engineering-market, acesso em maio de 2017.

[74] IoT Analytics, disponível em: https://iot-analytics.com/5-things-know-about-iot-platform/, acesso em maio de 2017.

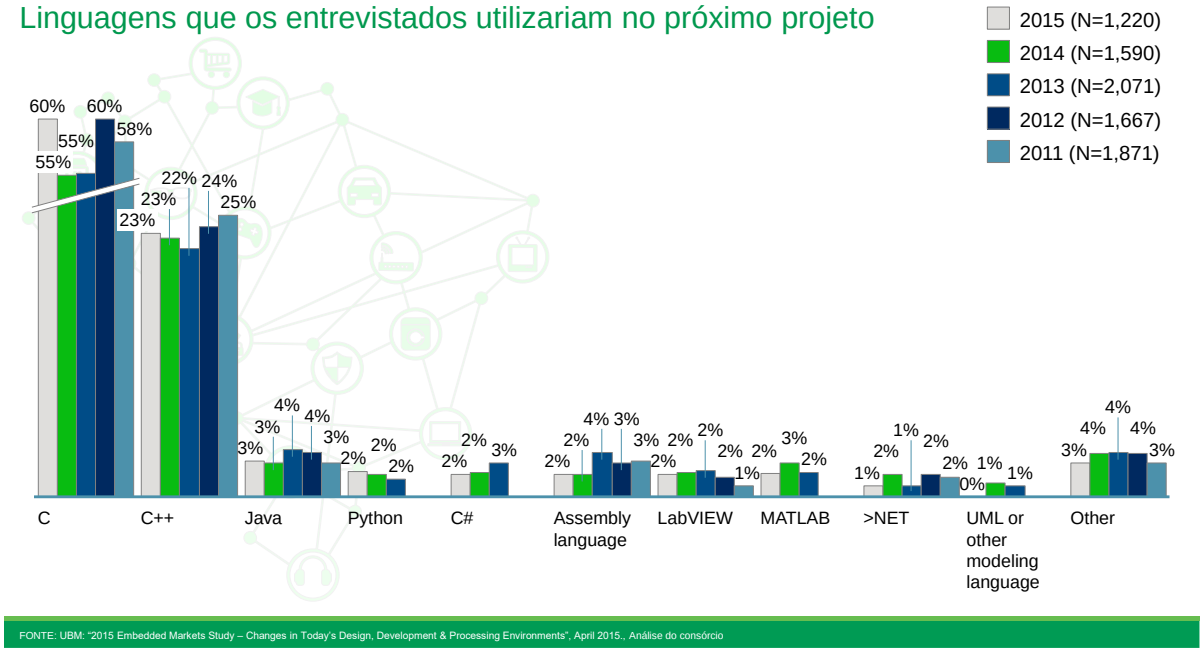
[75] UBM: "2015 Embedded Markets Study – Changes in Today's Design, Development & Processing Environments", April 2015.

diversas linguagens ao longo dos últimos anos e uma tendência de manutenção da predominância da utilização da linguagem C e da diminuição do uso de Assembly para o futuro próximo. O QUADRO 16 mostra as linguagens utilizadas em 2015 e o QUADRO 17 mostra as linguagens que seriam utilizadas em projetos futuros, segundo os entrevistados ouvidos no estudo.

QUADRO 16



QUADRO 17[76]



[76] Dados de 2015.

5.1.4 Energia

5.1.4.1 Baterias

No contexto de IoT, baterias possuem uma grande importância uma vez que muitos casos de uso devem se valer de dispositivos de dimensões bastante reduzidas e que requerem fontes de energia igualmente diminutas. A pesquisa e desenvolvimento de baterias tem se intensificado nas últimas décadas, principalmente pelo rápido desenvolvimento dos dispositivos eletrônicos móveis, tais como telefones celulares, máquinas de cartão de crédito/débito (PDA), notebooks, tablets, etc.

As baterias são classificadas como primária e secundária.

- **Bateria Primária**: não permite recarga, pois as reações químicas e elétricas que compõem o seu funcionamento são irreversíveis, possibilitando seu uso uma única vez. São utilizadas principalmente em aplicações em que a recarga é impraticável ou impossível, como em algumas aplicações militares, equipamentos aplicados em áreas classificadas com risco de explosão, sensores e dispositivos médicos implantados, etc. Essa classe de bateria é regulada pela norma IEC 60086 e utilizada em diversas aplicações médicas (marca-passo), medidores inteligentes, *beacons*, brocas inteligentes em mineração, relógios de pulso, entre outras;
- **Bateria Secundária**: permite a recarga e a possibilidade de ser usada muitas vezes sem danificar seus elementos internos - é também conhecida como bateria recarregável.

As principais vantagens das baterias primárias frente às baterias secundárias são:

- Alta energia específica;
- Autonomia maior, ou seja, uma maior capacidade de fornecer energia para a mesma carga;
- Disponibilidade instantânea de energia;
- Baixa taxa de auto descarga, o que permite manter praticamente sua capacidade original mesmo após longos períodos em repouso;
- Pode ser utilizada facilmente em regiões isoladas e sem acesso à energia elétrica comercial ou renovável.

Nos últimos anos, a convergência digital, que inclui a IoT, com sensoriamento e monitoração de vários dispositivos dos mais variados portes, tem demandado o uso de baterias de vários tamanhos. No entanto, os maiores desafios têm se concentrado nos dispositivos de pequeno porte, como dispositivos de consumo (sensores "vestíveis", ou seja, que o usuário carrega consigo, como roupas, óculos, relógios, joias, etc.) e médicos (monitoramento de implantes, supervisores de saúde, controles de medicação, etc.), que necessitam de baterias minúsculas de longa duração, denominadas microbaterias.

Atualmente, as microbaterias primárias (maiores que $1cm^2$) são as mais utilizadas nos sensores sem fio e sistemas integrados. Estas baterias apresentam baixo custo, o que representa um grande impeditivo para sua gradativa substituição por tecnologias

emergentes. Contudo, nos últimos anos, o aumento da demanda da miniaturização de dispositivos com microbaterias integradas, especialmente do tipo recarregável, tem despertado a atenção de pesquisadores e empresas. Microbaterias secundárias de diferentes químicas têm sido propostas em sistemas integrados que necessitam de micropotência, tais como lítio, níquel/zinco, zinco/prata e outras químicas.

Deve ser observado que quando se necessita de uma fonte de energia com tamanho e peso reduzido, a contribuição de materiais inativos, tais como o empacotamento, na massa e volume total torna-se significativo. Desta forma, todos os componentes inativos que poderão adicionar peso e complexidade para o processo de fabricação devem ser projetados cuidadosamente.

Neste sentido, as microbaterias de estado sólido são candidatas para esta aplicação, pois não necessitam de separadores especiais, o empacotamento pode ser simples e integrado com os condutores de corrente e eletrodos, além de serem intrinsecamente seguras devido à inexistência de eletrólito em estado líquido (geralmente orgânico e inflamável). Adicionalmente o desenvolvimento de sistemas em estado sólidos com novos materiais cerâmicos e poliméricos tem contribuído para a inovação de todas as microbaterias em estado sólido.

As subseções a seguir apresentam algumas tecnologias que vêm sendo estudadas com vistas à futuros desenvolvimentos de baterias.

5.1.4.1.1 Baterias de lítio

Uma das tecnologias mais aplicadas é a bateria de lítio-íon. O lítio é um elemento pequeno, leve e com elevado potencial eletroquímico, características que contribuem para a obtenção de baterias com altas densidades de energia e de potência, elevada tensão e baixa taxa de auto descarga. Estas características contribuem para que esta bateria apresente elevada autonomia, baixo peso, ocupe pouco espaço e, nas baterias secundárias, apresente baixo tempo de recarga e excelente desempenho em aplicações que exigem elevados ciclos de descarga/recarga.

Esta tecnologia tem sido utilizada intensamente em praticamente todos os modelos atuais de veículos elétricos e híbridos comerciais, além dos telefones celulares, *notebooks e tablets* (o mercado *consumer* ainda é o que demanda maior volume de bateria de lítio), o que tem contribuído significativamente para que seja fabricada em maior escala, reduzindo seu custo. Outro fator que contribui para a redução nos custos é o aumento da demanda nos últimos anos, com previsão de continuidade até a próxima década. Devido ao grande investimento no desenvolvimento desta tecnologia, gerado pela necessidade de mercado, há uma tendência de desenvolvimento de baterias com maior densidade de energia (menor peso, maior autonomia). Outros exemplos de aplicações que utilizam baterias de lítio são:

- Equipamentos médicos (marca-passos, desfibriladores, aparelhos auditivos, etc.) e dispositivos microeletrônicos (sensores, mini transmissores, atuadores, etc.)[77];
- Sistemas de telemetria acústica de filhotes de salmão (JSATS) utilizam microbaterias primárias de lítio com alta densidade de energia desenvolvidos pela *Pacific Northwest National Laboratory* (PNNL).

As microbaterias de filme fino adotam o *design* 2D planar[78] e são as mais tradicionais e populares usadas em micro aplicações apresentando melhor desempenho na recarga e sendo mais resistentes a degradação em temperatura elevadas.

O eletrólito em estado sólido contribui para o design e fabricação de baterias de filme fino integradas com circuitos eletrônicos e painéis solares. Este é um fator que favorece o sucesso e comercialização das microbaterias de filme fino em aplicações como etiquetas de identificação por rádio frequência (RFIDs). Exemplos de fabricantes de microbaterias de filme fino: *Thinergy, EnerChip e Flexion*.

Apesar das vantagens e do sucesso comercial, microbaterias de filme fino apresentam limitações de densidade de energia, sendo mais indicadas para aplicação em sistemas que necessitam de potência não muito elevada (média).

O aumento do desempenho das microbaterias pode ser alcançado com o emprego de design em dimensão 3D. O uso da geometria 3D aumenta a área superficial dos eletrodos, com consequente aumento da corrente e quantidade de material ativo dos eletrodos. As microbaterias 3D têm geometria similar a microbateria de filme fino. O objetivo do design 3D é dobrar a estrutura básica de camadas dentro de uma estrutura 2D mantendo a condução iônica e de corrente.

Atualmente, há um interesse crescente em fabricar microbaterias de lítio-íon mecanicamente flexíveis para serem integradas em conjunto com componentes eletrônicos flexíveis, tais como memórias, sensores, etc., para serem utilizados em displays, eletrônica em vestimentas, transplantes médicos, etc. Há também demanda de microbaterias flexíveis para utilização em dispositivos flexíveis. Fabricantes de dispositivos eletrônicos já têm planos para produzir baterias flexíveis, devido ao aumento da demanda dos microeletrônicos com maiores funcionalidades, capacidade e flexibilidade do design[79].

Pesquisas recentes têm colocado esforços no desenvolvimento de microbaterias flexíveis focando dois aspectos: flexibilidade do material e design do dispositivo eletrônico no qual a microbateria será usada. Esta categoria de microbateria utiliza eletrodos flexíveis,

77 Wang: Y. Wang et al., "Lithium and lithium ion batteries for applications in microelectronic devices: A review", Journal of Power Sources, 286, 2015.

78 Ferrari: Stefania Ferrari, Melanie Loveridge, Shane D. Beattie, Marcus Jahn, Richard J. Dashwood, Rohit Bhagat, "Latest advances in the manufacturing of 3D rechargeable lithium microbatteries", Journal of Power Sources, 286, 2015.

79 Wang: Y. Wang et al., "Lithium and lithium ion batteries for applications in microelectronic devices: A review",Journal of Power Sources, 286, 2015.

eletrólito polimérico, condutor flexível de corrente (grafeno fino, polímero condutor), substratos e materiais para empacotamento (PDMS) para melhorar a flexibilidade da geometria de camadas dos eletrodos. Nesta categoria de microbateria, uma flexibilidade extra pode ser alcançada com um bom projeto de design para todos os componentes da microbateria.

Embora a redução de tamanho e flexibilidade da microbateria sejam dois conceitos diferentes, as ideias de design são, em muitos casos, compatíveis e se sobrepõem. Por exemplo, o uso de eletrólitos poliméricos e materiais nano estruturados são abordagens viáveis em ambos os projetos. Além disso, o grau de flexibilidade e as novas arquiteturas são pontos chaves para o sucesso das microbaterias.

5.1.4.1.2 Prata/Zinco

Outra tecnologia com excelentes características e em constante desenvolvimento é a bateria de prata/zinco (Ag/Zn). As baterias de prata/zinco (Ag/Zn) apresentam elevados valores teóricos de energia específica e densidade de energia, quando comparado com outras tecnologias disponíveis comercialmente.

Baterias recarregáveis de prata/zinco têm sido utilizadas com sucesso há décadas em aplicações militares e aeroespaciais, onde o requisito principal é a elevada densidade de energia e potência. Sua tensão nominal é 1,65 V, com final de descarga em 1,2 V e de recarga em 2,0 V.

Historicamente, as baterias de prata/zinco não têm sido difundidas comercialmente devido principalmente a sua baixa vida cíclica e custo elevado. Novas tecnologias de baterias de prata/zinco têm sido desenvolvidas, buscando aumentar a vida cíclica dessas baterias para 15 anos. O elevado custo da prata é um dos desafios a ser vencido e é uma das razões que levaram a focar o desenvolvimento desta tecnologia em baterias pequenas.

A bateria de prata/zinco apresenta volume menor e maior densidade de energia que as baterias de lítio-íon. Em ensaios as baterias botão de prata/zinco apresentaram 98 % de capacidade após 300 ciclos de carga/descarga. Esta bateria apresenta maior área superficial em relação a bateria de lítio-íon, assim é possível construir baterias com tamanhos menores que 600 mm^3 numa arquitetura planar, sendo uma vantagem em relação as baterias de lítio do tipo botão. Esta tecnologia se restringe a um fabricante, e há poucos dados na literatura sobre seu desempenho[80].

5.1.4.1.3 Zinco/Ar

80 Battery Power Online, disponível em: http://www.batterypoweronline.com/main/articles/energy-density-comparison-of-silver-zinc-button-cells-with-rechargeable-li-ion-and-li-polymer-coin-and-miniature-prismatic-cells/, acesso em maio de 2017.

Bateria que devido a sua elevada densidade de energia, oriunda do uso do oxigênio da atmosfera como um dos eletrodos, é uma excelente candidata para aplicações miniaturizadas que necessitam de microbaterias.

A bateria de Zinco/Ar (Zn/Ar) é uma das tecnologias mais maduras da família de Metal/Ar. Em 1970 foi introduzido no mercado a bateria tipo botão de Zn/Ar (bateria primária) para uso em aparelhos auditivos, tornando-se padrão nos anos 80 para aplicação nesses aparelhos.

Resultados experimentais têm demonstrado que técnicas de design 3D para microbateria de zinco têm sido promissoras. Assim como a bateria de lítio, as microbaterias desta tecnologia também estão em desenvolvimento na busca de soluções que agreguem flexibilidade, aumento da densidade de energia, potência e vida útil[81,82,83].

5.1.4.1.4 Bateria de Lítio/Ar

Um sistema eletroquímico com grande potencialidade para acumulação de energia é o Lítio/Ar devido à sua alta densidade energética. As pesquisas atuais indicam que a bateria Li/Ar apresenta desafios, que terão que ser solucionados para esta tecnologia se tornar um produto viável comercialmente, com destaque para:

- Consumo do eletrólito durante a reação no cátodo (no caso dos eletrólitos que contém duas camadas, envolvendo um eletrólito aquoso);
- Precipitação dos óxidos de lítio dentro do cátodo no caso do eletrólito não aquoso. Uma das grandes dificuldades é obter uma configuração de eletrodos contendo lítio metálico e oxigênio de forma a se conseguir uma bateria recarregável, eficiente e segura.

Para viabilizar esta tecnologia, há necessidades de se alcançar avanços tecnológicos, tanto do ponto de vista de engenharia como de materiais, principalmente relacionado à questão de porosidade, estrutura e composição da estrutura do cátodo (para prevenir a deposição do óxido de lítio). Atenção especial deverá ser dada para prevenir a entrada na célula de traços de CO_2 ou H_2O provenientes do ar, pois ambos reagem com o ânodo de lítio e o óxido de lítio (formado na descarga)[84].

81 Armutlulu: Armutlulu, Y Fang, S H Kim, C H J, S A Bidstrup Allen and M G Allen, "A MEMS-enabled 3D zinc–air microbattery with improved discharge characteristics based on a multilayer metallic substructure" Journal Of Micromechanics and Microengineering, 2011.

82 Chamran: Fardad Chamran, Hong-Seok Min, Bruce Dunn and Chang-Jin “CJ” Kim, "Zinc-Air Microbattery With Electrode Array of Zinc Microposts", MEMS 2007.

83 Kraytsberg: Alexander Kraytsberg, Yair Ein-Eli, Review on Li–air batteries-Opportunities, limitations and perspective, Journal of Power Sources 196, 2011.

84 Kraytsberg: Alexander Kraytsberg, Yair Ein-El, Review on Li–air batteries-Opportunities, limitations and perspective, Journal of Power Sources 196, 2011.

O sistema Li/Ar apresenta um elevado valor de capacidade, sendo um dos fatores que reforçam a importância desta bateria e justifica os investimentos que estão sendo realizados em pesquisas para torná-la viável. Uma vez que a tecnologia seja viabilizada, esta poderá ser otimizada e readequada para aplicações em microescala - é uma tecnologia que futuramente poderá ser utilizada em microbaterias[85].

5.1.4.2 Formas de captação de energia

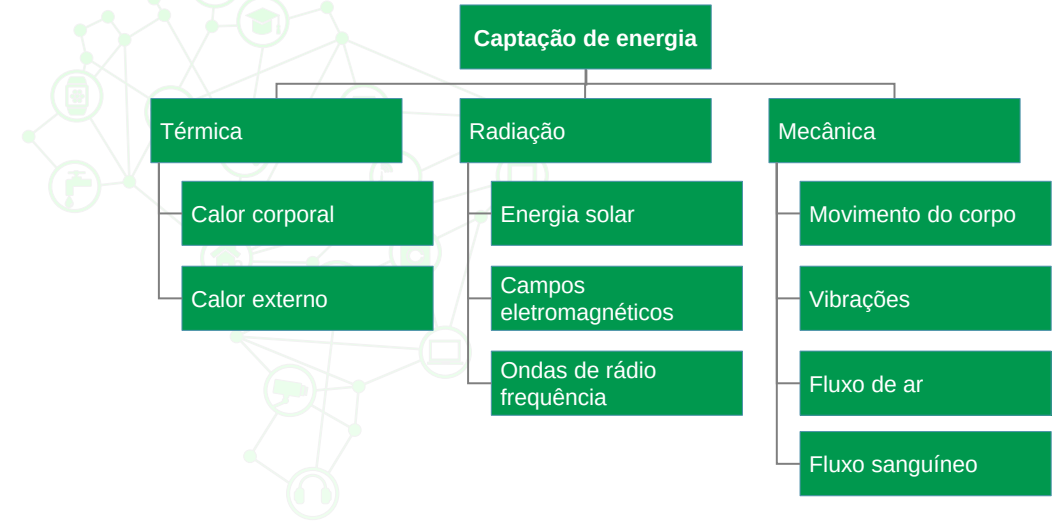
A captação de energia, também conhecida por *Energy harvesting* (EH) é o processo pelo qual a energia é derivada de fontes externas (por exemplo, energia solar, térmica, eólica, cinética), capturada e armazenada para aparelhos pequenos, autônomos e sem fio, como mostra o QUADRO 18. A colheita de energia provê uma pequena quantidade de energia para eletrônicos de baixa-energia. Dentre as características de *Energy harvesting* destacam-se:

- Livre de manutenção;
- Livre de poluição no ponto de criação de eletricidade e no ponto de uso desta eletricidade;
- Produz 0,1 microwatts até 1MW;
- Energia renovável (humano ou animal);
- A eletricidade gerada pelo EH precisa ser armazenada e disponibilizada em diferente tensão, impedância e corrente.

[85] University of Michigan, disponível em: http://www-personal.umich.edu/~adriaens/Site/UM_CleanTech_files/Sastry.pdf, acesso em maio de 2017.

QUADRO 18

Tipos de fontes de energia ambientes adequadas para Energy Harvesting



FONTE: Análise do consórcio

A classificação de *energy harvesting* pode ser organizada pela forma que a energia é captada. Por exemplo, dispositivos de colheita piezoeléctricos captam energia mecânica e converte em energia elétrica útil. As fontes para *energy harvesting* são:

- Turbinas eólicas
- Células fotovoltaicas
- Geradores termoelétricos
- Dispositivos de vibração mecânica, tais como dispositivos piezoeléctrico, eletromagnético, etc. A TABELA 3 abaixo mostra alguns dos métodos com sua capacidade de geração de energia.

TABELA 3 FONTES DE ENERGY HARVESTING

Método de *harvesting*	Densidade de potência
Célula solar	15 mW/cm^3
Piezoeléctrico	330 μW/cm^3
Vibração	116 μW/cm^3
Termoelétrico	40 μW/cm^3

As propriedades de EH a serem consideradas são:

- Propriedades elétricas: densidade de potência, tensão e corrente máxima;
- Propriedades físicas: tamanho, forma e peso;
- Propriedades ambientais: resistência a água e faixa de operação de temperatura;
- Propriedades operacionais e de manutenção.

5.1.4.3 Vibração mecânica

Quando um dispositivo é submetido a uma fonte de energia mecânica (vibração, por exemplo), uma massa inercial pode ser usada para criar movimento. Este movimento pode ser convertido em energia elétrica usando três mecanismos: piezoeléctrico, eletrostático e eletromagnético.

Materiais piezoeléctricos

Convertem energia mecânica de pressão, vibração ou força em eletricidade, sendo capazes de gerar carga elétrica quando uma carga mecânica é aplicada nela. Esta propriedade de material piezoeléctrico é considerada pelos pesquisadores para desenvolver uma série de coletores piezoeléctricos para atender diferentes aplicações.

Captação de energia eletrostática (capacitiva)

Este tipo de colheita é baseado na mudança capacitiva. As vibrações separam as placas de um (capacitor variável) inicialmente carregado, e a energia mecânica é convertida em energia elétrica.

Colheita de energia eletromagnética

EV eletromagnético pode ser obtido pelo princípio da indução eletromagnética. A indução eletromagnética é definida como o processo de geração de tensão num condutor pela mudança do campo magnético em torno do condutor. Um dos caminhos mais efetivos de produzir indução eletromagnética para EH é utilizando imãs permanentes, uma bobina e um feixe ressonante.

5.1.4.3.1 Células fotovoltaicas

Dispositivos que convertem energia luminosa em energia elétrica. A forma de energia explorada é tipicamente energia luminosa obtida usualmente do sol.

5.1.4.3.2 Geradores Termoelétricos

Geradores termoelétricos seguem o princípio da termoeletricidade para produzir a energia elétrica requerida. O fenômeno de criar potencial elétrico com uma diferença de temperatura e vice-versa pode ser chamado como termoeletricidade. A energia térmica é captada para obter energia elétrica para energizar dispositivos eletrônicos. Dispositivos termoelétricos são usados em aplicações espaciais e terrestres.

5.1.4.4 Tendências

As microbaterias são um dos componentes críticos para a nova geração de dispositivos microeletrônicos, no qual se inclui a IoT, que representa uma grande oportunidade para o desenvolvimento de microbaterias, que se diferem das baterias convencionais pela sua arquitetura e seleção de materiais.

Pesquisas em microbaterias têm focado na inovação do processo de fabricação e no design das células. Recentemente, tem surgido o interesse no desenvolvimento de microbaterias com design mecânico flexível. O desenvolvimento destes novos conceitos requer a busca de inovação dos materiais para empacotamento, bem como métodos e seleção de materiais para fabricação da bateria. O desenvolvimento das microbaterias tem buscado o aumento das densidades de energia e de potência em aplicações de micro *harvestin* energético.

Pesquisas de baterias de filme fino em estado sólido são relativamente recentes e têm buscado o aperfeiçoamento de materiais e métodos de fabricação. O aumento da capacidade de armazenamento de energia tem sido alcançado com a metodologia de fabricação 3D, que também permite a fabricação flexível de baterias. A tecnologia mais pesquisada e estudada de microbateria é a de lítio. Por exemplo, microbaterias de lítio são as mais pesquisadas para veículos elétricos e em grandes sistemas de armazenamento de energia.

Estudos revelam que há uma projeção de crescimento nas vendas das microbaterias de lítio, sendo o mercado estimado para 2017 em U$ 1,5 bilhões e para 2021 em U$ 3,4 bilhões. Este mercado está sendo impulsionados por diversas aplicações emergentes, tais como os dispositivos microeletrônicos e aplicações de IoT. Micro-drones, dispositivos eletrônicos inteligentes para vestimentas, dispositivos em chips já são comerciais e se tornam cada vez mais sofisticados. Estes dispositivos usualmente não requerem grande quantidade de energia, necessitando correntes na ordem de miliamperes.

Há diversos estudos teóricos de arquitetura e design para microbaterias. No entanto, poucos conseguem se viabilizar e gerar resultado comercial[86]. Baterias de diversos elementos químicos têm sido utilizadas no passado e continuam sendo aplicadas, com as microbaterias primárias ainda desempenhando um papel importante para a maioria das aplicações, devido às poucas alternativas viáveis para a fabricação de microbateria (quando comparada com as baterias de grande porte).

Um ponto a ser estudado e desenvolvido é a deposição do lítio metálico em camada fina; progressos estão sendo alcançados utilizando técnicas baseadas em radiofrequência. Embora o uso de lítio metálico seja menos preocupante para as microbaterias de lítio-íon, pois os riscos de crescimento de dendritos (formação de excrescências nos eletrodos que pode provocar curto-circuito na célula) é significativamente menor no eletrólito em estado

[86] Ferrari: Stefania Ferrari, Melanie Loveridge, Shane D. Beattie, Marcus Jahn, Richard J. Dashwood, Rohit Bhagat," Latest advances in the manufacturing of 3D rechargeable lithium microbatteries", Journal of Power Sources, 286, 2015.

sólido, a substituição do anodo do lítio continua a ser um grande desafio, devido ao seu elevado potencial eletroquímico, que é um dos pontos cruciais para a viabilidade das microbaterias.

Atualmente as microbaterias são comercializadas por poucos fabricantes, tais como: PowerPaper, Cymbet, Infinite Power Solutions, ST Microelectronics, etc. Em paralelo, outros fabricantes (exemplos: Johnson Battery Technology, Front Edge Technology e I-tem) estão trabalhando em protótipos e esperam comercializar suas microbaterias nos próximos anos. A competição é intensa e aquisições e fusões de empresas mostram que se espera um bom desempenho no mercado de microbaterias.

Cabe ressaltar que algumas inovações aplicadas em microbaterias poderão futuramente sofrer ampliação de escala e ajudar no desenvolvimento de baterias de maior capacidade, e vice-versa.

5.1.5 Sensoriamento

De forma geral, as aplicações de IoT se devem valer de soluções de sensoriamento. Soluções de sensoriamento são mais abrangentes que sensores propriamente ditos. Estas soluções tipicamente englobam outros componentes, fazendo com que um sensor, ou suas funções, sejam aplicadas em um contexto de *sensor node*, isto é, processando e transmitindo as informações detectadas pelo elemento sensor ou transdutor. Assim, pode-se dizer que uma solução de sensoriamento é composta pelos seguintes módulos:

- Sensor;
- Tratamento de sinais;
- Processamento e armazenamento (memória);
- Transporte de dados.

Para que se tenha uma maior compreensão das tecnologias das soluções de sensoriamento, suas tendências e os desafios para que estas estejam aptas a suportar as demandas de IoT, faz-se necessário entender os dispositivos sensores e suas principais tecnologias.

5.1.5.1 Introdução a sensores

De acordo com a ITU (*International Telecommunication Union*), em seu documento ITU-T Y.2221[87] sensores são dispositivos que detectam condições físicas ou químicas e fornecem um sinal eletrônico como resposta, proporcional ao estímulo detectado. O elemento ativo de um sensor, responsável pela detecção e eventual quantificação de um fenômeno, é chamado de transdutor. O transdutor atua na conversão de uma forma de energia (fenômeno) em outra. De acordo com a EDN Network, os sensores podem ser considerados o "sistema nervoso central" de qualquer solução de IoT.

[87] *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

No contexto de IoT, sensores são componentes de um *sensor node*. Ainda de acordo com a ITU-T Y.2221, um *sensor node* é composto por sensor (es), e opcionalmente por elementos atuadores, e possuem capacidade de processar dados detectados e transportá-los por meio de redes de comunicação. Redes de sensores por sua vez, compreendem a interconexão entre os *sensor nodes*, possibilitando a troca de informações por meio de comunicação com ou sem fio.

A Tabela 4 apresenta os fenômenos comumente detectados por sensores em um contexto de IoT, os principais métodos de conversão de energia e as principais grandezas mensuradas.

TABELA 4 FENÔMENOS COMUMENTE DETECTADOS POR SENSORES EM IOT

Fenômenos	Métodos de conversão	Grandeza
Biológico	Biológico (transformação biológica e transformação física)	Concentração de fluido (gás e líquido)
Químico	Químico (transporte químico, transformação física, conversão eletroquímica)	
Elétrico	Física (elétrico-elétrico)	Carga, Tensão, Corrente, Campo Elétrico, Condutividade e Permissividade
Magnético	Física (magneto-elétrica)	Campo magnético, Fluxo, Permeabilidade
Calor / temperatura	Física (termoelétrica, termomagnética, termo-óptica)	Temperatura, Fluxo, Calor específico, Condutividade térmica
Movimento mecânico	Física (mecânico-elétrica)	Posição, Velocidade, Aceleração, Força, Deformação, Estresse, Pressão, Torque, Onda (amplitude, fase, polarização, frequência e velocidade)
Óptico	Física (fotoelétrica, fotomagnética, fotoelástica)	Índice de refração, Refletividade, Refração

A classificação[88] dos sensores pode se dar em função dos fenômenos detectados ou, principalmente pelo princípio de operação de seus transdutores, como por exemplo:

- Fotovoltaicos;
- Piezoeléctricos;
- Químicos;
- Indução mútua;
- Eletromagnéticos;
- Efeito Hall;
- Fotocondutores;
- Baseados em semicondutores.

A escolha de um sensor para uma determinada demanda leva em conta três classes de fatores:

- Técnicos;
- Ambientais;
- Econômicos.

A Tabela 5 apresenta exemplos relevantes para cada uma das três classes de fatores relevantes para a escolha de sensores.

TABELA 5 FATORES RELEVANTES PARA A ESCOLHA DE SENSORES

Fatores Técnicos	Fatores Ambientais	Fatores Econômicos
Sensibilidade	Faixa de temperatura	Custo
Faixa de operação	Humidade	Disponibilidade
Estabilidade	Corrosão	Ciclo de vida
Repetibilidade	Dimensões	-
Linearidade	Susceptibilidade a interferências Eletromagnéticas	-
Fator de erro	Robustez	-
Tempo de resposta	Fonte/Consumo de Energia	-
Frequência de resposta	-	-

Somam-se aos aspectos mencionados na Tabela 5 características demandadas por aplicações de IoT como, por exemplo, a necessidade de sensores com dimensões reduzidas, baixo consumo de energia e custos compatíveis com o volume de objetos inteligentes que irão receber os sensores.

[88] Carstens, J, Electrical Sensors and Transducers, Prentice Hall, 1993.

5.1.5.2 Principais tecnologias de sensores

No contexto de IoT, pode-se afirmar que as principais tecnologias de sensores permitem a transformação da energia detectada, oriunda dos fenômenos físicos descritos na Tabela 4 acima. Dentre as principais tecnologias destacam-se os sensores baseados em:

- Semicondutores (*MEMS*/*SAW*/*CMOS*);
- Carbono.

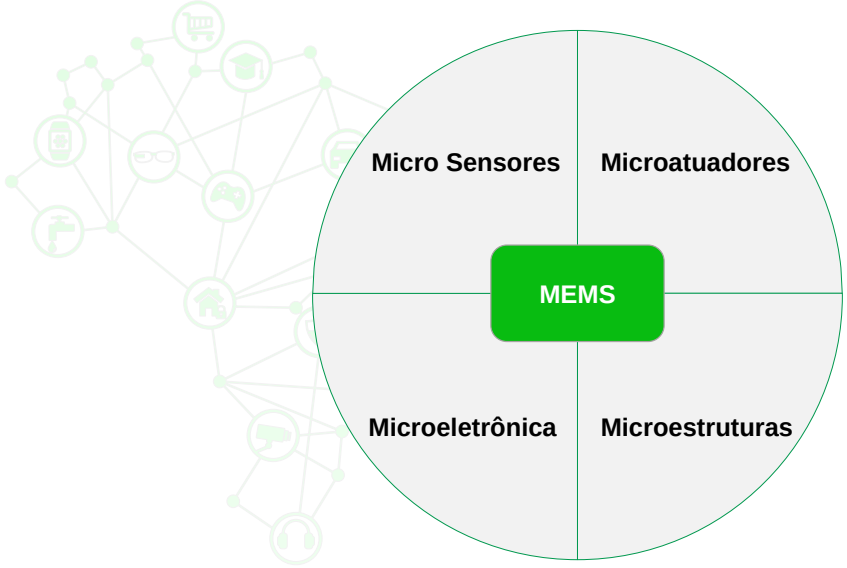
5.1.5.2.1 Sensores baseados em MEMS

Os sensores baseados na tecnologia MEMS (*Micro-Electro-Mechanical Systems*) são sistemas micro eletromecânicos desenvolvidos sob a intersecção de conceitos de eletrônica e mecânica. Os avanços tecnológicos e o amadurecimento da indústria ao final dos anos 80 possibilitaram que pesquisadores dessem início ao processo de inserção de funções mecânicas em chips até então empregados em funções eletrônicas.

Dispositivos MEMS são capazes de reagir a estímulos externos naturais de forma dinâmica e analógica e sua confecção se dá pela aplicação de técnicas de micro fabricação, por meio das quais, silício e outros substratos comumente aplicados em microeletrônica são manipulados e micro usinados com o intuito de promover a integração das estruturas mecânicas, dos elementos sensores, atuadores e componentes eletrônicos, culminando com a sintetização micrométrica destes sistemas. O QUADRO 19 descreve os principais componentes de dispositivos MEMS convencionais.

QUADRO 19

Composição típica de um dispositivo MEMS



FONTE: Análise do consórcio

Em um sistema MEMS, micro sensores são responsáveis pela detecção dos fenômenos para os quais foram projetados e pela conversão destes em sinais elétricos proporcionais. A camada de microeletrônica de MEMS é responsável pelo processamento das informações e, quando aplicável, pelo acionamento dos micro atuadores, convertendo assim os sinais elétricos em energia mecânica.

A versatilidade desta tecnologia, somada à maturidade atingida pela mesma, faz com que esta venha sendo amplamente empregada em diversos setores da indústria.

A Tabela 6 apresenta alguns exemplos de aplicações da tecnologia MEMS na indústria.

TABELA 6 EXEMPLOS DE APLICAÇÕES DA TECNOLOGIA MEMS NA INDÚSTRIA

Automotiva	Eletrônica	Médica	Comunicações	Defesa
Sensores internos de navegação	Smartphones e vídeo games	Sensores de pressão arterial	Componentes de redes de fibra óptica	Sistemas de orientação de mísseis
Sensor do compressor do ar condicionado	Cabeças de impressão de impressoras jato-de-tinta	Estimuladores musculares	Chaves, filtros e relês para sinais RF	Vigilância
Sensores de frenagem e controle de suspensão	Projetores de vídeo	Sensores implantados	Osciladores controlados por tensão (VCO)	Sistema de armas
Sensores de nível de combustível e pressão de vapores	Sistemas de armazenamento de dados	Próteses	Divisores e acopladores	Sensores embarcados
Sensores de sistemas airbag	Detecção de terremotos	Marca-passos	Lasers sintonizáveis	Controle de aeronaves

A demanda por dispositivos com dimensões cada vez mais reduzidas provocaram o desenvolvimento de soluções com dimensões inferiores a 01 (um) mícron. Nestes casos, os dispositivos passam a ser conhecidos como NEMS (*Nano Electro Mechanical Systems*). Estes sistemas demandam tratativas de produção diferentes dos MEMS convencionais, principalmente por estarem suscetíveis a conceitos da mecânica quântica.

Um ponto comum entre os dispositivos MEMS e NEMS é a criticidade de seus encapsulamentos, pois estes são extremamente sensíveis ao estresse mecânico. O encapsulamento de um MEMS deve ser capaz de proteger suas partes internas, mecânicas e eletrônicas e, ao mesmo tempo, permitir que o dispositivo possua interface com o meio físico no qual está instalado ou inserido.

5.1.5.2.2 SENSORES BASEADOS EM SAW

A tecnologia SAW (*Surface Acoustic Wave*) é diretamente ligada ao desenvolvimento de dispositivos piezoeléctricos. As características de propagação das ondas acústicas superficiais foram descritas em meados dos anos 1880, enquanto que as aplicações industriais da tecnologia tiveram seu início da década de 1950. Atualmente, os dispositivos SAW ocupam um papel no segmento de telecomunicações, onde são comumente aplicados em filtros de sinais de RF em diferentes bandas, como, 2G, 3G, 4G (LTE) e em soluções de sensoriamento.

Sensores SAW são dispositivos micro eletromecânicos (MEMS), que utilizam ondas mecânicas como mecanismo de interação sensível com analitos. Um dispositivo SAW é composto por um substrato piezoeléctrico e por transdutores digitais (IDT – *Interdigital Transducer*), dispostos nas extremidades. O espaço entre os dois IDTs, onde a onda acústica se propaga, é conhecido como linha de atraso (*delay-line*), pelo fato da onda mecânica se propagar muito lentamente de um IDT até o outro.

O substrato piezoeléctrico dos sensores SAW são confeccionados em materiais de um único cristal, como por exemplo, Quartzo (SiO2), Niobato de Lítio (LiNbO3), entre outros. Nestes casos, são utilizados diferentes ângulos de corte dos materiais para as mais diferentes aplicações.

No contexto de IoT, a tecnologia SAW apresenta benefícios significativos para uma ampla gama de aplicações, com destaque para:

- *Wireless* - Transmissão de dados sem fio;
- Passiva;
- Dimensões reduzidas;
- Custos reduzidos;
- Altas taxas de resposta;
- Imunidade a interferências eletromagnéticas;
- Aplicáveis em situações que demandem movimentação ou em que os objetos serão rotacionados;
- Resistentes à temperatura e ambientes hostis.

Dentre as aplicações mais comuns de sensores SAW citam-se:

- Biosensores (identificação de patologias epidêmicas);
- Sensoriamento de gases;
- Monitores de temperatura de umidade;
- Integridade de estruturas;
- Presença de agentes químicos.
- Radiação ultravioleta.
- Viscosidade. (Análise de petróleo);
- Campo magnético.

5.1.5.2.3 SENSORES BASEADOS EM CMOS

Os sensores baseados em tecnologia CMOS (*Complementary Metal-Oxide-Semiconductor*) estão presentes em uma parcela significativa dos dispositivos de sensoriamento empregados em soluções de IoT. Estes sensores são aplicados em demandas dos segmentos biomédico, químico, industrial, agricultura, segurança, defesa e ambientais. A adoção destes dispositivos se dá principalmente pela viabilidade de produção em larga escala de soluções miniaturizadas e que atingem o baixo custo demandado pelo mercado.

A tecnologia CMOS é dominante no campo de semicondutores para dispositivos de microeletrônica e fabricação de circuitos integrados, pois permite a deposição de milhões de transistores em uma área de 1 mm², com possibilidade de execução de funções complexas. Além disso, a tecnologia é amplamente aplicada em módulos de processamento de sinal elétrico. No entanto, também pode ser aplicada na implementação de transdutores, como por exemplo, os sensores CMOS óptico e eletroquímico como ISFET (*Ion-Sensitive Field-Effect Transistor*) e BioFET (*Field-Effect Transistor-based biosensor*).

5.1.5.2.4 SENSORES BASEADOS EM CARBONO

Dentre a gama de tecnologias de sensores utilizadas, vêm ganhando destaque as tecnologias baseadas em carbono, devido a sua alta sensibilidade, seletividade, curto tempo de resposta e baixo consumo de energia. São sensores de baixo impacto ambiental, em sua maioria biodegradáveis, sendo ideais para aplicações em ambientes altamente restritos como o sensoriamento em organismos vivos. Por suas características recebem destaque para a implantação de sensoriamento massivo para IoT à medida que permitem instalações mais simples, com precisão, boa durabilidade, baixo consumo e com ciclo de vida economicamente viável.

Dentre as principais tendências em desenvolvimento de sensores com essa tecnologia, podemos destacar:

- **OTFT (*Organic Thin-Film Transistor*)** - tecnologia baseada em carbono, que permite o desenvolvimento de moduladores de corrente com extrema precisão. Essa tecnologia habilita o desenvolvimento de nano/micro sensores capazes de serem inseridos em organismos vivos, permitindo medições a nível celular. As áreas médicas e farmacêuticas são as principais fomentadoras do desenvolvimento de sensores dessa tecnologia. Uma possível aplicação da tecnologia seria o monitoramento do nível de lactase em fibras musculares[89]. O sensor é inserido sobre a pele do usuário e monitora níveis de lactase nos músculos, de modo a avaliar o desgaste muscular em atividades físicas;

[89] Disponível em http://www.mdpi.com/2079-9292/3/2/234/htm, acesso em abril de 2017.

- **CNBS (*Carbon-nanotube based sensors*) -** utiliza nano tubos de carbono como antena omnidirecional de alta sensibilidade. Existem diversos tipos de aplicações de sensores CNBS. No entanto, a tecnologia é predominantemente utilizada para detecção de elementos e particulados em áreas com baixa densidade destes, por exemplo na aplicação de detecção de gases.

5.1.5.3 Principais tecnologias de transporte de informação de sensores

5.1.5.3.1 SMART *TAGS*

Um *Smart Tag* é um tipo de *sensor node*, composto, em geral, pelos módulos de detecção, tratamento de informações, processamento e armazenamento de dados, amplamente utilizado em soluções de detecção, sensoriamento e localização, e que comunica seus dados por meio de técnicas de transporte de dados baseadas em comunicação sem fio.

Detecção

A tecnologia de *Smart Tag* mais comum em aplicações de detecção é a RFID (*Radio Frequency IDentification*). A tecnologia RFID é uma técnica de AIDC (*Automatic Data Capture*) utilizada para identificar, rastrear e gerenciar desde produtos e documentos até animais ou mesmo indivíduos, sem contato e sem a necessidade de um campo visual. De uma forma geral, um sistema RFID é uma ferramenta de aquisição de dados em tempo real que possibilita a eliminação de intervenções humanas, aumentando a segurança e eficiência dos processos.

Atualmente, esta tecnologia é amplamente empregada em soluções de automação de processos logísticos, pois permite o aumento da eficiência na rastreabilidade de itens em todos os elos da cadeia de suprimentos. As soluções de detecção utilizando RFID são tipicamente compostas por transponders (*RF Smart Tags*), leitores com antenas e um dispositivo controlador, como por exemplo, um computador.

A detecção automática dos itens se dá pela captura e tratamento dos dados armazenados nas etiquetas inteligentes (*tags*), de modo que uma *tag* seja lida sem a necessidade de visada direta, através de desafios e objetos. Os *transponders* ou *tags* RFID são classificados em ativos, semiativos e passivos, dependendo do uso ou não de uma bateria para alimentação de seus circuitos eletrônicos, como detalhado a seguir:

- ***Tags* ativos:** possuem um circuito de alimentação, que energiza seu circuito de controle e seu microchip de modo ativá-lo e capacitá-lo a enviar informações de sua identificação de forma independente à excitação de um leitor. *Tags* ativos podem detectar temperatura, umidade, movimentação, violação, entre outros. Por exemplo, *tags* ativos são utilizados no sistema de cobrança automática de tarifa de pedágio. De forma geral, *tags* ativos possuem:

  - Capacidade de memória elevada, uma vez que sua eletrônica tem mais energia disponível, se comparada aos sistemas ativos e semiativos, além de possibilitarem a utilização de sensores acoplados aos seus circuitos;
  - Alcance de leitura significativamente superior aos demais tipos de *tags*, uma vez que, devido à alimentação externa, seus chips não dependem do uso da energia transmitida pelos leitores;
  - Custo consideravelmente superior aos outros tipos de *tags*, devido a maior complexidade dos *tags* ativos, fazendo com que estes sejam preferencialmente empregados na identificação e rastreabilidade de itens de alto valor agregado;
  - Possibilidade de configuração da periodicidade com que os *tags* devem ficar ativos e enviar seus sinais de identificação.
- ***Tags* semiativos:** apresentam níveis de sensibilidade superiores aos *tags* passivos, alcançando distâncias maiores de leitura; dependem de um nível mínimo de sinal do leitor para alimentar um circuito, que através de uma bateria, suplementa a energia fornecida ao chip para a realização de suas funções básicas;
- **T*ags* passivos:** são os mais comuns e amplamente utilizados, são aqueles que dependem totalmente da energia fornecida pelos leitores para "refletirem" as informações contidas em suas memórias.

O desafio atual dessa indústria é desenvolver *tags* com antenas que otimizem a captação de energia, considerando, principalmente, dimensões físicas, custo, e circuitos que operem com níveis de sinais mais baixos possíveis para que o alcance dos *tags* passivos possa ser cada vez maior.

A leitura dos *tags* RFID pode ocorrer em diferentes faixas de frequência. São elas:

- Baixa frequência ou do inglês *Low frequency (LF)* geralmente em 125/135 KHz;
- Alta frequência ou do inglês *High frequency (HF)* geralmente em 13,56 MHz;
- Frequência ultra alta ou do inglês *Ultra High Frequency (UHF)* geralmente em 433, 860, 900 MHz.

A Tabela 7 apresenta diferentes características e aplicações típicas para os sistemas RFID nas faixas de frequência existentes:

TABELA 7 CARACTERÍSTICAS E APLICAÇÕES TÍPICAS PARA OS SISTEMAS RFID

Faixa de Frequência	Características	Aplicações Típicas
***Low Frequency* (LF)** De 30 até 300 KHz (geralmente em 125KHz e 134,2KHz)	• Acoplamento magnético; • Geralmente são *tags* passivos; • Baixo alcance de leitura (<0,5m); • Baixa velocidade de leitura (baixa taxa de transferência de dados - <1kbps); • Baixo custo.	• Controle de acesso • Identificação animal • Controle de inventário • Chaves de veículos
***High Frequency* (HF)** De 3até 30 MHz (geralmente em 13,56MHz)	• Acoplamento magnético; • Geralmente são *tags* passivos; • Baixo a médio alcance de leitura (<1,5m); • Média velocidade de leitura (média taxa de transferência de dados <20Kbps); • Baixo custo.	• Controle de acesso; • *Smartcards*; • Identificação de objetos individuais; • NFC (*Near Field Communication*).
***Ultra-HighFrequency* (UHF)** De 300MHz até 3GHz (geralmente em 433MHz e entre 860 e 960 MHz)	• Acoplamento eletromagnético; • Médio alcance para *tags* passivos – 0,5m a 10m • Alto alcance *tags* ativos - <100m; • Alta velocidade de leitura (alta taxa de transferência de dados - ~30kbps); • Médio custo.	• Gerenciamento de itens; • Rastreamento em grandes velocidades (ex. *tags* em veículos); • Identificação de objetos em grupo (Paletes).
Microondas De 2 até 30GHz (geralmente em 2,4 e 5,8 GHz)	• Acoplamento eletromagnético; • Alto alcance (>10m) • Alta velocidade de leitura (alta taxa de transferência de dados - <100kbps); • Alto custo (principalmente em *tags* ativos).	• Gerenciamento de itens; • Aplicações industriais, científicas e médicas (ISM).

No Brasil, a atribuição de faixas de frequências destinadas ao uso de dispositivos de identificação por radiofrequência é feita pela Anatel – Agência Nacional de Telecomunicações – em sua resolução de número 506 de 2008. Nesta resolução apresentam-se características e requisitos de operação, com enfoque na preservação do espectro de frequências, para sistemas denominados de radiação restrita. Para sistemas RFID, esta resolução trata de aspectos como intensidade de campo, níveis de emissões intencionais e não intencionais (espúrias) e da densidade espectral de potência.

Monitoramento de grandezas

Os Smart *tags* voltados às aplicações de monitoramento de grandezas são tipicamente dispositivos ativos, isto é, dispõe de uma fonte interna de energia, diferentemente dos *tags* passivos (ex: *tags* RFID). Estes *sensor nodes* são integrados a módulos sensores, com os quais se comunicam por interfaces dos tipos I2C, SPI e entradas analógicas e digitais, interfaces amplamente empregadas nos principais módulos sensores disponíveis no mercado. A transmissão dos dados de sensoriamento ocorre por meio de tecnologias de comunicação sem fio de curto alcance, como por exemplo, Bluetooth, Bluetooth Low Energy, ZigBee e WiFi. A comunicação é comumente ponto a ponto, isto é, feita entre o *sensor node* e um dispositivo concentrador (*gateway*). No contexto de IoT, é crescente o número de aplicações, como, por exemplo, sensoriamento social, em que o *Smart tag* comunica-se diretamente com smartphones.

Localização

As aplicações de localização utilizando Smart *tags* se dão por meio de sistemas RTLS (Real Time Location System). A tecnologia RTLS permite a geolocalização de "coisas" dotadas de Smart *tags*. Smart *tags* emitem sinais que são recebidos por dispositivos leitores ou *gateways* que, com base na intensidade de sinal (RSSI - *Received Signal Strength Indicator*) e na aplicação de algoritmos de localização permitem determinar o geoposicionamento dos itens. A Tabela 8 apresenta as principais tecnologias de Smart *tags*, sua aplicabilidade em soluções de sensoriamento, os principais *atores* do mercado e as principais áreas de atuação.

TABELA 8 PRINCIPAIS TECNOLOGIAS DE SMART *TAGS*

Principais Tecnologias	Aplicabilidade	*Atores* no mercado	Principais Áreas de Atuação
RFID (passivo e ativo)	Detecção	RF Passivo - Alien, Impinj, Zebra, Jadac, Honeywell, NXP, Smartrac, Avery Dennison. RFID Ativo - RFCode.	Produção, Logística, Agronegócio
BLE	Detecção e Monitoramento de grandezas	BLE - Nordic, Cypress, NXP/Freescale, Texas	Produção, Transporte, Saúde, Ambiente, Consumidor, Agronegócio.

Principais Tecnologias	Aplicabilidade	*Atores* no mercado	Principais Áreas de Atuação
ZIGBEE	Detecção e Monitoramento de grandezas	DIGI (ZigBee)	Produção, Transporte, Saúde, Ambiente, Consumidor, Agronegócio.
WiFI	Detecção e Monitoramento de grandezas	Ekahau (WiFi)	Produção, Transporte, Saúde, Ambiente, Consumidor, Agronegócio.
UWB	Detecção e Monitoramento de grandezas	Ubisense (UWB)	Produção, Transporte, Saúde, Ambiente, Consumidor, Agronegócio.
Sistemas de localização (RTLS - *Real Time Location Systems*) baseados em *sensor nodes*	Detecção e Monitoramento de grandezas para fins de localização em tempo real	Ekahau (WiFi), RFCode (RFID ativo), Ubisense (UWB)	Produção, Logística, Saúde.

5.1.5.3.2 Redes de Sensores

Segundo a norma ITU-T Y.2221, rede de sensores são compostos de nós (*sensor nodes*) interligados que trocam dados coletados por comunicação com ou sem fio. O IEEE define uma rede de sensores sem fio (WSN), como sendo uma rede espacialmente distribuída de sensores autônomos, que monitoram condições físicas ou ambientais, tais como temperatura, som, pressão, etc, passando de forma cooperativa os dados, através da rede, ou seja, de um elemento para o outro, até uma localização central (*gateway* ou concentrador). Ainda, segundo o IEEE, uma WSN é constituída de centenas ou milhares de "nós", onde cada nó está conectado a um ou vários sensores. A função da WSN é a coleta coordenada de dados.

Ao relacionar a WSN com um sistema IoT, o IEEE define que o alcance ou abrangência de um sistema IoT é maior do que a atuação de uma rede WSN. Além disso, a identificação única das "Coisas" e sua conexão com a Internet é uma característica desejável de IoT e que uma WSN não possui. Em outras palavras, uma rede de sensores sem fio pode ser parte de IoT.

A Tabela 9 apresenta as principais tecnologias de redes de sensores, sua aplicabilidade em soluções de sensoriamento, os principais *atores* do mercado e as áreas de atuação.

TABELA 9 PRINCIPAIS TECNOLOGIAS DE REDES DE SENSORES

Principais Tecnologias	Aplicabilidade	*Atores* Mercado	Principais Áreas de Atuação
Rede de Sensores Sem Fio (*WSN - Wireless Sensor Network*)	Tecnologia colaborativa permitindo diferentes topologias de redes. Sistemas/dispositivos compostos por sensores, módulos de RF, micro controladores e módulos de alimentação/energia.	Ubisense (UWB), Nordic (BLE 5.0), DIGI (ZigBee)	Produção, Transporte, Ambiente, Consumidor

5.1.5.3.3 TRANSPORTADORES DE SENSORES

Consistem nos dispositivos tecnológicos aplicados no deslocamento, manipulação e controle de sensores nos mais diversos tipos de missões de sensoriamento. As informações de sensoriamento são obtidas por meio de sensores e instrumentos de alto desempenho, embarcados em meios de transporte radiocontrolados ou até mesmo autônomos.

O sensoriamento remoto consiste no tratamento, armazenamento e análise dos dados coletados, de forma que se conheçam melhor os fenômenos existentes na superfície monitorada. Esta técnica é capaz de revelar dados geográficos e até mesmo históricos de espaços naturais, como por exemplo, a distribuição das áreas florestais e o avanço do desmatamento em determinada região. O sensoriamento remoto vem sendo aplicado na agricultura de precisão, na qual a utilização de sensores e sistemas integrados possibilita a obtenção de diversas informações, como:

- **Estimativa de área plantada**: através das imagens consegue-se estimar toda extensão da plantação, podendo controlar e acompanhar o crescimento da área plantada;
- **Levantamento do número de plantas em determinada área**: utilizando as imagens como base e aplicando os algoritmos modernos é possível conhecer a quantidade de plantas existentes, detectar áreas de menor densidade e otimizar a plantação;
- **Saúde das plantas e culturas**: através das diferentes colorações das plantas nas imagens é possível perceber aquelas que não estão desenvolvendo como deveriam, e também, as que carecem de água e determinados nutrientes;
- **Detecção de pragas na plantação e gargalos no processo produtivo**: assim como no monitoramento da saúde das plantas, através da coloração das imagens consegue-se encontrar pragas e locais de baixa produção, permitindo evitar quedas significativas na produção.

Além disso, o sensoriamento remoto vem sendo utilizado em tecnologias como VANTs (Veículo Aéreo Não Tripulado) e VSORs (Veículo Submarino Operado Remotamente), que permitem diversas aplicações, como por exemplo:

- **Aplicações na costa**: monitoramento das mudanças nas margens, controlar o transporte de sedimentos, mapear a costa e prevenir contra erosão;

- **Aplicações marítimas**: monitoramento da circulação do oceano, medir temperatura da água e altura das ondas. Os dados ajudam a melhorar a gestão dos recursos marítimos;
- **Mapeamento de riscos**: controle de furacões, erosões e inundações. Consegue-se avaliar os impactos de desastres naturais e criar estratégias para a prevenção.

A Tabela 10 apresenta as principais tecnologias de transportadores de sensores, suas características, aplicabilidade, os principais *atores* do mercado e suas principais áreas de atuação.

TABELA 10 PRINCIPAIS TECNOLOGIAS DE TRANSPORTADORES DE SENSORES

Principais Tecnologias	Características	Aplicabilidade	*Atores* Mercado	Principais Áreas de Atuação
-Aéreo (Drone) - Terrestre (ROV/S) - Aquático (ROV)	Sistemas ou veículos autônomos portadores de sensores ou utilizados para captação de dados de *sensor nodes* ("*gateway* móvel"). Pode fazer parte de uma rede de sensores (WSN).	Transporte de sensores ou captura de dados de *sensor nodes* em locais de difícil acesso ou remotos para detectar e monitorar grandezas.	ABB, Kuka, Clearpathrobotics, General dynamics, Skydrone (Brasil)	Produção, Ambiente, Agronegócio, Energia.

5.1.5.4 Tendências

As soluções existentes de MEMS, desenvolvidas ao longo das últimas duas décadas, compreendem um grande número de microssensores para quase todos os tipos de detecção exigidos para IoT, incluindo temperatura, pressão, forças inerciais, espécies químicas, campos magnéticos, radiação, etc. Atualmente, o desempenho deste tipo de sensor apresenta-se igual ou superior ao de um sensor convencional. Adicionalmente, sensores baseados em MEMS podem ser produzidos em larga escala utilizando as mesmas técnicas de fabricação utilizadas na indústria de circuitos integrados, o que se traduz em menor custo de produção por sensor.

O potencial da tecnologia MEMS para soluções de sensoriamento começa a se cumprir, no qual seus sensores miniaturizados, atuadores e estruturas encontram-se agrupados em um único substrato de silício, juntamente com circuitos integrados ou circuitos de microeletrônica e outras tecnologias. Esta visão representa um importante avanço tecnológicos, permitindo o desenvolvimento de produtos inteligentes e acrescentado as capacidades de percepção (microssensores) e controle (microatuadores) à capacidade computacional da microeletrônica.

Uma série de novas tecnologias de materiais está permitindo que fabricantes de dispositivos MEMS atendam às demandas de desempenho e tamanho do mercado em expansão. Dentre as novas tecnologias citadas por SEMI tem-se: *Deep Reactive Ion Etch (DRIE)*, *High Uniformity Aluminum Nitride (AlN)*, *Low Temperature Silicon Germanium (SiGe)* e *Thick Epitaxial Silicon (Thick-Epi).*

Em função da variabilidade de objetos inteligentes, tem-se cada vez mais a necessidade de aglutinação de funcionalidades, muitas vezes significativamente distintas, em um mesmo dispositivo. Assim como empregado na tecnologia MEMS, a tecnologia *System-in-Package* (SiP) se caracteriza por uma combinação de um ou mais circuitos integrados com funcionalidades diferentes, os quais podem incluir componentes passivos e/ou MEMS montados em um único empacotamento, que atua como um sistema ou subsistema. Desta forma, um dispositivo SiP pode conter componentes que são tradicionalmente encontrados em uma placa de PC.

As demandas da indústria de semicondutores continuam impulsionando as soluções SiP, buscando níveis mais altos de integração, redução de custos e facilidade na configuração completa de um sistema via solução única. No cenário de IoT, as soluções SiP estão sendo mais empregadas em *wearables* e produtos *machine-to-machine* (M2M).

No que diz respeito às *smart tags*, de acordo com Industrial Distribution, as tecnologias de sensoriamento baseadas nelas estão evoluindo para os chamados sistemas híbridos, onde tecnologias passivas e ativas compartilham ou se complementam com outros tipos de sensores para atender demandas de detecção e/ou monitoramento das soluções em IoT. Como exemplo de uma solução híbrida, voltada para os setores industrial e de saúde, pode-se utilizar a tecnologia RFID passiva em UHF para rastreabilidade de objetos ou itens de baixo valor em grande volume, agregada à tecnologia RFID ativa (sistema de localização em tempo real - RTLS - baseado em WiFi em 2,4GHz) para rastreabilidade em tempo real de itens de alto valor.

Cita-se também a possibilidade de integração de sensores como RFID passivo e SAW. Deste modo, tem-se a obtenção das funcionalidades de detecção do item a ser verificado ou monitorado e a possibilidade de sensoreamento dos fenômenos. Todavia, a tecnologia Bluetooth Low Energy (BLE) associada a sensores provavelmente ocupará espaço das tecnologias RFID ativo, para algumas aplicações.

As questões de segurança, que permeiam todas as camadas de IoT, também são pertinentes nas tecnologias que compõem os sensores. Para as tecnologias compreendidas nos sensores baseados em Smart *Tags*, devem ser observados os seguintes aspectos de segurança:

- ***Smart tags* baseadas em RFID passivo**: evolução do padrão ISO/IEC 18000-6C (ou EPC Gen2) para ISO/IEC18000-63 (ou EPC Gen2v2) com a implementação de protocolo mais seguro leitores e *tags*. A norma ISO/IEC 29167-1 define os mecanismos de segurança, definindo os requisitos para métodos de autenticação e os métodos para uso da

criptografia (algoritmos de segurança). Como exemplo, a ISO/IE29167-10 define os *crypto suites* para AES-128;

- ***Smart tags* baseadas em BLE**: permite implementação de serviço de pareamento com senha (6 dígitos) para proteger o acesso aos outros serviços implementados no dispositivo (como por exemplo, serviços de configuração, controle de sensores, etc). Há a possibilidade de implementação de mecanismos de segurança para o broadcast destes dispositivos, seguindo ou não os padrões *iBeacon* (Apple) ou *Eddystone* (Google). O padrão Eddystone já disponibiliza um componente de segurança Eddystone-EID (*Eddystone Ephemeral Identifier*) para o *broadcast.*

Em relação às redes de sensores[90], quando aplicadas em ambientes industriais[91], utiliza-se tecnologias sem fio para acessar áreas remotas ou distribuídas a fim de monitorar, controlar e enviar sinais ou medições de sensores para um sistema centralizado de gestão e controle.

Dada a maturidade já atingida pelos principais fabricantes de soluções de sensores de IoT, em nível mundial, presume-se que as oportunidades deste mercado devem estar concentradas na customização de soluções globais, que abordem especificidades locais, tais como, questões relativas à agricultura e pecuária de precisão, saúde pública (detecção e prevenção de epidemias), preservação do meio ambiente (gestão de florestas, prevenção de catástrofes) e de exploração de petróleo. Em outras palavras, atividades como o projeto e a montagem das soluções de sensoriamento podem ser executadas localmente, enquanto serviços de fabricação e encapsulamento dos sensores devem permanecer sendo predominantemente realizadas em outros países, por exemplo, na China.

5.1.6 Questões de segurança

A padronização de protocolos de segurança para atender à grande diversidade de dispositivos que compõem as aplicações IoT necessita ser aperfeiçoada. Historicamente, provedores de tecnologia de IoT têm tomado abordagens próprias em relação a segurança, no intuito de proteger dispositivos, endereçando a segurança fim-a-fim em aplicações IoT. O processo de digitalização e automação de milhões de dispositivos provavelmente demandará uma nova abordagem de segurança. No entanto, iniciativas precisam ser avaliadas e testadas em ambientes e provas de conceito de IoT, tal como a iniciativa da Comissão Europeia no financiamento do projeto piloto de IoT em grande escala (LSPs) para teste e desenvolvimento[92]. À medida que o ambiente de IoT se desenvolve, deve-se adaptar leis e regulamentos de privacidade e segurança para proteger os indivíduos sem prejudicar o enorme potencial de crescimento de IoT.

[90] *Wireless sensor network* (WSN), em inglês, também classificadas como tecnologias de transporte de informações dos *sensor nodes*.

[91] Neste caso, IWSN – *Industrial Wireless Sensor Network*, em inglês.

[92] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, K. Wehrle, "Security challenges in the IP-based internet of things," Wireless Personal Communications. 2011.

A segurança de dispositivos de IoT não deve ser vista de forma binária (seguro ou não seguro), mas sim como um espectro, que varia desde dispositivos que apresentam vulnerabilidades expressivas de segurança até dispositivos com várias camadas de mecanismos para prover segurança[93]. Em linhas gerais, fabricantes de dispositivos devem observar os seguintes requisitos:

- ***Desenvolvimento de hardware seguro.*** Dependendo da criticidade da aplicação onde o dispositivo será utilizado, desenvolver desde a concepção um *hardware* seguro, estabelecendo recursos próprios de segurança, tais como: recursos de armazenamento seguro e criptografado, funcionalidade de inicialização segura (*boot* seguro) com base em módulo TPM (*Trusted Platform Module*);
- ***Hardware o mais restritivo possível.*** O *design* de *hardware* deve incluir o mínimo de recursos e portas necessárias para o objetivo e operação do dispositivo. Um exemplo seria a disponibilização de interfaces tais como USB, serial, cartão de memória, etc. somente se estas fossem estritamente necessárias para a operação do dispositivo. Qualquer recurso adicional poderia expor o dispositivo a vetores de ataque indesejados;
- ***Hardware e software embarcado à prova de adulteração.*** Implementação de mecanismos que detectem violação física e lógica, tal como extração do *firmware* instalado, abertura do dispositivo e até retirada de algum componente. Dependendo da criticidade da aplicação onde o dispositivo será utilizado, normas internacionais tais como NIST[94] e ISO[95] categorizam as ações a serem tomadas no caso de violação, que vão desde nenhum tipo de ação, alarme para a central de gerência, até a destruição de informações sensíveis e do próprio dispositivo;
- ***Mecanismos de atualizações segura.*** Mecanismos para atualização segura dos dispositivos que garantam as versões de *firmware* por meio de criptografia, permitindo assim que o dispositivo fique seguro durante o seu tempo de vida. As melhores práticas de segurança afirmam que atualizações de *firmware* durante o tempo de vida do dispositivo são imprescindíveis.

O estado atual da segurança para dispositivos de IoT merece atenção, segundo a BITAG[96], pelos seguintes motivos:

- Muitos dispositivos de IoT são fabricados com *software* desatualizado, ou que ficará desatualizado ao longo de seu ciclo de vida;
- Suscetibilidade a *software* malicioso e outros abusos com potencial para interrupção e negação de serviço;

[93] K. Rose, S. Eldridge, e C. Lyman. "The internet of things: an overview". Internet Society. 2015.

[94] NIST FIPS, disponível em: http://csrc.nist.gov/groups/STM/cmvp/standards.html, acesso em fevereiro de 2017.

[95] ISO/IEC 19790:2012. Disponível em http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52906, acesso em fevereiro de 2017.

[96] BITAG: "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

- Potencial de persistência (longevidade) dos problemas de segurança e privacidade, devido ao fato que muitos dispositivos nunca serão consertados, atualizações de *software* podem trazer novas falhas de segurança, e alguns consumidores não atualizarão seus dispositivos;

Por outro lado, o IEEE CYBSI[97] fomenta as seguintes boas práticas e mecanismos para codificação segura em dispositivos IoT:

- Evitar/detectar/remover vulnerabilidades de codificação e implementação: linguagens com alocação segura de memória, linguagens restritas, padrões de codificação segura, detecção automática de violação de espaços de memória, inclusão na compilação de proteção contra *buffer overflow*, análise automática de segurança de código, e remoção de código não usado;
- Assegurar a autenticidade e a integridade de *software*/*firmware*: assinatura digital de código, validação de atualização de *firmware* e lista positiva de aplicativos;
- Impedir a análise e exploração de vulnerabilidades: reconhecimento de *inputs* antes do processamento, páginas/áreas de dados não executáveis, privilégios mínimos de sistema operacional, anti-adulteração (*anti-tampering*) de segredos e de chaves embutidos no código do *software* dos dispositivos;
- Facilitar a detecção de ataques: *log* dos eventos de segurança;
- Apoiar a restauração das funções após ataques e para manutenção de *software* durante a operação do dispositivo: validação da atualização atual em relação a validação da atualização anterior.

Em relação às boas práticas existentes para o desenvolvimento seguro de sistemas, as seguintes já poderiam ser aplicadas aos dispositivos IoT e serviços relacionados, de acordo com a ENISA[98]:

- **Fase projeto**: aplicar defesa em profundidade e segurança em camadas; separação entre funções de segurança e funcionalidades do dispositivo; deixar explícitas as premissas de segurança; realizar revisões de segurança por parceiros externos confiáveis; considerar a interação do usuário com as funções de segurança (usable security);
- **Fase de desenvolvimento**: usar ferramentas de gestão de configuração e de controle de qualidade, como analisadores estáticos de código; considerar o aspecto segurança na escolha da linguagem de programação; utilizar as funções de segurança disponíveis nos sistemas operacionais; usar componentes ou frameworks de segurança de boa reputação e/ou padronizados; treinar e conscientizar a equipe de desenvolvimento nas questões de segurança cibernética;

[97] IEEE Cybersecurity, disponível em: http://cybersecurity.ieee.org, acesso em fevereiro de 2017.

[98] ENISA: "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

- **Fase de testes**: realizar avaliações de privacidade; realizar auditorias de segurança e testes de intrusão; testar a conformidade das funções de segurança contra os requisitos de segurança funcional e padrões.

Além da criptografia para dispositivos discutida a seguir, devem ser consideradas as seguintes funções de segurança gerais[99], porém personalizadas para IoT[100]. O NIST[101] entende que os aspectos de segurança devem ser considerados para sensores, atuadores e agregadores, se estes dispositivos, ou seus dados, puderem ser adulterados, roubados, apagados, descartados, transmitidos de modo inseguro ou acessados por terceiros não autorizados. Por outro lado, a engenharia de segurança dos sensores, atuadores, ou agregadores pode ser necessária, dependendo do caso de uso e do projeto geral do sistema em que estes dispositivos estarão inseridos. Por exemplo, poderá haver diferenças na segurança de sensores de uso doméstico, militar e industrial, mesmo em se tratando de dispositivos de uso dual (civil e militar). Os requisitos de segurança para sensores (atuadores e agregadores) são os seguintes[102]:

- Possuir uma identidade inequívoca no contexto de uso;
- Ter um proprietário que tem controle sobre os dados coletados e quem pode acessá-lo (e quando);
- Possuir um nível de integridade de dados associado, o qual depende de fatores como calibração, precisão, interferência do ambiente, etc.;
- Ter suas comunicações encriptadas;
- Ser capazes de serem autenticados como genuínos.

Finalmente, os sensores, agregadores e atuadores devem ser protegidos de defeitos em geral, de injeção de dados incorretos e de *software*s maliciosos, assim como de ataques de negação de serviço contra a sua capacidade de operar e funcionar corretamente[103].

5.1.6.1 Criptografia para dispositivos restritos

Criptografia leve[104] é a subárea da criptografia voltada para dispositivos com recursos computacionais restritos e se divide, *grosso modo*, em duas áreas de atuação: (1) a implementação eficiente de padrões existentes e (2) o projeto e análise de novos algoritmos e protocolos. Neste sentido, a criptografia leve endereça uma variedade de componentes de *hardware* e *software*. De um lado, estão os dispositivos de alta capacidade como *smartphones* e similares que não precisariam de algoritmos específicos para criptografia

[99] ENISA: "Cyber Security and Resilience of smart cars". 2017.
[100] ENISA: "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.
[101] J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.
[102] J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.
[103] Idem.
[104] ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

leve. De outro lado, estão os dispositivos muito restritos, como os sistemas embarcados, os dispositivos RFIDs e as redes de sensores. São estes os dispositivos endereçados pela criptografia leve. O NIST[105] identificou três situações em que a criptografia leve se faz necessária:

- Certos micro controladores de 4 a 8 bits, voltados para aplicações de custo baixíssimo, possuem conjuntos reduzidos de instruções simples, levando muitos ciclos de CPU para executar criptografia, resultando em alto consumo de energia e baixo desempenho;
- Micro controladores com quantidades extremamente reduzidas de memórias RAM e ROM, que não seriam capazes de armazenar os binários dos algoritmos criptográficos e nem de manter o estado da execução;
- *Tags* RFID sem alimentação elétrica e nem bateria, que só recebem energia por indução elétrica externa (sem fio), necessitam de criptografia que utiliza engenharia simples (por exemplo, poucas portas lógicas), mas que ao mesmo tempo tem requisitos de tempo e potência limitantes.

A ENISA[106] define em maior detalhe classes de dispositivos de IoT que requerem criptografia leve. Em se tratando de dispositivos restritos, há o seguinte:

- Dispositivos extremamente restritos que não seriam capazes de implementar medidas de segurança reais, tais como sensores com memória RAM muito menor que 10KB e armazenamento muito menor que 100 KB;
- Dispositivos capazes de executar protocolos projetados para dispositivos restritos (por exemplo, CoAP), mas que não conseguem atender aos padrões de segurança criptográfica, tais como dispositivos com memória RAM em torno de 10 KB e armazenamento em torno de 100 KB, como, por exemplo, as lâmpadas e fechaduras inteligentes;
- Dispositivos com memória RAM em torno de 50 Kb e armazenamento em torno de 250 KB que seriam capazes de implementar os protocolos de segurança, mesmo com limitações de comunicação.

Em se tratando de dispositivos de alta capacidade, a ENISA[107] considera aqueles dispositivos com memória RAM e armazenamento significantemente superiores a 50KB e 250 KB, respectivamente; que podem possuir *hardware* dedicado para segurança ou que possuem grande capacidade de processamento. Nesta categoria, estão os *gateways* (*smart hubs*) e *smart* TVs capazes de atuar na proteção de outros dispositivos na HAN.

105 Idem.

106 ENISA, "Securing Smart Airports". 2016.

107 Idem.

5.1.6.1.1 Boas práticas para segurança criptográfica em IoT

O NIST[108] recomenda os seguintes requisitos de segurança criptográfica para os sensores: integridade e encriptação de dados e capacidade de serem autenticados como genuínos.

A ENISA, no contexto dos carros inteligentes[109], estabelece que:

- Criptografia proprietária deve ser evitada em favor de padrões estabelecidos;
- *Hardware* criptográfico auditado por terceiros confiáveis deve ser preferido;
- Cuidados devem ser tomados para gestão segura de chaves criptográficas;
- Autenticação mútua deve ser usada na comunicação remota.

No contexto de casas inteligentes, a ENISA[110] estabelece que o suporte a criptografia nos dispositivos deve contemplar o seguinte:

- Autenticação de usuário, de entidade/dispositivo, assim como autenticação e integridade de mensagens e autenticação mútua entre dispositivos;
- Proteção de dados com criptografia simétrica, funções de hash e assinaturas digitais;
- Infraestruturas criptográficas para geração de números aleatórios e gestão de chaves;
- *Hardware* criptográfico dedicado nos dispositivos de alta capacidade;
- Em dispositivos não tão restritos, relativamente limitados em memória e CPU, criptografia de curvas elípticas deve ser preferida em vez do RSA;
- Geradores de números verdadeiramente aleatórios devem ser preferidos para geração de chaves, mas não seriam mandatórios na geração de salts e IVs;
- Dispositivos domésticos devem ter mecanismos para revogação de chaves e interfaces que permitam ao usuário resolver desafios relacionados.

O IEEE, no contexto da segurança cibernética de dispositivos médicos[111], recomenda que cuidados adicionais devem ser tomados pelos desenvolvedores de solução quando ao uso correto de algoritmos acreditados em implementações padronizadas, assim como de números aleatórios criptograficamente seguros. O IEEE entende que grande parte dos desafios de segurança relacionada à criptografia é derivada do mau uso da tecnologia e não de defeitos de implementação dos algoritmos.

A BITAG[112] estabelece uma série de recomendações administrativas relacionadas à segurança criptográfica dos dispositivos IoT:

- Comunicação entre dispositivos deve ser protegida por TLS ou criptografia leve;
- Se ICP é usada, então deve existir um mecanismo de revogação de certificados realizado por uma entidade confiável;

108 J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

109 ENISA, "Cyber security for Smart Cities - An architecture model for public transport". 2015.

110 ENISA, "Securing Smart Airports". 2016.

111 T. Haigh, C. Landwehr. "Building Code for Medical Device *Software* Security". 2015.

112 BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

- Comunicação de controle (comandos remotos de configuração, por exemplo) deve ser encriptadas;
- Dados sensíveis armazenados localmente devem ser encriptados;
- Comunicações para atualização de *software* e requisição de dados também devem ser autenticadas;
- Uso de credenciais únicas por dispositivo e com a capacidade de atualização;
- Uso de bibliotecas criptográficas confiáveis e ativamente mantidas.

5.1.6.1.2 Padrões internacionais para criptografia leve

A norma ISO/IEC 29192, por seu turno, estabelece os seguintes padrões para criptografia leve:

- Duas cifras de bloco[113] PRESENT (com bloco de 64 bits e chaves de 80 ou 128 bits) e CLEFIA (com blocos de 128 bits e chaves de 128, 192 ou 256 bits);
- Duas cifras de fluxo[114]: Enocoro (de 80 ou 128 bits) e Trivium (de 80 bits);
- Três mecanismos criptográficos assimétricos[115]: (1) autenticação unilateral baseada em curvas elípticas, (2) troca de chaves leve e autenticada para autenticação unilateral e estabelecimento de chaves de sessão e (3) um mecanismo de assinatura baseado em identidades;
- Três funções de hash[116], sendo duas otimizadas para *hardware*: PHOTON (com tamanhos de 80, 128, 160, 224 e 256 bits) e SPONGENT (de 88, 128, 160, 224 e 256 bits); e uma otimizada para implementação em *software*, Lesamnta-LW (com 256 bits).

A norma ISO/IEC 29167 publica sete suítes criptográficas consideradas leves para proteção da comunicação via RFID: AES-128[117], PRESENT-80[118], ECC-DH[119], Grain-128[120], AES

113 ISO/IEC 29192-1:2012. "Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General".

114 ISO/IEC 29192-2:2012. "Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers".

115 ISO/IEC 29192-3:2012. "Information technology -- Security techniques -- Lightweight cryptography -- Part 3: Stream ciphers".

116 ISO/IEC 29192-4:2013. "Information technology -- Security techniques -- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques".

117 ISO/IEC 29167-1:2014. "Information technology Automatic identification and data capture techniques Part 1: Security services for RFID air interfaces".

118 ISO/IEC 29167-10:2015. "Information technology Automatic identification and data capture techniques Part 10: Crypto suite AES-128 security services for air interface communications".

119 ISO/IEC 29167-11:2014. "Information technology Automatic identification and data capture techniques Part 11: Crypto suite PRESENT-80 security services for air interface communications".

120 ISO/IEC 29167-12:2015. "Information technology Automatic identification and data capture techniques Part 12: Crypto suite ECC-DH security services for air interface communications".

OFB[121], XOR (em desenvolvimento)[122], ECDSA-ECDH[123], cryptoGPS[124], Rabin-Montgomery (RAMON)[125].

Finalmente, vale mencionar duas iniciativas em criptografia leve: o padrão japonês, definido pelo *Cryptography Research and Evaluation Committees* (CRYPTREC[126]), com os algoritmos AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE e PRINCE; e a competição eSTREAM[127], promovida pela *European Network of Excellence for Cryptology*, com as cifras de fluxo: Grain, Trivium e Mickey.

5.1.6.2 Requisitos de *Hardware*

A grande variedade de cenários de utilização impede a definição de um conjunto de requisitos mínimos de *hardware* para dispositivos de IoT. Por exemplo, a engenharia de segurança dos sensores, atuadores, ou agregadores pode ser necessária, em vários níveis de rigor, dependendo do caso de uso e do projeto geral do sistema em que estes dispositivos estarão inseridos. Em termos de memória RAM e armazenamento, os requisitos seriam os seguintes[128]:

- Dispositivos com memória RAM em torno de 10 KB e armazenamento em torno de 100 KB, que devem ser capazes de executar protocolos de segurança projetados para dispositivos restritos, mas que não conseguem atender aos padrões de segurança criptográfica: dispositivos;
- Dispositivos com memória RAM em torno de 50 Kb e armazenamento em torno de 250 KB, que seriam capazes de implementar os protocolos de segurança, mesmo com limitações;
- Dispositivos com memória RAM muito maior que 50 KB e armazenamento muito maior que 250 KB, que devem ser capazes de possuir *hardware* dedicado para segurança ou que possuem grande capacidade de processamento.

121 ISO/IEC 29167-13:2015. "Information technology Automatic identification and data capture techniques Part 13: Crypto suite Grain-128A security services for air interface communications".

122 ISO/IEC 29167-14:2015. "Information technology Automatic identification and data capture techniques Part 14: Crypto suite AES OFB security services for air interface communications".

123 ISO/IEC PDTS 29167-15. "Information technology Automatic identification and data capture techniques Part 15: Crypto suite XOR security services for air interface communications".

124 ISO/IEC 29167-16:2015. "Information technology Automatic identification and data capture techniques Part 16: Crypto suite ECDSA-ECDH security services for air interface communications".

125 ISO/IEC 29167-19:2016. "Information technology Automatic identification and data capture techniques Part 19: Crypto suite RAMON security services for air interface communications".

126 Cryptography Research and Evaluation Committees (CRYPTREC), disponível em: http://www.cryptrec.go.jp/english, acesso em janeiro de 2017.

127 eSTREAM competition. European Network of Excellence for Cryptology, disponível em: http://www.ecrypt.eu.org/stream, acesso em janeiro de 2017.

128 Idem.

Em termos de processamento, o NIST[129] identificou três grupos restritos:

- Micro controladores de 4 até 8 bits, que possuem conjuntos reduzidos de instruções simples, levando muitos ciclos de CPU, que necessitam de criptografia leve;
- Micro controladores com quantidades extremamente reduzidas de memórias RAM e ROM, que necessitam de criptografia leve;
- *Tags* RFID sem alimentação elétrica e nem bateria, necessitam de criptografia com engenharia simples.

Em termos de criptografia, a ENISA[130] recomenda que, em dispositivos não tão restritos, relativamente limitados em memória e CPU, a criptografia de curvas elípticas deve ser preferida em vez do RSA.

5.1.6.3 Segurança de Firmware e Proteção de *Software*

Em termos da segurança dos *softwares* nos dispositivos (gerais, embarcados ou *firmware*), observou-se uma grande preocupação com a capacidade de atualização segura, muitas vezes ausente dos dispositivos de IoT[131]. Em linhas gerais, o fabricante do dispositivo deveria ser capaz de atender os requisitos listados a seguir[132]:

- Desenvolvimento de *hardware* seguro com recursos próprios de segurança tais como: recursos de armazenamento seguro e criptografado, funcionalidade de inicialização segura (boot seguro) com base em módulo TPM (*Trusted Platform Module*);
- Mecanismos de atualizações segura para todos os dispositivos que garantam de maneira criptográfica (com assinaturas digitais) das versões de firmware.

O IEEE CYBSI[133] recomenda práticas e mecanismos para assegurar a autenticidade e a integridade de *software/firmware*: assinatura digital de código, validação de atualização de *firmware* e lista positiva de aplicativos. O IEEE CYBSI[134] vê como uma linha de pesquisa a as técnicas de detecção em tempo de execução de corrupções de programas e uso de bases TCBs, em dispositivos restritos.

Em dispositivos de grande capacidade, como por exemplo dispositivos móveis, observa-se o ambiente de execução confiável (*Trusted Execution Environment* - TEE) e o elemento

[129] ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.
[130] ENISA, "Securing Smart Airports". 2016.
[131] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.
[132] K. Rose, S. Eldridge, e C. Lyman. "The internet of things: an overview". Internet Society. 2015.
[133] IEEE Cybersecurity, disponível em: http://cybersecurity.ieee.org, acesso em fevereiro de 2017.
[134] IEEE Cybersecurity, disponível em: http://cybersecurity.ieee.org, acesso em fevereiro de 2017.

Seguro (*Secure Element* - SE)[135,136] utilizados como mecanismos de proteção de *software* em geral.

Finalmente, a substituição de dispositivos antigos por outros mais novos aparece em muitos casos como a única alternativa para a atualização de *software*, em particular para dispositivos de menor valor[137].

5.1.6.4 Mecanismos Antiviolação (*Anti-tampering*)

Com respeito a mecanismos antiviolação, em linhas gerais, o fabricante do dispositivo deveria ser capaz de atender os seguintes requisitos para detecção e, em situações mais rigorosas, até a resistência a violações[138]:

- Desenvolvimento de *hardware* seguro com recursos próprios de segurança, tais como: recursos de armazenamento seguro e criptografado, funcionalidade de inicialização segura (boot seguro) com base em módulo TPM (*Trusted Platform Module*);
- *Hardware* e *software* embarcado à prova de adulteração, com mecanismos que detectem violação física e lógica tal como extração do firmware instalado, abertura do dispositivo e retirada de componentes.

As normas internacionais[139,140] categorizam as ações tomadas ao se detectar alguma violação: nenhum tipo de ação, alarme para a central de gerência, inclusive a destruição de informações sensíveis e do próprio dispositivo.

5.1.6.5 Desafios para melhorar a segurança de dispositivos de IoT

A BITAG[141] identificou os seguintes desafios para o aumento da segurança em dispositivos IoT:

- Falta de incentivos para desenvolver e implantar atualizações depois da venda;
- Dificuldades para atualizações de *software* over-the-network;
- Restrições de recursos (CPU, RAM, etc.) e de interface dos dispositivos;
- Inclusão de *software* malicioso já durante a fabricação dos dispositivos;

135 GlobalPlatform, "The standard for managing applications on secure chip technology". http://globalplatform.org.

136 Open-TEE, Open source project for a "virtual TEE based on *software*". Disponível em https://open-tee.github.io, acesso em janeiro de 2017.

137 BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

138 K. Rose, S. Eldridge, e C. Lyman. "The internet of things: an overview". Internet Society. 2015.

139 NIST FIPS, disponível em: http://csrc.nist.gov/groups/STM/cmvp/standards.html, acesso em fevereiro de 2017.

140 ISO/IEC 19790:2012, disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52906, acesso em fevereiro de 2017.

141 BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

- Falta de experiência dos fabricantes em segurança e privacidade;
- Riscos associados a dispositivos vulneráveis e já em operação.

A ENISA[142] observa que a segurança para dispositivos domésticos de IoT tem sido subestimada e aponta para falta de incentivos para melhorar a segurança. A BITAG[143] percebe ainda que a proteção criptográfica é geralmente encontrada apenas em dispositivos de alta capacidade, como, por exemplo, *gateways*, sendo muitas vezes implementada de modo vulnerável.

De acordo com o NIST[144], as funções de *hash* já padronizadas pelo governo americano e atualmente em uso (SHA-1, SHA-2, SHA-3) não são adequadas para uso em dispositivos restritos (micro controladores de 8 bits ou menos, por exemplo), devido à complexidade destes algoritmos. Ainda, funções de *hash* são implementadas com no mínimo 64 bytes de RAM. Existem variações leves do SHA3, mas estas não estão padronizadas. Além disso, as funções de encriptação autenticada e códigos de autenticação (MAC) só poderão ser construídos caso existam funções de *hash* e de encriptação aprovadas.

Ainda de acordo com o NIST[145] a maturidade neste campo só será atingida com o entendimento das seguintes questões de projeto:

- Segurança criptográfica de pelo menos 112 bits;
- Proteção contra-ataques por canais laterais em dispositivos restritos;
- Limites superiores claros para a quantidade de textos cifrados com a mesma chave;
- Resistência aos ataques por chaves relacionadas;
- Pouca ou nenhuma expansão de texto cifrado;
- Flexibilidade e variedade de implementações.

Além disso, esquemas criptográficos assimétricos (de chave pública) somente serão padronizados pelo NIST se forem robustos contra-ataques quânticos ou usarem uma combinação de criptografia leve e criptografia assimétrica de propósito geral já existente (padronizada).

Outro desafio para a adoção de criptografia de chave pública para dispositivos de IoT restritos é a necessidade atual de uma ICP para autenticação de chaves públicas. A autenticação de chaves públicas por ICP é custosa para dispositivos restritos porque é feita por meio de certificados digitais, com as seguintes desvantagens para IoT: a troca de certificados gera sobrecarga de comunicação, a verificação de certificados gera sobrecarga de computação e o armazenamento de (cadeias de) certificados gera sobrecarga de armazenamento.

142 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

143 BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

144 ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

145 Idem.

Finalmente, a ENISA, em relação às casas inteligentes[146], declara que a falta de mecanismos fortes para estabelecimento de relacionamentos de confiança[147] entre dispositivos de IoT é uma barreira a ser superada. Em particular, a ENISA declara que uma ICP tem os seguintes desafios a escalabilidade para IoT: complexidade de administração e manutenção para grandes volumes de dispositivos heterogêneos, limitações de interface facilitam vulnerabilidades inerentes a ICP (*man-in-the-middle*, por exemplo), dificuldade de implementação por não especialistas em criptografia aplicada, e incapacidade de implementação em todo o ecossistema de dispositivos restritos (devido às questões de desempenho citadas anteriormente).

5.1.6.6 Tendências

Em resposta aos sinais de aumento dos ataques cibernéticos envolvendo dispositivos de IoT, a BITAG[148] recomenda as seguintes ações para fortalecer a segurança dos dispositivos de IoT:

- Melhorias nos controles de versão e de mudança para garantir a utilização de *software*s atualizados;
- Desenvolvimento de mecanismos automáticos e seguros para atualização de *software*;
- Utilização de mecanismos de autenticação fortes;
- Melhorias em testes e robustecimentos de configurações;
- Maior conformidade às boas práticas de segurança, privacidade e criptografia;
- Melhoria na confiabilidade geral, em que um dispositivo deve continuar funcionando corretamente, mesmo em caso de falhas de comunicação e de seu servidor;
- Melhorias em mecanismos de endereçamento e resolução de nomes, com adoção de IPV6 e DNSSEC.

A BITAG[149] ainda identifica a existência de um dispositivo de rede doméstica HAN capaz de controlar e gerenciar o tráfego entre dispositivos e entre dispositivos e a Internet. Tal dispositivo é denominado genericamente de *Gateway* IoT, e tem recebido denominações específicas, tais como *smarthub*, agregador, concentrador, etc. Entre as capacidades deste dispositivo, ressaltam-se:

- Descoberta e inventário automáticos de dispositivos conectados à rede doméstica;
- Mecanismos para informar o usuário sobre que dados os dispositivos enviam para a Internet e quais dispositivos se comunicam entre si na rede doméstica HAN;

146 ENISA, "Securing Smart Airports". 2016.

147 Hierarquia fundamental para a construção de uma Infraestrutura de Chave Pública, necessária para que um dado dispositivo certifique que os outros dispositivos que façam parte da sua rede são legítimos.

148 BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

149 Idem.

- Mecanismos simples para o usuário desabilitar ou prevenir a comunicação de dispositivos entre si, na HAN, ou com servidores externos, sem comprometer seu funcionamento.

Finalmente, a ENISA[150] recomenda a observação das seguintes tendências para indústria europeia de dispositivos de IoT:

- Procura por consenso em relação aos requisitos de mínimos de segurança;
- Surgimento de modelos de negócio orientados a segurança;
- Desenvolvimento de métodos e *frameworks* de avaliação de segurança;
- Maior esclarecimento sobre os aspectos legais da segurança e da privacidade na HAN;
- Maior integração da segurança cibernética em projetos de pesquisa e desenvolvimento para IoT.

O IEEE CYBSI[151] estabeleceu uma agenda de pesquisa relacionada à programação segura de dispositivos de IoT em geral e dispositivos médicos em particular, que contempla os seguintes tópicos: utilização de *assurance cases* como argumento de segurança, proteção de dados e estados críticos, identificação de módulos em risco, detecção em tempo de execução de corrupções de programas, uso de bases TCBs, inclusão de proteções de código em tempo de compilação, por exemplo, contra *buffer overflow*.

A ENISA[152] identifica uma tendência de utilização de criptografia baseada em identidades (*Identity-Based Cryptography* - IBC) e, em especial, a encriptação baseada em identidades (*Identity-Based Encryption* – IBE) para suprir as deficiências da criptografia de chave pública tradicional e das ICPs. Porém, ainda sem resultados conclusivos.

O NIST[153] decidiu promover a criação de um portfólio de mecanismos criptográficos leves, em que os algoritmos criptográficos leves seriam recomendados para utilização apenas em contextos (perfis) específicos definidos por restrições de desempenho, segurança e empacotamento físico (RAM, armazenamento, etc.). No curto prazo, o foco inicial do trabalho do NIST estará na definição de cifras de bloco, funções de *hash* e códigos de autenticação (MAC). Em longo prazo, estes algoritmos deveriam oferecer segurança pós-quântica ou de fácil substituição por algoritmos criptográficos pós-quânticos. Ainda, o NIST alega que os protocolos criptográficos para dispositivos restritos não estão comtemplados no esforço de padronização.

150 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

151 IEEE Cybersecurity, disponível em: http://cybersecurity.ieee.org, acesso em fevereiro de 2017.

152 ENISA, "Securing Smart Airports". 2016.

153 ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

5.1.7 Conclusões

Na camada de dispositivos estão concentradas as maiores restrições não-funcionais inerentes à IoT, em especial: custo, consumo energético e espaço físico. Isso gera alguns desafios, dentre eles:

- Aumento significativo do custo total de objetos de baixo valor: Em objetos de baixo valor, a adição de sensoriamento, inteligência e comunicação aumenta significativamente o custo total dos objetos, impactando casos de uso como rastreio de latas de refrigerante e identificação de violação de embalagens de alimentos congelados;
- Restrições quanto ao consumo de energia: Em grande parte dos casos de uso de IoT, não é possível conectar os objetos à rede. Portanto, objetos inteligentes precisam ser alimentados por bateria ou indução eletromagnética-um processo limitado em termos de fornecimento de energia. Desta forma, o consumo de energia deve ser suficientemente baixo. Esse desafio afeta casos de uso com objetos de menor tamanho, como uma pílula que mede a temperatura interna do paciente e transmite os dados para um aplicativo do smartphone.

Contudo, a evolução dos processos da integração de microeletrônica, ainda aderentes à lei de Moore, tem propiciado a superação desses desafios para um número cada vez maior de aplicações. As principais tendências da camada de dispositivos estão elencadas a seguir.

O crescimento nas vendas das arquiteturas de micro controladores de 32 bits, que já superam em valor de mercado as arquiteturas de 8 bits, é um efeito da IoT no mercado de semicondutores. Tais arquiteturas de 32bits são mais propícias para o desenvolvimento de objetos inteligentes, uma vez que estes não requerem apenas capacidade de processamento, mas também de comunicação, o que, por sua vez, demanda uma grande quantidade de protocolos e sistemas operacionais embarcados.

Apesar dessa evolução, é provável que arquiteturas mais robustas, como a de microprocessadores, não se tornem dominantes em sensor nodes para a maioria dos casos de uso de IoT nos próximos anos. Assim, superado o patamar de micro controladores de 32 bits operando a algumas dezenas de mega-hertz, e com capacidade de algumas dezenas de kilobytes de memória volátil e centenas de kilobytes de memória não-volátil, é provável que, comparada ao aumento de capacidade, a redução de custos seja o fator determinante para massificar a implantação, pois permite atender a um número maior de casos de uso.

Dada a grande amplitude de aplicações de IoT, alguns objetos devem demandar capacidade computacional bastante elevada. Para exemplificar, os veículos autônomos terão capacidade computacional local similar à de servidores em data centers.

A massificação de aplicações baseadas em micro controladores tem um impacto na mão de obra. Arquiteturas microcontroladas, mesmo de 32 bits, em geral não permitem de

forma satisfatória o uso de linguagens de programação de alto nível, como Java e Python. Nesses ambientes prevalece, o uso de linguagem C/C++. Assim, restringe-se significativamente o número de profissionais para o desenvolvimento de *software* embarcado capacitados em linguagens com C/C+, hoje estimado em cerca de 500 mil em todo o mundo.

Essa restrição de mão de obra também se configura como uma oportunidade para países que desejam atender a demandas de desenvolvimento de projetos de objetos inteligentes. Para tal, o investimento de recursos para formação de engenheiros de *software* embarcado pode resultar na criação de um diferencial estratégico. No entanto, a formação desse tipo de profissional pressupõe a capacitação necessária em projetos de código livre de referência, como sistemas operacionais de tempo real, que já implementam diversas funcionalidades necessárias à IoT. Desta forma, a proficiência em linguagens de programação de menor nível e a customização de soluções já desenvolvidas para demandas específicas, serão qualidades esperadas do profissional que desenvolve software embarcado para IoT.

Diante do amplo espectro de casos de uso de IoT, abre-se a oportunidade para novos atores no segmento de microeletrônica de propósito específico. Embora as previsões de crescimento de dispositivos conectados à rede indiquem valores da ordem de dezenas de bilhões implantados nos próximos anos, os inúmeros casos de uso, com necessidades distintas, devem impedir uma predominância de um ou poucos tipos de objetos inteligentes. Isso se configura como um desafio para o desenvolvimento de componentes integrados para atender a um grande número de casos de uso diversos, uma vez que a previsão relativamente baixa de volume não justifica o alto investimento exigido por esses projetos.

De forma geral, os casos de IoT podem ser agrupados em três blocos, de acordo com o volume de vendas e o número de casos de uso atendidos, como mostram o QUADRO X e a descrição a seguir:

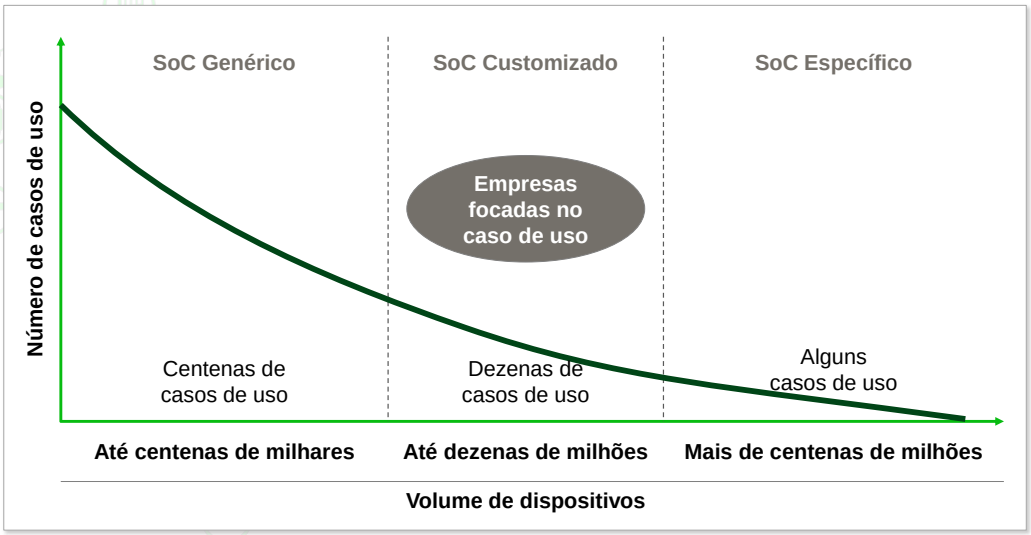
- **SoC específico**: Pequeno número de casos de uso, que demandam um volume de vendas de centenas de milhões de SoCs; nesses casos, é justificado o desenvolvimento de semicondutores específicos. Estão bem posicionadas nesse mercado grandes empresas de semicondutores;
- **SoC customizado**: Maior número de casos de usos (dezenas), com volumes de até dezenas de milhões de dispositivos por ano, o que abre espaço para inovações em microeletrônica, como SoCs customizados, que, no contexto de um ecossistema de IP (*Intellectual Property*), cores e técnicas de desenvolvimento ágil, permitem a criação em poucos meses de semicondutores mais competitivos que as soluções especializadas em nível de eletrônica discreta, e com desenvolvimentos que se pagam com volumes a partir da ordem de poucos milhões de unidades. Da mesma forma, técnicas como MPW (*Multi Project Wafer*) tornam possível a viabilização das primeiras amostras com

investimentos moderados. Neste caso, merecem destaque os atores cujo foco recaia na criação de soluções para o atendimento de casos de uso específicos;

- **SoC genérico**: Grande número de casos de uso (centenas), que devem gerar demandas na ordem de até centenas de milhares de unidades por ano. Neste caso, são utilizados SoCs genéricos, capazes de tratar de forma não ótima diversos casos de uso por meio da especialização em nível de eletrônica discreta e *software* embarcado.

QUADRO 20

Casos de uso versus volume de dispositivos



FONTE: Análise do consórcio

*Gateway*s devem ser utilizados para uma grande quantidade de casos de uso, prestando serviços (por exemplo, acesso à rede e segurança) aos dispositivos. Os *gateway*s de IoT devem ter por base o uso de processadores similares aos aplicados em microcomputadores, configurando um mercado mais concentrado e com poucas oportunidades locais em semicondutores. Contudo, também em razão da grande diversidade de casos de uso, poderá haver espaço para o desenvolvimento de soluções no âmbito da eletrônica, empacotamento mecânico e *software* que implemente funções complementares às capacidades, em geral limitadas, dos *sensor nodes*.

5.2 Redes

5.2.1 *Introdução*

A IoT abrange inúmeros casos de uso com requisitos específicos de rede. Por exemplo, para aplicações em tempo real, a latência de comunicação, assim como o tempo de resposta, está diretamente relacionada à rede. A camada de conectividade apresenta uma série de desafios, que demandam uma evolução das tecnologias de rede. Por exemplo, redes com largura de banda insuficiente podem dificultar o escoamento do tráfego gerado por aplicações que geram alto volume de dados. Locais distantes dos centros urbanos e com baixa densidade populacional geralmente possuem conectividade bastante restrita, o que representa um desafio para o aproveitamento do grande potencial de negócios desses ambientes.

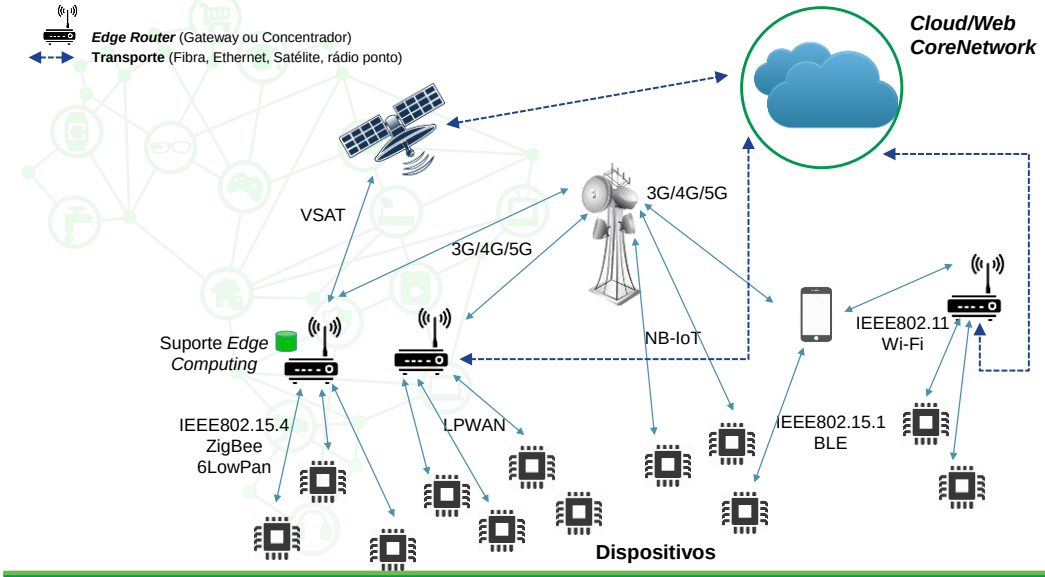
A camada de rede é composta por um conjunto de tecnologias que possibilitam o transporte das informações geradas pelos dispositivos responsáveis pela capilaridade do sistema, e estão organizadas em dois importantes grupos:

- Tecnologias de rede de dados;
- Tecnologias de acesso.

No QUADRO 21 é apresentada uma descrição da arquitetura sistêmica da camada de rede, com os elementos da rede de dados e de acesso.

QUADRO 21

Arquitetura sistêmica da camada de conectividade e rede



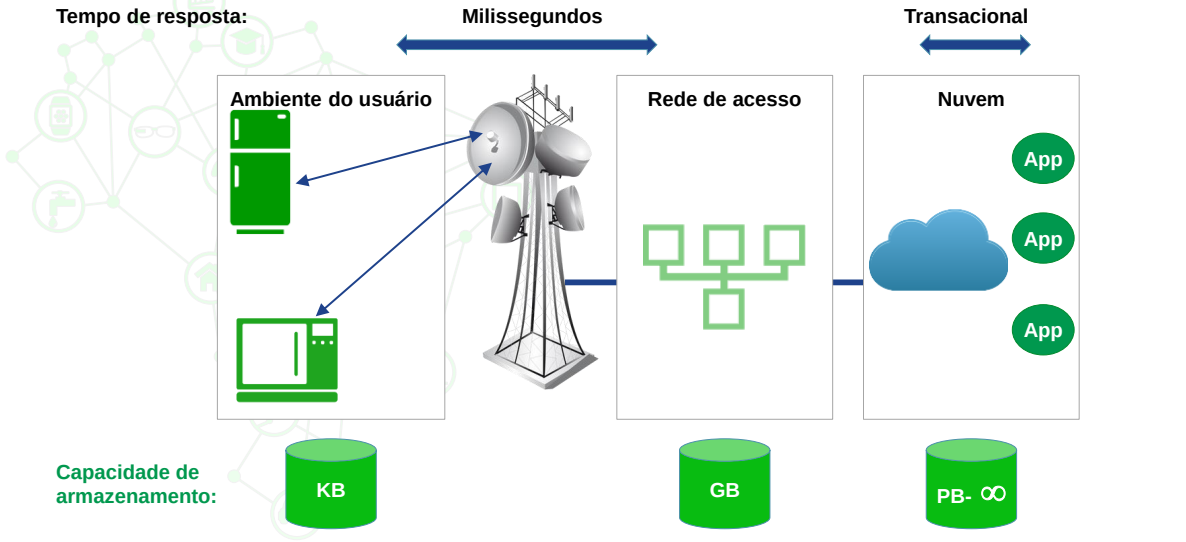
FONTE: Análise do consórcio

Os elementos da rede de dados, representados por linhas pontilhadas, contribuem com a integração dos elementos da rede de acesso à Internet. Nesta mesma figura, é possível distinguir as diferentes possibilidades pelas quais as redes de acesso providenciam capilaridade aos diversos tipos de dispositivos segundo o tipo de aplicação, passando por tecnologias de acesso de curta distância até sistemas de transmissão via satélite.

O QUADRO 22 apresenta, de forma geral, as principais necessidades de capacidade e requisitos de rede. No entanto, é importante lembrar que existem variações nos requisitos, como a largura de banda e tempo de resposta, em cada camada. Essa arquitetura minimiza os impactos na rede relativos à transferência do alto volume de dados gerado pelos dispositivos de IoT e possibilita aplicações em tempo real com requisitos rigorosos de latência.

QUADRO 22

Arquitetura de rede com divisão em camadas



FONTE: Análise do consórcio

As subseções a seguir apresentam as tecnologias para IoT nessas camadas.

5.2.2 Tecnologias de rede de dados

5.2.2.1 Núcleo

No ecossistema de IoT, os dados gerados pelos dispositivos, sejam eles brutos ou tratados em camadas intermediárias, são enviados à *Cloud* transitando pelo núcleo das redes que constituem a Internet. Apesar do núcleo da rede estar dimensionado com alta capacidade para agregar o tráfego das redes adjacentes, o tráfego gerado pela IoT pode trazer impactos e consequentemente exigir adequações no núcleo da rede.

Com a previsão de dezenas de bilhões de dispositivos conectados à Internet na próxima década, estima-se que haverá um aumento significativo do volume do tráfego de rede e principalmente uma mudança no padrão de tráfego. Diferentemente da comunicação entre humanos, a comunicação entre as máquinas tem um caráter periódico e regular, independente do período do dia, do mês ou do ano. Se os dados de dezenas de bilhões de dispositivos forem todos para nuvem simultaneamente, podem ocorrer gargalos de rede. No entanto, existem apostas no modelo arquitetural de *Edge Computing*, no qual o processamento e armazenamento dos dados ocorre em camadas da hierarquia de rede mais próximas ao dispositivo final, o que minimizaria o impacto no core das redes.

Ao reduzir o volume de dados trocados entre os dispositivos e a *Cloud*, o tráfego no núcleo da rede é minimizado. Todavia, o aumento significativo na quantidade de dispositivos conectados à rede deve demandar maior capacidade do núcleo, que poderá evoluir de forma gradual em termos de largura de banda e exigir investimentos em técnicas de engenharia de tráfego para evitar gargalos.

As tecnologias de comunicações ópticas têm evoluído rapidamente, atingindo taxas de Tbps, o que provavelmente atenderá à demanda por aumento de capacidade no núcleo da rede, principalmente considerando tecnologias de roteamento de canais ópticos (ROADM e WSS). Com o surgimento das Redes Definidas por Software, o roteamento multicamada ganhou fôlego e tem apresentado grande evolução. Realizar o roteamento do tráfego levando-se em consideração informações das camadas WDM, OTN e IP/MPLS oferece maior eficiência na utilização da rede e proporciona mecanismos avançados de redundância e proteção contra falhas. Os fabricantes do setor têm investindo nessa técnica e já têm produtos disponíveis em seus portfólios.

5.2.2.2 *Backhaul*

A rede de transmissão é responsável pelo *backhaul* entre a tecnologia de acesso e o núcleo da rede que sua vez está conectada com a Internet. Na IoT, apesar de a grande parte dos dispositivos requererem baixa taxa de banda (poucos kbps), a entrada em operação de um grande número destes elementos apresentará um aumento significativo da vazão de banda no *backhaul* para as redes de acesso e no backbone. Neste último, poderá ocorrer um grande impacto com as transferências de um grande volume de dados entre os *data centers* que armazenam os dados. Portanto, a capacidade instalada em conexões fixas é fundamental para o desenvolvimento da camada de conectividade. A expansão da capilaridade e capacidade da última milha para *backhaul*, juntamente com a camada de transporte/core são fundamentais para suportar a demanda de IoT.

As redes de acesso e backbone IP/MPLS e de transporte óptico tem evoluído para velocidades cada vez maiores (100G, 400G e 1T), permitindo acomodar este crescimento de tráfego. Entretanto, a capilaridade do *backhaul* pode ser um desafio, dependendo da infraestrutura da região a ser implantada.

A introdução de tecnologias de redes definidas por software (SDN) e a virtualização de funções de rede (NFV) permitirá a automação das redes de acesso e transporte, incluindo a configuração multicamada (*multilayer*) IP/MPLS e Óptico, além do chamado "fatiamento da rede" (*network slicing*), permitindo criar domínios de rede de acordo com os requisitos de qualidade de serviço.

Os impactos da IoT na rede de dados incluem:

- O alto volume de dados gerado pela quantidade expressiva de dispositivos de IoT trará um impacto substancial nos sistemas de redes;
- O movimento de dados de forma eficiente para uma rede distribuída e para a nuvem se tornará uma tarefa crítica;
- *Data center*s distribuídos devem ser necessários para diversas aplicações críticas realizadas em tempo real.

Portanto, os sistemas atuais de gestão devem evoluir para realizar funções de:

- Flexibilidade, escalabilidade e custo de aprovisionamento de serviços de rede;
- Visibilidade e controle de rede centralizados para provedores de serviços de rede;
- Plataforma de rede evolutiva.

Desta forma, de maneira análoga às redes tradicionais, deve-se considerar funções de gerenciamento de redes tipo FCAPS, além de gestão da topologia da rede e do tráfego, incluindo capacidade de detectar aumentos atípicos e reservar recursos para aplicações críticas, bem como aspectos relacionados à segurança como autorização, autenticação, confidencialidade e integridade dos dados e da sinalização na rede.

5.2.2.3 SDN/NFV

As tecnologias SDN e NFV trazem o conceito de redes virtualizadas, em que os recursos da infraestrutura de rede são compartilhados por diversas aplicações, garantindo que as ações e o comportamento do tráfego de uma rede virtual não afetem outras redes virtuais. Redes definidas por software (Software *defined network* – SDN – em inglês)[154,155] vêm ganhando espaço no universo de redes de dados com a proposta de separação dos planos de controle e encaminhamento, permitindo a evolução independente entre os planos. O objetivo é tornar o plano de controle mais flexível e de rápida evolução sem impacto em performance, tornando as redes mais dinâmicas e inteligentes.

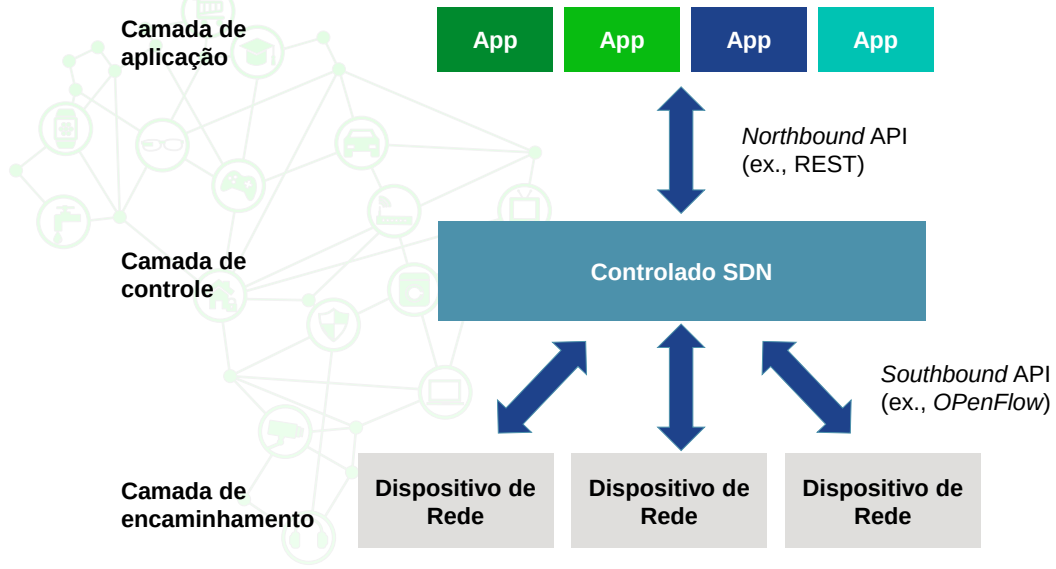
Em sua essência, a arquitetura SDN move o plano de controle, antes embarcado no equipamento, para um equipamento externo, como um servidor x86, e define uma API padronizada e aberta para comunicação entre os equipamentos de rede (plano de encaminhamento) e o controlador de rede (plano de controle), como mostrado no QUADRO 23.

154 Open Networking Foundation, disponível em: https://www.opennetworking.org/sdn-resources/sdn-definition, acesso em fevereiro de 2017.

155 D. Kreutz et al., "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

QUADRO 23

Arquitetura SDN



FONTE: Análise do consórcio

Além disso, a SDN apresenta um grande potencial de inovação para as redes de dados que pode trazer benefícios para o cenário de IoT[156,157], devido às seguintes características:

- Controle logicamente centralizado, com conhecimento da rede, permitindo automatizar o controle baseado em políticas para redes complexas e de alta densidade. Dado o alto potencial de escalabilidade de ambientes IoT, SDN tem um papel crítico para facilitar o gerenciamento e operação dessas redes;
- Abstração de detalhes de uma enorme quantidade de dispositivos e protocolos na rede permite às aplicações de IoT acessar dados, fazer *analytics* e controlar os dispositivos sem precisar conhecer os detalhes das camadas de infraestrutura. SDN simplifica a criação, implantação e gerenciamento de dispositivos e de aplicações que os utilizam;
- Flexibilidade para ajustar e otimizar componentes para maximizar o desempenho e segurança, de acordo com mudanças em fluxo de dados e necessidade de negócios. A habilidade de SDN para alterar o comportamento da rede dinamicamente com base nos padrões de tráfego, políticas e eventos de segurança podem contribuir com os cenários de IoT.

156 David Geer. SDN to support Internet of Things devices, disponível em: http://internetofthingsagenda.techtarget.com/feature/SDN-to-support-Internet-of-Things-devices, acesso em maio de 2017.

157 Sreekanth. S.S. Software-Defined Networking -A Critical Enabler of IoT, disponível em: https://medium.com/@Infosys/software-defined-networking-a-critical-enabler-of-iot-eb4e6e4b411f#.lg4p89kli, acesso em maio de 2017.

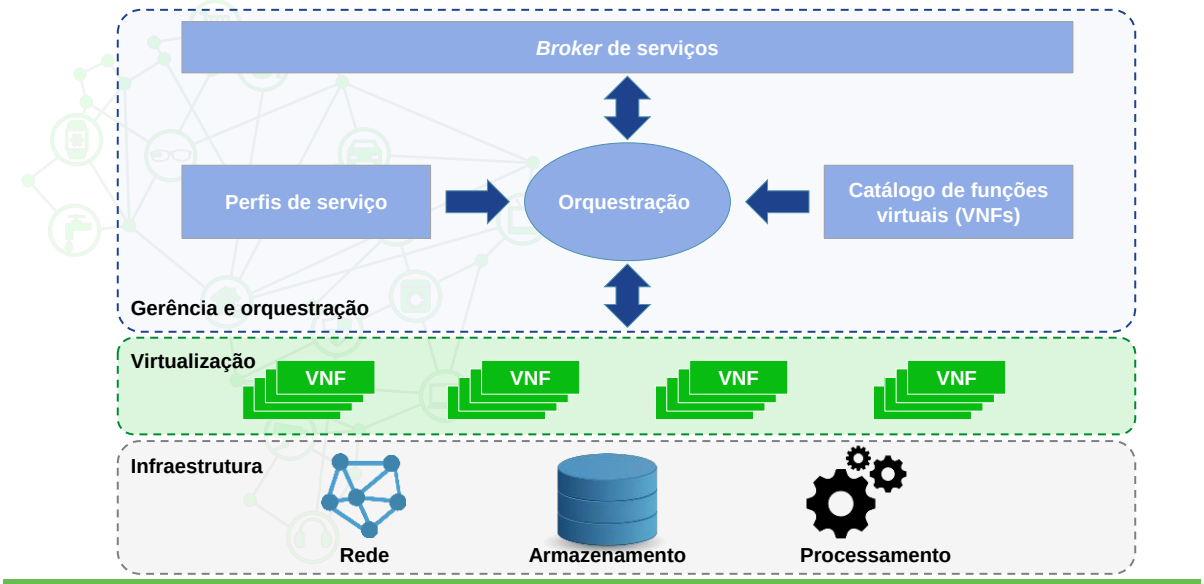
Na mesma direção de tornar o ambiente de redes mais dinâmico e flexível, a tecnologia de Virtualização de Funções de Rede (NFV) surgiu para somar com SDN, trazendo novos conceitos e características importantes para a inovação das redes de dados[158].

As tecnologias de virtualização apresentaram grande evolução nos últimos anos, devido ao sucesso do modelo de *Cloud*. A partir de uma infraestrutura de *data center*, passou-se a oferecer recursos de processamento, armazenamento e conectividade como serviço. Nessa direção, as operadoras de rede e provedores de Internet enxergaram a oportunidade de utilizar a *Cloud* para executar as funções de rede antes desempenhadas por equipamentos especializados (*appliances*), de maior custo.

Funções de rede podem ser desempenhadas por um hardware dedicado, ou em software dentro de máquinas virtuais na *Cloud*, como por exemplo roteadores, firewalls ebalanceadores de carga. O avanço tecnológico dos servidores de propósito geral (x86) e das interfaces de rede possibilitaram virtualizar as funções de rede (VNFs - *Virtual Network Functions*) na *Cloud* garantindo alto desempenho no processamento de pacotes em software. O QUADRO 24 ilustra a arquitetura de uma plataforma de virtualização de funções de rede, na qual existe uma camada central de orquestração, sobre a qual são oferecidos os serviços, além das camadas de infraestrutura e de funções virtualizadas.

QUADRO 24

Arquitetura de virtualização de funções de rede



FONTE: Análise do consórcio

158 R. Mijumbi et al., "Network function virtualization: State-of-the-art and research challenges," IEEE Commun. Surveys Tuts. vol. 18, no. 1, pp. 236–262, 1st Quart. 2016.

A virtualização dos elementos de rede oferece diversos benefícios aos provedores de serviços e operadoras como:

- Flexibilidade e agilidade na implantação de novos serviços. Em uma rede mais flexível e adaptável, os serviços são rapidamente instalados e aprovisionados;
- Redução dos custos por meio de uma infraestrutura baseada em COTS (*Commercial Off-The-Shelf*) com serviços virtualizados. Custos elevados são uma das considerações mais relevantes para os provedores e operadoras, com destaque para o custo de equipamentos de rede, licenças e operações;
- Escalabilidade, para se adaptar rapidamente às mudanças das necessidades dos clientes e prover novos serviços. As operadoras precisam ser capazes de expandir rapidamente sua infraestrutura de rede através de múltiplos servidores;
- Melhoria da segurança. As operadoras buscam permitir que seus clientes executem seus próprios firewalls nos ambientes virtuais, de forma a aprimorar o nível de segurança da rede.

As tecnologias SDN e NFV apresentam um grande potencial para contribuir com o uso mais eficiente e inteligente da infraestrutura de rede para atender às necessidades e desafios de conectividade do universo de IoT[159], abordando questões de alta densidade, alto volume de tráfego, baixo tempo de resposta, qualidade de serviços, segurança, entre outras.

A tecnologia conhecida como *Network Slicing*, ou fatiamento de rede, consiste em segmentar o tráfego, de forma a aplicar políticas de rede específicas para diferentes aplicações, garantindo uma melhor qualidade e segurança de conexão. Em ambientes onde existem diversas aplicações competindo pelo uso da banda de conectividade, é importante que o grau de prioridade estabelecido entre as aplicações seja garantido na rede.

O fatiamento do tráfego de rede provavelmente será suportado por tecnologias da camada de encaminhamento, seja na rede acesso, *backhaul* ou núcleo. Para se atingir qualidade de serviço fim-a-fim é imprescindível que os níveis da rede implementem o *Network Slicing*[160,161].

159 N. Omnes, M. Bouillon, G. Fromentoux and O. L. Grand, "A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges," 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, 2015, pp. 64-69.

160 Qian (Clara) Li, Geng Wu, Apostolos (Tolis) Papathanassiou, Udayan Mukherjee. An end-to-end network slicing framework for 5G wireless communication systems, disponível em: https://arxiv.org/pdf/1608.00572.pdf, acesso em fevereiro de 2017.

161 Navid Nikaein, Eryk Schiller, Romain Favraud, Kostas Katsalis, Donatos Stavropoulos, Islam Alyafawi, Zhongliang Zhao, Torsten Braun and Thanasis Korakis. Network Store: Exploring Slicing in Future 5G Networks, disponível em: http://www.eurecom.fr/en/publication/4641/download/cm-publi-4641.pdf, acesso em fevereiro de 2017.

5.2.3 Tendências

O conceito de redes definidas por softwares tem mostrado grandes benefícios para a evolução de redes de dados como um todo. As tecnologias ainda estão em fase de maturação e em breve devem transformar a maneira como as redes são controladas e gerenciadas de forma inteligente e autônoma.

Alguns fabricantes estão desenvolvendo a tecnologia NFV para o 5G, onde acredita-se que grande parte dos elementos da rede serão virtualizados. A virtualização de funções de rede já está presente em alguns ambientes de produção, mas estará disponível para uso em massa em 2 anos, segundo a Gartner.

Outro caso de uso que tem ganhado espaço e deve trazer grandes benefícios ao universo de IoT é a Software *Defined WAN* (SD-WAN), que traz os aspectos de dinamismo e adaptação de redes para a WAN através das tecnologias SDN e NFV.

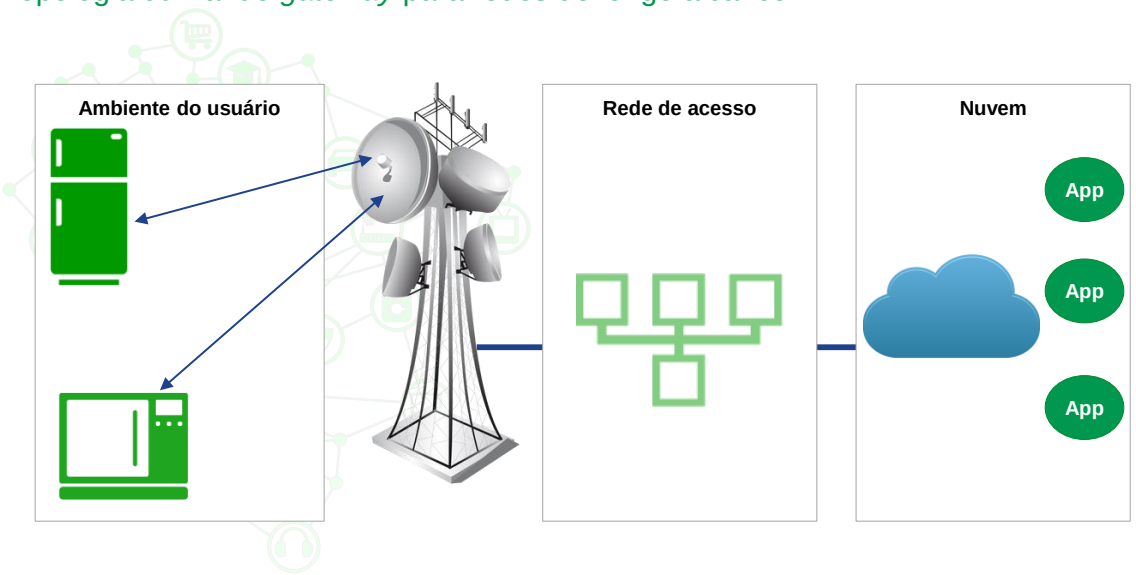
5.2.3.1 Tecnologias de acesso

Devido à heterogeneidade da rede de comunicação para aplicações de IoT, existem diferentes tecnologias disponíveis para transmitir dados gerados pelos elementos da camada de dispositivos, que atendem requisitos específicos de comunicação, tais como: operação com cobertura ampla ou cobertura reduzida, vazão de dados restrita ou larga, baixo custo do terminal, baixo consumo de energia, faixa de frequência de operação, etc.

Para o acesso, a IoT poderá ser impactada pelo aumento da disseminação das comunicações sem fio, dada a sua facilidade de implantação, quando comparadas às estruturas de redes fixas, tais como de fibra óptica e a cabo. As tecnologias de rede de acesso são caracterizadas por inserir capilaridade na rede através de tecnologias de múltiplo acesso, geralmente representadas pela topologia ponto - multiponto. Usualmente, é necessária uma arquitetura com um *gateway* alocado na infraestrutura do provedor de rede que sirva de interface entre a rede de área ampla e a rede de longo alcance, conforme topologia apresentada no QUADRO 25.

QUADRO 25

Topologia utilizando *gateway* para redes de longo alcance



FONTE: Análise do consórcio

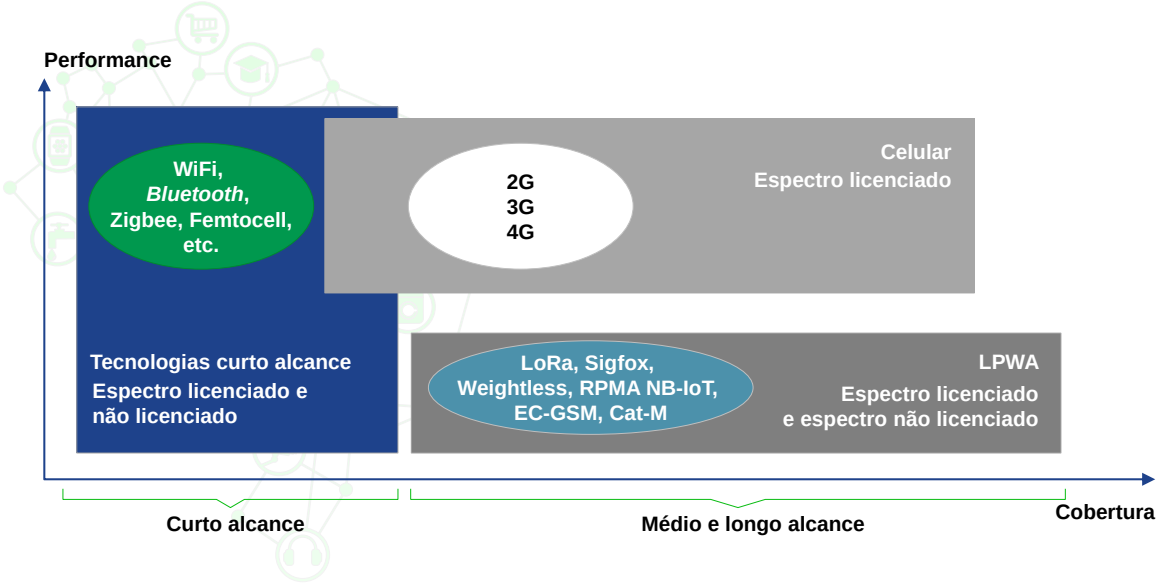
O acesso sem fio de um dispositivo de IoT envolve o equilíbrio de requisitos por vezes conflitantes, como faixa, duração da bateria, largura de banda, densidade, custo do ponto final e custo operacional. Com base nos casos de uso e/ou aplicações para IoT, as tecnologias de acesso podem ser categorizadas de acordo com os requisitos técnicos descritos a seguir.

- Raio de cobertura da rede sem fio;
- Consumo de energia (tempo de vida do dispositivo sem necessidade de substituição de bateria);
- Disponibilidade/confiabilidade;
- Latência;
- Suporte a massivo número de dispositivos por célula (densidade) e pela rede;
- Mobilidade, roaming e nomadicidade;
- Grau de segurança;
- Gerenciamento.

Como exemplo, no QUADRO 26 são descritas a tecnologias de rede de acesso segundo a vazão e o raio de cobertura.

QUADRO 26

Tecnologias de acesso conforme sua vazão e cobertura



FONTE: Análise do consórcio

Adicionalmente, os seguintes aspectos podem ser considerados para se analisar as tecnologias de acesso:

- Baixo custo de hardware;
- Baixo custo operacional;
- Consumo de energia pelo dispositivo;
- Licenciamento de espectro de frequência.

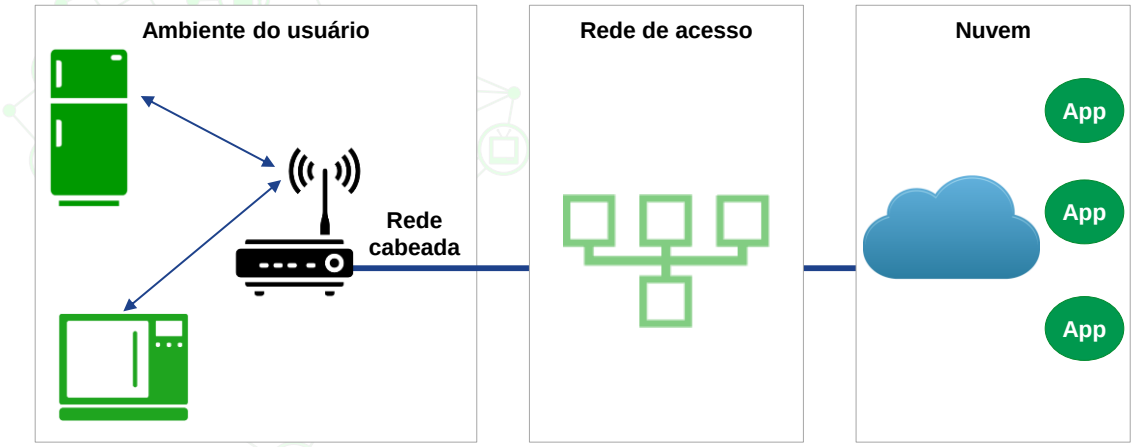
Devido aos inúmeros tipos de opções de tecnologias sem fio, neste relatório as mesmas foram subdivididas em categorias de redes, de acordo com o raio de cobertura: tecnologias *sem fio* de longo alcance e tecnologias de médio e curto alcance.

5.2.3.2 Redes de acesso de médio e curto alcance

As redes de médio e curto alcance fornecem conectividade sem fio na última milha entre os dispositivos e a Internet. Por exemplo, estas tecnologias conectam os dispositivos pessoais (ou *wearables*) com o smartphone, ou possibilitam o monitoramento de energia inteligente e controle dentro de casas. Usualmente, é necessária uma arquitetura com um *gateway* (que eventualmente pode ser um smartphone ou outro dispositivo móvel) que sirva de interface entre a rede de área ampla e a rede de curto alcance, conforme topologia apresentada no QUADRO 27.

QUADRO 27

Ilustração de topologia utilizando *gateway*



FONTE: Análise do consórcio

Muitas tecnologias competem nesse espaço, incluindo padrões internacionais e tecnologias proprietárias. Diferentes casos de uso em IoT requerem diferentes soluções de conectividade, como por exemplo:

- ***Smart wearables***: nos últimos anos, nota-se um crescimento de mercado dos chamados *smart wearables*. Os *wearables hype* são dispositivos tipicamente centralizados no celular, resultando em uma conexão com a Internet através de algum padrão sem fio disponível no smartphone (Wi-Fi, Bluetooth ou Bluetooth Low Energy). Desse modo o celular atua como um *gateway* à nuvem;
- **Casas ou prédios**: existem possibilidades (6LowPAN, WirelessHART, EnOcean, ANT, RF4CE) baseadas na camada física do padrão IEEE 802.15.4, além de outros consórcios como Z-Wave e RFXCOM. Nesse cenário, a ausência de interoperabilidade impede a adoção generalizada de conectividade sem fio. Entretanto, como no caso dos *wearables*, a infraestrutura dos *gateways* pode definir o padrão. Um forte candidato

é o roteador WiFi presente em quase todas as casas, que pode ser fortemente potencializado com uma nova versão do Wi-Fi chamado IEEE 802.11ah, operando em bandas sub-1GHz, o qual otimiza o desempenho estendendo o raio de cobertura a alguns quilômetros. Outro candidato é o set-top box que tem integrado ZigBee PRO para operar como *gateway* no controle das casas;

- **Ambientes com infraestrutura pública e industrial**: a conectividade de médio e curto alcance é fundamental para estender a cobertura na última milha. Cidades inteligentes estão enfrentando desafios como mobilidade, energia e médio ambiente. Nesse contexto, *Wireless Sensor Networks* (WSN) possibilitam um controle distribuído dos semáforos, luzes de sinalização de tráfico e iluminação pública, além de aplicações de *Smart Grid*. Outras aplicações importantes são o monitoramento da poluição do ar, vigilância e gerenciamento de desastres em regiões de alta densidade urbana. Nesses cenários, são utilizados padrões como IEEE 802.15.4g, KNX-RF e *Wireless* MBUS. Embora eles utilizem a mesma camada física, eles se diferenciam na camada MAC (*Media Access Control*) e camadas superiores da pilha OSI (*Open System Interconnection*).

Um fato importante dos rádios de médio e curto alcance é que operam maioritariamente em bandas não licenciadas (por exemplo Wi-Fi opera em 2.4 GHz), o que facilita seu desenvolvimento. As subseções a seguir mostram as principais tecnologias de rede de acesso de curto e médio alcance para IoT.

5.2.3.2.1 Tecnologias WiFi

A tecnologia de rede de acesso de curto e médio alcance mais representativa é o WiFi, embora seu consumo de energia seja alto. As primeiras versões desse padrão visam a criar conectividade sem fio, de curto alcance, com altas taxas que variam entre 11 Mbps, 54 Mbps e 600 Mbps, para os padrões 802.11b, 802.11g e 802.11n, respectivamente, os quais são utilizados por aplicações de IoT como redes de transporte de dispositivos com módulos WiFi, conectividade de *gateways* e controladores para criar capilaridade com tecnologias como 802.15.4 (ZigBee) e Bluetooth.

Tecnologias WiFi usualmente possuem requisitos menos críticos de consumo de energia, visto que seus terminais normalmente fazem parte de um *Gateway*, possuindo múltiplas interfaces de diferentes tecnologias, sendo uma voltada para a rede de sensores. Estas redes de sensores podem utilizar a rede WiFi como *backhaul*, agregando a comunicação de múltiplos *sensores*, dentro de um ambiente *indoor*. As tecnologias WiFi surgiram para operação de banda e frequência acima de 1 GHz, mas com demanda de operação em banda Sub 1GHz, foram criados os padrões 802.11af (utiliza conceitos de rádios cognitivos na banda dos *White Spaces*) e 802.11ah, mais conhecido como WiFi HaLow, com cobertura maior que o WiFi regular. As principais aplicações do WiFi HaLow são casas inteligentes, carro conectados, saúde e cidades inteligentes. O baixo consumo de energia facilita a

utilização de sensores e *wearables*. Além disso, o 802.11ah é oferece uma conectividade mais robusta em cenários desafiadores (por exemplo: atravessar paredes).

As altas taxas das tecnologias WiFi, tal como a tecnologia celular, são obtidas utilizando múltiplas antenas para transmissão/recepção, em uma técnica conhecida como MIMO, podendo ser operado tanto no modo *Access Point* como no modo terminal com até 8 antenas. O padrão 802.11ad tem a proposta de utilizar frequência na faixa de 60 GHz para oferecer acesso a altas taxas de dados, ao passo que o padrão IEEE 802.11p foi desenvolvido especificamente para uso em veículos, em comunicação V2V e V2X com simplificações no processo de associação, eliminando o processo de autenticação do terminal para o início da comunicação.

5.2.3.2.2 802.15.4

O padrão 802.15.4, além de ser utilizado na tecnologia Zigbee, aplica-se em outras tecnologias com particularidades nas camadas superiores da pilha de protocolos, tais como o 6LowPAN (concebido para uso em aplicações específicas de IoT), Thread (voltada para dispositivos de automação residencial), ISA 100 e *Wireless* HART (voltada para dispositivos de automação industrial, na qual o consumo de energia não é requisito crítico, mas a imunidade a interferências é importante), em topologia estrela ou mais comumente *Mesh*. Devido ao uso de arquitetura de comunicação *Mesh*, exige um hardware de capacidade suficiente para operar protocolos de roteamento dinâmico e, muitas vezes, com outras interfaces físicas de comunicação redundantes.

Além destas tecnologias, que utilizam a camada física IEEE 802.15.4, existem várias implementações proprietárias de comunicação desenvolvidas para aplicações específicas, tais como o controle de luminárias públicas. Desta forma, encontram-se diferentes fornecedores de módulos e *transceivers* para esta tecnologia com especificações de RF de diferentes potências e sensibilidade.

5.2.3.2.3 802.15.4G

Este padrão é uma derivação do IEEE 802.15.4 com especificações de taxas com maior capacidade e com maior cobertura para aplicações principalmente em *Smart Grid.* Este possui 3 opções de camada PHY atendendo a diferentes requisitos de taxas de comunicação. Desta forma, este padrão é utilizado em *Gateways* como *backhaul* utilizando arquitetura *Mesh*, ou mesmo, com *front end* de rádio frequência (RF) com maior capacidade de potência de transmissão e maior sensibilidade.

5.2.3.2.4 ZIGBEE

Utiliza subcamada PHY padrão IEEE 802.15.4, com especificação das subcamadas L2 e L3 para usos voltados para aplicações tais como automação em dispositivos residenciais, comerciais e médicos. Atinge taxas de até 250 kbps e, para alcançar distâncias significativas, opera na topologia de uma rede *mesh*. Para suportar a conectividade IPV6 recentemente foi desenvolvido o ZigBee IP.

5.2.3.2.5 NFC

O NFC (*Near Field Communication*) é um conjunto de padrões para comunicação sem fio, para distância de até 10 cm entre elementos. Está baseada na modulação ASK. Este padrão foi desenvolvido com 3 modos de operação. Possui opções de hardware para o *transceiver* que regularmente possui capacidade de operar com NFC e também com RFID, e o sensor ou *transponder* que permite a mobilidade com baixo consumo.

5.2.3.2.6 Z-WAVE

Tecnologia baseada na modulação MCE (*Manchester Channel Encoding*) e tipicamente opera em topologias *Mesh*. Foi desenvolvida para automação residencial como padrão aberto, utilizando hardware simples de baixo consumo. Existem fornecedores de hardware para diferentes aplicações de automação.

5.2.3.2.7 BLUETOOTH

Utilizado inicialmente para aplicações de uso pessoal, médico e comercial, utilizando tecnologia simples de baixo consumo para a troca de informações de dados, voz ou *streaming*. Para suportar as novas necessidades do mercado, foi padronizado o padrão Bluetooth-Low Energy (BLE), com menor capacidade de vazão e menor alcance que o Bluetooth clássico. Assim, o hardware possui menor custo e menores dimensões, podendo ser utilizado em *wearables*.

5.2.3.2.8 TENDÊNCIAS

No caso das tecnologias de rádio de médio e curto alcance, existem uma tendência de se otimizar algumas de suas características. Por exemplo, a última versão do Bluetooth, chamado Bluetooth 5, promete quadruplicar o raio de cobertura, duplicar a velocidade e multiplicar por oito a capacidade de *broadcasting* em comparação com o BLE.

Em termos gerais, existe a tendência de expandir o raio de cobertura operando em bandas não licenciadas sub-1GHz como é o caso do IEEE 802.11.ah e otimizar o consumo de energia com a utilização de rádios chamados ULP (*Ultra-Low Power*) com consumo de energia de mW e sua futura evolução para reduzir esse consumo até sub-mW com os U²LP.

5.2.3.3 Redes de acesso de longo alcance

Até recentemente, os padrões de comunicação móveis celulares eram focados em prover altas taxas de transmissão. Com os novos requisitos vislumbrados para parte das aplicações na IoT (baixa taxa de transmissão, baixo custo, duração de bateria, cobertura, escalabilidade, etc.), surgiram soluções de acesso celular em banda estreita, ou ainda, em ultra banda estreita. Com o mesmo objetivo, foram desenvolvidas soluções majoritariamente proprietárias, fazendo uso de frequências não licenciadas, classificadas como ISM (*Industrial Sientific and Medical*). Estas soluções são classificadas como Low-Power Wide-Area Network (LPWAN) e fazem uso de estação rádio base em comunicação ponto-multiponto (ou *Gateway* de WAN), assim, usualmente não utilizam *Gateway*/Concentrador na rede local.

Tecnologias LPWAN se dividem em duas categorias importantes: aquelas que fazem uso de espectro licenciado, explorado pelas operadoras de serviços móveis, e aquelas que fazem uso de faixas de espectro não licenciado (ISM).

As tecnologias para espectro não licenciado vêm sendo exploradas por novos entrantes. Todavia, via de regra, a tecnologia é proprietária, o ecossistema de atores em torno dessas soluções ainda não se encontra maduro e há maior risco de aprisionamento (*lock in)* tecnológico.

Por outro lado, as tecnologias LPWAN em espectro licenciado abrangem soluções móveis celulares. Atualmente o padrão GPRS é a tecnologia mais utilizada para comunicação M2M, entretanto, a comunicação se dá a baixas taxas (menor que 200kbps) e com custo relativamente baixo por terminal.

O GPRS ainda é a rede com a maior cobertura em muitos países, porém, é baseada numa tecnologia antiga, se comparada com o LTE-A (3GPP Release 12). Esta última tecnologia, por sua vez, é focada em prover altas taxas e não consegue, por exemplo, suprir os requerimentos de consumo de bateria, custo e cobertura, necessários à implementação de grande parte das aplicações da IoT.

Desta forma, os organismos de padronização de comunicação celular evoluíram os padrões existentes para atender as demandas da IoT massiva, sendo que o GSM evoluiu para o EC-GSM (por meio de técnicas de transmissão mais modernas) e o LTE-A fornece suporte específico a transmissões de baixas taxas através do NB-IoT (para baixíssimas taxas) e MTC Cat-M (para serviços de até 1Mbps), estes padronizados no 3GPP Release 13. Tais tecnologias são apresentadas a seguir.

5.2.3.3.1 SIGFOX (ESPECTRO NÃO LICENCIADO)

A Sigfox é uma provedora de serviços de comunicação dedicada a IoT. A solução utilizada pela Sigfox é baseada em tecnologia proprietária e corresponde ao nome da empresa. A tecnologia proposta está baseada na modulação *Ultra-Narrow Band* (UNB), na qual o mapeamento dos símbolos é feito com DBPSK no *UpLink* e GFSK no *Downlink* e complementa a modulação *Ultra-Narrow Band* (UNB) com saltos em frequência para proteção contra interferências.

A tecnologia Sigfox baseia-se em hardware simples, de forma que mesmo a Estação Base é de tamanho reduzido. Os receptores têm uma potência máxima de 15 dBm, inferior a outras tecnologias. Contudo, a empresa promete uma cobertura de até 50 km em área rural, devido ao uso de canalização UNB em faixa de frequência sub-GHz, que permite atingir distâncias maiores. O método de acesso ao meio está baseado no ALOHA, que simplifica o hardware e o software do módulo Sigfox, comparado a tecnologias que utilizam técnicas de acesso ao meio baseadas em multiplexação, tais como o TDMA ou FDMA. Os módulos e *transceivers* que compõem o hardware são disponibilizados por diferentes fabricantes que desenvolvem terminais para aplicações IoT, mas existem restrições quanto à operação da rede Sigfox pelo fato que a estação base é operada diretamente pela SigFox, ou um único parceiro exclusivo[162].

A visão da Sigfox é criar uma rede global usando as faixas ISM sub-GHz - 868 MHz (ETSI) e 902-928MHz (FCC), inclusive com roaming internacional. Nos países em que as faixas ISM não coincidam com as definidas pelo ETSI e FCC, devido a alterações no *firmware* dos dispositivos e equipamentos, as bandas são restritas às faixas autorizadas, podendo ocorrer limitações para o uso.

5.2.3.3.2 LORA

O LoRa é uma tecnologia baseada em uma técnica de espalhamento espectral conhecida por "*chirp spread spectrum modulation*". A tecnologia LoRa refere-se somente a camada PHY, e foi desenvolvida pela Semtech de forma proprietária. A tecnologia LoRaWAN foi criada pela LoRA Alliance, que define a arquitetura do sistema bem como os parâmetros de comunicação usando a tecnologia LoRa. A LoRaWAN aborda outras camadas além da PHY e define outros elementos da rede de comunicação LoRa, sendo um padrão parcialmente aberto, com hardware comercializado por diferentes fornecedores. Este último padrão define 3 classes de dispositivos:

[162] U. Raza, P. Kulkarni, M. Sooriyabandar, "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials · January 2017.

- **Classe A:** Permite comunicação bidirecional com priorização para comunicação *uplink*, sendo que a comunicação *downlink* ocorre somente em tempos agendados após a transmissão *uplink* do *sensor node*;
- **Classe B**: Também permite a comunicação bidirecional, tal como na classe A, mas, além disto, existe uma janela adicional para transmissão *downlink*;
- **Classe C**: Permite comunicação bidirecional sem restrições de janelas de agendamento.

Os módulos comerciais para os nós de sensores são disponibilizados para uma das 3 classes de dispositivos. Tal como o SIGFOX, esta tecnologia utiliza a técnica de acesso ao meio ALOHA. O uso de modulação CSS permite proteção quanto a interferências e o hardware compreendendo módulos e *transceivers* é disponibilizado por diferentes fabricantes[163].

5.2.3.3.3 Ingenu RPMA

Tecnologia proprietária com hardware comercializado de forma proprietária, incluindo os *chipsets*, os módulos e dispositivos. A sigla RPMA se refere método de acesso ao meio *Random phase multiple access*, com argumento de ser uma tecnologia robusta. Este foi desenvolvido para uso em comunicação M2M utilizando a faixa de frequência de 2,5 GHz[164].

5.2.3.3.4 Weightless -W, -N, -P

O padrão Weightless se baseia em conceitos de UNB e *frequency hopping*. Assim como o SIGFOX e LoRa, os módulos existentes são simples e de baixo custo. Apesar de ser um padrão aberto, a quantidade de fornecedores de módulos e *transceivers* ainda não é expressiva[165].

O padrão Weightless possui 3 opções de subcamada PHY: -W, -N e -P, com diferentes opções de vazão e de cobertura. A subcamada W trabalha em frequências hoje ocupadas para transmissão de TV (designado como *white space*), com taxas da ordem de dezenas de Megabits por segundo, enquanto a -N e -P operam na faixa ISM. A versão Weightless -N é unidirecional e tem um alcance de até 5 km. A versão P é bidirecional, com recursos mais completos que a versão N, porém com um alcance menor, de 2 km. Finalmente, a versão W tem uma conectividade bidirecional, com alcance de até 5 km. A Tabela 11 apresenta as principais características das diferentes versões do Weightless.

163 U. Raza, P. Kulkarni, M. Sooriyabandar, "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials · January 2017.

164 U. Raza, P. Kulkarni, M. Sooriyabandar, "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials · January 2017.

165 Idem.

TABELA 11 TABELA COMPARATIVA DAS VERSÕES DO WEIGHTLESS

Característica	Weightless-W	Weightless-N	Weightless-P
Bidirecional	Sim	Não	Sim
Cobertura (km)	5	3	2
Duração da bateria (anos)	3-5	10	3-8
Custo do terminal	Médio-baixo	Muito baixo	Baixo
Custo da rede	Médio	Inferior	Médio

5.2.3.3.5 LTE-MTC (ESPECTRO LICENCIADO)

Introduzida no padrão 3GPP Release 10 para otimizar o sistema LTE para aplicações de comunicação M2M. A tecnologia LTE-MTC utiliza blocos de recursos visando cumprir com requisitos para o atendimento de um grande número de dispositivos com o acesso à rede e com criação de classes de terminais visando o controle de congestionamento. Na Release 12 foi especificado o terminal Cat 0 otimizado com baixo consumo de energia, menor custo, com funcionalidade de DRX para a operação em modo *idle*/ativo de forma otimizada e, com complexidade reduzida. Este terminal utiliza largura de banda de 20 MHz com taxa de 1 Mbps.

O terminal LTE CAT M1 foi especificado pelo 3GPP na sua *Release* 13, em 2016, sendo uma evolução dos terminais LTE designados como CAT 1 e CAT 0 orientada ao desenvolvimento de terminais de baixo custo e consumo de energia. O padrão define e especifica, além da subcamada física, as demais subcamadas da pilha de protocolos. Estes terminais são voltados, por exemplo, para comunicação M2M em redes *Smart Grid* que possuem dispositivos sensores, atuadores e medidores de energia. Alguns fabricantes anunciam a comercialização de hardware para terminais CAT M1, mas ainda não são encontradas as especificações técnicas destes produtos no mercado[166].

O 3GPP Release 13 também especifica uma funcionalidade de DRX optimizada, designando este como eDRX (*evolved* DRX). Este terminal utiliza um conjunto de subportadoras OFDM correspondentes a 6 x (15 x 12) kHz (designado como 6 *Resource Blocks*) uma largura de banda igual a 1,4 MHz e atinge taxas de até 1 Mbps.

166 U. Raza, P. Kulkarni, M. Sooriyabandar, "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials · January 2017.

5.2.3.3.6 LTE-NB-IoT e EC-GSM (espectro licenciado)

O LTE-NB-IoT foi especificado pelo 3GPP na sua Release 13, com especificações voltadas para requisitos de comunicação de IoT, estando, portanto, dentro das classes de dispositivos de IoT *narrowband* de longo alcance, com hardware com consumo reduzido, igualando aos terminais UNB, devido a técnicas de operação e modo *Idle* (dormente).

O padrão define a especificação para, além da subcamada PHY, as demais subcamadas da pilha de protocolos. As Estações Base LTE que atenderem a Release 13 devem ser capazes de atender a comunicação em banda larga 4G, comunicação M2M (este designado como MTC no sistema LTE) e a comunicação IoT. Desta forma, estas estações compreendem um hardware de alto custo e de dimensões consideráveis, incluindo *hardware* de *front end* de RF para múltiplas bandas de frequência de operação[167].

Nesta Release também foi adicionada a padronização do EC-GSM (*Extended Coverage* GSM), sendo um sistema celular IoT para o mercado de GSM. EC-GSM está baseado na tecnologia eGPRS onde são definidos novos canais de controle e de dados sob o sistema legado GSM. Dentro do NB-IoT, foi especificado o terminal CAT-M2 (embora o 3GPP não tenha definido nenhum nome específico para este tipo de terminal) com utilização de um conjunto de subportadoras OFDM correspondentes a 1 x (15 x 12) kHz (definida como 1 *Resource Block*) com uma largura de banda total de 180 kHz, ou seja, com banda mais estreita que comparado ao terminal CAT-M. Adicionalmente, foi especificado a opção de *single tone* para comunicação uplink, permitindo o uso de uma única subportadora padrão de 15 kHz e mais uma nova opção de largura de subportadora de 3,75 kHz, permitindo comunicação UNB no uplink. As modulações são OFDMA no downlik e FDMA ou GMSK no uplink. As taxas disponíveis são de 128 kbps no downlink e 48/64 kbps no uplink.

Pode operar em 3 cenários bem definidos: *Stand-alone operation* para utilizar o espectro utilizado por sistemas GERAN para substituir, por exemplo, uma portadora GSM; *Guard band operation* utilizando blocos de recurso não utilizados pela portadora LTE; e *In-band Operation* utilizando os blocos de recurso dentro de uma portadora LTE. O EC-GSM utiliza largura de banda de 200 kHz com taxa de 10 kbps com modulação GMSK no *downlink* e *uplink*.

Tanto NB-IoT quanto EC-GSM permitem um *link budget* adicional de 8 dB comparado ao terminal CAT-M, assim, fornecendo atendimento ao requisito de cobertura de áreas amplas.

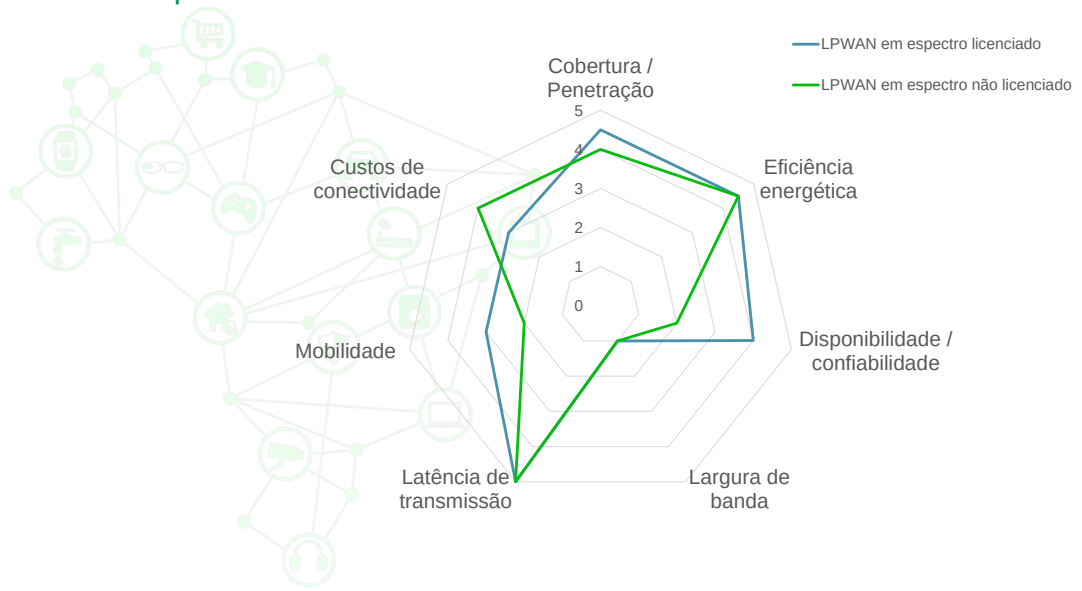
[167] U. Raza, P. Kulkarni, M. Sooriyabandar, "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials · January 2017.

5.2.3.3.7 TENDÊNCIAS

As redes de acesso de longo alcance em IoT devem ser formadas predominantemente por LPWAN (em espectro licenciado e não licenciado). As necessidades das aplicações de IoT resultam em requisitos específicos que as LPWAN atendem, conforme apresentado no QUADRO 28.

QUADRO 28

LPWAN: requisitos e características



FONTE: Análise do consórcio

Além disso, o uso do espectro é relevante no cenário de IoT massivo, considerando o uso de frequência licenciada e não licenciada. No caso de frequência não licenciada, tem-se a preocupação com o uso massivo de dispositivos compartilhando um mesmo espectro. O uso de frequências licenciadas garante a segregação da rede de sensores para determinado detentor da faixa de frequência.

Assim, espera-se que inicialmente os primeiros *deployments* de IoT para grandes áreas devem ocorrer em espectro não licenciado, e à medida que soluções padronizadas no âmbito do 3GPP estejam disponíveis, as operadoras de telecomunicações passem a ocupar esses espaços, valendo-se de sua infraestrutura existente.

5.2.3.4 Comparação das tecnoclogias de acesso

Os QUADROS 29 a 31 seguir apresentam comparações das diferentes tecnologias de acesso descritas. As tabelas apresentam as especificações dos *sensor nodes*, que atendem ao requisito de baixo consumo, com tempo de duração da bateria de mais de 10 anos.

QUADRO 29

Comparação entre as tecnologias de longo alcance

	SigFox	LoRa/LoRaWAN	Ingenu RPMA	Weightless			CATM1	EC-GSM-IoT	CAT NB1 (NB-IoT)
				-W	-N	-P			
Frequência	Sub 1 GHz (ISM)	Sub 1 GHz (ISM)	2,4 GHz (ISM)	TV white space (470-790 MHz)	Sub 1 GHz (ISM)	Sub 1 GHz (ISM)	3 GP licency bands	GSM licency bands	3 GPP licency bands
Alcance máximo (km)	50 (rural) 10 (urbano)	5 (rural) 15 (urbano)	20 (rural) 15 (urbano)	5 (urbano)	3 (urbano)	2 (urbano)	30	35	35
Vazão máxima – downlink (kbps)	Mensagens de 8 bytes/dia	50 (EU)/100 (US)	156	1-10,000	30-100	0,2-100	200-1.000	140	200
Vazão máxima – uplink (kbps)	100 bps a 140 mensagens/dia	50 (EU)/100 (US)	624 kbps	1-10.000	30-100	0,2-100	200-1.000	140	20 (single-tone)/200 (multi-tone)
Roaming fim a fim	Sim	Sim	Informação não disponível	Sim	Não	Sim	Sim	Não	Sim
Implantações comerciais	>100	>100	<100	Informação não disponível	Informação não disponível	Informação não disponível	–	–	–
Eficiência espectral	Alta	Baixa	Média	–	–	–	Alta	Alta	Alta
Topologia	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela
Tecnologia proprietária/aberta	Proprietária	Proprietária/ aberta	Proprietária	Aberta	Aberta	Aberta	Aberta	Aberta	Aberta
Organismo	SigFox (Ultra Narrow Band)	LoRa Alliance	Ingenu (on ramp)	Weighless SIG	Weighless SIG	Weighless SIG	3 GPP	GSM extension	3 GPP
Vantagens	Baixo custo, rápida e fácil deploy do serviço	Rede pública e privada Camadas de rede e MAC são abertas Baixo custo Diversos fornecedores	Rede pública e privada Comunicação bidirecional Utilização de faixa de frequência disponível em todo o mundo. É o membro fundados do IEEE 802154 k	Padrão aberto Flexibilidade na taxa de vazão (até 10 Mbps)	Padrão aberto Baixo custo Rápida e facil deploy do serviço	Padrão aberto Comunicação bidirecional a taxas variáveis	Uso de espetro licenciado o qual previne interferências	Uso de espetro licenciado o qual previne interferências	Uso de espetro licenciado o qual previne interferências
Desvantagens	Necessidade de utilziar rede pública Taxa de transferência muito baixa Máxima transferência de 140 mensagens/dia Uso limitado para sensores, monitoramento, etc.	Camada física proprietária Alta latência para downstream	Utiliza faixa de frequência de 2,4 GHz (mais poluída e com menor penetração)	Baixa adoção Uso de faixas whitespace de TV – diferentes regulamentos no mundo	Taxa de transferência muito baixa Uso limitado para sensores, monitoramento, etc.	Poucos fornecedores Menor cobertura	Utilização restrita a operadoras celulares	Não disponível/ tecnologia não avaliada	Não disponível/ tecnologia não avaliada

FONTE: Análise do consórcio

QUADRO 30

Comparação entre as tecnologias WiFi

	802.11g	802.11n	802.11ac	802.11ad	802.11af	802.11ah	802.11p
Frequência	2,4 GHz	2,4 GHz, 5 GHz	5GHz	60 GHz	54-790 MHz	900 MHz	5,9 GHz
Alcance máximo	38 m	70 m	35 m	60 m	5 Km (rural)	1 Km	1 Km
Vazão máxima	54 Mbps	450 Mbps/600 Mbps	7 Gbps	7 Gbps	426,7 Mbps	347 Mbps	27 Mbps
Topologia	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela	Estrela
Organismo	WiFi Alliance	WiFi Alliance	WiFi Alliance	WiFi Alliance	WiFi Alliance	WiFi Halow	WiFi Alliance
Características	Uso de antena única (sem MIMO)	Uso de até 4 antenas (4 x 4 MIMO)	Uso de até 8 antenas (8 x 8 MIMO)	Também conhecido como WiGig, Uso em 60 GHz (milimeter wave) Uso de antena única (sem MIMO)	Para uso em frequências Sub 1 GHz, incluindo TV white space Utiliza tecnologia de rádio cognitivo Uso de até 4 antenas (4 x 4 MIMO)	Para uso em frequênciassub-GHz Cobertura estendida Uso de até 4 antenas (4 x 4 MIMO) Padrão 802.11 desenvolvido para IoT	Padrão definido para Wireless Access in Vehicular Environments (WAVE) dedicado para uso em Intelligent Transportation System (ITS) ou V2X Suporta comunicação com veículos em altas velocidades
Consumo	Alto	Alto	Alto	Alto	Alto	Médio-baixo	Alto

FONTE: Análise do consórcio

QUADRO 31

Comparação entre as tecnologias de curto alcance

	Bluetooth clássico	Bluetooth-Low Energy (BLE)	ZigBee	802.15.4	802.15.4g (Wi-Sun)	NFC	Z-WAVE
Frequência	2,4 GHz (ISM)	2,4 GHz (ISM)	868 MHz; 915 MHz; 2,4 GHz (ISM)	2,4 GHz (ISM)	Sub 1 GHz; 1,4 GHz; 2,4 GHz	13,56 MHz (ISM)	868,42 MHz; 908,42 MHz; 919,8 MHz; 921,4 MHz
Alcance máximo	100 m	100 m	100 m	10-100 m	> 1 Km	10 cm <20 cm	30 m
Vazão máxima	2,1 Mbps	0,27 Mbps	20 Kbps (sub GHz) 250 Kbps (2,4 GHz)	250 Kbps	13 a 2,4 Mbps	424 Kbps	10-100 Kbps
Topologia	Scatterned	Scatterned	Mesh	Mesh	Mesh	Ponto a ponto	Mesh
Organismo	Bluetooth Special Interest Group (SIG)	Bluetooth Special Interest Group (SIG)	ZigBee Alliance	IETF/IEEE	Wi-Sun Alliance	NFC Forum	Z-Wave Alliance
Características	Tecnologia simples de baixo custo Uso de beaconing com potencial de aplicações Maior ecossistema (smartphones, tablets, etc.)	Tecnologia simples de baixo custo Uso de beaconing com potencial de aplicações Maior autonomia da bateria e alcance comparado ao Bluetooth clássico Maior ecossistema (smartphones, tablets, etc.)	Baseado em PHY e MAC 802.15.4 com camadas superiores padronizads Arquitetura Mesh Desenvolvido para automação e smart grid	A 802.15.4, além de ser utilizada para o ZigBee, é utilizada também em tecnologias (com camadas superiores específicas) 6LowPAN, Thread, ISA 100, Wi-Sun e Wireless HART, em arquiteturas estrela ou Mesh	Voltado para redes Smart Grid e smart metering	Coexistência com RFID. Não requer pareamento	Protocolo simples. PHY baseado em ITU-T G.9959 Arquitetura Mesh Desenvolvido para controle e automação predial
Consumo	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo

FONTE: Análise do consórcio

5.2.3.5 Evolução da rede celular para IoT

5.2.3.5.1 5G

Com o desenvolvimento da 4ª Geração de rede celular, o 3GPP verificou que seria necessário desenvolver uma nova tecnologia para atender ao crescente aumento de demandas de banda, de serviços de M2M massivo e comunicação ultra confiável. Assim, iniciaram-se os estudos inicias da Quinta Geração de redes celulares (5G). A proposta do 5G é atender as altas taxas de transmissão, a grande quantidade de terminais, alta eficiência espectral, cobertura estendida e baixa latência.

A tecnologia 5G já contempla implantações do tipo *Massive Machine Type Communications* (MMTC). As funcionalidades que afetam o atendimento de requisitos do MMTC e de IoT e são descritas a seguir.

Com o objetivo de aumentar a eficiência espectral e melhorar o uso do espectro, um novo método de multiplexação espacial não ortogonal é empregado, atendendo assim ao número massivo de terminais, sendo estudados os potenciais métodos:

- *Sparse code multiple access* (SCMA);
- *Resource spread multiple access* (RSMA);
- *Pattern division multiple access* (PDMA), entre outros.

Com o objetivo de aumentar o espectro disponível para transmissão, é provável que a quinta geração lancer mão do conceito do uso de espectro não licenciado de forma assistida, este sendo designado como LTE *Unlicensed spectrum* (LTE-U) com *Licensed-Assisted Access* (LAA), bem como é provável que se utilize do conceito de Rádio Cognitivo (*Cognitive radio* - CR) com objetivo de utilizar espectros não ocupados, tais como, o do *White Space*, espectro atualmente ocupado pelas operadoras de TV e que no futuro poderá estar disponível.

A quinta geração também poderá também empregar os conceitos de virtualização com o Software *Defined Networking* (SDN), *Network Functions Virtualization* (NFV), *Edge computing* e *Cloud Computing*.

Para aumento de cobertura, o 4G de *Small cell* e HetNet farão parte do 5G. Para serviços missão crítica, é planejada a obtenção de latências de 1 ms (designado como *ultra-reliable low latency communication* - URLLC).

Outro conceito iniciado no 4G, e que fará parte do 5G, é a comunicação entre dispositivos (designado como *Device to Device* - D2D) que consiste na comunicação direta entre terminais 5G. Adicionalmente, é planejada a utilização de funções de *Relay*, ou seja, terminais poderão servir de *backhaul* para comunicação entre a estação base e um terminal remoto. Por fim, a quinta geração também abordará a comunicação veicular com o conceito de *Cellular Vehicle-to-Everything* (V2X).

Por todas essas características, a tecnologia 5G tem sido apontada como candidata a endereçar uma ampla quantidade de casos de uso. A previsão é de início de implantação em 2020.

5.2.3.5.2 eSIM

Com a dinâmica do mercado de IoT, o tradicional SIM *card* (*Subscriber Identity Module*) não se mostra adequado para implementações nas quais os dispositivos foram instalados em locais remotos ou atachados a objetos de difíceis acesso. Por exemplo, o SIM card tradicional deve ser trocado caso seja necessário substituir a operadora de celular.

A especificação do *embedded* SIM (e-SIM) pela GSMA fornece um mecanismo padrão para o provisionamento e gerenciamento remoto de conexões máquina a máquina (M2M), permitindo o provisionamento "*over the air*" e a mudança de um operador para outro. Com a adoção do e-SIM, as seguintes vantagens podem ser ressaltadas:

- Integração do SIM card no dispositivo e compatibilidade com todas as operadoras celulares;
- Alterações podem ser realizada remotamente e de modo seguro, dispensando a troca física do SIM card;
- Redução dos custos logísticos e de provisionamento associados ao uso de cartões SIM tradicionais sem alterar os níveis de segurança;
- Garantia de disponibilidade de solução para dispositivos com ciclo de vida estendido;
- Maior flexibilidade em relação à fabricação, restrições globais e contratos de conectividade local.

5.2.4 Protocolos relevantes para comunicação em IoT

Propostas de novos protocolos têm surgido para cenários de redes IoT, considerando características de ambientes com potencial para aplicações em IoT que enfrentavam desafios de conectividade, como redes de sensores com limitações de consumo de energia, processamento e memória. Por outro lado, a adoção de protocolos anteriores à IoT tem sido intensificada, dada a evolução natural das redes, como por exemplo o IPv6.

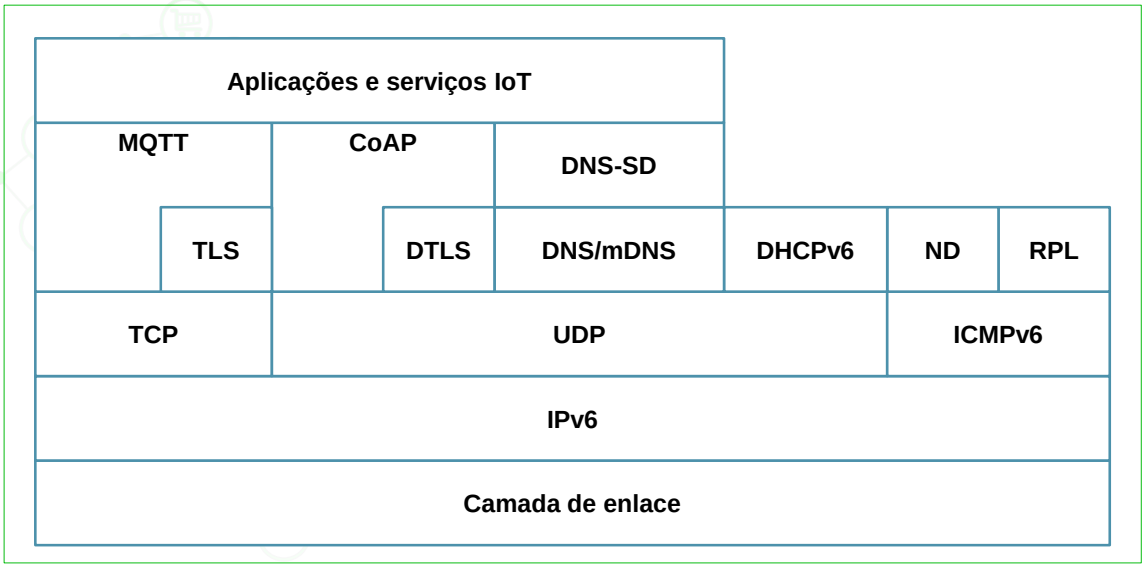
5.2.4.1 Protocolo IP baseado em IPv6

O IP representa o protocolo padrão da camada de rede utilizado atualmente na Internet. Através do IP, é possível endereçar qualquer dispositivo visível na rede. A versão 4 do protocolo possui um espaço de endereçamento de 32 bits, ou seja, comporta um pouco mais do que 4 bilhões de endereços. Com a chegada dos dispositivos móveis como smartphones e tablets, os endereços IPv4 se esgotaram rapidamente e a versão 6 do protocolo passou a ser implantada, ainda que lentamente. IoT irá pressionar ainda mais a evolução para IPv6, que conta com 128 bits de endereços, uma vez que dezenas de bilhões de dispositivos serão conectados à rede.

A estrutura de camadas na comunicação entre dispositivos para IoT não sofre alterações em relação ao modelo padrão TCP/IP ou OSI, como ilustrado no QUADRO 32. A tendência é que o IPv6 assuma a camada de rede, substituindo a versão anterior. Essa mudança irá impactar inúmeros serviços de infraestrutura que proveem suporte à camada de comunicação IP, tal como ICMP, DHCP, *Neighbor Discovery* (ND), DNS e RPL.

QUADRO 32

Pilha de protocolos de rede para IoT



FONTE: Análise do consórcio

Na camada de transporte, os protocolos existentes e já estabelecidos, UDP e TCP continuam como base da comunicação para IoT. No entanto, o padrão de tráfego de dispositivos com perfil de baixo consumo de energia e restrições de acesso podem não se adequar à implementação atual do TCP, que apresenta uma lógica de controle de sessão elaborada para um cenário com estabilidade de conexão.

Nesse contexto, uma vertente[168] do IoT tem investido na utilização do protocolo UDP na camada de transporte, atribuindo o controle de sessão à camada superior, como é o caso do protocolo CoAP. Ao mesmo tempo, existem alguns estudos sobre o TCP que buscam adaptá-lo ao cenário de IoT[169,170].

168 Wentao Shang, Yingdi Yu, Ralph Droms, Lixia Zhang. Challenges in IoT Networking via TCP/IP Architecture. NDN, Technical Report NDN-0038, February 10, 2016.

169 Y. Cheng, J. Chu, S. Radhakrishnan, A. Jain. "TCP Fast Open", draft-ietf-tcpm-fastopen-10, September 2014.

170 Christian Legare, Micrium. Reworking the TCP/IP stack for use on embedded IoT devices, disponível em: http://www.embedded.com/design/connectivity/4429865/Reworking-the-TCP-IP-stack-for-use-on-embedded-IoT-devices, acesso em fevereiro de 2017.

5.2.4.2 Protocolos de Roteamento em rede IoT

A grande variedade de cenários dentro do universo de IoT implica em características de redes que podem ter uma vasta diferenciação com relação ao padrão de tráfego, tamanho da rede e grau de mobilidade. Portanto, os protocolos de roteamento necessitam levar em consideração as especificidades de cada cenário. Os domínios dos requisitos de rede podem ser classificados em quatro categorias[171]:

- **Padrão de tráfego**: o protocolo de roteamento deve se adequar ao padrão de tráfego da rede, que pode apresentar variações de acordo com o cenário de implantação;
- **Eficiência energética**: em muitas aplicações de IoT, o consumo energético é crucial para manter a rede operando por um longo período de tempo, portanto o protocolo de roteamento deve levar em consideração o consumo energético (*energy-awareness*) na decisão de encaminhamento do tráfego;
- **Escalabilidade**: redes de IoT podem variar de poucas unidades até milhares de nós, portanto o protocolo de roteamento deve ser escalado conforme o tamanho da rede, de forma a manter seu desempenho sem aumentar significativamente o consumo de memória com a tabela de roteamento;
- **Mobilidade**: algumas aplicações de IoT podem necessitar de mobilidade, por isso o protocolo de roteamento deve suportar a mudança de localização de nós na rede.

Data a enorme variedade de aplicações, não seria factível ter um único protocolo de roteamento para todos os cenários de IoT. Nesse sentido, estão surgindo protocolos de roteamento para tratar de especificidades de ambientes de IoT que não são atendidas pelos protocolos atuais, especialmente considerando limitações como o baixo consumo energético.

Existem diferentes protocolos de roteamento sendo propostos para redes IoT, como o *Optimized Link State Routing Protocol* (OLSR)[172] e o A*d hoc On-Demand Distance Vector* (AODV)[173], sendo o mais promissor o protocolo de roteamento dinâmico *IPv6 Routing Protocol for LLN - Low-Power and Lossy Networks* (RPL) (RFC6550). O RPL é um protocolo do tipo *Distance Vector*, o qual utiliza como métrica padrão o número de saltos (hops), possuindo outras métricas, para a decisão da escolha do melhor caminho, como, por exemplo, o estado do nó, latência do link, dentre outras.

É importante ratificar a opção destas métricas, principalmente o *Hop Count*, *Link Throughput* e *Link Latency* com a opção de configuração de pesos, para que o protocolo RPL crie uma arquitetura lógica para o encaminhamento das mensagens seguindo a topologia hierárquica para a rede estratificada em rede *Mesh* dos concentradores (*Gateway* IoT) e a rede *Mesh* dos end devices/controlador.

[171] Lotte Steenbrink, Routing in the Internet of Things, Hamburg University of Applied Sciences, 2014, disponível em: http://www.inet.haw-hamburg.de/teaching/ss-2014/master-projekt/aw1_lotte_steenbrink.pdf, acesso em maio de 2017.

[172] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR), "RFC 3626, IETF, October 2003.

[173] Anamika Sharma, Er. Sonia Saini, Energy Efficient AODV Protocol for Internet of Things. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 5, Issue 8, August 2016.

5.2.4.3 Protocolos de adaptação

A utilização de endereçamento IPv6 na Internet é um movimento que está sendo intensificado pela IoT, dado o grande número de dispositivos conectados na rede. Neste cenário, permitir a comunicação transparente entre os dispositivos IoT com a Internet é fundamental, e exigiria a utilização de IPv6. No entanto, o MTU de pacotes IPv6 é de 1280 bytes e representaria um obstáculo considerando as limitações das redes de IoT, como baixo consumo energético, baixa capacidade de processamento e memória.

Nesse contexto, foi criado o protocolo de adaptação 6LowPAN[174], que trabalha com compressão[175] do IPv6 para sua utilização sobre o padrão IEEE 802.15.4, o qual restringe o MTU dos pacotes a 127 bytes. Assim como o IPv6, o protocolo 6LowPAN pertence à camada de rede, sobre a qual atuam os protocolos da camada de transporte e aplicação, incluindo segurança, com uso dos protocolos *Transport Layer Security* (TLS) ou *Datagram Transport Layer Security* (DTLS) e, inclui o protocolo de roteamento RPL.

5.2.4.4 Escalabilidade necessária para IoT

Do ponto de vista da escalabilidade, a chave para conectar a enorme quantidade de dispositivos é a utilização do protocolo IPv6. Já os protocolos de roteamento não parecem ser uma preocupação, uma vez que diferentes redes podem utilizar o protocolo que melhor atender aos seus requisitos; se ainda for necessário, é possível lançar mão do protocolo de roteamento utilizado atualmente, o *Border Gateway Protocol* (BGP), que é o protocolo de roteamento que conecta todas as redes. Ao contrário de outras tecnologias fundamentais da Internet, o BGP não é hierárquico. O BGP omite informação com o objetivo de manter o roteamento tratável, operando satisfatoriamente apesar de obter uma visão local da Internet.

5.2.4.5 Tendências

Apesar das limitações, o IPv6 parece atender ao propósito de conectar com a Internet a enorme quantidade de dispositivos esperada da IoT e, portanto, é provável que continue sendo a tecnologia fim-a-fim da rede global.

Os protocolos de roteamento para atender aos diversos cenários e aplicações de IoT ainda estão em fase de experimentação e pesquisa, portanto devem existir novas propostas conforme forem surgindo cenários. É provável que não exista um único protocolo que atenda de forma geral às inúmeras demandas de IoT. Na camada de transporte, o TCP e o UDP continuam como as tecnologias predominantes e devem atender à demanda de IoT. Algumas otimizações e variações do TCP podem surgir para cenários específicos de redes, especialmente em redes de sensores.

[174] G. Montenegro, N. Kushalnagar, , J. Hui, D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007.

[175] J. Hui, Ed., P. Thubert. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, 2011.

5.2.5 Questões de segurança

Do ponto de vista da segurança, temos vertentes que afirmam que a camada de conectividade e redes teria protocolos suficientemente maduros e escaláveis para receber os bilhões de dispositivos esperados para os próximos anos, desde que os cuidados necessários sejam tomados. Por outro lado, há pesquisadores e entidades que têm apontado alguns pontos de atenção, descritos a seguir.

5.2.5.1 Mecanismos

Segurança e confiabilidade apresentam particularidades para IoT[176]. Por exemplo, um sensor pode parecer estar falhando, quando de há de fato uma falha de comunicação, por interferências, atrasos e interrupções. Neste sentido, a redundância do canal de comunicação pode aumentar a confiabilidade da comunicação com sensores. Além disso, medidas adicionais de segurança de redes devem ser tomadas, tais como:

- A proteção das comunicações deve compreender[177]: confidencialidade e integridade fim a fim, mitigação de vulnerabilidades em *softwares* de segurança de comunicação, e proteções contra-ataques de negação de serviço à infraestrutura de comunicação;
- Boas práticas para integração de serviços às redes domésticas *Home Area Network* (HAN)[178] devem ser seguidas, tais como: *hardwares* protegidos contra interrupções de energia, congestionamento de tráfego e erros de formatação de dados; uso de emparelhamento seguro entre dispositivos;
- Segurança da HAN[179]: uso de um *gateway* e segregação de redes para mitigar a propagação de ataques de/para a HAN e diminuir a exposição de dispositivos vulneráveis; usar *gateway* para separar o acesso a medidores inteligentes.

5.2.5.2 Criptografia e troca de chaves para redes e comunicações

A ENISA[180], quando trata de casas inteligentes[181], entende que a segurança criptográfica da rede está relacionada à proteção das comunicações. O documento afirma que toda comunicação deveria ser protegida contra revelação indevida, modificação não autorizada e repetição (*replay*). Nas comunicações sobre TCP, o protocolo TLS (em versões recentes e atualizadas, como uma boa prática) é considerado como a escolha mais adequada atualmente para a segurança da camada de transporte, enquanto que o protocolo DTLS é

176 J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

177 ENISA, "Cyber Security and Resilience of smart cars". 2017.

178 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

179 Idem.

180 European Union Agency for Network and Information Security.

181 ENISA, "Securing Smart Airports". 2016.

visto como a melhor escolha para proteção das comunicações sobre UDP. Vale lembrar que o HTTP sobre TLS é chamado de HTTPS.

Outro ponto importante levantado pela ENISA é a autenticação mútua entre as partes (de dispositivos entre si, ou entre dispositivos e servidores). A autenticação mútua consiste em demonstrar criptograficamente, para as partes comunicantes, que seus interlocutores são autênticos. Atualmente, os protocolos de autenticação mútua (por exemplo, utilizados pelo TLS) utilizam Infraestruturas de Chaves Públicas (ICPs), que devem ser implantadas obedecendo a determinadas premissas para que sejam confiáveis: existência de certificados digitais para clientes/dispositivos e servidores, validação de toda a cadeia de certificação, verificação das listas de revogação, obrigatoriedade de que todos os acessos sejam autenticados. Quando a verificação de cadeias de certificação longas é inviável, a técnica de pinagem de certificados (*certificate pinning*) pode ser usada.

A BITAG[182][183] identificou que os principais desafios de segurança em redes para IoT são: vazamentos de dados em nuvens, comunicação não autenticada, comunicação não encriptada, falta de isolamento de redes e falta de autenticação mútua. Além disso, a BITAG[184] identificou que os principais desafios relacionados à segurança criptográfica na camada de rede das casas inteligentes são: comunicação não autenticada, comunicação não encriptada e falta de autenticação mútua para viabilizar a autorização de acesso de forma assertiva. De fato, a BITAG sugere que a única proteção criptográfica implementada, atualmente, é a segurança das comunicações, porém frequentemente mal implementada. Por exemplo, por TLS sem pinagem de certificados.

O NIST[185] identifica uma possível dificuldade de sincronização de tempo quando *snapshots* de dados de muitos sensores necessitarem de sincronismo na sua rede. O NIST não se posiciona em relação ao uso de relógios globais para sincronização de dispositivos de IoT.

5.2.5.3 Proteção Fim-a-Fim e Segmentação de Redes

Segurança em camadas é fundamental para IoT, por exemplo para o correto funcionamento de dispositivos e redes. Os dispositivos devem ser capazes de executar suas tarefas e reconhecer e neutralizar as ameaças. Isso requer que tecnologias e controles já empregados e validados nas atuais redes de TI evoluam e se adaptem aos novos desafios da IoT, principalmente às restrições dos dispositivos. O que se nota, é que cada provedor de tecnologia IoT tem tomado uma abordagem própria com relação à segurança, no intuito

[182] Broadband Internet Technical Advisory Group.

[183] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

[184] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

[185] J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

de proteger dispositivos, na tentativa de endereçar a segurança fim-a-fim em aplicações IoT.

A adoção de mecanismos de autorização do tipo FGAC (*Fine Grained Access Control*), que permitem um controle mais flexível dos recursos e tolerância ao enfrentar riscos desconhecidos, deve ser empregada. Além disso, as variantes de protocolo de segurança IP para IoT com primitivas criptográficas de chave pública, tais como, DTLS (*Datagram Transport Layer Security*), DEX (HIP *Diet Exchange*) e IKEv2, podem atender aos requisitos da IoT relacionados a escalabilidade e interoperabilidade.

Já a segmentação de rede, técnica amplamente difundida e utilizada como melhor prática nas atuais redes, é considerada essencial a IoT, pois é utilizada para garantir que os dispositivos conectados não prejudiquem a segurança da rede no geral. Isso se deve ao fato de que este tipo de segmentação assegura que o acesso a informações ou dispositivos – informações sensíveis ou ainda dispositivos de missão crítica – sejam consistentemente mantidos segregados, evitando assim o acesso indevido e a possível propagação de *malware* na rede. Outra abordagem é utilizar mecanismos de segregação dinâmicos, como o controle para conter um ataque e limitar os danos de um incidente.

A tecnologia e mecanismos de segmentação já estão disponíveis, em praticamente toda implementação de conectividade e redes, portanto, no momento de implementação de uma rede de sensores, por exemplo, os projetos de conectividade e redes devem ser revisitados e analisados, para que seja possível avaliar se as regras e estratégias de segmentação estão aderentes à IoT.

5.2.5.3.1 Pontos importantes para implantação

Numa implementação de IoT, observa-se que, além de utilizar os protocolos já conhecidos da Internet convencional como TCP/IP, HTTP/REST, WiFi e Ethernet, novos protocolos estão sendo desenvolvidos e ganhando mercado, principalmente, nas camadas físicas e de enlace. Isso se deve ao fato de que grande parte dos dispositivos, que formam WSNs (*Wireless Sensor Network*), possuem restrições relativas a consumo e processamento.

O conhecimento desses protocolos é essencial no processo de definição da arquitetura e projeto do ambiente de IoT, de modo a prover segurança. Desafios como a negação de serviços, interceptação de dados, *spoofing*, ataques à autenticação, entre outros, podem ocorrer caso a definição e escolha do protocolo não seja feita de maneira correta e direcionada pelas especificações e limitações dos dispositivos escolhidos.

É consenso que para termos a camada de rede de forma segura, respeitando os pilares da segurança da informação (Seção 5.4.3), devemos escolher e definir os protocolos e

mecanismos mais adequados para atender tais requisitos, levando em consideração a aplicação a ser desenvolvida[186].

Por exemplo, na camada de rede, observa-se que o uso de TLS (*Transport Layer Security*) e o seu equivalente DTLS (*Datagram Transport Layer Security*) permitem tornar os dados confidenciais, enquanto se encontram em trânsito[187]. Possibilita-se, assim, abranger dispositivos mais ou menos capazes e com diferentes restrições energéticas.

Para cumprir os princípios de segurança fim-a-fim e os requisitos inerentes a uma aplicação de IoT tais como, autenticação fim-a-fim, confidencialidade, integridade e privacidade, é recomendável utilizar uma abordagem distribuída, devido ao fato de que os dispositivos estão se tornando mais inteligentes, capazes de tomar suas próprias decisões de autorização.

Com isso, temos que segurança deve ser integrada ao processo como um todo, desde a etapa de arquitetura, desenvolvimento, integração, testes e homologação, até o descarte. É mandatória uma análise aprofundada dos protocolos e mecanismos que serão utilizados, pois cada caso de uso tem exigências próprias de segurança, arquitetura, limitações dos dispositivos e vulnerabilidades entre outros, para definir corretamente as especificações e configurações[188].

5.2.5.3.2 Possíveis ataques (Negação de Serviço em Massa e outros)

Ataques de negação de serviço em massa – DDoS (*Distributed Denial of Service*) não têm o objetivo direto de invadir e coletar informações, mas sim de exaurir recursos e causar indisponibilidade do alvo, ou seja, consumir a banda disponível ou recursos do equipamento, dispositivo, *software, hardware*, etc. Esses ataques têm sido um dos grandes problemas enfrentados pelas organizações e usuários de Internet ultimamente. Usualmente são utilizadas redes autônomas de agentes de software (*bots*), denominadas *botnets*, que executam, autonomamente, os ataques em massa.[189].

Uma das maiores *botnet* de dispositivos de IoT registradas é a Mirai IoT[190] que conta atualmente com mais de 500.000 dispositivos contaminados pelo *malware* de mesmo nome (Mirai significa "O futuro" em Japonês), utilizada para efetuar diversos tipos de ataques.

186 J. Granjal, E. Monteiro, J.Silva. "Security for the internet of things: A survey of existing protocols and open research issues". IEEE Communications Surveys and Tutorials.

187 Idem.

188 G. Magalhaes. "Estudo de segurança nos principais protocolos da Internet das Coisas, Universidade de Brasília". Instituto de Ciências Exatas Departamento de Ciência da Computação. 2016.

189 Forbes, disponível em: http://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#4f68e31b3046, acesso em fevereiro de 2017.

190 SearchSecurity, disponível em: http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet, acesso em fevereiro de 2017.

Um dos últimos ataques, divulgados amplamente pela mídia internacional[191,192], foram originados por cerca de 100.000 dispositivos de IoT que geraram um volume do tráfego de ataque de aproximadamente 1,2 Tbps, o suficiente para tirar do ar o DYN, um dos maiores provedores de sistema de domínio de nomes – DNS (*Domain Name System*), que deixaram indisponíveis por horas grandes corporações como Twitter, PayPal, Netflix, Spotify e SoundCloud[193].

Ataques do tipo DoS/DDoS são realizados de forma comum através de *jamming*, o qual são mitigados pelo uso da técnica de comunicação DSSS de espalhamento espectral na subcamada PHY. As tecnologias LTE que utilizam camada física com OFDM/SC-OFDM possuem funcionalidade de *Frequency Selective Scheduling* (FSS) que escolhe o melhor conjunto de subportadoras para cada um dos terminais na situação de interferência do canal de transmissão ou mesmo de ataque do tipo *jamming*.

Ataques do tipo captura da informação, ou *man-in-the-middle* são mitigados pelo uso do protocolo RPL, que utiliza a autenticação entre os nós para a criação da árvore de roteamento, ou seja, nenhum Nó faz parte da árvore de encaminhamento, sem que este seja autenticado. O 6LowPAN possui proteção na camada de transporte das mensagens em IPv6, com o uso do TLS ou do DTLS com integridade, autenticação e confidencialidade. O protocolo *Lightweight* IPSEC também pode ser utilizado em redes de IoT.

A segurança na interface aérea dentro da tecnologia móvel *Narrowband IoT* (NB-IoT), por sua vez, utiliza infraestrutura de rede LTE (*Long Term Evolution*) provida pelo método de autenticação EPS (*Evolved Packet System*) *Authentication Key Agreement* (EPS-AKA), que utiliza informações contidas no SIM Card do terminal, além de informações do usuário configuradas no núcleo da rede. Este mecanismo de autenticação EPS-AKA consiste na autenticação mútua tanto do terminal como do Núcleo da rede, com a geração de chaves e de vetores de autenticação, com o compartilhamento da mesma chave de sessão, a qual não é transmitida na rede.

Além do processo de autenticação mútua na interface aérea, tem-se o uso de algoritmo de confidencialidade e integridade das informações de controle e confidencialidade das informações no plano de dados. O padrão não prevê segurança na interface entre a Estação Rádio Base e o Núcleo da rede com uso de protocolos de segurança tal como o IPSEC.

Para o caso do IEEE 802.11p, encontra-se em desenvolvimento o *Security Credential Management System* (SCMS), para a gestão dos certificados, sendo um item crítico devido ao alto requisito de segurança necessário na comunicação veicular.

191 Idem.

192 Kaspersky Lab, disponível em: https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/, acesso em fevereiro de 2017.

193 DYN Corp, disponível em: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/, acesso em fevereiro de 2017.

Além das melhores práticas ou recomendações internacionais já listadas, que tratam da segurança de dispositivos, software, processos de autenticação, upgrade de Software e *Firmware*, entre outros, existem iniciativas e recomendações para minimizar o impacto de um ataque DDoS, que vão desde impossibilitar a entrada na rede (Internet) de um dispositivo inseguro[194]; atuar nos fabricantes de dispositivos para que façam *recall* dos dispositivos conhecidamente inseguros[195]; até a conscientização dos usuários e proprietários dos dispositivos de IoT para que desconectem seus dispositivos da rede quando estes estiverem efetuando um ataque ou ainda serem inseguros e suscetíveis a executarem ataques[196].

No entanto, não é possível eliminar por completo o risco de um ataque DDoS, porém, é possível sim minimizá-lo com algumas ações sejam elas no core da rede ou ainda nos dispositivos.

5.2.6 Questões de gerenciamento

Sob o aspecto de gerenciamento, o modelo de referência IoT especificado pelo ITU-T[197], contempla as camadas de dispositivo (*Device*), rede (*Network*), suporte a serviços e aplicações (*Service Support and Application Support*), e aplicação (*Application*). Em IoT, as Capacidades de Gerenciamento (*Management Capabilities*) seguem o modelo tradicional FCAPS[198], de Falha (*Fault*), Configuração (*Configuration*), Contabilização (*Accounting*), Desempenho (*Performance*) e Segurança (*Security*).

As Competências de Gerenciamento são subdividas em:

- **Competências de Gerenciamento Genéricas (*generic management capabilities*),** que incluem:
  - Gerenciamento de Dispositivo (*device management*) com recursos de ativação, desativação, diagnóstico, atualização de firmware/software, estado operacional;
  - Gerenciamento de topologia de rede local;
  - Gerenciamento de trafego e congestionamento para identificação de congestionamento de rede e reserve de recursos de atendimento a fluxos críticos.
- **Competências de Gerenciamento Específicas (*Specific management capabilities*):** relacionadas aos requisitos de gerenciamento das aplicações de específicas. Como exemplo, a monitoração de linhas de transmissão de energia em um cenário *Smart grid*.

194 Schneier, B., disponível em: https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html, acesso em fevereiro de 2017.

195 Vitkowsky, V., disponível em: https://litigationconferences.com/wp-content/uploads/1955/12/Are-You-and-Your-Insurer-The-Internet-of-Things.pdf, acesso em fevereiro de 2017.

196 Warner, M. R., disponível em: http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CD1BBB25-83E0-494D-B7E1-1C350A7CFCCA, acesso em fevereiro de 2017.

197 ITU, "Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things". Disponível em: https://www.itu.int/rec/T-REC-Y.2060, acesso em janeiro de 2017.

198 TMN recommendation on Management Functions - M.3400.

O modelo de referência proposto pelo "IoT World Forum Architecture Committee"[199] [200] complementa o modelo proposto pelo ITU-T. Enquanto o modelo do ITU-T é mais detalhado nas camadas mais baixas, próximas aos dispositivos, a camada das aplicações está resumida em uma única camada. Tal como ocorre no modelo do ITU-T, o modelo do IoT World Forum considera competências de gerenciamento permeando as várias camadas. No modelo ITU, os *gateways* estão posicionados na camada de dispositivos, enquanto que no modelo IWF estão na camada de conectividade.

De todo modo, o gerenciamento deve ser integrado, permitindo que se consiga estabelecer correlações entre camadas. Exemplo, a indisponibilidade de um determinado recurso (por exemplo, *gateway*, roteador) deve ser detectada, localizada e correlacionada com os eventos derivados, de tal forma que as equipes técnicas concentrem seus esforços na recuperação efetiva do recurso. Vale ressaltar que em um cenário de milhares de recursos gerenciados em áreas geograficamente distribuídas, ações de detecção, localização e recuperação ágeis e precisas são fundamentais para recuperação dos serviços prestados. Conforme o modelo de negócio estabelecido pelo provedor de serviços, os acessos devem ser via APIs (por exemplo, WebServices) e não diretamente com os equipamentos envolvidos.

5.2.7 Conclusões

Na **Camada de Rede, que inclui os equipamentos que promovem a conectividade entre os dispositivos e a nuvem,** há desafios bastante heterogêneos, uma vez que a IoT abrange inúmeros casos de uso para os quais os requisitos de rede são específicos, tais como:

- Para aplicações de tempo real, como a comunicação entre veículos autônomos, a latência de comunicação, assim como o tempo de resposta, são fatores cruciais que estão diretamente relacionados à rede;
- Cenários em que aplicações demandam baixo tráfego de dados e onde existe uma grande dispersão geográfica (por exemplo, agricultura de precisão) impõem um novo paradigma para a evolução das tecnologias, na contramão do que tem sido desenvolvido na última década, onde a maior capacidade de banda era o objetivo predominante.

Devido à diversidade de dispositivos e aplicações, com os mais variados requisitos de qualidade de serviço, a camada de acesso da IoT provavelmente será de natureza heterogênea, com **tecnologias de acesso gerais e de nicho compondo um vasto ecossistema**. As principais tendências dessa camada são elencadas a seguir.

[199] O IWFAC IoT World Forum Architecture Committee é composto por empresas interessadas em criar um framework para acelerar a expansão das iniciativas de IoT.

[200] Cisco, A Proposed Internet of Things Reference Model, disponível em: http://cdn.iotwf.com/resources/72/iot_reference_model_04_june_2014.pdf, acesso em fevereiro de 2017.

As tecnologias **SDN (Software *Defined Network*)** e **NFV (*Network Function Virtualization*)**, que podem ser empregadas não apenas no *backhaul*, mas também no *core*, devem minimizar o impacto da IoT nas redes. Diferentemente do que ocorre com usuários humanos, a comunicação entre as máquinas, tem em geral um caráter periódico e regular, independentemente do período do dia, do dia da semana, do mês ou do ano. Se os dados, que podem ser da ordem de dezenas de bilhões de dispositivos, forem todos para a nuvem, simultaneamente, poderão gerar gargalos de rede. Ambas as tecnologias permitem reconfigurar a rede de maneira rápida e eficiente, reservando recursos e garantindo qualidade de serviço para as aplicações, conforme necessário.

Para as tecnologias de **conectividade de curto alcance *indoor*, tende a ser maior a adoção dos padrões 802.11 do IEEE**. Com o aumento expressivo de dispositivos WLAN em IoT, é provável que seja necessário utilizar uma maior quantidade de soluções baseadas em espectro não licenciado, assim como *femtocells*, para complementar os serviços celulares fornecido pelas operadoras por meio de novas tecnologias complementares às coberturas *outdoor*, por exemplo: LTE-U (*Long Term Evolution – LTE in Unlicensed spectrum*).

Alguns casos de uso devem utilizar **dispositivos móveis pessoais** (*smartphones* e *tablets*) como ***gateways* para sensores e atuadores sem fio**, por meio da tecnologia BLE (*Bluetooth Low Energy*).

As **diversas tecnologias para conectividade de longo alcance devem coexistir para atender a diferentes casos de uso**, utilizando faixa de frequência licenciada (com **tecnologias padronizados pelo 3GPP**), ou não licenciada (**tecnologias** proprietárias ou semiproprietárias **em faixas não licenciadas como Sigfox e LoRa**).

As primeiras implantações dessas redes de longo alcance têm sido baseadas em tecnologias proprietárias ou semiproprietárias. Entretanto, no médio e longo prazos, os padrões baseados no 3GPP, como o Narrowband IoT (NB-IoT), tendem a ganhar espaço onde houver cobertura de rede celular, uma vez que se valerão desta infraestrutura e da operação preexistente.

Com respeito aos protocolos, o **principal habilitador para tratar** dos elementos conectados à rede **provavelmente será o IPv6**. O IPv6 oferece uma série de vantagens, como o acesso a mão de obra familiarizada, o fato de ser o padrão mais utilizado da indústria, além de proporcionar uma série de melhorias de segurança em relação à versão 4. Para contornar as limitações em dispositivos restritos, têm sido desenvolvidos diversos protocolos, como 6LoWPAN (IPv6 *over Networks of Resource-constrained Nodes*), CoAP (*Constrained Application Protocol*) e MQTT (*Message Queuing Telemetry Transport*).

5.3 Suporte a serviços e aplicações

5.3.1 Introdução

A camada de suporte à aplicação concentra a infraestrutura, *softwares* e técnicas computacionais habilitadoras para o desenvolvimento e implantação de aplicações em Internet das Coisas. Trata-se da camada que permitirá transformar os dados em informação e ações inteligentes. A seguir serão apresentados o estado corrente e as principais tendências relevantes a IoT desta camada.

5.3.2 Infraestrutura computacional

5.3.2.1 Impacto de IoT nos *data centers*

A conectividade gerada pela IoT está aumentando rapidamente, atingindo uma grande variedade de aparelhos, sensores e sistemas. O tráfego gerado pela grande quantidade de aparelhos conectados, bem como as novas demandas de armazenamento e processamento, irá causar um maior *stress* nas infraestruturas responsáveis por receber e armazenar esses dados para análise. Por exemplo:

- Sistemas de *backend* devem se adaptar a uma arquitetura da IoT de forma a acompanhar as novas demandas de armazenamento e processamento exigidas pela IoT;
- Sistemas de acesso corporativos e sistemas hospedados remotamente podem ser sobrecarregados sem um planejamento adequado;
- Sistemas de armazenamento de maior capacidade serão exigidos para armazenar esse novo volume de dados;
- A IoT exigirá um controle unificado, uma maior coordenação entre recursos distribuídos ao longo de diversos *data centers*, além da capacidade de se adaptar rapidamente às variações de demanda. Prevê-se que os *data centers* não devem ficar mais concentrados em uma única instalação, podendo estar próximos das bordas e dos

aparelhos, para que sejam mitigados gargalos de *links* e da latência excessiva inerente à transmissão de dados a locais mais distantes;

- Para acompanhar a necessidade de aproximação da borda, mini e micro *data centers* tendem a se tornar auto gerenciáveis, em que se torna menos importante a seleção do melhor *hardware* e mais importante a automatização do ambiente e a seleção dos melhores métodos de processamento inicial e a filtragem dos dados antes que eles sejam enviados para outras localidades como um *data center* central.

O novo paradigma para a IoT será encontrar o lugar mais adequado para processar os dados (por exemplo, nos dispositivos, nuvem, ou em algum elemento entre ambos), com o menor custo, gerando as informações que agreguem maior valor para as organizações.

5.3.2.2 Data Centers

5.3.2.2.1 Infraestrutura

Processadores

Novas tecnologias são necessárias para elevar a capacidade de processamento dos *data centers*, de forma a atender as altas demandas de processamento e de análise do enorme volume de dados gerados pelos aparelhos conectados aos servidores que compõem os *data centers*, onde estes dados serão tratados.

A união dos processadores atuais com as tecnologias de FPGA abre um novo leque de possibilidades, em que os processadores se tornam capazes de se adaptar a cenários, ajustando sua arquitetura para modelos mais adequados às diferentes demandas de processamento. Também é possível modificar áreas do processador para lidar de forma mais adequada com demandas paralelas de processamento inerentes à análise de grandes volumes de dados.

Para atender às demandas de processamento de grandes volumes de dados e *machine learning*, outra tendência para *data centers* vem na adição de GPUs (Processadores Gráficos) aos servidores, cuja arquitetura se sobressai em casos onde o processamento em tempo real de enormes volumes de dados se faz necessário. O mercado de GPUs para *data centers* vem sendo abordado principalmente por dois grandes fabricantes, NVIDIA e AMD, que têm expandido seu mercado para outras áreas, além do processamento gráfico, usando GPUs.

O uso de CPUs e GPUs é complementar, pois cada alternativa se sobressai em um modelo de aplicação diferente. No entanto, o uso conjunto de CPUs e GPUs em *data centers* tende a aumentar significantemente as capacidades dos servidores para as demandas de "*Big Data*" provenientes da IoT.

Além disso, existe a tendência do uso de servidores com processadores ARM, que possuem uma maior capacidade de paralelização das aplicações, apesar do desempenho

ligeiramente inferior comparado com processadores x86. Atualmente, o uso de servidores ARM é apoiado por uma maior maturidade de aplicações desenvolvidas para essa arquitetura. Se defende que servidores baseados no modelo ARM teriam reduções consideráveis de consumo de energia em relação aos *data centers*.

Virtualização em *Hardware*

A crescente demanda por virtualização faz com que o *hardware* trate diretamente com a virtualização. A virtualização de I/Os é uma tecnologia emergente que se faz cada vez mais presente em servidores, e permite que interfaces físicas sejam enxergadas como múltiplas interfaces virtuais com acesso direto às funcionalidades do *hardware*. A virtualização de interfaces, como, por exemplo, interfaces de rede e interfaces PCIe, minimizam o número de camadas necessárias para que essas interfaces sejam oferecidas para máquinas virtuais, tornando o fluxo de dados mais eficiente.

5.3.2.2.2 Arquitetura

Infraestrutura Convergente

Em *data centers* tradicionais, a infraestrutura é organizada em silos, contendo conjuntos de recursos dedicados a tecnologias ou a modelos de aplicações específicos. Por exemplo, o *data center* é segmentado em áreas de processamento, armazenamento e gerência; cada área tem um *hardware* dedicado à execução dessas funções. Esta organização cria dependências com fornecedores especializados para cada tipo de recurso. A infraestrutura convergente consiste na agregação dessas múltiplas funções em um único chassi contendo o *hardware* necessário para cada função. Dessa forma, é possível centralizar o gerenciamento de recursos, consolidar sistemas, reduzir incompatibilidades, minimizar o espaço ocupado pelo *hardware* e otimizar a distribuição dos recursos existentes por meio da implementação de conjuntos de recursos virtualizados de computação, armazenamento e rede, que podem ser compartilhados por uma variedade de aplicações, usando políticas coletivas de alocação. Além disso, a infraestrutura convergente consegue alavancar o potencial de sistemas em nuvem por centralizar gerências de conjuntos variados de recursos.

Infraestrutura Hiperconvergente

Em uma infraestrutura hiperconvergente, por sua vez, a infraestrutura passa a ser definida por *software*, podendo ser executada por *hardwares* de prateleira e deixando de ser dependente de *hardwares* específicos, resultando em uma maior aproximação dos recursos computacionais, de armazenamento, de rede e de virtualização. Dessa forma, a expansão da capacidade computacional é possível com a adição de mais nós ao conjunto.

As principais vantagens da infraestrutura hiperconvergente são:

- Permitir que todas as camadas de *software* e *hardware* sejam gerenciadas por uma única plataforma administrativa responsável pela integração de todos os sistemas;
- Aumentar a flexibilidade na alocação de recursos, permitindo direcionar o *hardware* disponível para atender às maiores demandas funcionais/*software*;
- Aumentar a velocidade da adaptação e atualização das funções disponíveis, para atender às demandas, sem necessidade de substituição do *hardware*;
- Reduzir os custos de montagem do *data center,* devido ao fato que *hardwares* de prateleira são mais econômicos, por serem menos especializados;
- Permitir que *data centers* tenham tamanhos adequados às necessidades, podendo ter tamanho reduzidos, com um investimento inicial baixo, porém rapidamente escaláveis quando necessário.

Mini e Micro Data Centers

Data centers precisam se adaptar para atender às demandas trazidas pela IoT, em que se torna importante aproximar os novos aparelhos e sensores conectados aos *data centers,* com o objetivo de evitar gargalos de rede e diminuir a latência das requisições. *Data centers* precisam ser mais ágeis, flexíveis e escaláveis.

Para suprir as novas exigências de IoT, prevê-se a aproximação dos *data centers* das bordas, onde *data centers* menores e otimizados são distribuídos em uma variedade de localidades, aproximando-os das demandas de seus clientes. Essa aproximação requer uma abordagem diferente para a construção de *data centers*, que tradicionalmente ocupam áreas extensas e demandam uma infraestrutura de apoio complexa, como, por exemplo, subestações de energia e torres de refrigeração para ar condicionado.

Com o modelo de infraestrutura hiperconvergente, torna-se muito mais simples a criação de mini e micro *data centers*, que trazem as seguintes vantagens:

- Suprir as necessidades de uma localidade utilizando uma pequena quantidade de *hardware,* de menor custo e maior flexibilidade, devido ao fato que os recursos dos *data centers* são definidos por *software*;

- Exigir a completa automação dos sistemas, além de permitir a gestão remota, diminuindo a necessidade de funcionários trabalhando nas localidades onde os *data centers* estão presentes;
- Possibilitar a construção modular e conteinerizada, onde sistemas de refrigeração, energia e segurança já estão presentes;
- Permitir que *data centers* sejam transportados e ligados rapidamente, inclusive em locais remotos ou temporários, possibilitando que empresas se adaptem e se espalhem mais rapidamente, atendendo às variações nas demandas de seus clientes;
- Reduzir custos de consumo de banda devido à diminuição do tráfego nos *backbones*;
- Aproximar ao conceito de "*Cloudlets*", onde pequenos ambientes de nuvem dedicados e otimizados são utilizados para executar as aplicações, que possuem uma maior necessidade de proximidade com a borda, compondo um elemento intermediário entre o aparelho e a nuvem[201].

Data Center as a Service

O uso do modelo de *data centers* como um serviço pelas companhias responsáveis pela infraestrutura computacional por trás de aplicações de IoT representa outra forma de suprir a necessidade de aproximação da borda, demandada pelo crescimento dos dados gerados pela IoT.

Nesse modelo, empresas oferecem espaço físico e infraestrutura de suporte (energia elétrica, refrigeração, segurança) para outras empresas que desejam adicionar capacidade computacional naquela localidade. Além do espaço, fornecedores de *data center* como serviço podem oferecer parte de sua planta de servidores, rede e armazenamento. O uso da infraestrutura de provedores de acesso também se encaixa neste modelo, onde os provedores já possuem infraestrutura em pontos de presença próximos a usuários.

201 Disponível em https://www.microsoft.com/en-us/research/wp-content/uploads/2016/11/Micro-Data-Centers-mDCs-for-Mobile-Computing-1.pdf, acesso em abril de 2017.

5.3.2.2.3 Gerência e Automação

Automação do *Data Center*

A automação dos *data centers* será primordial para que o modelo de *data centers* distribuídos seja sustentável. A existência de múltiplos micros *data centers*, localizados inclusive em locais de difícil acesso, tornará a autonomia desses ambientes essenciais. *Data centers* deverão ser gerenciados por *softwares* e não por pessoas, oferecendo recursos de telemetria remoto e sendo capazes de adaptar a sua infraestrutura em tempo real.

Esse tipo de gestão permite adicionar uma camada de gerência com uma visão mais completa da alocação de recursos no *data center*, de forma a permitir uma melhor utilização desses, melhorar a disponibilidade dos serviços, além de abrir um canal para que sejam feitas previsões de demanda, para que o *data center* possa crescer ou reduzir carga para economizar energia.

5.3.2.3 Cloud

5.3.2.3.1 Modelos de serviço

IaaS

O modelo mais básico usado por fornecedores de *cloud*, entre os modelos de serviços de *cloud* existente, é o IaaS (Infraestrutura como um serviço), na qual é oferecida infraestrutura computacional por meio de máquinas virtuais, que fazem o papel de servidores virtuais com capacidade de processamento, memória, rede e disco. Os recursos utilizados são obtidos por meio de agrupamentos de recursos virtualizados presentes em grandes *data centers*.

A necessidade de sistemas mais centralizados para processamento de dados será sustentada pelo modelo de infraestrutura como um serviço, na qual serão alocados os recursos necessários para atender às novas demandas computacionais, principalmente dos pequenos desenvolvedores de aplicações e aparelhos que não possuem capacidade de construir seus próprios *data centers*.

Além disso, os fornecedores de IaaS dependerão de um controle mais fino e da melhoria nos métodos de gestão sobre a localização das máquinas virtuais, contratadas, de forma que elas fiquem mais distribuídas e próximas aos usuários, de acordo com a necessidade dos clientes em contextos de nuvens compostas por múltiplas regiões.

PaaS

No modelo PaaS (Plataforma como um serviço), o fornecedor apresenta uma plataforma de desenvolvimento de aplicações na nuvem, na qual é oferecida toda a infraestrutura, além de sistemas de apoio à aplicação, como filas de mensagens e bancos de dados. Apesar de diminuir a complexidade no desenvolvimento de novas aplicações, o modelo PaaS torna o cliente mais dependente das aplicações do fornecedor de PaaS.

Para atender às grandes demandas de processamento de dados dos novos aparelhos conectados, é provável que cresça a demanda por serviços capazes de facilitar o recebimento e tratamento de dados. No modelo de PaaS, serviços de "*Big Data*" serão demandados para a análise de grandes volumes de dados. Desenvolvedores que desejam mais velocidade e facilidades no desenvolvimento de novas aplicações, precisarão que suas *clouds* forneçam sistemas que facilitem o desenvolvimento de aplicações para tratamento de dados.

Além de serviços de apoio ao modelo "Big Data", serviços como *middlewares* devem se tornar importantes para abstrair a comunicação com os *devices* e a variedade de protocolos existentes. O oferecimento de *middleware* como parte de PaaS trará diferenciais para as plataformas de nuvem que desejam atender o mercado de IoT.

5.3.2.3.2 Gerenciamento

Frameworks

Para atender às demandas que a IoT depositará sobre os ambientes de armazenamento e processamento de dados, faz-se necessário o uso de *frameworks* que sejam capazes de entregar uma visão unificada e realizar a abstração do *hardware* de um *data center*, provendo isolamento entre diversos clientes e fornecendo um ambiente onde as aplicações possam ser executadas. Para tal, múltiplas formas de realizar esses objetivos estão em evolução, entregando para o usuário da nuvem formas de instanciar serviços, tanto em máquinas virtuais quanto em *containers*.

O uso de sistemas operacionais para nuvem em *data centers* permite que os recursos de *hardware* sejam controlados por meio de interfaces que dão ao administrador a capacidade de distribuir os recursos disponíveis entre múltiplos usuários/locatários, de forma que cada usuário tenha uma visão unificada e isolada dos recursos que lhe foram reservados. Usualmente, é oferecida uma interface gráfica com a intenção de facilitar a navegação e a exibição do ambiente, além de estatísticas relevantes para usuários e administradores.

Os sistemas operacionais de nuvem são constituídos por múltiplos módulos, cada um responsável por parte das funções, desde gerenciamento do *hardware* do *data center* até a adição de camadas de abstração para o fornecimento de serviços mais complexos no modelo PaaS, por exemplo.

Outra forma de gerenciar o *hardware* disponível no *data center* é por meio de gerenciadores de *cluster*, que entregam aos usuários uma visão unificada dos recursos do *data center*, e oferecem a capacidade de criar tarefas e aplicações isoladas, onde parte dos recursos disponíveis podem ser reservados ou priorizados para aplicações críticas. Ambos tipos de sistemas provêm isolamento e ambientes de execução para os usuários por meio da criação de *containers* ou máquinas virtuais.

5.3.2.3.3 Processamento

Conteinerização

O modelo arquitetural para desenvolvimento de aplicações, baseado em serviços leves e menos interdependentes de micro serviços, é o mais apoiado atualmente para o desenvolvimento de aplicações para IoT. Novas tecnologias de *containers* estão em constante evolução e têm apoiado este modelo de desenvolvimento, estando cada vez mais presentes nos ambientes de nuvem e trabalhando de forma complementar com as tecnologias de máquinas virtuais já estabelecidas. As principais vantagens do uso de *containers* são:

- Otimizar os recursos de *hardware*, por diminuir a dependência da execução de um *hypervisor* e de um sistema operacional para cada uma das máquinas virtuais executadas;
- Aumentar a flexibilidade e velocidade de execução, por serem mais leves e baseados em padrões bem definidos de implementação;
- Permitir que sistemas de orquestração criem *containers* mais próximos a *data centers* adjacentes às bordas, onde a demanda de tráfego e processamento gerado por clientes é maior;
- Abrir espaço para a virtualização dos aparelhos e sensores de IoT, que podem atuar como "sombras" dos *devices*, mantendo o estado dos aparelhos para aplicações que necessitem dessas informações, mesmo quando o sensor está momentaneamente inacessível pela rede.

Sistemas Operacionais

Novos modelos especializados de sistemas operacionais têm surgido para atender às demandas de IoT nos *data centers*, caracterizadas pelo uso de *containers* e a virtualização de dispositivos. Sistemas operacionais especializados na execução de *containers* possuem as seguintes vantagens:

- Prover um maior cuidado no isolamento e segurança dos processos associados aos *containers*, bem como otimizações no *kernel* para atribuição mais eficiente de recursos, permitindo um maior número de *containers* em um mesmo sistema;

- Simplificar o desenvolvimento de aplicações por desenvolvedores que trabalham com *containers*, complementando outros componentes em um modelo de PaaS para aplicações de IoT;
- Facilitar a atualização e adaptabilidade dos ambientes de execução frente às mudanças nos sistemas e ao rápido surgimento de novos aparelhos conectados.

Alguns exemplos de sistemas operacionais especializados são Windows Nano Server, CoreOS, RancherOS, Photon OS e Project Atomic.

5.3.2.3.4 Armazenamento

Armazenamento de Objetos

Na arquitetura de armazenamento de objetos, dados são armazenados como objetos sem tipos ou estruturas definidas, diferentemente do que ocorre em outras arquiteturas de armazenamento, como o modelo de armazenamento em blocos ou em arquivos, que se demonstram ineficientes para comportar a velocidade, diversidade e crescimento massivo de dados gerados pela IoT.

No modelo de armazenamento de objetos, cada objeto contém o próprio dado, além de metadados associados a um identificador único. Consequentemente, é possível fornecer as seguintes capacidades:

- Interfaces programáveis por aplicações e funções para gerência de dados com replicação e distribuição mais granular em nível de objetos, tornando possível a retenção de enormes volumes de dados não estruturados, de forma econômica e escalável. Este tipo de sistema é usado hoje para, por exemplo, armazenar fotos no Facebook e músicas no Spotify;
- Funcionamento em conjunto com sistemas para análise de grandes volumes de dados, pois a inclusão de metadados (por exemplo, datas, sentimento do usuário, localização) aos objetos aumenta significantemente a capacidade de classificação e mineração dos dados.

Software Defined Storage

Uma das alternativas para evitar as limitações presentes nas arquiteturas atuais é o armazenamento definido por *software (Software Defined Storage)*, na qual características tipicamente encontradas em *hardware* são movidas para uma camada de *software*, eliminando a dependência de *hardwares* proprietários e permitindo maior flexibilidade, velocidade e escalabilidade para atender às demandas de armazenamento provenientes da IoT. Outras vantagens do modelo definido por *software* são:

- Diminuição do custo e atendimento das crescentes exigências de armazenamento, permitindo que administradores de uma nuvem escolham um *software* único para todos os *devices* de armazenamento, sem impactos significativos de custo ou desempenho, como feito para a infraestrutura virtualizada computacional;
- Compatibilidade com arquitetura hiperconvergente de *data centers*, na qual ocorre uma grande aproximação do armazenamento com os recursos computacionais virtualizados, pelo fato de todos serem parte do mesmo *hardware*, permitindo, assim, uma melhora nas taxas de leitura e escrita entre as áreas de armazenamento e os sistemas responsáveis pelo processamento e análise dos dados coletados;
- Horizontalização da arquitetura que direciona e redistribui os dados, eliminando pontos únicos de acesso e potenciais gargalos na entrada de dados.

5.3.2.3.5 Orquestração

Escalonamento e Elasticidade

O uso de sistemas de orquestração de serviços inteligentes tem sido cada vez mais importante em cenários de IoT com ambientes de nuvem, os quais estão instanciados os serviços de recebimento e tratamento de dados dos diversos aparelhos, de forma distribuída.

Sistemas inteligentes de orquestração permitem que os serviços sejam distribuídos fisicamente para se adaptar às demandas de clientes, bem como tornam automática a solução de problemas, como adaptação a variações de carga, movimentação de serviços, detecção e correção de falhas, além de avisarem ao operador quando ocorrem problemas críticos que não podem ser resolvidos de forma automatizada. A maioria dos ambientes de nuvens públicas e privadas tendem a integrar uma variedade de modelos de sistemas de orquestração de serviços. Um sistema de orquestração é constituído por três principais conjuntos de componentes:

- **Camada de modelagem das aplicações**: responsável por modelar a aplicação que será utilizada, definindo parâmetros de funcionamento e as peças que a compõe;
- **Camada de integração**: responsável por integrar com os ambientes de nuvem ou de contêiner sobre o qual será executada a orquestração e instanciar o serviço de acordo com o modelo previamente definido;
- **Camada de monitoração do estado dos serviços e aplicações:** permite que a camada de integração tome ações para que o sistema se recupere de falhas e se adapte às variações de carga, de modo a manter a aplicação funcionando em um estado ótimo.

No modelo de aplicações da IoT, a orquestração de serviços se torna peça fundamental, visto que as aplicações cada vez mais tendem a serviços pequenos e altamente

distribuídos, o que torna muito difícil que o controle do sistema seja feito por humanos, tornando a automatização dos processos cada vez mais importante.

5.3.2.4 Tendências

Para se adequar às demandas da IoT, a infraestrutura computacional fornecida pelos *data centers* terá que se adaptar aos novos modelos de geração e armazenamento de dados necessários para suportar as novas aplicações.

A tendência é que sejam criados novos micros *data centers* distribuídos e mais próximos das bordas, bem como dos clientes, seguindo um modelo de *cloudlets*, onde ambientes de *cloud* reduzidos executam aplicações especializadas no tratamento e filtragem inicial dos dados e na resposta a demandas que exigem baixa latência e maior agilidade nas respostas.

Os *data centers* devem ficar cada vez mais automatizados, com todas as suas camadas de *hardware* virtualizadas e definidas por *software*. Os modelos de armazenamento de dados devem ser unificados por meio de interfaces centralizadas e bem definidas. Há também uma tendência de migração de aplicações em máquinas virtuais para o modelo de *containers*, além da adição de sistemas de orquestração de serviços mais inteligentes e dinâmicos.

5.3.3 *Middleware*

O *middleware* de IoT corresponde a uma camada de *software* que conecta/integra os componentes da solução, isto é, os dispositivos, os serviços de suporte e as aplicações; abstraindo sua heterogeneidade e complexidade de forma a simplificar e acelerar o desenvolvimento e a implantação de soluções de IoT.

Os casos de uso de IoT são abrangentes, envolvendo os mais diferentes tipos de dispositivos e serviços. Devido à heterogeneidade e aos novos dispositivos e serviços surgindo constantemente, torna-se difícil sua padronização; sendo imprescindível uma camada de *software* que os integre, de forma que as aplicações se concentrem nas regras de negócio. Além disso, existe um conjunto de funcionalidades, tais como virtualização, gerenciamento de dispositivos e processamento e armazenamento de dados/eventos que se aplicam a maioria dos casos de uso em IoT. Logo, um *middleware* que agregue todo esse valor é uma componente chave para facilitar e reduzir o custo/tempo de desenvolvimento e implantação em IoT.

5.3.3.1 Principais funções

Apesar de ser um habilitador para o desenvolvimento e implantação de soluções em IoT, não existe um consenso em relação às fronteiras do *middleware*, ou seja, em relação às fronteiras entre *middleware*, serviços de suporte a aplicações e aplicações. Uma vertente advoga que o *middleware* é simplesmente um "barramento de *software*" para conectar os

componentes da solução, enquanto, outra defende que o *middleware* agrega funções como *dashboard*, armazenamento, análise de dados e aprendizagem de máquinas.

Um escopo muito abrangente dificulta a análise e a comparação das abordagens. Portanto, optamos por limitar o *middleware* a uma camada de *software* que suporta um conjunto **básico** e **essencial** de funcionalidades, às quais se aplicam a maioria dos casos de uso de IoT, destacando-se:

- **Mediação com dispositivos**: conecta/integra os diferentes dispositivos de IoT ao *middleware*, permitindo a coleta de dados, o gerenciamento e a atuação, independentemente do protocolo ou modelo de comunicação adotado pelo dispositivo. Por meio do encapsulamento de protocolos M2M, como MQTT, COAP, DDS, XMPP e AMQP, a mediação facilita a integração dos dispositivos que compõem a solução, permitindo que o *middleware* forneça uma abstração dos dispositivos. Portanto, serviços e aplicações não precisam focar em integração e, sim, nos dados gerados. Isto hoje é possível para dispositivos e *middlewares* bem específicos. No entanto, em um contexto mais abrangente, ainda se faz necessária uma maior padronização dos modelos de dados dos dispositivos.
  Além disso, existem preocupações com relação à segurança e à privacidade, uma vez que o mediador faz uso da camada de redes. Consequentemente, o mediador deve garantir um canal seguro de comunicação, seja pelo uso de protocolos seguros, mecanismos de autenticação ou por meio de arquiteturas que garantam o atendimento dos requisitos de segurança;
- **Virtualização e gerenciamento de dispositivos**: abstrai os dispositivos físicos, virtualizando-os no *middleware* e permitindo gerenciar o seu ciclo de vida. A virtualização de dispositivos agrega ao *middleware* a capacidade de abstrair dispositivos físicos, permitindo que se foque no modelo de dados, facilitando, por exemplo, a criação de gêmeos (*twins*) digitais e o desenvolvimento de aplicações. Além de um mapeamento 1:1 (físico: virtual), a virtualização permite a criação de dispositivos virtuais que associem atributos de mais de um dispositivo físico ou virtual, agregando diversas possibilidades no contexto de aplicações. Além disso, casos de usos com centenas ou milhares de dispositivos são comuns, e gerenciá-los e de maneira individualizada sobre cada dispositivo mostra-se desafiador. Dessa maneira, um serviço que permita centralizar esse gerenciamento é vital para o sucesso da solução de IoT. Neste contexto, o protocolo de gerenciamento de dispositivos LWM2M (Lightweight M2M) tende a ser o padrão a ser seguido, sendo, para a IoT, o que o OMA-DM é para dispositivos móveis. Atualmente, este protocolo é encapsulado sobre COAP, o que, de certa maneira, é restritivo, pois obriga que os dispositivos suportem este protocolo. Visando uma adoção em larga escala, é necessário que o protocolo de comunicação se torne mais agnóstico;
- **Processamento e armazenamento de dados/eventos**: processa e armazena para acesso posterior dados/eventos de diversas naturezas, volumes e taxas gerados por dispositivos por serviços de suporte a aplicações. Neste contexto, bancos de dados não

relacionais[202], como MongoDB[203], Cassandra e Hadoop/HBase[204], são apontados como a melhor alternativa para o armazenamento de dados em IoT[205]. No entanto, bancos de dados SQL podem continuar sendo aplicáveis para casos de uso em que os dados são estruturados e uniformizados. Como resultado, dada a heterogeneidade das aplicações de IoT, a escolha do tipo de armazenamento depende do caso de uso, o que traz a necessidade de os *middlewares* serem capazes de se integrarem a diferentes modelos/base de dados para não serem restritivos. Além disso, *middlewares* devem escalar, rotear, filtrar, agregar processar os dados/eventos de maneira inteligente, baseada em contextos e em prioridades. No caso em que uma mesma instância do *middleware* processa e armazena dados de diferentes clientes/usuários, surge o desafio de isolamento de dados/contextos, forçando a arquitetura do *middleware*, assim como o armazenamento, serem *multitenant*;

- **Mediação com os serviços de suporte a aplicações e aplicações**: agrega os serviços de suporte a aplicações ao *middleware*, aumentando o seu escopo funcional; e as aplicações de IoT, permitindo-as acessar os serviços/recursos do *middleware*. *Web-services*[206] consolidam-se como a tecnologia de interface para comunicação e integração de serviços e aplicações ao *middleware*, com predominância de interfaces do tipo REST (*Representational State Transfer*)[207], por serem mais leves. No entanto, existe uma falta de padronização no protocolo de comunicação, sendo que cada *middleware* adota a sua própria interface/API. A falta de padronização dificulta tanto a interoperabilidade entre *middlewares* quanto a migração de aplicações de um *middleware* para outro.

Além dos requisitos funcionais acima citados, os *middlewares* devem satisfazer um conjunto de requisitos não funcionais, destacando-se:

- **Escalabilidade**: capacidade de escalar para atender ao aumento do número de dispositivos e/ou serviços. O ideal é que a plataforma seja elástica, capaz de se adaptar automaticamente ao aumento ou diminuição da demanda por recursos;
- **Robustez**: continuidade das operações, mesmo em condições de falha de componentes individuais, a fim de garantir o atendimento dos serviços. Logo, a robustez precisa ser tratada em todos os aspectos, como comunicação, processamento e armazenamento de dados/eventos, etc;

202 eSTREAM competition. European Network of Excellence for Cryptology, disponível em: http://www.ecrypt.eu.org/stream, acesso em janeiro de 2017.

203 MongoDB, disponível em: https://www.mongodb.com/, acesso em fevereiro de 2017.

204 Hadoop/HBase disponível em: http://hbase.apache.org/, acesso em fevereiro de 2017.

205 Emil Berthelsen. Why nosql databases are needed for the internet of things. Research Note, Machina Research (Apr 2014), disponível em: https://machinaresearch.com/report/research-note-why-nosql-databases-are-needed-for-the-internet-of-things/, acesso em fevereiro de 2017.

206 Eric Newcomer. Understanding Web Services: XML, WSDL, SOAP, and UDDI. 2002. Primeira Edição. Addison-Wesley Professional.

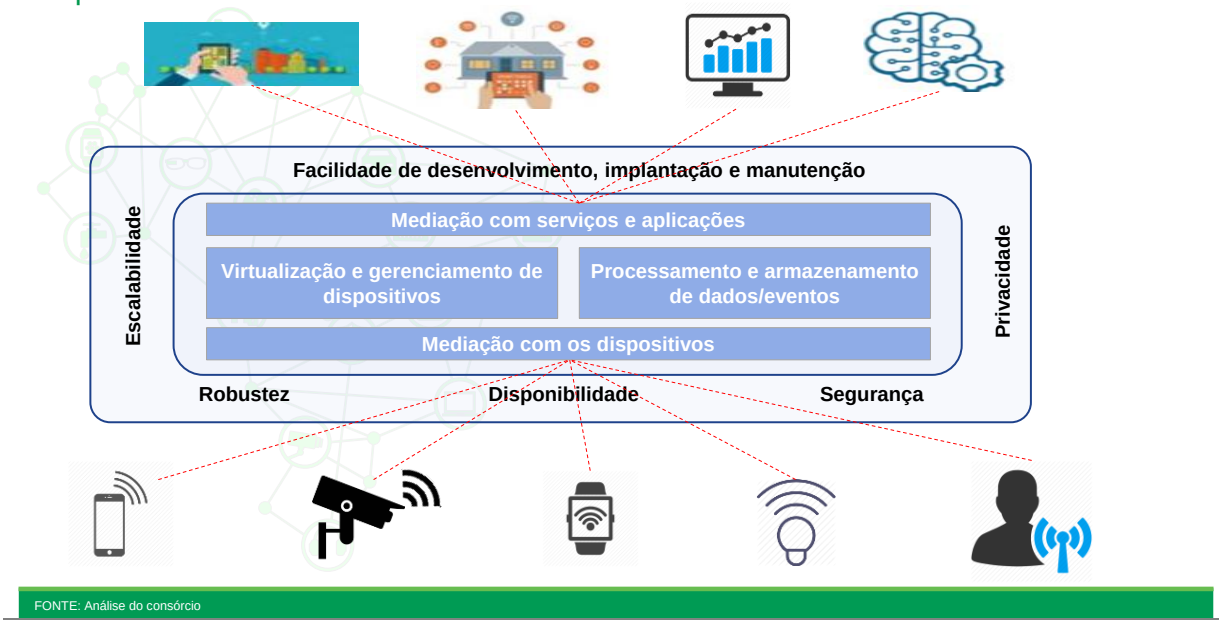
207 Leonard Richardson, Sam Ruby. RESTful Web Services. 2007. Primeira Edição. O'Reilly Media.

- **Segurança e privacidade**: proteção da segurança de todos os componentes do *middleware*, de forma a evitar ameaças e riscos. Como parte dos dados sob responsabilidade do *middleware* envolve dados pessoais, de localização ou informações sigilosas, torna-se necessário garantir sua privacidade e inviolabilidade;
- **Facilidade de desenvolvimento, implantação e manutenção**: capacidade de ser facilmente extensível, seja por meio de *plugins* ou novos serviços, assim como de fácil implantação no ambiente a que se destina (seja um *gateway* ou servidor ou nuvem) e de fácil manutenção. Esses requisitos colaboram para seu sucesso e popularidade.

Do ponto de vista funcional, o *middleware* de IoT pode ser sintetizado na arquitetura representada no QUADRO 33.

QUADRO 33

Arquitetura funcional do *middleware* IoT



FONTE: Análise do consórcio

5.3.3.2 Mediação com os dispositivos (MQTT, CoAP, XMPP, etc)

Para comunicação M2M, existe um conjunto de protocolos, como MQTT (*Message Queuing Telemetry Transport*), CoAP (*Constrained Application Protocol*), XMPP (*Extensible Messaging and Presence Protocol*), DDS (*Data Distribution Service*) e AMQP (*Advanced Messaging Queue Protocol*), que têm se destacado como protocolos para IoT[208,209] e serão detalhados a seguir:

- **MQTT**[210]: protocolo orientado à mensagem do tipo *publish/subscribe*, que utiliza um *broker* para desacoplar as entidades. O protocolo é leve, utiliza TCP, que pode ser oneroso para cenários com conexão instável ou restrições de consumo de energia; suporta três níveis de confiabilidade (*Fire and Forget*, *Delivered at Least Once* e *Delivered*

208 Buyya R.. Internet of Things Principles and Paradigms. 2016. Elsevier.

209 Understanding The Protocols Behind The Internet Of Things. Disponível em: http://electronicdesign.com/iot/understanding-protocols-behind-internet-things, acesso em fevereiro de 2017.

210 MQTT. Disponível em: http://mqtt.org/, acesso em fevereiro de 2017.

Exactly Once) e segurança via TLS. Este protocolo é otimizado para coleta e análise centralizada de dados, por exemplo, conectando dispositivos à nuvem;

- **CoAP**[211]: segue um modelo *request/reply* de transferência de dados, similar ao HTTP, mas otimizado para dispositivos com recursos restritos. Trata-se de um protocolo *Restful*, leve, utiliza UDP, que pode exigir um tratamento dos pacotes em relação à transmissão e ordenação na camada de aplicação; suporta transmissão de mensagens, com e sem confirmação de recebimento, e segurança via DTLS;
- **XMPP**[212]: protocolo projetado para mensagens instantâneas; pode ser facilmente interpretado por humanos comparado com outros protocolos de IoT. Como é baseado em XML, as mensagens têm um tamanho considerável, não sendo ideal para casos de uso com restrição de banda; é considerado um protocolo lento, utiliza TCP e implementa segurança via SASL e TLS;
- **DDS**[213]: protocolo otimizado para processamento distribuído e aplicações de tempo real, ideal para comunicação entre dispositivos; pode ser utilizado para comunicação entre dispositivo e servidor. Trata-se de um protocolo orientado à mensagem do tipo *publish/subscribe* totalmente distribuído; suporta diferentes níveis de qualidade de serviço; utiliza TCP ou UDP e segurança via TLS ou DTLS;
- **AMQP**[214]: segue um modelo *publish/subcribe* baseado em filas, em que um dos principais objetivos é evitar a perda de dados. Tem suporte a transacionalidade e prioridades; utiliza TCP e segurança via TLS. No contexto de IoT, apesar de poder ser utilizado em dispositivos, o principal caso de uso deve ser na comunicação entre *middlewares* e serviços.

Os principais protocolos de comunicação de IoT estão listados na TABELA 12 a seguir.

TABELA 122 PROTOCOLOS DE COMUNICAÇÃO IOT

Protocolo	Paradigma	Transporte	Segurança	Caso de uso
MQTT	Publish/Subscribe	TCP	TLS	Coleta de dados em dispositivos
CoAP	Request/Response	UDP	DTLS	Gerenciamento / Coleta de dados em dispositivos restritos

211 CoAP. Disponível em: http://coap.technology/, acesso em fevereiro de 2017.
212 XMPP. Disponível em: https://xmpp.org/, acesso em fevereiro de 2017.
213 DDS. Disponível em: https://xmpp.org/, acesso em fevereiro de 2017.
214 AMQP. Disponível em: https://www.amqp.org/, acesso em fevereiro de 2017.

Protocolo	Paradigma	Transporte	Segurança	Caso de uso
XMPP	Request/Response Publish/Subscribe	TCP	SASL/TLS	Conexão dos dispositivos com pessoas
DDS	Publish/Subscribe	UDP/TCP	DTLS/TLS	Missão crítica / Tempo real
AMQP	Publish/Subscribe	TCP	TLS	Integração de sistemas

Apesar de serem considerados protocolos para comunicação M2M, os protocolos de comunicação descritos acima têm características distintas e são apropriados para casos de uso distintos. Por isso, esses protocolos devem coexistir no ecossistema de IoT, assim como novos protocolos devem surgir.

5.3.3.3 Arquiteturas

A heterogeneidade dos cenários de IoT origina requisitos específicos, por exemplo, em relação à tolerância, latência, volume, natureza e privacidade dos dados/eventos; levando a diferentes arquiteturas de *middleware*. Existe uma tendência por três arquiteturas: *Service-based*, *Cloud-based* e *Edge-based*[215,216,217,218,219,220].

Na arquitetura *Service-based* (ver o QUADRO 34), o *middleware* adota uma arquitetura do tipo SOA (*Service Oriented Architecture*), na qual as funcionalidades do *middleware* baseiam-se em serviços. Trata-se de uma arquitetura escalável e de alto-desempenho, porém com custos de implantação, demandando uma infraestrutura de nuvem ou *gateways* com alto poder computacional. Neste tipo de arquitetura, o *middleware* não está "amarrado" a uma infraestrutura, o que dá a liberdade de implantação em nuvens privadas ou até mesmo em *gateways*, estando mais próximo dos dispositivos.

215 Mohammad A. Razzaque, Marija Milojevic-Jevric, Andrei Palade, Siobhán Clarke. Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal. 2016.

216 Anne H. H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, Michael Z. Sheng. IoT Middleware: A Survey on Issues and Enabling technologies. IEEE Internet of Things Journal. 2016.

217 Hasan Derhamy, Jens Eliasson, Jerker Delsing, Peter Priller. A survey of commercial frameworks for the Internet of Things. 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). 2015.

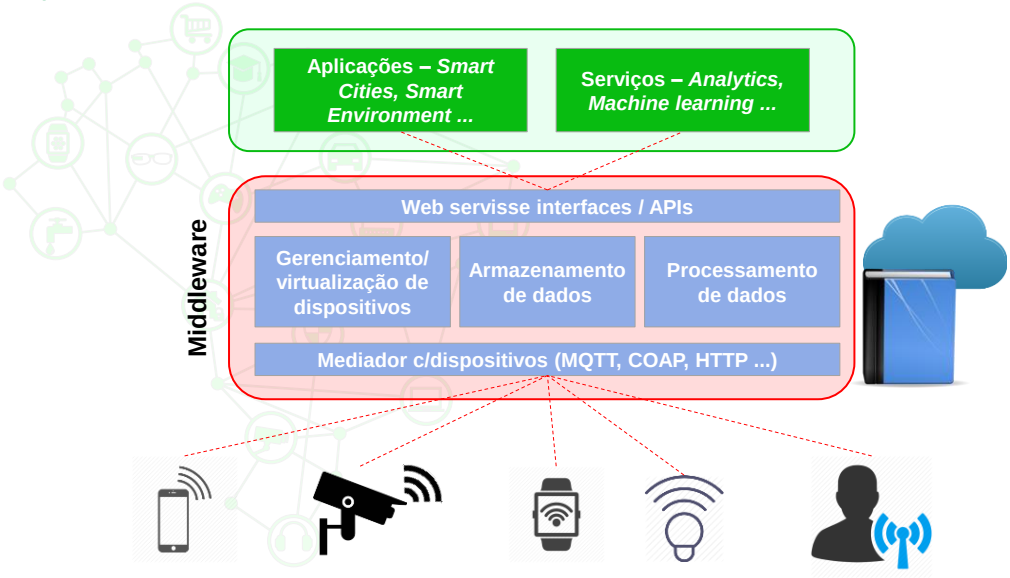
218 Artur Oliveira, Daniel Melo, Geiziany Silva, Thiago Gregório. Comparing IoT Platforms under Middleware Requirements in an IoT Perspective. UBICOMM 2016 : The Tenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. 2016.

219 Bhumi Nakhuva, Tushar Champaneria. Study of Various Internet of Things Platforms. International Journal of Computer Science & Engineering Survey (IJCSES). 2016.

220 Soma Bandyopadhyay, Munmun Sengupta, Souvik Maiti, Subhajit Dutta. Role of Middleware for Internet of things: A Study. International Journal of Computer Science & Engineering Survey (IJCSES). 2011.

QUADRO 34

Arquitetura de *Middleware Service-based*

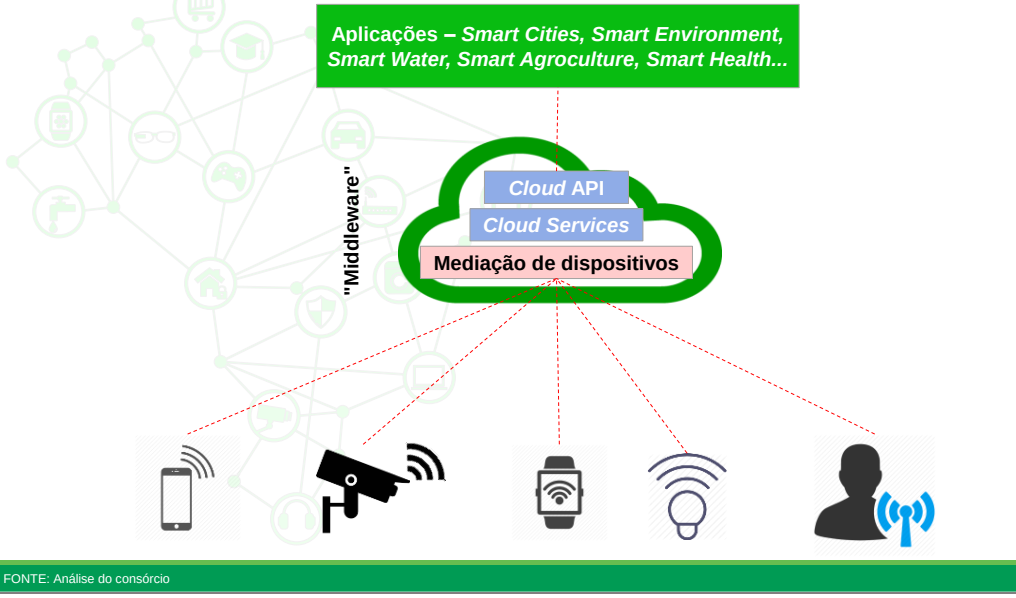


FONTE: Análise do consórcio

Na arquitetura *Cloud-based* (ver o QUADRO 35), os dispositivos de IoT são conectados à nuvem via um serviço de mediação, permitindo uma comunicação bidirecional entre dispositivos e serviços de nuvem.

QUADRO 35

Arquitetura de *middleware Cloud-based*



FONTE: Análise do consórcio

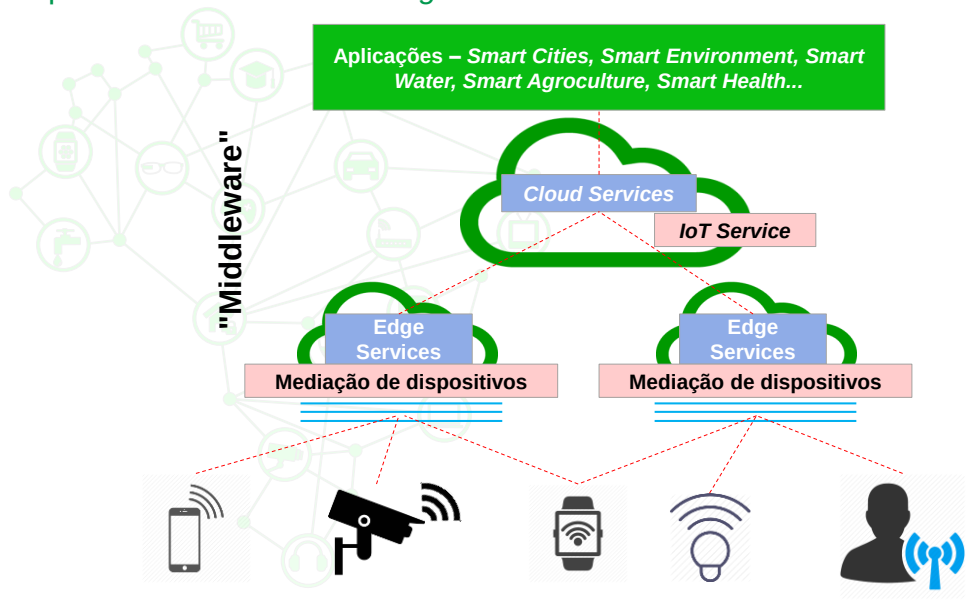
Uma vez conectadas à nuvem, as aplicações podem fazer uso de todos os serviços/recursos da nuvem. Note que, nesta arquitetura, tem-se um "*middleware*" já integrado a um conjunto de serviços de suporte a aplicações, constituindo o que podemos chamar de uma plataforma de IoT.

Esta abordagem tem sido amplamente empregada pelos provedores de PaaS (*Platform as a Service*) como forma de se posicionar no mercado, e conta com um forte marketing, que enfatiza a facilidade do desenvolvimento e implantação de aplicações. No entanto, apesar das facilidades e de fazer uso de serviços já maduros no contexto de aplicações de nuvem, a aplicabilidade desta arquitetura para IoT restringe-se a cenários tolerantes à latência, pois dados/eventos e controles fazem uso da nuvem. Além disso, essa arquitetura pode não ser atraente ou factível dependendo da quantidade e da velocidade dos dados/eventos gerados, da capacidade da rede de dados, do custo da infraestrutura (rede/nuvem) e da segurança e da privacidade exigidas pelo caso de uso.

Na arquitetura *Edge-based* (ver o QUADRO 36, o processamento e o armazenamento estão distribuídos entre a nuvem e a borda, ou seja, com um "*middleware*" distribuído para processar e armazenar os dados na borda ou na nuvem.

QUADRO 36

Arquitetura de *middleware Edge-based*



FONTE: Análise do consórcio

Nesta arquitetura, a tomada de ações em tempo real ou armazenamento de dados sensíveis, é feito na borda, enquanto que análises estáticas ou visões consolidadas de diferentes *sites*, são mais apropriadas para a nuvem. Ademais, com o processamento e o armazenamento nas bordas, torna-se possível reduzir o tráfego de dados para a nuvem, o qual pode ser imensurável, e contribuir positivamente para o aumento da segurança e privacidade dos dados, uma vez que a borda pode ser confinada em uma rede privada.

5.3.3.4 Iniciativas

Devido às dimensões do mercado de IoT, incontáveis iniciativas de *middleware*s/plataformas comerciais e de código aberto têm surgido com o objetivo de simplificar a conexão dos dispositivos com uma infraestrutura de *software* que habilita o rápido desenvolvimento e implantação de aplicações de IoT. A maioria das inciativas é baseada em uma arquitetura *Cloud-Based*, tais como, Amazon AWS IoT[221], Microsoft Azure IoT Suite[222], IBM Watson IoT[223], Oracle IoT Cloud Service[224] e Xively IoT Platform[225], ThingWorx[226], onde o principal objetivo é conectar os dispositivos a um conjunto de serviços de nuvem. Existem algumas iniciativas de código aberto, tais como Fiware[227] e Kaa[228], que seguem uma arquitetura *Service-Based*, permitindo que o *middleware*/plataforma seja instanciado tanto em ambiente de nuvem como em *Gateways* ou servidores locais com alto poder de processamento. Mais recentemente, começaram a surgir iniciativas voltadas para arquiteturas *Edge-Based*, como, por exemplo, Cisco IOx[229], que fornecessem uma infraestrutura para *Fog-Computing*, mas ainda carecem de funcionalidades básicas de um *middleware* de IoT.

221 Amazon AWS IoT, disponível em: https://aws.amazon.com/iot/, acesso em fevereiro de 2017.

222 Microsoft Azure IoT Suite, disponível em: https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite, acesso em fevereiro de 2017.

223 IBM Watson IoT, disponível em: https://www.ibm.com/internet-of-things/iot-solutions/watson-iot-platform/, acesso em fevereiro de 2017.

224 Oracle IoT Cloud Service, disponível em: https://cloud.oracle.com/iot, acesso em fevereiro de 2017.

225 Xively IoT Platform, disponível em: https://www.xively.com/, acesso em fevereiro de 2017.

226 ThingWorx, disponível em: https://www.thingworx.com/, acesso em fevereiro de 2017.

227 Fiware, disponível em: https://www.fiware.org/, acesso em fevereiro de 2017.

228 Kaa, disponível em: https://www.kaaproject.org/, acesso em fevereiro de 2017.

229 Cisco IOx, disponível em: http://www.cisco.com/c/en/us/products/cloud-systems-management/iox/index.html, acesso em fevereiro de 2017.

As principais características das plataformas mencionadas estão sumarizadas na Tabela .

TABELA 13 *MIDDLEWARES*/PLATAFORMAS PARA IOT

Middleware/ Plataforma	Mediação - Dispositivos	Virtualização, Gerenciamento	Processamento/ Armazenamento	Mediação - Aplicações
Amazon AWS IoT	MQTT, HTTP1.1, Websocket	Gerenciamento, Virtualização, SDK	Eventos, Regras e Armazenamento em nuvem	Rest API
Microsoft Azure IoT Suite	MQTT, AMQP, HTTP	Gerenciamento, Virtualização, SDK	Workflow, Eventos, Regras e Armazenamento em nuvem	REST API
IBM Watson IoT	MQTT, HTTPS	Gerenciamento, SDK	Eventos e Armazenamento em Nuvem	REST API / Real-Time APIs
Oracle IoT Cloud Service	MQTT	Gerenciamento, Virtualização, SDK	Eventos, Regras e Armazenamento em Nuvem	REST API
Xively Iot Platform	MQTT, HTTP, HTTPS, Websocket	Gerenciamento, Virtualização, SDK	Eventos, Time Series Database	REST API
ThingWorx	MQTT, AMQP, XMPP, CoAP, Websocket	Gerenciamento, Virtualização, SDK	Workflow, Eventos, Regras e Armazenamento em Nuvem	REST API
Fiware	HTTP, MQTT	Gerenciamento, Virtualização	Workflow, Eventos, Regras e Integração com diferentes DBs	REST API
Kaa	MQTT	Gerenciamento, SDK	Eventos, Regras e Integração com diferentes DBs	REST API

5.3.3.5 Tendências

Em relação à *middleware* de IoT, existe um conjunto de tendências já consolidadas e um conjunto de *gaps* tecnológicos que devem direcionar novas tendências, destacando-se:

- Devido à natureza diversa dos casos de uso em IoT, é pouco provável que uma única arquitetura ou *player* de *middleware* se consolide; diferentes arquiteturas devem coexistir para diferentes nichos de casos de uso;
- Requisitos, como análise e processamento em tempo real, necessidade de reduzir o tráfego de dados para a nuvem e aumento da segurança e privacidade dos dados, devem levar os provedores *Cloud-based* a evoluir para suportarem uma arquitetura *Edge-based*;
- Dependendo do caso de uso de tempo real, as fronteiras da arquitetura *Edge-based* devem avançar além dos *gateways*, chegando aos dispositivos, para se beneficiarem de comunicação direta e tomada de decisões nos mesmos;
- Existe uma grande quantidade de *middlewares*/plataformas IoT; com o amadurecimento da tecnologia de IoT; provavelmente ocorrerá a consolidação de alguns *middleware* (tanto de código fechado quanto aberto), tornando necessária a interoperabilidade. Atualmente, a interoperabilidade é um desafio, assim como a migração de aplicações entre *middlewares*/plataformas. Isto pode levar a uma padronização ou ao surgimento de mediadores/orquestradores para facilitar a integração;
- Assim como devem coexistir várias arquiteturas de *middlewares*, o mesmo é válido para os protocolos de comunicação M2M. Cada protocolo tem características específicas, o que justifica a sua aplicabilidade para casos de usos específicos. Portanto, os *middlewares* devem ser integráveis aos protocolos M2M do seu nicho de aplicação;
- Dentre os protocolos de IoT, existe uma tendência na utilização do protocolo MQTT para cenários de integração com aplicações centralizadas e na utilização do protocolo DDS para cenários de tempo real com foco na comunicação entre dispositivos;
- O armazenamento de dados em IoT é um desafio de *Big Data*; consequentemente, banco de dados não relacionais devem ser comuns em diversos casos de uso, tais como MongoDB, Cassandra e Haddop/HBase. Bancos de dados relacionais deverão ser restritos a cenários específicos, em que os dados são estruturados e uniformes;
- *Webservices Restfull* devem continuar sendo o meio para integração entre *middleware*, serviços e aplicações. No entanto, faz-se necessária uma padronização dos APIs para se permitir maior integração e interoperabilidade;

5.3.4 Big Data e Analytics

Big Data e *Analytics* são duas expressões muito utilizadas atualmente. Um dos principais motivos é a possibilidade de se obter um conjunto de funções especializadas para facilitar a análise de diversos tipos de dados para a tomada de decisão.

O *Big Data* necessitará de desenvolvimento de aplicações capazes de correlacionar as informações geradas pelos sensores e dispositivos de IoT por algoritmos complexos e dinâmicos que possam atender, com mais velocidade, a um maior volume e variedade, conseguindo veracidade e valor dos dados. Para isto, são necessárias a organização e a estruturação do fluxo de geração, coleta, agregação e análise de dados. Descobrir, interpretar e comunicar, no contexto de *Big Data*, é o desafio do *Analytics*. Novas técnicas e/ou combinação de técnicas existentes serão necessárias para possibilitar os ganhos pretendidos do *Analytics* em *Big Data,* e necessários para as soluções de IoT.

5.3.4.1 Armazenamento não estruturado

Devido ao grande volume de dados o qual não é viável estruturar, surge a necessidade de métodos de recuperação de dados, como o NoSQL, um termo usado para descrever bancos de dados não relacionais de alto desempenho. NoSQL vem ganhando espaço e se tornando uma opção para atender a situações em que bancos de dados relacionais não são adequados, devido aos requisitos de computação distribuída e volume de dados em larga escala, muitas vezes com dados não estruturados.

Diversas técnicas serão necessárias para transição entre dados não estruturados para dados semiestruturados, usando outras técnicas, como Ontologia e Web Semântica. No entanto, como a maiorias dos pontos no contexto de IoT aqui levantados, combinações de tecnologias devem ser utilizadas, ao invés de uma tecnologia específica, e, portanto, dados estruturados e não estruturados devem conviver para suportar o ambiente de IoT.

5.3.4.2 Stream processing e Batch processing

Stream e *Batch processing* consistem em tecnologias diferentes para tratar grandes volumes de dados. A técnica de *stream processing* é mais indicada para casos que exigem tomadas de decisões em um curto espaço de tempo. A técnica do *batch processing*, por sua vez, é mais indicada em casos em que é necessário analisar grandes volumes de dados de forma mais aprofundada, usando técnicas como *MapReduce*, e processá-los para uso por outros sistemas.

5.3.4.3 Tendências

A tendência para os próximos anos, no contexto de IoT, provavelmente será trabalhar mais próximo do *realtime* em ambientes heterogêneos, grande parte dos quais não são estruturados e geram grandes volumes de dados. Para isso, o uso do modelo de dados espaço-temporal será importante para dividir os dados por local e horário de ocorrência. Esta evolução alavancará dados para diversos usos, como monitoramento de prevenção (modelos preditivos), aprimoramento da automação via validação e enriquecimento de dados, além de diversos usos do *analytics*, como: *Streaming analytics*, *Sentiment analytics*, *Prescriptive analytics*, *Advanced quantitative analytics*, *Distributed analytics* e *Social media analytics*.

5.3.5 Computação cognitiva

Computação cognitiva, também conhecida no meio técnico como Inteligência Artificial fraca (ou *narrow/weak AI*, no inglês), é um campo da área de inteligência artificial que busca implementar, em computador, mecanismos capazes de executar tarefas específicas associadas com a inteligência, como raciocínio, aprendizado e identificação de padrões. Contrapõe-se à IA forte (ou *general/strong AI*, no inglês), que visa implementar, em máquinas, a capacidade do ser humano de executar tarefas de mais alto nível e com maior grau de generalização. Enquanto, atualmente, a IA forte funcional é considerada restrita à ficção científica, aplicações de IA fraca são vistas em diversos produtos, voltados tanto à melhoria das cadeias de produção, como diretamente ao mercado consumidor. Exemplos dessa aplicação são os assistentes virtuais, como a Alexa, da Amazon, e a Siri, da Apple, que são capazes de entender comandos de fala, executar ações e trazer respostas faladas aos usuários.

5.3.5.1 Machine learning

Nos últimos anos, o grande interesse acerca de IA tem sido dirigido, principalmente, pelos resultados alcançados por uma de suas subáreas, conhecida como aprendizado de máquina (ou *machine learning*, no inglês). Diferentemente de métodos clássicos de IA, como sistemas especialistas, que buscam emular computacionalmente a forma como humanos tomam decisões, as técnicas de *machine learning* são orientadas a dados, ou seja, o desenvolvedor cria um conjunto de modelos que poderá se adaptar aos padrões observados nos dados de treinamento, de modo a definir uma forma adequada de tomar uma decisão.

Considerando a quantidade massiva de dados gerados continuamente por sensores e usuários, em situações muitas vezes desconhecidas ao projetista e que mudam com o tempo, abordagens baseadas em *machine learning* são consideradas essenciais para o controle de sistemas de IoT, dada a capacidade de se adaptar a novos cenários sem precisarem ser reprogramadas.

A área de *machine learning* é composta por diferentes técnicas: técnicas de aprendizado supervisionado, técnicas não-supervisionadas e aprendizado por reforço, detalhadas a seguir:

- **Técnicas de aprendizado supervisionado:** são interessantes para situações nas quais os dados são rotulados, ou seja, a resposta que se deseja que o sistema dê está listada para cada amostra de entrada disponível para treinamento. Por exemplo, tarefas que humanos conseguem executar bem, como identificação de objetos em uma imagem ou do gênero de uma música, costumam ser resolvidas usando esse tipo de técnica. Usualmente, técnicas de aprendizado supervisionado são focadas em dois tipos de desafios correlatos:
  - **Classificação**: aprender a relação entre variáveis de entrada e um conjunto de categorias conhecido, para que, dada uma nova amostra de entrada, o sistema identifique a que categoria a nova amostra de entrada pertence. Possíveis usos são a identificação do gênero de uma música, ou a classificação se uma linha de montagem está chegando ao final de sua vida útil, permitindo que seja realizada sua manutenção preditiva. Exemplos de técnicas: regressão logística, redes neurais, *support vector machines* (SVM), modelos gráficos probabilísticos;
  - **Regressão**: aprender a relação entre um conjunto de variáveis de entrada e de saída, para que, dada uma nova amostra de entrada, o sistema consiga informar qual é a saída associada. Pode ser usada para medir a evolução da pressão e colesterol de um paciente, ou prever a avaliação que um determinado usuário fará de um filme ou música. Exemplos de técnicas: regressão linear, redes neurais, *support vector regression* (SVR).
- **Técnicas não-supervisionadas** são utilizadas quando há especial dificuldade em se prever os tipos de entradas que serão observados pelo sistema em produção (ex.: um motor de um carro pode falhar de diversas formas, inclusive devido a fatores externos, sendo muito difícil coletar dados de treinamento, representando todas as possíveis situações que levam a falhas). Neste caso, costumam ser usadas técnicas de aprendizado não-supervisionado, as quais se busca identificar padrões estruturais nos dados observados. Estas técnicas costumam ser usadas para tarefas como:
  - **Clusterização**: identificação de grupos de amostras nos dados que apresentam maior similaridade entre si. Pode ser usada para identificar grupos de consumidores com um perfil de compras parecido ou agrupar diagnósticos médicos similares entre si. Exemplos de técnicas: *k-means* e suas variantes, DBSCAN, modelos de mistura;
  - **Redução de dimensionalidade**: aprendizado de formas mais simples de representar um determinado conjunto de dados com perda mínima de informação. Além de ser uma etapa útil para vários desafios de *machine learning*, este tipo de técnica é útil para tarefas de *analytics*, por permitir representar dados com altas dimensões em espaços menores, mais interpretáveis por humanos. Exemplos de técnicas: PCA, *autoencoders*;

- **Detecção de anomalias:** identificação dos padrões que caracterizam um determinado conjunto de dados, para que o sistema, uma vez apresentado a uma nova amostra, possa identificar se ela pertence ao conjunto aprendido ou não. Detecção de anomalias é uma tarefa particularmente relevante para aplicações de IoT, uma vez que permite identificar quando as observações desviam do padrão esperado, possibilitando, por exemplo, a identificação de falhas em máquinas e sensores ou de comportamentos anômalos em vídeos de vigilância. Exemplos de técnicas: SVM de uma classe, métodos de estimação de densidade, além de técnicas usadas para clusterização.
- **Aprendizado por reforço:** são úteis quando as respostas desejadas do sistema não estão disponíveis, mas é possível obter uma realimentação sobre a qualidade da solução gerada pelo sistema. Essa realimentação pode ser obtida por meio de simulações ou de interação com um ambiente real. Possíveis aplicações vão desde controle robótico até sistemas de recomendação de músicas.

Estas abordagens costumam ser combinadas para permitir a execução de tarefas complexas. Um exemplo recente é o sistema AlphaGo, que foi capaz de derrotar o campeão mundial de Go[230], combinando aprendizado supervisionado, reforçado por treinamento. Em aplicações voltadas para vigilância, por exemplo, uma rede neural poderia ser treinada de forma supervisionada para identificar objetos e ações em um vídeo, repassando as informações identificadas para um mecanismo de detecção de anomalias, que identificaria se esses objetos estão agindo conforme o esperado. Outro exemplo é visto em biometria de voz, na qual métodos de clusterização e redução de dimensionalidade podem ser usados para acelerar a busca por vozes similares a um dado áudio de entrada, enquanto que classificadores podem ser utilizados para identificar se o áudio de entrada pertence a alguma das vozes retornadas.

Uma das possibilidades mais relevantes da combinação de IoT com técnicas de *machine learning* é a personalização radical de produtos e serviços. A análise de dados sobre usuários, produzidos diretamente por eles ou por meio de sensores e outros equipamentos, permite mais do que a personalização de anúncios, abrindo portas para tecnologias como medicina personalizada ou aulas projetadas de acordo com a necessidade e o perfil de aprendizado de cada aluno (uma tarefa abordada em um subcampo conhecido como *learning analytics*).

Dentro da perspectiva de personalização radical, ganham relevância a análise de redes sociais e os sistemas de recomendação. O estudo de redes sociais permite uma maior incorporação em mecanismos de personalização de dados produzidos diretamente pelos usuários (ex.: textos, fotos, vídeos e afins), bem como dos dados de suas conexões sociais. Sistemas de recomendação, por sua vez, combinam essas informações com outras fontes de dados, para prever (usando um regressor, por exemplo) como um usuário avaliaria um determinado item, permitindo recomendar apenas os itens que o sistema acredita que o

[230] Jogo de tabuleiro.

usuário mais apreciaria. Aplicações deste tipo de sistema passam pela recomendação de conteúdo, como vídeos (Netflix e Youtube), músicas (Spotify e Last.fm), artigos científicos (Google Scholar) e sites (StumbleUpon), além de produtos (Amazon), encontros românticos (OkCupid) e vagas de emprego (Linkedin), entre outros. Dados do Netflix, por exemplo, indicam que seus sistemas de recomendação influenciam 80% do conteúdo transmitido na plataforma.

Dentre as técnicas de *machine learning*, *deep learning* (ou aprendizado profundo), tem se destacado nos últimos anos, obtendo resultados muito positivos em áreas relevantes, mas que tradicionalmente representavam um grande desafio em IA, como processamento de fala e visão computacional. O termo *deep* se refere a um conjunto de técnicas baseadas em redes neurais artificiais com múltiplas camadas de neurônios, nas quais cada neurônio combina e processa as saídas dos neurônios da camada anterior (ex.: informações sobre bordas ou *core*s em uma imagem), passando, para a próxima camada, uma informação de mais alto nível (ex.: informações sobre formas geométricas).

5.3.5.2 Processamento de fala e linguagem natural

O surgimento de assistentes virtuais comerciais baseados em diálogo, como Siri (Apple) e Cortana (Microsoft), foi propiciado pelos grandes avanços nas áreas de processamento de fala e linguagem natural vistos nos últimos anos. As interfaces de usuário baseadas em diálogo têm se tornado um foco de atenção do mercado, uma vez que elas são capazes de prover formas mais naturais de interação.

Do ponto de vista técnico, a compreensão automática da fala apresenta alguns desafios: reconhecimento automático de fala (transcrição da fala em texto), compreensão de linguagem natural (responsável pela análise semântica da entrada) e gerenciamento de diálogo (componente responsável por manter informações sobre o contexto da conversação, definindo as ações a serem tomadas em resposta a cada entrada). Além disso, um sistema baseado em diálogo, como um assistente virtual, ainda apresenta o desafio adicional da produção da resposta por meio de fala. Para isso, é necessário gerar a fala natural (definir o que deve ser respondido) e sintetizar a fala.

Enquanto as etapas de compreensão e geração de linguagem são geralmente feitas por meio de gramáticas que relacionam sequências de palavras a comandos específicos, métodos que possuem a capacidade de aprender informações sobre sequências costumam ser usados para lidar com sub tarefas ligadas a fala. Por muito tempo, usaram-se modelos ocultos de *Markov* (ou *hidden Markov models*, HMM) combinados com métodos projetados por especialistas para conversão entre áudios e vetores numéricos. Com o sucesso de *deep learning*, no entanto, tem sido cada vez mais comum o uso de redes neurais recorrentes, especialmente redes do tipo *long short-term memory* (LSTM), tanto para o aprendizado de como a fala ocorre no tempo como para aprender formas melhores de representar estes áudios como vetores. Com essa mudança de métodos, tem havido a união de sub tarefas

que costumavam ser executadas por componentes separados que demandavam conhecimentos da língua para a qual o sistema foi desenvolvido. Ao usar técnicas de *deep learning*, essas sub tarefas têm sido aprendidas diretamente dos dados de treinamento. Esta abordagem já tem chegado a soluções comerciais, como visto para alguns conjuntos de línguas do tradutor automático *Google Translate*.

Por fim, vale notar que outras tarefas relacionadas ao processamento de fala e linguagem tendem a ser necessárias para o desenvolvimento de sistemas mais completos. Biometria de voz, por exemplo, pode ser útil para melhorar a segurança e a personalização de assistentes baseados em diálogo, enquanto que *soft biometrics* (identificação de traços sobre o falante, como idade, sexo, etnia e local de origem) e a análise de sentimentos podem auxiliar o sistema na compreensão de contexto.

5.3.5.3 Visão computacional

Assim como no processamento de fala e linguagem, na área de visão computacional, as técnicas de *deep learning* têm levado a grandes avanços, de modo que já existem sistemas capazes de superar humanos em tarefas específicas de visão, como reconhecimento de objetos em fotos. Esses avanços têm se estendido para subáreas específicas de visão computacional, como a biometria de face, na qual redes como a VGG-face têm sido capazes de superar tecnologias que até então encontram-se no estado-da-arte. Os resultados alcançados em tarefas mais clássicas permitiram que, nos últimos anos, passasse-se a trabalhar intensamente em desafios mais complexos, como a geração automática de descrição de imagens ou a geração de imagens a partir de uma descrição.

Enquanto, para fala, as redes usadas são focadas no aprendizado de sequências, para visão computacional, são utilizadas, principalmente, redes convolucionais (*convolutional neural networks*, ou CNN), que são capazes de identificar padrões independentemente da posição destes na imagem. Com essa mudança, saiu-se de um panorama no qual especialistas criavam métodos para representar imagens, como vetores de números (ex.: SIFT, histogramas de gradientes, filtros de Gabor), para um no qual as representações são aprendidas automaticamente a partir de dados, algo conhecido como *feature learning*.

Essas abordagens orientadas a dados, no entanto, são mais suscetíveis a aprenderem vieses contidos na base de treinamento. Além de não aprenderem bem como classificar imagens de algumas categorias, desafios no treinamento podem trazer dificuldades sistemáticas em lidar com situações como iluminação, ruído ou posicionamentos muito diferentes dos vistos na base usada para treinamento.

Sistemas treinados em bases de dados heterogêneas, no entanto, têm mostrado grande capacidade de generalização. Graças a uma técnica chamada *transfer learning*, partes de redes treinadas para identificação de objetos têm sido usadas para a resolução de outros desafios de visão para os quais há menos dados de treinamento disponíveis, como identificação de patologias em imagens, como fotos ou raios-X. Esse tipo de abordagem

tem permitido reduzir grandemente o tempo necessário para o desenvolvimento de novas soluções baseadas em visão computacional, diminuindo a demanda por dados rotulados e por profissionais especializados.

5.3.5.4 Processamento vetorial

Apesar de algumas das principais técnicas de *machine learning* já existirem há décadas (ex.: redes neurais artificiais foram inventadas nos anos 40 e redes convolucionais foram propostas nos anos 80), apenas recentemente (especialmente a partir de 2010), as técnicas de *machine learning* chegaram ao centro das aplicações em computação. Isso ocorre pela atual disponibilidade de dados de fontes diversas -- *e-commerce*, redes sociais, governos etc -- e de poder de processamento, suficientes para permitir que técnicas de *machine learning* alcancem resultados superiores ao estado-da-arte em diversos desafios, como identificação e localização de objetos em imagens e processamento de linguagem natural.

Um dos grandes saltos oferecidos veio com o uso dos milhares de *core*s disponibilizadas por GPUs (*graphical processing units*), projetadas inicialmente para o processamento gráfico de jogos e animações. Atualmente, todas as principais bibliotecas de *deep learning* (ex.: Theano, TensorFlow, Torch) e visão computacional (ex.: OpenCV) possuem suporte ao uso de GPUs, enquanto que os fornecedores deste tipo de *hardware* (ex.: NVidia NVLink) e de computação em nuvem (ex.: IBM, Google, Amazon) têm oferecido serviços de GPU otimizados para métodos de IA.

Devido ao constante aumento na quantidade de dados usados para treinamento e na complexidade dos modelos desenvolvidos, alguns grupos começaram a explorar alternativas além de GPUs. Enquanto a Microsoft afirma utilizar um cluster de placas FPGA (*field programmable gate array*) otimizadas para aplicações de *deep learning* em seu buscador *Bing*, a Google anunciou que tem usado um ASIC (*application-specific integrated circuit*) chamado *Tensor Processing Unit* (TPU) otimizado para a execução de sua biblioteca de *deep learning* (TensorFlow). Dentre os provedores de computação em nuvem, a Amazon já anunciou que passará a oferecer máquinas com placas FPGA.

5.3.5.5 Otimização

A realização de modelagens precisas utilizando dados do funcionamento dos sistemas traz o potencial de otimizar as ações tomadas, tanto para um melhor desempenho quanto para redução de custos. Um exemplo pode ser visto em uma aplicação de controle industrial, na qual um mecanismo de *machine learning* pode requisitar a manutenção preventiva de uma máquina, enquanto que um mecanismo de otimização selecionaria o melhor período para a execução da manutenção e reorganizaria o fluxo da produção de modo a minimizar custos.

Deste modo, no controle de sistemas de IoT, há um grande potencial de ganho ao se integrar métodos de *machine learning* com técnicas já existentes de pesquisa operacional para a resolução de desafios como roteamento, alocação de recursos e escalonamento de atividades.

5.3.5.6 Tendências

Em aplicações atuais de IoT, há a tendência de que os serviços de inteligência artificial sejam implementados junto da própria aplicação, usualmente com o suporte de algumas bibliotecas padronizadas, como o Scikit-learn (para *machine learning* em geral), TensorFlow, CNTK e Torch (específicos para *deep learning* e patrocinados, respectivamente, por Google, Microsoft e Facebook). Alguns *atores*, no entanto, estão buscando oferecer, em suas plataformas, serviços de IA mais ou menos complexos. Exemplos são a IBM com o Watson/Bluemix, a Amazon com o AWS e a Microsoft com o Azure. Nota-se, no entanto, que, atualmente, a adoção destas plataformas tem sido restrita, especialmente devido ao fato de que atualmente o uso eficiente de IA demanda alto grau de customização. Essa customização por aplicação deixa aberta a questão de quais tipos de arquitetura acabarão dominando o uso de computação cognitiva em IoT: enquanto que a implementação de um controle "inteligente" separado para cada aplicação de IoT é tecnicamente mais simples, a concentração da "inteligência" do sistema em um único dispositivo orquestrador pode levar a uma maior integração dos dispositivos disponíveis.

Outra dúvida que surge é como a alta demanda por mecanismos de IA será conciliada com o pequeno número de profissionais capacitados na área. Um maior uso de métodos baseados em *transfer learning* poderá acelerar o desenvolvimento de aplicações por meio do reuso de modelos, mas ainda demandaria grande customização para cada aplicação. Um maior desenvolvimento de técnicas de *meta-learning* -- sistemas de IA capazes de projetar automaticamente mecanismos de *machine learning* -- poderá ser uma solução de médio a longo prazo para este desafio.

Por fim, considerando a necessidade de sistemas mais dinâmicos e adaptáveis para o controle de IoT, provavelmente ganhará relevância o aprendizado a partir de fluxos de dados (*stream*), em contraposição ao atual domínio das técnicas cujos treinamentos são baseados em grandes cargas de dados (*batch*). Formas de aprendizado contínuo, como aprendizado *online* e por reforço, tendem a ganhar relevância no médio prazo.

5.3.6 Computação Avançada

Computação Avançada engloba tecnologias e técnicas para a programação de algoritmos complexos; estruturação, processamento distribuído e gerenciamento de diversos tipos de informações e a interação adequada dos sistemas com o usuário, garantindo a execução sobre uma rede computacional em diversos ambientes tecnológicos.

5.3.6.1 Geoprocessamento

O uso de dados geoespaciais em SIG (Sistema de Informação Geográfica, em inglês, GIS *Geographic Information System*) ganhou destaque entre o público em geral, principalmente pelos dispositivos de navegação dos automóveis, como o *Google Earth* e *Google Maps*, e, posteriormente, o *Waze*. Além disso, surgiram vários aplicativos para transporte pessoal particular e táxi que usam esta tecnologia. Existem diversos usos de dados geoespaciais, como para geração de indicadores para atletas profissionais ou amadores, no campo para acompanhamento das plantações, e para a localização de animais de estimação.

Atualmente, padrões estão bem estabelecidos no mercado Geoespacial, graças a iniciativa do consórcio OGC[231] (*Open Geospatial Consortium*), formado pela maioria das empresas e comunidades Geoespaciais. Um dos grandes objetivos do consórcio é a definição de padrões para facilitar a interoperabilidade. O consórcio ajudou a superar questões de confiança entre os grandes *atores,* impulsionando novos negócios. Com isso, está havendo uma expansão no uso de técnicas geoespaciais para apoiar os sistemas tradicionais nas mais diversas formas e mercados.

No Brasil, existe o movimento da INDE[232] (Infraestrutura Nacional de Dados Espaciais), que foi criado para ser o Diretório Brasileiro de Dados Geoespaciais, definindo os metamodelos. A sua missão é oferecer um "conjunto integrado de tecnologias; políticas; mecanismos e procedimentos de coordenação e monitoramento; padrões e acordos, necessário para facilitar e ordenar a geração, o armazenamento, o acesso, o compartilhamento, a disseminação e o uso dos dados geoespaciais de origem federal, estadual, distrital e municipal." Cabe ressaltar que a INDE propõe a padronização da estrutura dos dados, e não das técnicas, com foco em órgãos governamentais, seguido de empresas privadas.

O GIS/SIG está saindo de um patamar de sistema complexo das grandes empresas para uma tecnologia ágil e abrangente na solução de desafios acessíveis a empresas de todos os portes. Esta tecnologia poderá ter um papel importante na IoT, possibilitando utilizar a posição dos objetos inteligentes nas tomadas de decisão.

[231] Organização internacional para padronização, criada em 1994, com mais de 500 membros.

[232] A Infraestrutura Nacional de Dados Espaciais – INDE foi instituída pelo Decreto Nº 6.666 de 27/11/2008, com o propósito de catalogar, integrar e harmonizar dados geoespaciais existentes nas instituições do governo brasileiro.

5.3.6.2 *User Experience* – UX

Existem vários desafios de UX no contexto de IoT, principalmente nas formas de interação, devido tanto às limitações ou às mudanças constantes, quanto ao surgimento de novos *devices*. De acordo com as projeções atuais, os novos dispositivos de IoT devem surgir em uma proporção muito maior que os celulares, *tablets* e computadores, de onde possuímos a maioria dos conceitos consolidados em UX.

Lidar com aplicações que têm que ser distribuídas por múltiplos *devices* com diferentes capacidades e recursos de interação também é um grande desafio que, no passado, apareceu em proporções menores, quando surgiram diversos tamanhos de telas, e pode ser potencializado no contexto de IoT, pois as mudanças podem estar associadas à ausência de tela, além do tamanho.

Nesse contexto, várias tecnologias devem se desenvolver, como realidade aumentada, realidade virtual e os assistentes virtuais, que podem acelerar a capacidade de se aproximar dos usuários.

5.3.6.3 Tendências

A tendência para os próximos anos, no contexto de IoT, provavelmente combinará as diversas tecnologias existentes de forma mais ágil. Para isso, será necessário disponibilizar as funcionalidades de computação avançada de forma genérica e como serviço, diferentemente do que é mais comum atualmente, em que estas tecnologias são construídas como soluções dedicadas.

5.3.7 Questões de segurança

Os serviços disponíveis nessa camada não devem ser diferentes com a adoção maciça de aplicações específicas para IoT. A área de *analytics*, que interage diretamente com segurança, merece destaque devido ao fato de que tudo que abrange o universo de IoT para interação entre pessoas, produz, utiliza e transmite informações, que precisam ser tratadas para terem valor. Além disso, a segurança e privacidade não são extraídos somente de textos, áudios e vídeos, mas também incluem informações sensoriais e contextuais, disponíveis nas redes sociais, por exemplo.

Do ponto de vista da segurança em IoT, o NIST[233,234] define as tecnologias de suporte de modo amplo, como bases de dados, dispositivos móveis, nuvens computacionais, fornecedores de energia, etc. Sem o objetivo de ser exaustivo, é importante notar que cada

[233] National Institute of Standards and Technology, agência governamental da administração de tecnologia do Departamento de Comércio dos Estados Unidos.

[234] J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

tecnologia de apoio tem seus próprios requisitos de segurança, que devem ser combinados e confrontados com as necessidades particulares de IoT.

Duas tecnologias têm demonstrado potencial em aumentar a segurança em IoT, no contexto da infraestrutura de apoio a aplicações e serviços. A primeira é o *Blockchain*[235], que pode aumentar a confiança geral na troca de informações entre aplicações e sensores. A outra é o ambiente de execução confiável (*Trusted Execution Environment* - TEE) em dispositivos móveis[236,237].

5.3.8 Gerenciamento de dispositivo (*device management*)

Excetuando-se os extremamente triviais, dispositivos de IoT exigirão gerenciamento e monitoramento, principalmente devido ao longo ciclo de vida. A evolução da IoT altera a escala de dispositivos que necessitam ser gerenciados. As ferramentas de gerenciamento deverão ser capazes de gerenciar e monitorar milhares ou talvez até milhões de dispositivos. No gerenciamento dos dispositivos, estão inclusas atualizações de *firmware* e *software*, aprovisionamento de serviços, manutenção, configuração, solicitações de dados, diagnósticos, análise de falhas, gerenciamento físico e gerenciamento de segurança.

Como exemplo de aplicação de DM, em um *recall* de veículos de um fabricante[238], 29.000 veículos foram atualizados remotamente (*Over the Air*), enquanto que, para veículos de outro fabricante, 380.000 proprietários de veículos precisaram ir até uma concessionária para realizar atualização similar. A incorporação de protocolos de DM pode representar uma grande economia, com impactos positivos na redução de custos, logística, imagem e satisfação do usuário.

No contexto da camada de suporte à aplicação, as funcionalidades e competências do *device management* são oferecidas como um serviço comum às aplicações de IoT. Dessa forma, as aplicações IoT podem fazer uso dessas funcionalidades sem ter que acessar diretamente os dispositivos (*devices*) ou *gateways*. No entanto, aplicações podem acessar os dispositivos diretamente, conforme mostrado no QUADRO 37 [239].

235 Swan, Melanie. "Blockchain: Blueprint for a new economy", 2015.

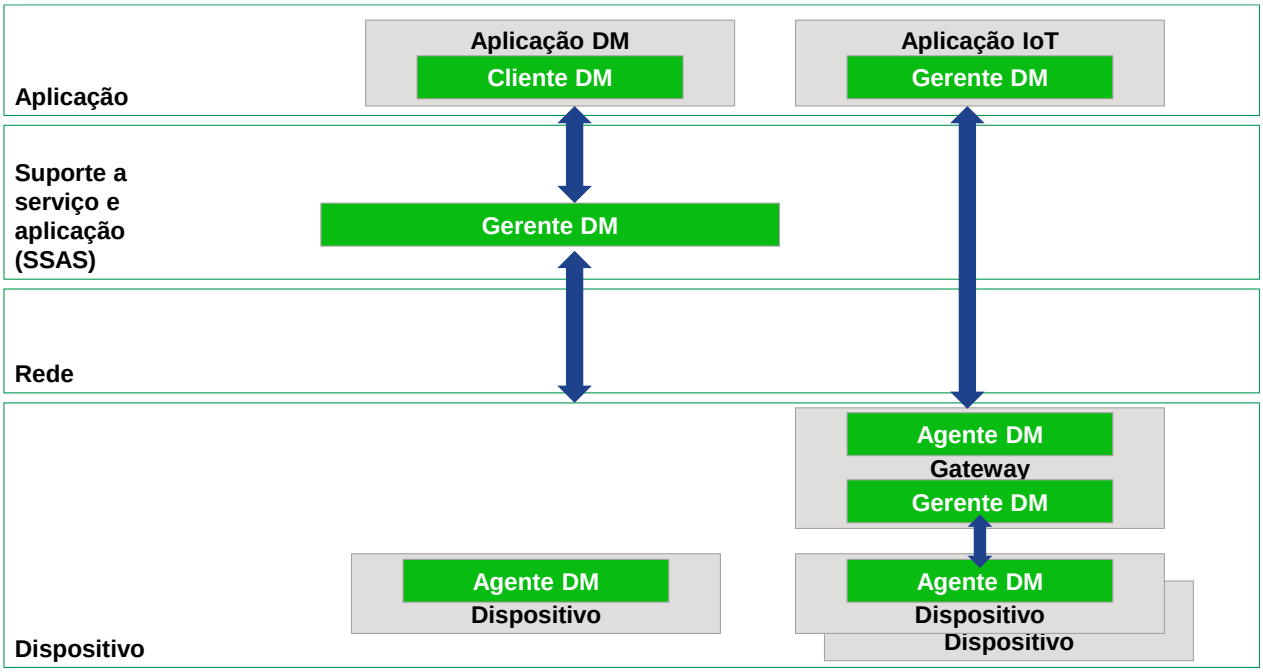
236 GlobalPlatform. "The standard for managing applications on secure chip technology". Disponível em: http://globalplatform.org, acesso em maio de 2017.

237 Open-TEE. Open source project for a "virtual TEE based on *software*". Disponível em: https://open-tee.github.io, acesso em janeiro de 2017.

238 Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? Disponível em: https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/, acesso em fevereiro de 2017.

239 Fonte: Adaptada de ITU-T Y.4702.

QUADRO 37



O DM provê um conjunto de competências (*capabilities*) que permitem a execução de tarefas de gerenciamento de forma local ou remota. Pelo DM, os dispositivos (*devices*) podem ser configurados; informações sobre estados operacional e administrativo, falhas, desempenho são coletados.

5.3.8.1 Protocolos para Device Management

Os protocolos *Device Management* utilizados na IoT são o *Lightweight* M2M (LWM2M), OMA-DM e TR-69. Cada protocolo tem um uso mais adequado conforme as capacidades do dispositivo e da rede, além da escolha ser impactada pela entidade que faz o gerenciamento, como por exemplo, operadora de telecomunicações, fabricante, aplicação.

5.3.8.1.1 LIGHTWEIGHT M2M

O *Lightweight* M2M[240] é um protocolo aberto desenvolvido pelo OMA para fornecer um meio de realizar remotamente a ativação de serviços e o gerenciamento de dispositivos da IoT (inclusive *hubs* e *gateways*), de forma simples e de baixo custo. É um protocolo de comunicação para uso entre *software* cliente em um dispositivo M2M e *software* de gerenciamento nas plataformas de IoT (plataforma de suporte à aplicação e a serviço).

240 OMA LightweightM2M V1.0 Overview. Disponível em: http://www.openmobilealliance.org/wp/Overviews/lightweightm2m_overview.html, acesso em fevereiro de 2017.

LWM2M é complementar a outras soluções de gerenciamento de dispositivos produzidas *Device Management* v.1.x / v.2.0 (OMA) e TR-69 (*Broadband Forum*), e abarca uma maior gama de dispositivos que podem ser gerenciados. O LWM2M é o protocolo adequado para dispositivos com capacidades restritas de processamento e redes de banda estreita. O padrão foi desenvolvido para atender à necessidade de um mecanismo de ativação de serviço e gerenciamento remoto de baixo custo que funciona em redes e dispositivos com capacidades restritas. Com a padronização do LWM2M, é esperado que, com o desacoplamento dos componentes por meio de interfaces padronizadas, o gerenciamento dos dispositivos da IoT seja adequado às necessidades futuras. O padrão LWM2M define um recurso e modelo de dados e faz uso do CoAP[241]. O mecanismo de gerenciamento remoto padronizado foi projetado para criar as seguintes oportunidades e benefícios de negócios para a indústria M2M:

- Permitir soluções *plug-and-play* entre uma variedade crescente de dispositivos M2M e as plataformas de IoT;
- Possibilitar dispositivos com capacidades restritas e de baixo custo serem monitorados e gerenciados remotamente;
- Expandir o uso de LWM2M em áreas de mercado que acabam por se beneficiar mais de suas características de *design*;
- Melhorar a capacidade de gerenciamento dos dispositivos, fornecendo uma solução que pode ser usada tanto para o gerenciamento de dispositivos como da aplicação, independentemente de como os componentes do sistema estão hospedados.

5.3.8.1.2 OMA-DM

O OMA-DM[242] é um protocolo de *Device Management* estabelecido pela *Open Mobile Alliance* (OMA). Inicialmente desenvolvido para gerenciamento de dispositivos móveis (por exemplo, celulares, PDAs, *tablets*) por operadoras de redes móveis e por fabricantes, e tem sido utilizado para gerenciamento de dispositivos de IoT. O OMA-DM atende a necessidade de aprovisionamento, configuração de dispositivo, atualizações de *firmware* e supervisão de falhas. Em razão do tipo de necessidade, o OMA-DM tem um pequeno *footprint* (baixo uso de recursos memória e armazenamento) e a capacidade de transmitir dados utilizando meio de transmissão limitado em banda.

A maior parte das instalações do protocolo OMA DM 1.x foi feita em *Smartphones*. No entanto, para determinados dispositivos, o protocolo pode não atender às restrições de *footprint* e banda[243]. Essa versão pode ser adequada para dispositivos com maior capacidade computacional. O OMA DM 2.0, por sua vez, mantém compatibilidade com os padrões FUMO, SCOMO e LAWMO. O objetivo da OMA foi reduzir e otimizar o uso

241 Disponível em http://openmobilealliance.org/about-oma/work-program/device-management/, acesso em abril de 2017.

242 OMA Device Management Overview, disponível em: http://www.openmobilealliance.org/wp/overviews/dm_overview.html, acesso em feveiro de 2017.

243 Redbend, "Making Sense of IoT Standards". Disponível em: http://www.redbend.com/data/upl/whitepapers/Making%20Sense%20of%20IoT%20Whitepaper.pdf, acesso em fevereiro de 2017.

dos recursos computacionais, transferindo as questões de segurança e autenticação para o protocolo de camada inferior, o HTTP(S). Adicionalmente, houve melhora no uso de banda para comunicação.

5.3.8.1.3 TR-069

O protocolo TR-69, também conhecido como CPE WAN Management Protocolo (CWMP), define uma comunicação padrão entre uma gerência remota e equipamentos de usuários (por exemplo, roteadores, *cable modems*). Permite que o equipamento ou dispositivo se autoconfigure de forma automática, sem depender do usuário, além de possuir outras funções de gerência.

Embora não seja um protocolo concebido para acesso sem fio em dispositivos com restrições de recursos computacionais, o TR-O69 é citado como uma alternativa, com o uso de dispositivos de capacidades de processamento maiores e com redes de maior banda disponível, principalmente quando utilizado por operadoras de telecomunicações.

5.3.9 Conclusões

Na camada de suporte a serviços e aplicações ocorre a concentração dos dados gerados e transmitidos pelos objetos inteligentes para serem processados e analisados, gerando o valor esperado dos casos de uso de IoT. Assim, há o desafio de se armazenar e tratar a imensa quantidade de dados, em especial quando existem rígidos requisitos de tempo de respostas, por exemplo:

A IoT deve impactar diretamente a infraestrutura de *data centers*, fazendo com que estes evoluam para atender às novas aplicações. Desta forma, espera-se que sejam criados novos **micro *data centers* distribuídos** e mais próximos das bordas (*edge computing*), seguindo um modelo de *cloudlets*, onde ambientes de nuvem reduzidos executam aplicações especializadas no tratamento, filtragem inicial dos dados e resposta a demandas que exigem baixa latência e maior agilidade na resposta.

Adicionalmente, esses *data centers* ficarão cada vez mais **automatizados,** tendo suas **funcionalidades virtualizadas e definidas por *software***. Os modelos de armazenamento de dados devem ser unificados por meio de interfaces centralizadas e bem definidas.

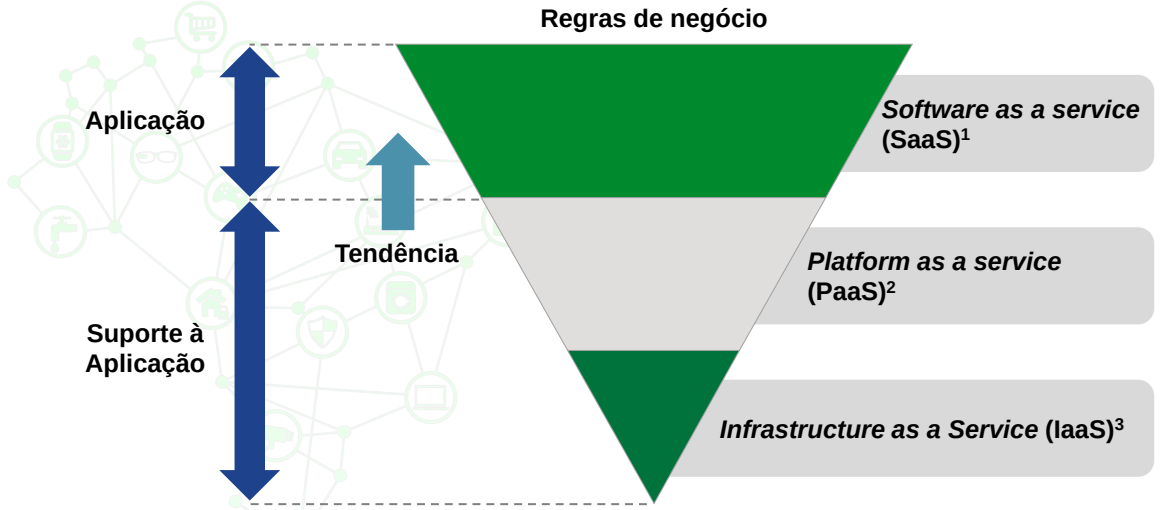
Em relação ao ***middleware***, devido à natureza diversa dos casos de uso em IoT, **é provável que várias arquiteturas coexistam**. Com o amadurecimento do ecossistema, tende a haver uma consolidação de alguns deles, tornando necessário interoperá-los. Esse fato provavelmente resultará na padronização ou no surgimento de mediadores/orquestradores para facilitar a integração.

Assim como **devem coexistir várias arquiteturas de *middleware***, também devem coexistir vários protocolos de comunicação, uma vez que cada protocolo tem características específicas que justificam sua aplicabilidade a casos de uso definidos. Os produtos de *middleware* devem ser integráveis aos protocolos do seu nicho de aplicação.

O **desenvolvimento de soluções customizadas tende a ser facilitado** na medida em que **funcionalidades preexistentes em diversas plataformas em nuvem se tornem disponíveis**. Com isso, o desenvolvimento de aplicações tende a ter um *time-to-market* cada vez menor, dependendo menos de *expertise* em programação e mais de conhecimento dos negócios em si, como pode ser visto no QUADRO 38.

QUADRO 38

Tendência para desenvolvimento de aplicações de IoT



1 Modelo de entrega em que o software é licenciado em uma base de assinatura e é hospedado centralmente
2 Categoria de serviços de computação em nuvem que fornece uma plataforma que permite aos clientes desenvolver, executar e gerenciar aplicativos
3 Tipo de computação em nuvem que fornece recursos de computação virtualizados pela Internet

FONTE: Análise do consórcio

O armazenamento de dados em IoT é um desafio de *Big Data*, consequentemente, **bancos de dados não relacionais tendem a ser comuns em diversos casos de uso**. Já os **bancos de dados relacionais devem ficar restritos a cenários específicos**, em que os dados são estruturados e uniformes. Outra forma de tratar o volume de dados vem da adoção do conceito de dados espaço-temporais, por ser uma forma relevante de dividi-los por local e horário de ocorrência. Essa evolução tende a alavancar os dados para diversos usos, como monitoramento de dados para prevenção, dados para valorizar a automação via validação e enriquecimento de dados, além dos mais diversos usos do *analytics*.

A **Inteligência Artificial (IA)** é atualmente incorporada à própria aplicação, com o suporte de bibliotecas padronizadas. Alguns atores, no entanto, buscam oferecer, em suas plataformas, serviços de IA mais ou menos complexos. A adoção dessas plataformas, porém, tem sido restrita, devido ao fato de que o uso eficiente de IA demanda alto grau de customização para explorar características específicas de cada desafio abordado.

Outro ponto que merece destaque é como conciliar a alta demanda de mecanismos de IA com o **pequeno número de profissionais capacitados na área**. O uso de métodos baseados em *transfer learning* pode acelerar o desenvolvimento por meio do reuso de modelos. No entanto um maior desenvolvimento de técnicas de *meta-learning* pode vir a ser a solução adequada no médio e longo prazos.

Adicionalmente, considerando a necessidade de sistemas mais dinâmicos, provavelmente ganhará relevância o **aprendizado a partir de fluxos de dados** (*stream*), em contraposição ao atual domínio das técnicas baseadas em grandes cargas de dados (*batch*). Formas de **aprendizado contínuo**, como aprendizado *online* e por reforço, tendem a crescer em relevância no médio prazo.

No que diz respeito à **experiência do usuário**, várias tecnologias tendem a se desenvolver, como **realidade aumentada**, **realidade virtual** e os **assistentes virtuais**.

5.4 Segurança

5.4.1 Introdução

A camada de segurança compreende importantes funções em todas as demais camadas do framework da IoT definido pela recomendação ITU-T Y.2060[244]. Toda implementação de IoT precisa oferecer segurança e suporte à proteção de privacidade durante todo o ciclo de vida da informação, desde a concepção, passando pelo armazenamento, transmissão, processamento, agregação e mineração. A ITU propõe as seguintes definições para segurança e privacidade:

- **Segurança**: em IoT, todas as "coisas" estão conectadas, o que resulta em ameaças de segurança significativas, tais como: ameaças à confidencialidade, autenticidade e integridade de dados e serviços;
- **Privacidade**: a proteção de privacidade precisa ser amplamente discutida e implementada em IoT. Todas as "coisas" possuem seus respectivos donos e usuários e possuem, consequentemente, dados sensíveis que podem conter informações privadas.

Além disso, a ITU classifica funções de segurança em dois tipos: funções genéricas e funções específicas, detalhadas a seguir

- **Funções genéricas:** não dependem da aplicação/solução em questão e incluem as seguintes funções**:**
  - **Camada de suporte à aplicação**: autorização, autenticação, confidencialidade de dados de aplicação e proteção de integridade, proteção de privacidade, auditoria de segurança e antivírus;
  - **Camada de rede:** autorização, autenticação, utilização de dados e proteção, confidencialidade e integridade dos dados de sinalização;

244 ITU, "Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things". Disponível em: https://www.itu.int/rec/T-REC-Y.2060, acesso em janeiro de 2017.

- **Camada do dispositivo**: autenticação, autorização, validação da integridade do dispositivo, controle de acesso, proteção, confidencialidade e integridade dos dados.

- **Funções específicas:** são direcionadas e estão intimamente ligadas aos requisitos específicos da aplicação ou solução de IoT.

5.4.2 Segurança da Informação em IoT

Acredita-se que em um curto prazo de tempo, dispositivos serão capazes de interagir, comunicar e trocar informações entre si, reagindo aos eventos do mundo físico real sem intervenção direta do ser humano, tornando-se participantes ativos em diversos ambientes como casas, carros, cidades, etc. Com isso, dispositivos se tornam mais vulneráveis a receber ou executar um ataque, gerando inúmeros riscos, tais como violação de privacidade, roubo de identidade e, em casos extremos, ameaças contra a vida humana. Por exemplo, em um ataque a um veículo conectado, o atacante assumiu o total controle do veículo, atuando desde o centro de entretenimento do veículo até o freio e acelerador. Na última grande transformação digital – era da Internet – os ataques cibernéticos aconteciam por meio de computadores; em IoT, no entanto, objetos como carros, geladeiras, câmaras e DVRs IP podem ser alvos de ataques. Ataques a objetos relacionados a IoT tem aumentado e foram amplamente divulgados pela mídia nos últimos meses do ano de 2016[245,246,247].

A segurança é considerada um dos componentes críticos de qualquer solução IoT. A grande maioria dos pesquisadores e instituições afirmam que a adoção em massa de IoT só será possível se a confidencialidade, autenticidade e privacidade dos usuários forem garantidas e explicitadas[248].

Vários pesquisadores têm proposto arquiteturas seguras para IoT, abordando as diversas camadas da segurança em profundidade. Além disso, existem propostas de padronização e normatização que atuam nas técnicas de proteção dos ambientes inteligentes, comunicações entre dispositivos, dados dos sensores e dos mecanismos e algoritmos de criptografia leves apropriados para dispositivos restritos. Ainda não existe um consenso sobre uma arquitetura segura de IoT; deficiências ainda estão presentes nos processos atuais, principalmente nos dispositivos que já se encontram no mercado[249]; todavia, é

[245] Forbes. Disponível em: http://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#4f68e31b3046, acesso em fevereiro de 2017.

[246] SearchSecurity. Disponível em http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet, acesso em fevereiro de 2017.

[247] Kaspersky Lab. Disponível em: https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/, acesso em fevereiro de 2017.

[248] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges". Ad Hoc Networks. 2012.

[249] H. Suo, J. Wan, C. Zou, J. Liu, "Security in the internet of things: A review". International Conference on Computer Science and Electronics Engineering (ICCSEE). 2012.

amplamente aceito que a melhor forma de abordar a segurança em IoT está em implementar segurança desde a concepção da arquitetura a ser utilizada, passando pela definição e desenvolvimento da aplicação, da comunicação, do dispositivo até a conscientização do usuário.

5.4.3 Pilares da Segurança em IoT

Os pilares da segurança em IoT, definidos pela ISO[250], são:

- **Confidencialidade dos dados:** apenas pessoas ou "coisas" autorizadas podem ter acesso e/ou modificar o conteúdo dos dados[251]. Além disso, deve-se considerar todo o ciclo de vida dos dados (armazenamento, transmissão, processamento, agregação e mineração);
- **Integridade dos dados:** garantia que a informação não será modificada entre a origem e o destino sem ser identificada. A integridade dos dados é um tópico importante dentro de segurança da informação. No contexto da IoT, garantir a integridade dos dados é considerado mandatório[252];
- **Disponibilidade:** capacidade de o dispositivo estar acessível e garantir a fluidez dos serviços de sua responsabilidade. Em IoT, ataques do tipo DDoS (*Distributed Denial of Service*) tem se popularizado, principalmente devido ao aumento dos dispositivos com acesso à Internet, além da capacidade de processamento desses dispositivos[253], no caso de ataques direcionados a dispositivos de pequena capacidade;
- **Autenticidade (autenticação e autorização):** capacidade de garantir que remetentes não se passem por terceiros ou que a mensagem sofra alterações durante o envio.

5.4.4 Privacidade

O direito à privacidade é considerado um direito básico e inalienável do ser humano. Sob o aspecto tecnológico, a privacidade se refere às limitações de acesso de outros a um indivíduo ou "coisas"[254].

De forma geral, os usuários devem ter conhecimento pleno das suas informações pessoais durante todo o ciclo de vida das informações (armazenamento, transmissão, processamento, agregação e mineração), se permissão foi disponibilizada, e para qual

250 ISO/IEC 27001:2005. Tecnologia da informação – Sistema de gestão de segurança da informação.

251 D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges". Ad Hoc Networks. 2012.

252 L. Atzori, A. Iera, G. Morabito, "The internet of things: A survey," Computer Networks. 2010.

253 H. Suo, J. Wan, C. Zou, J. Liu, "Security in the internet of things: A review". International Conference on Computer Science and Electronics Engineering (ICCSEE). 2012.

254 X. Caron, R. Bosua, S. Maynard, A. Ahmad. "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective". Computer Law & Security Review.

conjunto de informações, a fim de que os usuários possam revogar o acesso às suas informações a qualquer momento.

5.4.5 Segurança Criptográfica em IoT

O presente estudo levou em consideração as camadas do ITU e adotou uma metodologia de revisão estruturada da literatura, voltada ao entendimento do estado da arte e tendências em criptografia leve (*lightweight cryptography*).

Considerando as camadas tecnológicas para IoT definidas pelo ITU, percebe-se que a segurança criptográfica está presente em todas as camadas, porém em diferentes níveis de intensidade e inovação. De fato, a segurança criptográfica tem desafios maiores na camada de dispositivos. Em particular, a existência de dispositivos de IoT restritos em suas capacidades de processamento (CPU), memória (RAM) e comunicação traz à tona a necessidade de criptografia leve (*lightweight cryptography*).

Neste contexto, de acordo com o NIST[255,256], padrões criptográficos foram projetados para obterem o melhor desempenho em computadores de propósito geral. Porém, recentemente, tem havido implantações de dispositivos muito restritos, com recursos computacionais limitados, mas que ainda assim necessitam implementar criptografia. O NIST afirma que existem diversos tipos de aplicações em IoT nas quais dispositivos muito restritos estão interconectados, com exemplos destas aplicações em sistemas automotivos, redes de sensores, *healthcare*, sistemas de controle distribuído e *smartgrids*.

Ainda de acordo com o NIST[257], uma vez que a maioria dos algoritmos criptográficos foi projetada para ambientes *desktop* e servidor, muitos destes algoritmos não podem ser implementados nos dispositivos muito restritos. Mesmo quando os padrões criptográficos existentes podem ser implementados nos dispositivos muito restritos, o desempenho é geralmente insatisfatório e até proibitivo. Por este motivo, a criptografia leve se faz necessária.

5.4.6 Iniciativas e Padrões

Observa-se que desde o surgimento da Internet, grupos de pesquisadores, instituições e empresas têm se unido para discutir e elaborar projetos e soluções para desafios de segurança. A importância e contribuição de tais projetos é enorme, pois a união de conhecimento e expertises distintos traz à luz novas e melhores soluções, que

255 National Institute of Standards and Technology, agência governamental da administração de tecnologia do Departamento de Comércio dos Estados Unidos.

256 K. A. McKay, L. Bassham, M. S. Turan, N. Mouha, "DRAFT NISTIR 8114 Report on Lightweight Cryptography". 2016.

257 ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

normalmente são compartilhadas, maximizando os benefícios. Algumas dessas iniciativas são listadas a seguir.

5.4.6.1 OWASP - Open Web Application Security Project

O projeto mais amplo do OWASP[258], idealizado e iniciado em dezembro de 2001 para ser totalmente *open source*, tem como principal missão tornar a segurança de *software* mais acessível para a sociedade, no intuito de que decisões sejam tomadas com base em riscos de segurança em *software*.

Foi criado um projeto voltado exclusivamente para a segurança de IoT – Projeto OWASP *Internet of Things* –para auxiliar fabricantes, desenvolvedores e consumidores a entenderem melhor os desafios de segurança associados à IoT e tomem melhores decisões de segurança ao construir, implementar ou avaliar tecnologias de IoT. O projeto define uma estrutura para vários subprojetos de IoT, como superfície de ataque, guias de teste e vulnerabilidades[259].

5.4.6.2 SITP – Secure Internet of Things Project

Iniciativa que reúne esforços da Universidade de Stanford, UC Berkeley e a Universidade de Michigan. O projeto foi iniciado em setembro de 2016 e terá duração inicial de 5 anos, com foco em três áreas fundamentais para segurança em IoT: i. *Analytics*; ii. Segurança, e iii. Desenvolvimento seguro de *hardware* e *software*. O projeto tem como principais objetivos para os próximos cinco anos:

- Pesquisar e definir novos modelos computacionais criptográficos e mecanismos de segurança para dispositivos de IoT a serem seguros por décadas ou mais;
- Pesquisar e implementar em protótipo um *framework* para desenvolvimento seguro de *hardware* e *software*, baseados em código aberto[260].

[258] OWASP. Disponível em: https://www.owasp.org, acesso em janeiro de 2017.

[259] OWASP. Disponível em: https://www.owasp.org, acesso em janeiro de 2017.

[260] Stanford. "Rethinking a Secure Internet of Things". Disponível em: http://iot.stanford.edu/doc/SITP-summary-2016-project.pdf, acesso em janeiro de 2017.

5.4.6.3 IERC - European Research Cluster on the Internet of Things

IERC[261,262] é um *cluster* dos projetos de pesquisa da comunidade europeia financiada pelo Fundo FP7[263]. O objetivo do grupo é explorar o potencial das capacidades baseadas em IoT na Europa.

Com relação à segurança em IoT, o IERC indica que será necessário pesquisar e desenvolver novas soluções de segurança para lidar com os desafios de segurança, os quais, se não forem abordados, podem se tornar barreiras para a implantação em larga escala de IoT[264].

O IERC tem proposto projetos piloto em larga escala para IoT (LSPs IoT – *Large Scale Pilots* IoT) para colocar em prova as tecnologias e aplicações de IoT produzidas pelos centros de pesquisa da Europa. Neste contexto, as recomendações para a implementação dos pilotos para segurança e privacidade são resumidas como[265]:

- Utilizar como referência para as implementações dos LSPs os resultados dos projetos do IERC que abordaram pesquisa, desenvolvimento e implantação de tecnologias e aplicações IoT;
- Utilizar uma abordagem distribuída para cumprir os princípios de segurança fim-a-fim e os requisitos inerentes a IoT;
- Proporcionar soluções técnicas de IoT que minimizam a quantidade de dados coletados e criptografam os dados coletados, enquanto permitem ao usuário final saber quais dados são coletados e como são usados;
- Utilizar mecanismos escaláveis e baseados em contexto nas soluções de privacidade do usuário final/consumidor para proteger os dados pessoais dos indivíduos;
- Desenvolver uma abordagem específica de "Privacidade e Segurança por Design", refletindo o conteúdo desenvolvido pelo WG04 da AIOTI[266][267];
- Proporcionar implementações de IoT interoperáveis e padronizadas nos diferentes domínios de aplicação e em todos os domínios verticais.

261 European Research Cluster on the Internet of Things, organização que visa definir uma visão comum para o desenvolvimento da IoT na Europa.

262 IERC. Disponível em: http://www.internet-of-things-research.eu, acesso em fevereiro de 2017.

263 7 th Framework Programme for Research and Technological - FP7. Disponível em: https://ec.europa.eu/research/fp7/index_en.cfm, acesso em fevereiro de 2017.

264 IERC Internet of Things Applications. AIOTI WG01 – IERC. Disponível em: http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG01Report2015.pdf, acesso em janeiro de 2017.

265 European Comission. Horizon 2020 Work Programme 2016-2017: Internet Of Things Large Scale Pilots. Disponível em: https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots, acesso em janeiro de 2017.

266 Alliance for Internet of Things Innovation (AIOTI), organização criada pela Comissão Européia para promover interação entre os vários atores de IoT na Europa. O relatório fruto do grupo de trabalho WG04 identifica barreiras que podem restringir a IoT, incluindo questões relacionadas a privacidade, segurança e responsabilidade.

267 AIOTI WG04. Disponível em: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-20-0, acesso em fevereiro de 2017.

5.4.6.4 ENISA - European Union Agency for Network and Information Security

A ENISA[268] (*European Union Agency for Network and Information Security*) é uma agência especializada em segurança cibernética criada em 2004, trabalhando em conjunto com governos e indústria para proporcionar recomendações e soluções de segurança da informação e de redes. Recentemente, a ENISA tem oferecido análises detalhadas sobre a segurança cibernética em diversos nichos de aplicação em IoT[269,270,271,272,273,274]. A ENISA[275] estabelece as seguintes boas práticas de segurança organizacional e de operações:

- **Governança de segurança**: especificar papéis e responsabilidades de segurança; criar políticas e procedimentos de segurança; elaborar/oferecer treinamentos e programas de conscientização;
- **Gerenciamento de riscos**: identificar ativos, riscos e ameaças; desenvolver planos de contingência;
- **Conformidade e asseguração**: adotar padrões, realizar auditorias de segurança periódicas; acordar cláusulas contratuais com fabricantes e fornecedores;
- **Adotar medidas de arquitetura de segurança cibernética**: implementar mecanismos de monitoramento e detecção/prevenção de intrusão; reforçar a segmentação (dinâmica) de redes e o uso de sistemas de *firewalls*; utilizar sistemas *antimalwares*; fazer *backups* regularmente.

5.4.6.5 NIST - National Institute of Standards and Technology

O Centro de recursos em segurança computacional (NIST-*Computer Security Resource Center* - CSRC)[276] da divisão de segurança computacional do NIST é um órgão do governo norte americano que facilita o compartilhamento de ferramentas e práticas sobre segurança da informação, promovendo a elaboração de orientações e padrões, assim como identificando fontes de informação para apoiar a indústria, o governo e a academia. Em particular, o NIST-CSRC tem avaliado algoritmos e módulos criptográficos.

[268] ENISA. Disponível em: https://www.enisa.europa.eu, acesso em fevereiro de 2017.

[269] ENISA, "Cyber security and resilience for Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures". 2016.

[270] ENISA, "Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations". 2015.

[271] ENISA, "Cyber security for Smart Cities - An architecture model for public transport". 2015.

[272] ENISA, "Cyber Security and Resilience of smart cars". 2017.

[273] ENISA, "Securing Smart Airports". 2016.

[274] ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

[275] ENISA, "Cyber security and resilience for Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures". 2016.

[276] NIST-CSRC. Disponível em: http://csrc.nist.gov, acesso em fevereiro de 2017.

Recentemente, este instituto tem atuado na elaboração de boas práticas para redes de IoT e criptografia leve[277,278,279].

5.4.6.6 BITAG - Broadband Internet Technical Advisory Group

A BITAG[280] (*Broadband Internet Techbical Advisory Group*) tem como missão reunir engenheiros e outros especialistas para atingir consenso sobre as práticas de gerenciamento de rede de banda larga e outras questões técnicas que afetam os usuários. Fazem parte da BITAG organizações como Mozilla, CISCO, AT&T, T-Mobile, Disney, entre outros. Recentemente, a BITAG tem oferecido análises consolidadas e recomendações de segurança para IoT.

5.4.6.7 IEEE Cyber Security Initiative (CYBSI)

A iniciativa em segurança cibernética do IEEE[281,282] foi lançada em 2014 e tem por objetivo promover a presença on-line para profissionais da IEEE em segurança e privacidade, melhorar a compreensão de estudantes e educadores sobre segurança cibernética, e melhorar os projetos e implementações de segurança cibernética. Recentemente, o IEEE CYBSI tem elaborado documentos voltados ao projeto e implementação seguros de dispositivos de IoT e *softwares* relacionados.

277 ITU, "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

278 J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

279 R. ROSS, M. McEVILLEY, J. C. OREN, "NIST Special Publication 800-160 - Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems". 2016.

280 BITAG – Broadband Internet Technical Advisory Group. Disponível em: http://www.bitag.org, acesso em fevereiro de 2017.

281 Instituto de Engenheiros Eletricistas e Eletrônicos, organização profissional sem fins lucrativos, dedicada ao avanço de tecnologias em engenharia elétrica e eletrônica, telecomunicações, engenharia da computação e disciplinas associadas.

282 IERC Internet of Things Applications. AIOTI WG01 – IERC. Disponível em: http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG01Report2015.pdf, acesso em janeiro de 2017.

5.4.7 Internet das Coisas e Blockchain

Pesquisas[283,284,285,286] apontam que a utilização da tecnologia blockchain pode contribuir para a mitigação dos desafios relacionados à segurança e privacidade, sendo que alguns dos benefícios mais diretos na utilização da tecnologia blockchain são:

- Rastreamento da história única de cada dispositivo, registrando a troca de dados com outros dispositivos, serviços web e usuários humanos;
- Permissão para que dispositivos inteligentes atuem de forma autônoma em uma variedade de transações;
- Monitoramento remoto de ativos de elevado valor para verificar, por exemplo, se estão sendo usados corretamente;
- Monitoramento, controle e autorização de solicitação de determinado equipamento para reposição de alguma peça ou matéria-prima (máquina de lavar solicitando sabão, por exemplo);
- Controle de identidade dos dispositivos de IoT para registro e controle de acesso lógico a diferentes aplicações.

A tecnologia blockchain possui aplicações em uma ampla variedade de áreas, financeiras e não financeiras. Atualmente, instituições financeiras apresentam a maior quantidade de casos de uso; nos últimos três anos foram investidos US$ 1,4 bilhões em projetos blockchain no setor financeiro[287]. As aplicações não financeiras são diversas, passando por IoT descentralizada, controle de registros de propriedade, gestão de direitos autorais, prova de existência de documentos, gestão de identidade, dentre outras.

Observa-se que, independente do setor de aplicação, a tecnologia blockchain permite rastrear a história única de cada dispositivo, registrando a troca de dados com outros dispositivos, serviços web e usuários humanos. Além disso, possibilita que dispositivos inteligentes se tornem agentes independentes, capazes de conduzir uma variedade de transações de forma autônoma.

283 TechTarget. Details emerging on Dyn DNS DDoS attack, Mirai IoT botnet. Disponível em: http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet, acesso em maio de 2017.

284 Dorri A.; Kanhere S.; Jurdak R.; Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. IEEE, disponível em: http://ieeexplore.ieee.org/abstract/document/7917634, acesso em maio de 2017.

285 Jun Zhou J.; Cao Z., Dong X.; Vasilakos A. Security and Privacy for Cloud-Based IoT: Challenges. IEEE, disponível em: http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=7823317, acesso maio de 2017.

286 Fremantle P.; Aziz B.; Kirkham T. Enhancing IoT Security and Privacy with Distributed Ledgers - a Position Paper. Abril de 2017.

287 World Economic Forum. The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. Agosto de 2016.

A medida que o número de dispositivos conectados cresce de milhões para bilhões[288], e governos e corporações buscam controlar dispositivos e dados, pode ser necessária pode ser necessária uma nova estratégia tecnológica para construir soluções de baixo custo que levem em consideração privacidade e segurança.

No nível mais abstrato, as próprias redes podem se tornar autônomas, suplantando sistemas já estabelecidos que dependem de uma autoridade centralizadora[289]. Nesse sentido, qualquer solução de IoT descentralizada deveria suportar: (i) mensagens P2P confiáveis, (ii) comunicação intrinsecamente confiável e (iii) autonomia descentralizada.

Numa visão de IoT descentralizada, blockchain pode ser considerado o arcabouço de suporte ao processamento e coordenação das transações entre dispositivos. Neste contexto, cada dispositivo gerencia seus próprios papéis e comportamento, resultando na *Internet of Decentralized, Autonomous Things*[290].

A tecnologia blockchain poderá suportar, por meio da descentralização: (i) mensagens P2P confiáveis, (ii) comunicação intrinsecamente confiável e (iii) autonomia descentralizada. Com isso, possibilita a criação de malhas de comunicação mais seguras, nas quais os dispositivos de IoT se interconectam de forma confiável, evitando ameaças ao processo de identificação e autorização.

Para isso, é necessário estabelecer um *ledger,* em que cada nó legítimo é registrado. Dessa maneira, os dispositivos serão capazes de identificar e autenticar uns aos outros, estabelecendo uma rede de confiança sem a necessidade de servidores centrais ou autoridades de certificação, possibilitando que a rede seja escalável para suportar bilhões de dispositivos, resolvendo assim um dos desafios relacionados a escalabilidade.

Além disso, a utilização da tecnologia blockchain em IoT pode permitir que as aplicações sejam desenvolvidas e utilizadas com um nível maior de segurança e privacidade, considerando características intrínsecas da tecnologia blockchain, tais como: como segurança, rastreabilidade, imutabilidade e auditoria, assim, IoT e blockchain estarão implementando um "*Ledger of Things*" ou ainda um "*Ledger of Everything*"[291].

O blockchain também pode ajudar a melhorar a segurança de dados pessoais, como por exemplo, informações de dispositivos de monitoramento médicos. Os dados são armazenados de forma segura em um registro distribuído, e os participantes têm acesso

[288] McKinsey. The IoT the value of digitalizing the physical world. Disponível em: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world, acesso em maio de 2017.

[289] IBM Institute of Business Value. Fast forward: Rethinking enterprises, ecosystems and economies with blockchains. Disponível em: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03757usen/GBE03757USEN.PDF, acesso em maio de 2017.

[290] IBM Institute of Business Value. Device democracy: Saving the future of the Internet of Things. Disponível em: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF, acesso em maio de 2017.

[291] Tapscott, D.; Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Maio de 2016.

baseado em regras inteligentes definidas no blockchain (por exemplo, a aprovação de 3 ou mais partes). Isso também pode ajudar a fornecer dados confiáveis do paciente em tempo real para os atores relevantes (como seguradoras, serviços de emergência, etc.) e ajudá-los a liberar pagamentos ou prestar socorro com base em dados mais precisos.

Contudo, é prematuro afirmar que a tecnologia blockchain será a tecnologia predominante para tratar os desafios dos casos de uso de IoT. Para alguns casos de uso, a tecnologia blockchain pode facilitar a implementação, graças a características intrínsecas, tais como:

- **Geração distribuída**: incluindo controle, qualidade e micro-pagament;
- **Prontuários de saúde**: confidencialidade dos dados, auditoria de exames, etc.;
- **Inventário de dispositivos**: verificação do tempo de vida, testes, ações proativas, descarte, etc.;
- **Logística e qualidade da mercadoria**: sensores verificando a temperatura de um frigorífico, tempo de armazenamento, qualidade de armazenagem, tempo de transporte, etc.

5.4.8 Tendências para segurança da informação em IoT

A questão de segurança e privacidade dos dados e usuários deve ser vista como um desafio a ser trabalhado, pois as informações geradas pelos aplicativos de IoT são essenciais tanto para a obtenção de melhores serviços como para a gestão dos dispositivos.

A segurança de dados e a proteção de dados é um desafio no processo de integração para as diversas aplicações IoT a serem desenvolvidas. Os recursos de rede definida por *software* (SDN) e funções de virtualização (NVF) para as plataformas de IoT exigem a implementação de facilidades de automação e disparadores de eventos que devem atuar para isolar esses componentes da operação propriamente dita, atuando como segregador de função – quando necessário – fornecendo assim, segurança em tempo real[292].

A privacidade do usuário final/consumidor provavelmente exigirá uma nova forma de tratativa, no intuito de proteger os dados pessoais dos indivíduos à medida que os objetos inteligentes se tornam cada vez mais digitalizadas, o que pode ser feito por meio de mecanismos escaláveis e baseados em contexto.

As aplicações de IoT requerem uma estrutura flexível baseada em padrões que facilitem o suporte e a implementação de políticas de privacidade e segurança nos aplicativos. As políticas precisam ser claras, fornecer melhores práticas e princípios relacionados à segurança da informação, e oferecer diretrizes para o desenvolvimento de soluções operacionais para questões de privacidade nos diversos domínios de aplicação.

292 IERC Internet of Things Applications. AIOTI WG01 – IERC. Disponível em: http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG01Report2015.pdf, acesso em janeiro de 2017.

Percebe-se que a gestão de segurança para IoT tem sido considerada com mais intensidade pelas grandes áreas de aplicação, tais como hospitais inteligentes[293], cidades inteligentes[294] e transportes inteligentes[295], mas também tem sido relevante para carros autônomos[296] e casas inteligentes[297]. Ao mesmo tempo, as grandes áreas supracitadas não costumam tratar com profundidade os aspectos tecnológicos de dispositivos e *software*s de aplicações para IoT.

Setores da indústria de IoT voltados para a indústria automobilística e carros autônomos manifestam uma grande preocupação com a responsabilização de fornecedores por vulnerabilidades e incidentes ocorridos dentro da cadeia de valor[298]. Medidas de segurança operacional incluem[299]: pesquisas periódicas de vulnerabilidades e validações das premissas de segurança; processos para divulgação responsável de vulnerabilidades e de correções de segurança; oferecimento de interfaces amigáveis para gestão de segurança em serviços e dispositivos.

Finalmente, foram identificadas as seguintes tendências para fabricantes e provedores de soluções de gestão de segurança em IoT[300]:

- Criação de produtos e soluções especializados que atendam aos requisitos de segurança cibernética específicos para nichos de aplicação particulares, tais como hospitais inteligentes[301], cidades inteligentes[302], transportes inteligentes[303], carros autônomos[304] e casas inteligentes[305];
- Aumento da colaboração entre os participantes na criação de padrões específicos para os nichos de aplicação;
- Maior troca de informação sobre riscos e vulnerabilidades entre fabricantes e provedores de solução em geral e em nichos de aplicação;
- Disponibilização de informações sobre segurança cibernética em complemento às orientações já oferecidas sobre sistemas, produtos e soluções.

293 ENISA, "Cyber security and resilience for Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures". 2016.

294 ENISA, "Cyber security for Smart Cities - An architecture model for public transport". 2015.

295 ENISA, "Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations". 2015.

296 ENISA, "Cyber Security and Resilience of smart cars". 2017.

297 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

298 ENISA, "Cyber Security and Resilience of smart cars". 2017.

299 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

300 ENISA, "Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations". 2015.

301 ENISA, "Cyber security and resilience for Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures". 2016.

302 ENISA, "Cyber security for Smart Cities - An architecture model for public transport". 2015.

303 ENISA, "Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations". 2015.

304 ENISA, "Cyber Security and Resilience of smart cars". 2017.

305 ENISA, "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

5.4.9 Conclusões

Independentemente da camada tecnológica, em um curto prazo de tempo, os dispositivos inteligentes ou "coisas" devem se tornar participantes ativos no ambiente, onde serão capazes de interagir e comunicar-se entre si, trocar informações coletadas e reagir aos acontecimentos do mundo físico sem intervenção direta do ser humano. Contudo, essa realidade traz inúmeros desafios referentes à segurança de IoT, como aumento da superfície de ataque à rede, restrição dos dispositivos no sentido de suportar técnicas e mecanismos robustos de segurança, mau uso por parte do usuário e até mesmo falhas de projeto do produto. Assim, a segurança pode ser considerada um dos componentes críticos de qualquer solução de IoT. Por exemplo, a confidencialidade, a autenticidade e a privacidade dos interessados devem ser asseguradas para permitir a adoção em massa de IoT. As principais tendências dessa camada são elencadas a seguir.

Novas **soluções de IoT tendem a ser cada vez mais voltadas para o princípio de *security by design***, considerando desde a arquitetura a ser utilizada, passando pela definição e desenvolvimento da aplicação, da comunicação, do dispositivo, até a conscientização do usuário, seguindo os pilares da segurança em IoT: confidencialidade, integridade, disponibilidade, autenticidade e privacidade.

Os **maiores desafios têm sido observados na camada de dispositivos**, em particular dispositivos restritos em termos de processamento, memória e comunicação, que demandarão **criptografia leve** (*lightweight cryptography*). Uma alternativa é contar com **suporte complementar nos *gateways***, para assegurar proteção fim-a-fim.

No que diz respeito à **segurança das redes**, a adoção de variantes de protocolo de segurança IP para IoT com primitivas criptográficas de chave pública, tais como DTLS (*Datagram Transport Layer Security*), DEX (HIP *Diet Exchange*) e IKEv2, podem atender aos requisitos da IoT relacionados a escalabilidade e interoperabilidade. Adicionalmente, a **segmentação de rede**, técnica amplamente difundida e utilizada como melhor prática nas atuais redes, pode ser essencial em IoT, pois garante que os dispositivos conectados não prejudiquem a segurança da rede, evitando assim o acesso indevido e a possível propagação de *malware* por seu intermédio. Outra possível abordagem seria a utilização de mecanismos dinâmicos de segregação, como controle para conter um ataque e limitar os danos de um incidente.

Em termos de soluções de segurança fim-a-fim (entre o dispositivo e a aplicação), dada a falta de uma padronização amplamente adotada nesta área, observa-se a verticalização por fornecedor, o que desfavorece o amadurecimento de um ecossistema mais robusto, em que o usuário pode adquirir dispositivos e aplicações de fornecedores distintos que interoperem.

Com o amadurecimento da IoT, no que diz respeito à **gestão de segurança para IoT**, a falta de padrões tem levado organismos de padronização a **abordar o assunto de maneira segmentada**, tratando de grandes **áreas temáticas**, tais como casas, saúde, cidades e transportes inteligentes.

6. Atores

Ainda que a IoT esteja em estágio de desenvolvimento, muitos atores já vêm se posicionando com o objetivo de alavancarem competências existentes, criar vantagem competitiva, e se firmarem como atores relevantes no ecossistema de IoT. Além disso, IoT abrange uma grande diversidade de casos de uso, atingindo diversos setores além da tradicional cadeia de TICs.

Tal fragmentação pode gerar oportunidades para atuação em nichos, ou eventualmente possibilitar a entrada de novos atores em alguns setores. Por exemplo, a entrada em operação da operadora SigFox ocupou um espaço deixado pelas prestadoras incumbentes de telecomunicações.

A diversidade inerente à IoT também abre oportunidades para que atores se aglutinem por meio de alianças comerciais, para unir competências e endereçar uma maior quantidade de casos de uso. A falta de um padrão unificado para IoT tem levado ao surgimento de várias alianças com foco em padronização.

Por fim, a IoT pode agregar valor aos negócios de muitas maneiras, como pelo aumento da eficiência operacional, criação de novos modelos de negócio ou melhoria da qualidade de vida. Contudo, a distribuição e a evolução do valor agregado ao longo dos elos da cadeia de valor podem ocorrer de forma desigual, fazendo com que a atuação em alguns elos se torne mais relevante.

Essa seção apresenta o mapeamento e análise dos principais atores de IoT no cenário internacional, suas associações por meio de consócios e as oportunidades de nicho sendo exploradas. A análise é complementada pelas dinâmicas na geração e transferência de valor, modeladas por meio de uma proposta de cadeia de valor, na qual os elos da cadeia representam os papéis desempenhados pelos atores para que o valor gerado pelas

tecnologias de IoT seja entregue ao cliente, ou usuário final. Essa dinâmica da cadeia é apresentada em termos da situação atual e das tendências futuras.

Cumpre ressaltar que, analogamente às tendências tecnológicas observadas, o mapeamento dos atores da cadeia de valor de IoT compreende o levantamento dos principais atores atuantes à época do estudo[306], e não tem por objetivo trazer uma lista exaustiva. Assim, eventualmente, atores mais recentes ou inovadores no ecossistema podem não figurar nas análises realizadas.

[306] Primeiro semestre de 2017.

6.1 Atores mais bem posicionados

A análise de atores mais bem posicionados em cada camada tecnológica (Dispositivos, Conectividade e Rede, Suporte a serviços e aplicações) e nas principais verticais do projeto será apresentada a seguir. Esses atores são, essencialmente, empresas fornecedoras de soluções para IoT.

6.1.1 Método para seleção dos principais *atores*

A seleção visou identificar os principais atores de IoT com base na participação em projetos de IoT no cenário mundial. A classificação foi feita seguindo a abordagem ilustrada no QUADRO 39, que consiste em seis passos:

1. **Seleção de uma base de dados atual e abrangente**: foi escolhida a base de dados elaborada pela empresa IoT Analytics, referência em tendências de mercado para IoT, comunicação M2M e Indústria 4.0. A base de dados consolida 643 projetos de aplicações em IoT desenvolvidos em diversos países[307,308];

[307] A base conta elenca projetos desenvolvidos em 63 países dos cinco continentes. Destes, cerca de 34% dos projetos são de países da Europa, e em torno de 36% são projetos desenvolvidos nos Estados Unidos.

[308] Para cada inciativa, apresentavam-se as seguintes informações: nome do projeto; descrição do projeto; segmento da indústria em que o projeto está inserido; país e região em que o projeto está sendo desenvolvido; página web com detalhes do projeto; informações relativas à empresa que está realizando o projeto e sua motivação; informações relativas aos fornecedores de soluções (segmentados por integrador do projeto ou fornecedor líder, fornecedores de infraestrutura, fornecedores de *software*, fornecedores de conectividade ou outros) e vertical de mercado.

2. **Filtragem dos atores por participação em projetos**: seleção de 313 empresas, originalmente classificados como integradores de projetos, fornecedores de infraestrutura, *software*, *hardware*, conectividade, entre outros;
3. **Filtragem de atores com mais de três participações em projetos de IoT**: com o objetivo de se destacar os atores mais relevantes, foram selecionados aqueles que apresentavam ao menos três participações em projetos de IoT;
4. **Inclusão de atores relevantes**: com o objetivo de não excluir atores relevantes da análise, foram incluídos aqueles que possuíam notória presença no mercado de IoT, apesar de apresentarem menos de três participações em projetos de IoT;
5. **Levantamento de informações complementares**: uma vez obtida uma relação inicial dos atores mais relevantes, foram levantadas as seguintes informações sobre cada um dos atores:
   - Data da criação da empresa;
   - País de origem;
   - Presença no Brasil;
   - Número de funcionários;
   - Página web.
6. **Contabilização dos *atores* por camada e vertical**: atores foram segmentados com base em sua atuação em cada uma das três camadas tecnológicas; verificou-se, inclusive, sua atuação em termos de Segurança de Informação e Gerenciamento. No próximo passo, a atuação nas principais verticais do projeto foi analisada com base nas descrições sobre a aplicação das soluções presentes na base de dados, em termos das seguintes verticais de mercado:
   - Automotivo;
   - Petróleo e gás;
   - Mineração;
   - Bens de cons. e varejo;
   - Cidades Inteligentes;
   - Manufatura avançada;
   - Logística;
   - Saúde;
   - Agricultura;
   - Aeroespacial;
   - Serviços financeiros;
   - Setor público e *utilities.*

QUADRO 39

Método e critérios de seleção dos *players*

1	▪ Seleção de base de dados sobre projetos de IoT (base de dados IoT *Analytics,* 640+ projetos de IoT*)*
2	▪ Ordenação dos *players* por participação nos projetos
3	▪ Filtragem de *players* com mais de três participações
4	▪ Inclusão de *players* com uma ou duas participações e notória presença no mercado de IoT
5	▪ Levantamento de informações complementares (origem, presença, número de funcionários, setor, elos da cadeia, vertical)
6	▪ Contabilização de participação de players por camada, tipo (incumbente, novos entrantes) e vertical

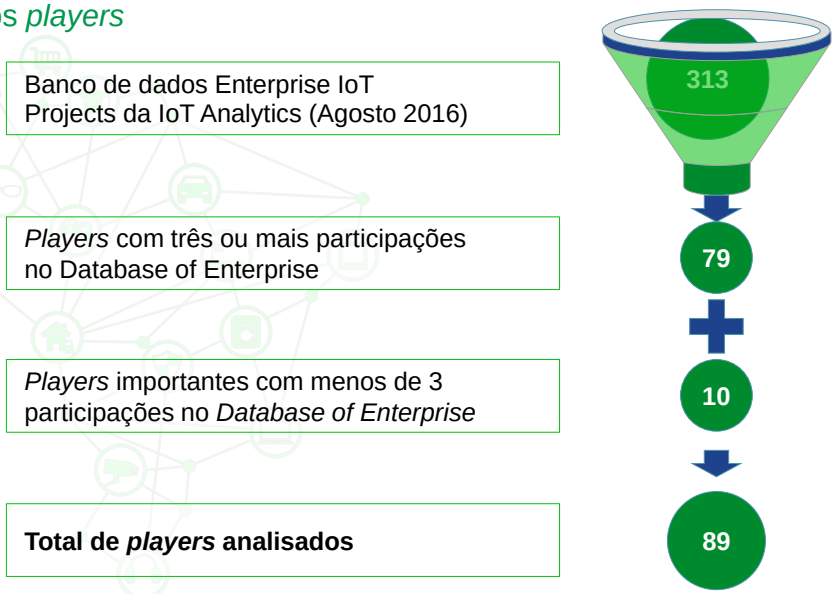
FONTE: Análise do consórcio

6.1.2 Resultados da seleção de atores

O QUADRO 40 sintetiza o resultado do processo de filtragem dos atores, indicando a quantidade resultante nos quatro principais passos da análise.

QUADRO 40

Seleção dos *players*



FONTE: Análise do consórcio

A distribuição dos 313 atores, por frequência de participação nos 643 projetos da base de dados, é apresentada na Tabela 13. Nota-se a tendência de concentração dos *atores* participantes de projetos; a grande maioria dos atores são citados como fornecedores de soluções em um ou dois projetos, enquanto que relativamente poucos *atores* apresentaram participação em mais de dois projetos.

TABELA 13 DISTRIBUIÇÃO DOS *ATORES* POR PRESENÇA NOS PROJETOS

Uma ou duas citações	243
Três a cinco citações	39
Seis a dez citações	19
11 a 20 citações	9
21 a 30 citações	4
Mais de 30 citações	8

Uma vez obtido o número de participações de cada empresa selecionada nos projetos da base de dados, procedeu-se à seleção daquelas que possuíam ao menos três citações, resultando em uma amostre de 79. Posteriormente, foram acrescentadas dez empresas consideradas com notória presença no mercado de IoT e que apresentavam menos de três citações na base de dados da IoT Analytics, resultando na amostra de 89 *atores* considerados nessa análise. A Tabela 14 lista os dez *atores* mais citados como fornecedores dos projetos.

TABELA 14 *ATORES* MAIS CITADOS

Player	Número de Citações
Cisco	166
Silver Spring Networks	91
IBM	71
Intel	55
Libelium	52
Telit	44
Sierra Wireless	42
Huawei	32
Microsoft	26
Jasper	25

A lista completa dos 89 *atores* considerados na análise está representada em ordem alfabética na Tabela 15.

TABELA 15 LISTAGEM DOS *ATORES* SELECIONADOS

Atores com três ou mais citações na IoT Analytics Database 2016			Atores selecionados por notória presença no mercado de IoT
ABB	Dell	Rockwell	Blackberry
Advantech	Digi	Automation	Cloudera
Advanticsys	Echelon	SAP	Glassbeam
Aeris	Electric Imp	Schneider Electric	M2Mi
AeroScout	Enel Sole	SemperCon	Nokia
Altiux	Eurotech	Semtech	NXP Semiconductors
Altizon Systems	EVRYTHNG	Shanghai DS	Oracle
Amazon	eWON	Siemens	Samsung
ArduSat	GE	Sierra Wireless	Splunk
Arqiva	Gemalto	SIGFOX	Thingworx
Arrayent	Green City	Silver Spring	
Arrow Electronics	solutions	Networks	
AT&T	Huawei	SK Telecom	
Atos	IBM	*Software* AG	
Autodesk	Ingenu	Solair	
Autofind	Intel	Telefonica	
Axeda	Jasper	Telensa	
Ayla Networks	KORE Telematics	Telit	
Bitstew Systems	Landis+Gyr	Verizon	
Bosch	Libelium	Vodafone	
Bright Wolf	Mesh Systems	Wi-NEXT	
BSQUARE	Microsoft	Wireless Sensors	
C3 IoT	ntels	Wyless	
Carriots	Numerex	Xively	
Cisco	OSISOFT	Zebra	
Concirrus	Pacific	Zonar Systems	
Cumulocity	environment	Zonoff	
	PTC		
	Qualcomm		

6.1.3 Incumbentes da camada de Dispositivos

Uma vez selecionados os atores com presença significativa em projetos internacionais de IoT, buscou-se uma classificação adicional que representasse um *proxy* para discriminação entre incumbentes e novos entrantes. Essa classificação foi feita principalmente com base no porte dos atores. Assume-se, como critério de incumbentes, empresas que possuíam mais de 200 funcionários. Verificou-se que, em geral, essas empresas apresentam mais de dez anos de existência.

Para a camada Dispositivos, *atores* ofertam soluções que compreendem componentes e dispositivos concentradores, capazes de coletar e enviar os dados, responder a comandos remotos e realizar operações baseadas em configuração prévia. Os incumbentes mais relevantes, de acordo com a participação nos projetos considerados, são exibidos no QUADRO 41.

QUADRO 41

Principais incumbentes da camada de Dispositivos

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Complementando essa análise, a Tabela 16 lista, em ordem alfabética, todos os incumbentes da camada de Dispositivos.

TABELA 16 INCUMBENTES NA CAMADA DE DISPOSITIVOS

ABB	BSQUARE	Nokia	Samsung	Silver Spring
Advantech	Eurotech	Numerex	Schneider	Networks
Arqiva	Gemalto	NXP	Electric	Telit
Arrow	Intel	Semiconductors	Siemens	Xively
Electronics	Landis+Gyr	Qualcomm	Sierra	Zebra
Blackberry		Rockwell	Wireless	Zonar
		Automation	SIGFOX	Systems

6.1.4 Novos entrantes na camada de Dispositivos

Do mesmo modo, definiu-se um novo entrante como sendo uma empresa nova e pequena, isto é, com menos de 10 anos de atuação no mercado e menos de 200 funcionários. Com base nesse critério, o QUADRO 42 apresenta os principais novos entrantes na camada de Dispositivos.

QUADRO 42

Principais novos entrantes na camada de Dispositivos

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

A Tabela 17 apresenta a relação completa dos novos entrantes nessa camada.

TABELA 17 NOVOS ENTRANTES NA CAMADA DE DISPOSITIVOS

Advanticsys	Autofind	EVRYTHNG	Wi-NEXT
Aeris	Bright Wolf	Green City solutions	Wireless Sensors
AeroScout	Echelon	Libelium	
Altiux	Electric Imp	Mesh Systems	
ArduSat	Enel Sole	Telensa	

6.1.5 Incumbentes na camada de Rede

Na camada de Rede, de modo geral, os *atores* ofertam um conjunto de soluções que possibilitam o transporte das informações geradas pelos dispositivos, que são posteriormente tratadas pelos sistemas de armazenamento e análise de dados. Os principais incumbentes são exibidos no QUADRO 43. Observa-se a presença de gigantes dessa indústria, com sólida atuação no setor de redes de comunicações.

QUADRO 43

Principais incumbentes da camada de Rede

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

A relação completa dos incumbentes na camada de rede é listada na Tabela 18.

TABELA 18 INCUMBENTES NA CAMADA DE REDE

ABB	Gemalto	NXP Semiconductors	Silver Spring Networks
Advantech	Huawei	Qualcomm	SK Telecom
Arqiva	Intel	Rockwell Automation	Telefonica
AT&T	KORE Telematics	Samsung	Telit
Cisco	Landis+Gyr	Semtech	Verizon
Cumulocity	Microsoft	Sierra Wireless	Vodafone
Digi	Nokia	SIGFOX	Zebra
Eurotech			

6.1.6 Novos entrantes na camada de Rede

Os *atores* classificados como novos entrantes e com maior presença na camada de Rede são apresentados no QUADRO 44.

QUADRO 44

Principais novos entrantes na camada de Rede

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

A relação completa dos *atores* classificados como novos entrantes, em ordem alfabética, para essa camada, é apresentada na Tabela 19.

TABELA 19 NOVOS ENTRANTES NA CAMADA DE REDE

Advanticsys	Echelon	Libelium	Wi-NEXT
AeroScout	Electric Imp	Mesh Systems	Wyless
Autofind	eWON	ntels	
Bright Wolf	Ingenu	Telensa	

6.1.7 Incumbentes na camada de Suporte a serviços e aplicações

De modo geral, *atores* da camada de Suporte a serviços e aplicações oferecem soluções que possibilitam a coleta, armazenamento e análise das informações geradas nos dispositivos inteligentes, segundo regras de negócios ou aplicações específicas, com vistas à geração de valor para o usuário final. Além disso, esta camada visa prover a visualização e o gerenciamento dos dispositivos inteligentes conforme as regras de negócio previamente estabelecidas.

Os incumbentes de maior relevância da camada são exibidos no QUADRO 45. Nota-se que esta camada apresenta uma maior concentração de *atores*, abrangendo, inclusive, *atores* com presença marcante em outras camadas. Exemplo disso são a Verizon e a AT&T, conhecidas por sua atuação em Redes.

QUADRO 45

Principais incumbentes da camada de Suporte a serviços e aplicações

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

A relação completa dos *atores* classificados como incumbentes, em ordem alfabética, para a camada de Suporte a serviços e aplicações, é apresentada na Tabela 20.

TABELA 20 PRINCIPAIS INCUMBENTES NA CAMADA SUPORTE A SERVIÇOS E APLICAÇÕES

ABB	Dell	NXP Semiconductors	Silver Spring Networks
Advantech	GE	Oracle	SK Telecom
Amazon	Gemalto	OSISOFT	*Software* AG
AT&T	Huawei	PTC	Splunk
Atos	IBM	Qualcomm	Telit
Autodesk	Jasper	Rockwell Automation	Thingworx
Blackberry	KORE Telematics	SAP	Verizon
Bosch	Landis+Gyr	Schneider Electric	Vodafone
BSQUARE	Microsoft	Siemens	Xively
Cisco	Nokia	Sierra Wireless	Zebra
Cloudera	Numerex	SIGFOX	Zonar Systems
Cumulocity			

6.1.8 Novos entrantes na camada de Suporte a serviços e aplicações

Ainda na camada de Suporte a serviços e aplicações, os *atores* classificados como novos entrantes e com maior relevância são exibidos no QUADRO 46. Observou-se que a camada de Suporte a serviços e aplicações destaca-se das demais em termos de atuação de novos *atores*. Em geral, são empresas jovens, com menos de 10 anos, com foco, principalmente, no segmento de análises computacionais.

QUADRO 46

Principais novos entrantes na camada de Suporte a serviços e aplicações

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

A relação completa dos novos entrantes selecionados para a camada de Suporte a serviços e aplicações apresenta-se na Tabela 21.

TABELA 21 NOVOS ENTRANTES NA CAMADA DE SUPORTE A SERVIÇOS E APLICAÇÕES

Advanticsys	Bitstew Systems	eWON	SemperCon
Aeris	C3 IoT	Glassbeam	Shanghai DS
Altiux	Carriots	Green City solutions	Solair
Altizon Systems	Concirrus	Libelium	Telensa
Arrayent	Echelon	M2Mi	Wi-NEXT
Axeda	Electric Imp	Ntels	Wyless
Ayla Networks	EVRYTHNG	Pacific environment	Zonoff

6.1.9 *Atores* de Segurança de Informação

Ofertas de soluções de segurança para IoT são orientadas, principalmente, para as camadas de Rede e de Suporte a serviços e aplicações. A maioria dos *atores* oferece soluções para a camada de Suporte a serviços e aplicações, enquanto que uma pequena parte oferece soluções para ambas camadas. O QUADRO 47 apresenta os *atores* que ofertam soluções de segurança da informação.

QUADRO 47

Players com ofertas de Segurança da informação

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.1.10 *Atores* presentes no Brasil

Além da identificação dos principais *atores* por camadas, buscou-se identificar quais deles atuam no Brasil. Com base em informações declaradas em suas respectivas páginas na Internet, foi possível verificar os *atores* com atuação no país, sendo considerada a presença de um escritório ou representante local no Brasil. Dentre os 89 *atores* selecionados, 39 deles (aproximadamente 43%) indicaram presença no Brasil. A Tabela 22 relaciona, em ordem alfabética, os *atores* com declarada atuação no Brasil. Notou-se que, na maioria dos casos, são empresas de grande porte com atuação em diversos países.

QUADRO 48

Players com presença no Brasil

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

TABELA 22 *ATORES* PRESENTES NO BRASIL

ABB	Gemalto	Rockwell Automation
Advantech	Huawei	Samsung
Amazon	IBM	SAP
Arrow Electronics	Intel	Schneider Electric
AT&T	KORE Telematics	Siemens
Atos	Landis+Gyr	Sierra Wireless
Autofind	Microsoft	SIGFOX
Blackberry	Nokia	Silver Spring Networks
Bosch	NXP Semiconductors	*Software* AG
Cisco	Oracle	Telefonica
Dell	OSISOFT	Telit
eWON	PTC	Vodafone
GE	Qualcomm	Zebra

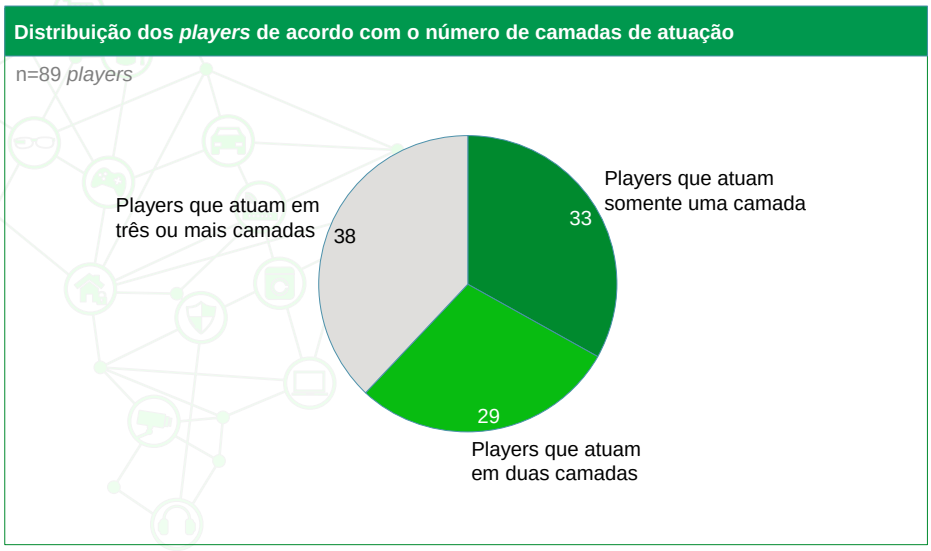
6.1.11 *Atores* segmentados pelo número de camadas de atuação

A atuação de *atores* em distintas camadas foi avaliada. Verificou-se que os principais *atores* geralmente ofertam soluções de IoT em distintas camadas. Foram observados, por exemplo, *atores* com ofertas fim a fim de *Smart Home* que abrangem as três camadas. Isto é, disponibilizam sensores ou objetos inteligentes, soluções de conectividade, armazenamento em nuvem, análise dos dados coletados e opções de controle à distância dos objetos inteligentes.

O QUADRO 49 apresenta os percentuais de atuação dos *atores* em termos do número de camadas nas quais atuam. Observa-se que 38% deles oferecem soluções de IoT nas três ou mais camadas (segurança e gerenciamento).

QUADRO 49

Atuação dos *players* por camada

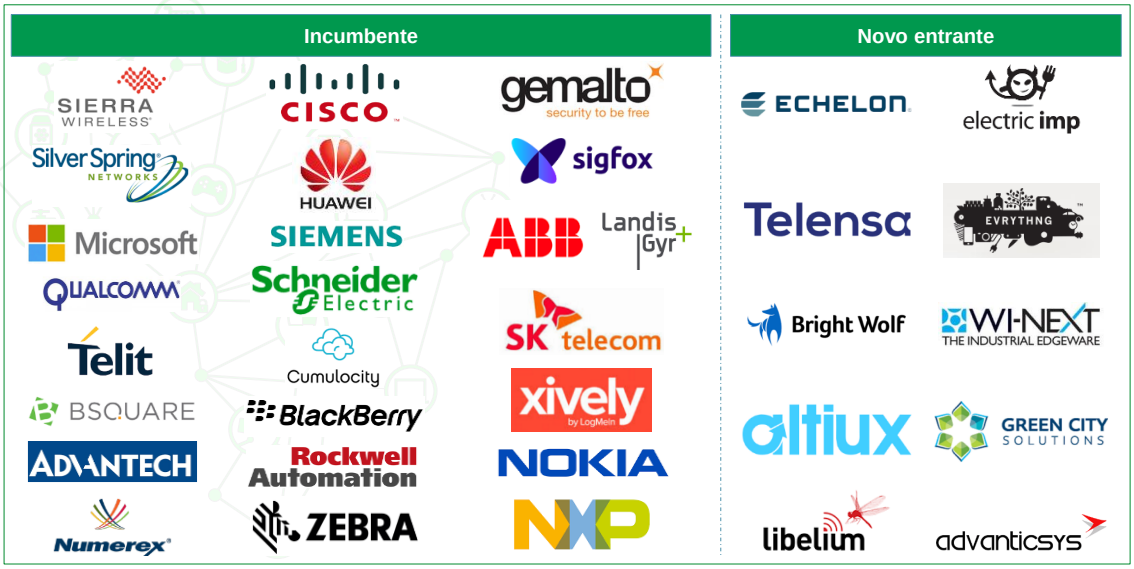


FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Para *atores* que oferecem soluções em três ou mais camadas, o QUADRO 50 apresenta-os classificados entre incumbentes e novos entrantes.

QUADRO 50

Players com atuação em três ou mais camadas



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Uma vantagem competitiva desses *atores* é a possibilidade de ofertarem soluções fim a fim integradas, em múltiplas camadas, eventualmente para uma vertical específica.

6.1.12 *Atores* segmentados por porte nas camadas

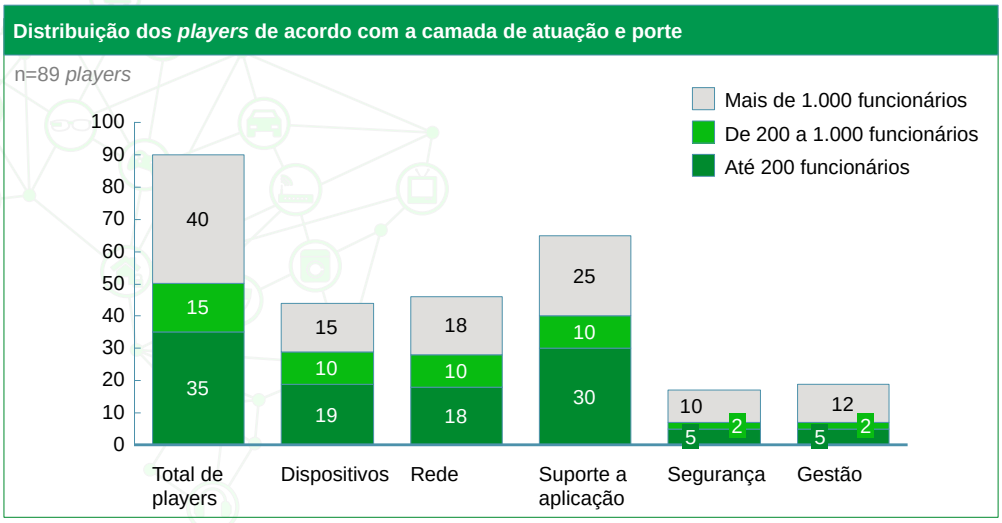
Dada a relevância de se compreender melhor a distribuição de *atores* por porte e por camada, buscou-se quantificar esses aspectos. Por exemplo, a elevada participação de *atores* de pequeno porte em uma camada pode indicar oportunidades para novos entrantes. Desse modo, realizou-se uma segmentação do porte dos *atores*, com base no número de funcionários, da seguinte forma:

- **Pequenos *atores*:** até 200 funcionários;
- **Médios *atores*:** entre 200 e 1000 funcionários;
- **Grandes *atores*:** mais de 1000 funcionários.

O resultado dessa distribuição, por camada, incluindo Segurança de Informação e Gerenciamento de Dispositivos, é apresentado no QUADRO 51. Verifica-se que a camada de Suporte a serviços e aplicações é a preferida, em números absolutos, tanto pelos grandes quanto pelos pequenos *atores*. A camada de Rede se mostrou a segunda preferida entre os grandes *atores*, enquanto que a camada de Dispositivos foi a segunda camada com maior participação de pequenos *atores*.

QUADRO 51

Distribuição dos *players* por porte e atuação em verticais de mercado



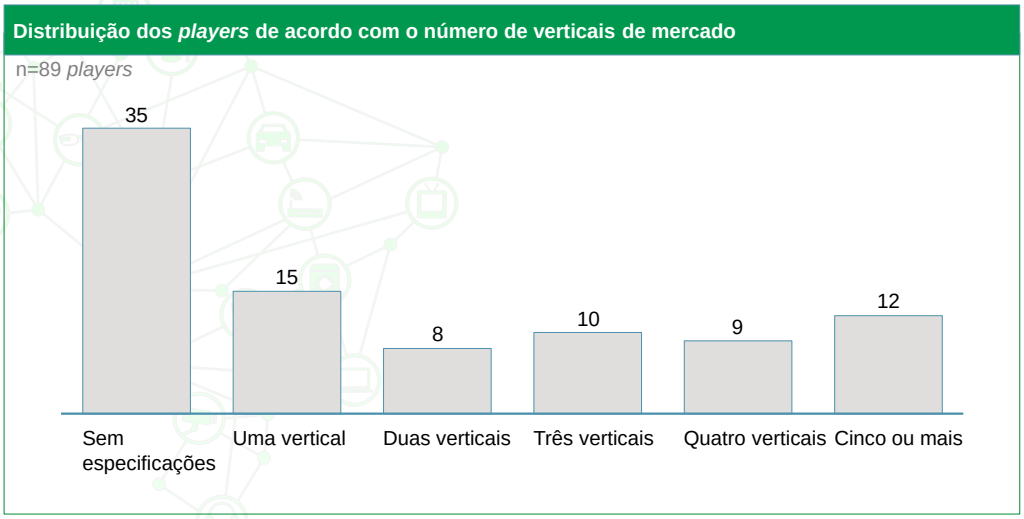
FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.1.13 *Atores* segmentados por presença nas verticais

Embora o estudo nas verticais de aplicação de IoT será aprofundado mais adiante, considerou-se relevante aportar uma análise de *atores* segmentados por vertical, como subsídio para a seleção de verticais, na próxima fase do estudo. Primeiramente, quantificou-se a participação dos *atores* por número de verticais onde declaram atuar. O QUADRO 52 apresenta o resultado dessa análise.

QUADRO 52

Players segmentados por presença nas verticais de mercado



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Observa-se que a maioria dos *atores* analisados não especifica a vertical de atuação. De modo geral, esses *atores* oferecem uma plataforma genérica, que pode ser customizada para atender a uma vasta gama de soluções. Além disso, a segunda maior concentração de *atores* oferece soluções para uma única vertical de mercado. Em geral, essas soluções são extremamente especializadas e, em muitos casos, são soluções de nichos de mercado.

6.1.14 Principais *atores* por vertical

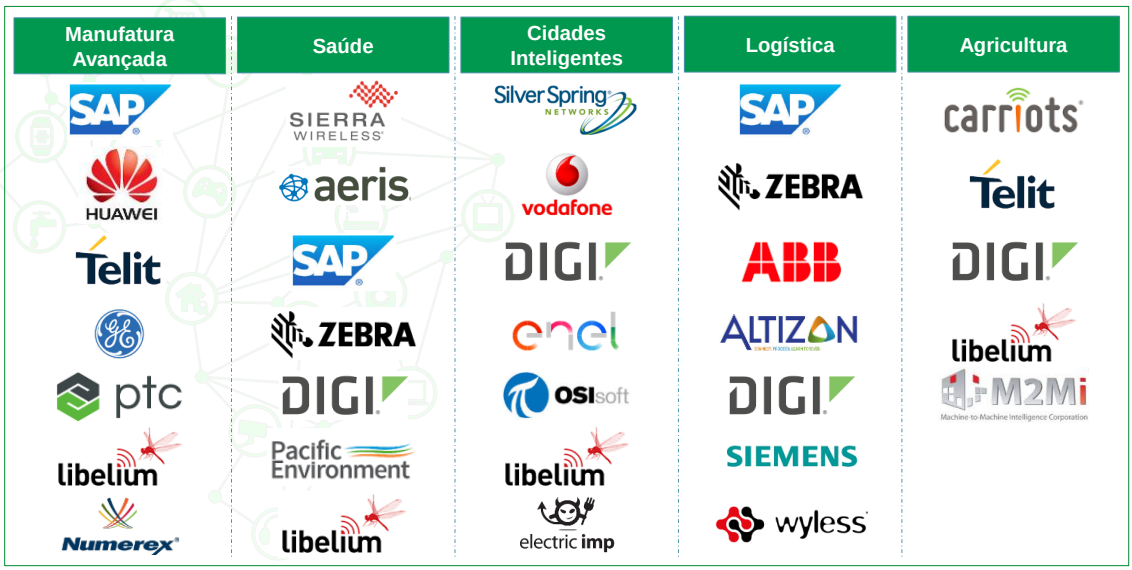
Adicionalmente, realizou-se uma análise para identificação dos *atores* nas principais verticais de mercado consideradas no estudo, isto é:

- Manufatura avançada;
- Saúde;
- Cidades Inteligentes;
- Logística;
- Agricultura;
- Setor público e *utilities*;
- Automotivo;
- Petróleo e gás;
- Bens de consumo e varejo;
- Serviços Financeiros.

O QUADRO 53 e o QUADRO 54 apresentam a atuação dos principais *atores*, nessas verticais. Observa-se que grandes *atores*, em geral, ofertam soluções para diversas verticais. Foram excluídos *atores* que não especificaram suas verticais de atuação.

QUADRO 53

Players posicionados nas verticais de mercado (1/2)



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

QUADRO 54

Players posicionados nas verticais de mercado (2/2)

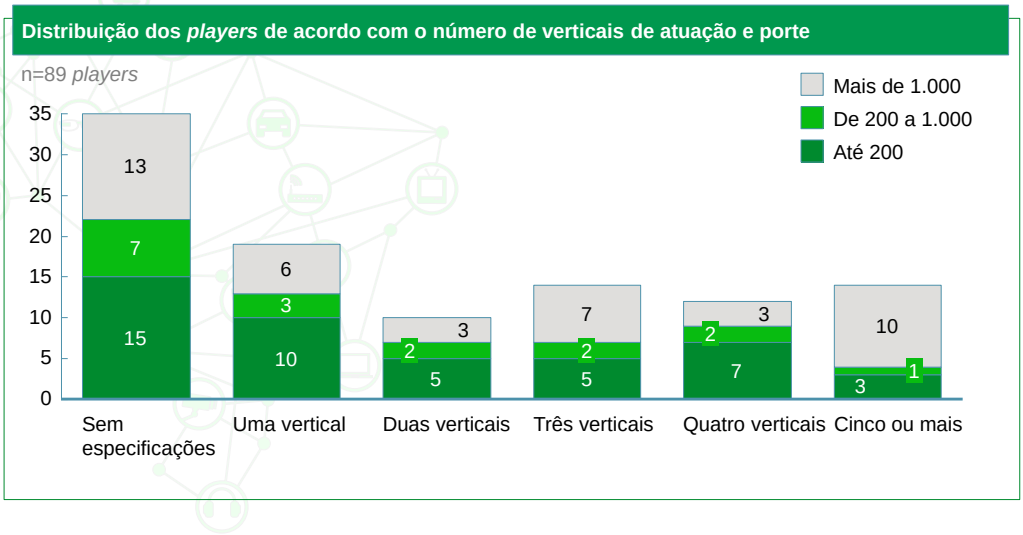
FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.1.15 Segmentação dos *atores* por porte nas verticais

Por fim, com objetivo de entender melhor o perfil dos *atores* nas verticais de mercado, realizou-se uma segmentação em função da vertical e do porte (quantidade de funcionários). O QUADRO 55 mostra essa segmentação. Verifica-se que a maioria dos *atores* médios não especificam a vertical de mercado, ou seja, ofertam soluções genéricas, que pode ser customizada a fim de atender uma ampla gama de soluções. Os grandes *atores*, por sua vez, atuam principalmente em cinco ou mais verticais. A maioria dos *atores* de pequeno porte oferece soluções genéricas, sem especificação de vertical. Entretanto, existe uma parcela significativa desses que atuam somente em uma vertical de mercado.

QUADRO 55

Players por porte e atuação em verticais de mercado



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.1.16 Conclusões

A análise dos *atores* mais bem posicionados em IoT foi desenvolvida a partir de uma base de dados das principais iniciativas internacionais[309], que descreve, caso a caso, os *atores* envolvidos e os tipos de solução fornecidas.

A análise permitiu verificar que grandes *atores* atuam, em geral, em mais de uma camada e vertical de mercado. Empresas de menor porte, por sua vez, atuam principalmente em um vertical única, e na camada de Suporte a serviços e aplicações, ofertando, na maioria dos casos, soluções para análises computacionais, que podem ser customizadas para mercados de nicho. A camada de Suporte a serviços e aplicações destaca-se, também, por ser a que apresenta o maior número de *atores*.

No Brasil, com o desenvolvimento desse mercado, há espaço para a entrada de novos *atores* internacionais, ou o desenvolvimento de novos entrantes, já que, dentre aqueles analisados, apenas 43% atuam localmente, entre os quais predominam *atores* de grande porte e de reconhecida atuação internacional.

[309] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

6.2 Principais Alianças e Relações Comerciais

6.2.1 Consolidação das principais alianças por camada

A partir da análise dos principais *atores*, buscou-se identificar as alianças mais representativas do universo de IoT. O termo "aliança", aqui discutido, compreende a associação de empresas e representantes de governos e da sociedade, com o objetivo de estabelecer padrões técnicos a serem adotados pela indústria de IoT, facilitando a interoperabilidade entre os componentes das soluções. Algumas alianças buscam desenvolver e disseminar práticas e conhecimentos que auxiliem na difusão das soluções. É importante notar que as alianças não se referem a associações comerciais entre *atores*.

Segundo esse conceito, foram identificadas alianças que se destacam no âmbito da IoT; a participação dos *atores* nessas alianças foi verificada, principalmente enquanto patrocinadores (*sponsors*) dessas alianças. Considerou-se que a participação, enquanto patrocinador indicaria um elevado interesse na missão da aliança, bem como na possibilidade de participação em ações deliberativas.

O conjunto de alianças consideradas nessa análise foi obtido a partir de um guia de alianças e consórcios, denominado *Handbook: Internet of Things Alliances and Consortia*[310]. Nesse guia encontram-se segmentadas as alianças em algumas camadas tecnológicas, distintas das camadas desse estudo, e em algumas verticais.

[310] Handbook. Internet of Things Alliances and Consortia. Disponível em: http://www.postscapes.com/internet-of-things-alliances-roundup/, acesso em 21/02/2017.

Primeiramente, analisou-se a distribuição das alianças por camadas, conforme apresentado em suas respectivas páginas na Internet. Em um segundo momento, verificaram-se quais *atores* patrocinadores faziam parte da relação dos principais *atores*, identificados anteriormente. O QUADRO 56 apresenta o resultado da estratificação das alianças nas camadas da arquitetura de IoT.

QUADRO 56

Estratificação das alianças por camada da arquitetura de IoT

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Além da estratificação das alianças, buscou-se registrar uma breve descrição para cada aliança, incluindo a missão, principais iniciativas, membros e página na *web*.

6.2.1 Alianças – Dispositivos

Nesta seção, apresenta-se essa descrição sobre as alianças relativas à camada Dispositivos. Além de informações na página *web* das alianças, houve complementação de informações a partir de suas páginas na plataforma *Linkedin*.

6.2.1.1 GSA – Global Semiconductor Alliance

A GSA Alliance foi criada em 1994, com foco de atuação no segmento de semicondutores, desempenhando um papel vital após o surgimento e adoção, em escala mundial, do modelo de negócios *fabless*, que concentra esforços no design e terceiriza a fabricação de dispositivos e *chips*.

A GSA realiza, com frequência, eventos globais e regionais com foco na indústria de semicondutores a fim de promover oportunidades de *networking* aos seus membros, bem como a participação em programas de elevado conteúdo técnico. As principais características da *GSA Alliance* são:

- **Missão:**
  - Promover o crescimento e a rentabilidade de toda a cadeia de suprimentos de semicondutores, com foco no modelo de negócio *fabless* e na inovação;
  - Identificar e articular oportunidades de negócio;
  - Estimular o empreendedorismo do setor de semicondutores;
  - Fornecer dados de inteligência de mercado a seus membros.

- **Iniciativas relacionadas à IoT:**
  - Fomentar estudos sobre o papel da IoT no segmento de semicondutores;
  - Identificar direcionadores e oportunidades associadas à IoT para a indústria de semicondutores.

- **Principais membros**: Extensa lista de fabricantes, empresas prestadoras de serviços, etc.

- **Página web**: http://www.gsaglobal.org/

6.2.1.2 Continua Alliance

A *Continua Health Alliance* foi criada em 2006 e atua para estabelecer sistemas de dispositivos e serviços de *e-health plug and play*. Sua atuação se concentra em três categorias:

- Gerenciamento de doenças crônicas;
- Envelhecimento independente;
- Saúde e aptidão física.

Principais características da *Continua Alliance*:

- **Missão:**
  - Desenvolver diretrizes que permitirão aos fornecedores criar sensores interoperáveis, redes domésticas, plataformas de *e-health* e serviços de saúde e bem-estar.

- **Iniciativas relacionadas à IoT:**
  - Estabelecer um programa de certificação de produtos com um logotipo reconhecível pelo consumidor, garantindo a interoperabilidade entre produtos certificados;
  - Colaborar com as agências reguladoras do governo para fornecer métodos para o gerenciamento seguro e eficaz de diversas soluções de fornecedores;
  - Trabalhar com líderes nas indústrias de cuidados de saúde para desenvolver novas formas de abordar os custos de fornecer sistemas de *telehealth* pessoal.

- **Principais membros**: BodyMedia, Cisco Systems, GE Healthcare, IBM, Intel, Kaiser Permanente, Medtronic, Motorola, Nonin Medical, Omron Healthcare, Panasonic, Partners HealthCare, Polar Electro, Royal Philips Electronics, RMD Networks, Samsung Electronics, Sharp, The Tunstall Group, Welch Allyn, Zensys.

- **Página web**: http://www.pchalliance.org/continua/

6.2.2 Alianças – Rede

Nesta seção, serão abordadas as alianças relativas à camada de Rede.

6.2.2.1 LoRa

A Aliança LoRa é uma associação aberta e sem fins lucrativos criada por líderes da indústria com a missão de padronizar soluções de *Low Power Wide Area Networks (LPWAN),* no contexto de IoT, comunicação máquina-a-máquina *(M2M),* cidades inteligentes, e aplicações industriais. Os membros da aliança colaboram para impulsionar o sucesso global do protocolo LoRaWAN, compartilhando conhecimentos e experiências para garantir a interoperabilidade entre operadores em um único padrão global aberto.

Principais características da *LoRa Alliance*:

- **Missão:**
  - Padronizar Low Power Area Networks (LPWAN) em desenvolvimento com vistas a fomentar aplicações de IoT, M2M, cidades inteligentes e aplicações industriais;
  - Compartilhar conhecimento e experiências para a formação de padrões abertos globais que garantam a interoperabilidade.

- **Iniciativas relacionadas à IoT:**
  - Promover o protocolo LoRa como alternativa para comunicação de aplicações IoT;
  - Elaborar especificações e programas de certificação de produtos compatíveis;
  - Trabalhar na evolução do protocolo LoRa.

- **Principais membros:** Actility, Bouygues, Cisco, Flashnet, Giesecke & Devrient, ENDETEC, IBM, Kerlink, KPN, Orange, Proximus, Sagemcom, Semtech, SK Telecom, Life.augmented, ZTE.

- **Página web**: https://www.lora-alliance.org/

6.2.2.2 Wi-Fi Alliance

A *Wi-Fi Alliance* é uma organização sem fins lucrativos fundada em 1999 que promove a tecnologia Wi-Fi e certifica os produtos Wi-Fi que estejam em conformidade com o padrão IEEE 802.11 de interoperabilidade.

Principais características da *Wi-Fi Alliance*:

- **Missão:**
  - Coordenar, de forma colaborativa a evolução das tecnologias WiFi, de forma a atender requisitos de comunicação, como, por exemplo, latência, velocidade, alcance nos mais variados ambientes, tais como, residências, prédios, cidades, indústrias, etc;
  - Desenvolver e elaborar especificação de novos padrões para tecnologias Wi-Fi;
  - Promover a adoção das tecnologias Wi-Fi;
  - Defender regras proporcionais para uso do espectro de RF;
  - Garantir compatibilidade das novas tecnologias com os produtos no mercado.

- **Iniciativas relacionadas à IoT:**
  - Wi-Fi HaLow baseado na tecnologia IEEE 802.11 ah para dispositivos com restrições de energia e requisitos de comunicação de longo alcance;
  - *Dedicated Short Range Communications* (DSRC) – baseado na tecnologia IEEE 802.11p, com foco na comunicação de veículos para veículos (V2V).

- **Principais membros:** Apple, Broadcom, Cisco, Comcast, Dell, Huawei, Intel, LG, Microsoft, Nokia, Qualcomm, Samsung, Sony, T-Mobile USA e Texas Instruments.

- **Página web:** https://www.wi-fi.org/

6.2.2.3 Bluetooth Special Interest Group (SIG)

O *Bluetooth Special Interest Group (SIG)*, criado em 1998, é o órgão que supervisiona o desenvolvimento de padrões Bluetooth, o licenciamento das tecnologias Bluetooth e marcas comerciais para os fabricantes. A SIG não produz ou comercializa produtos habilitados com Bluetooth.

A tecnologia Bluetooth fornece um padrão para troca de informações entre dispositivos sem fio, como telefones celulares, laptops, computadores. Oferecendo uma solução de curto alcance e de baixo custo, desenvolvido inicialmente pela Ericsson, atualmente a tecnologia Bluetooth é utilizada por diversos fabricantes.

Principais características da *Bluetooth Special Interest Group*:

- **Missão:**
  - Fortalecer a marca *Bluetooth* por meio do trabalho colaborativo de seus membros com vistas a criar tecnologias sem fio inovadoras para conexão de diversos dispositivos;
  - Definir de forma colaborativa novos padrões do *Bluetooth*;
  - Definir programas de certificação.

- **Iniciativas relacionadas à IoT:**
  - *Bluetooth 5*: evolução da tecnologia *Bluetooth* com vistas a atender os requisitos de conectividade sem fio para a IoT por meio do aumento do alcance da comunicação, da velocidade e da capacidade de transmissão das mensagens.

- **Principais membros:** Apple, Ericsson AB, Intel Corporation, Lenovo, Microsoft, Nokia, Toshiba.

- **Página web:** https://www.bluetooth.com

6.2.2.4 IEEE

O Instituto de Engenheiros Eletricistas e Eletrônicos (*Institute of Electrical and Electronics Engineers – IEEE*), é uma organização sem fins lucrativos fundada nos Estados Unidos em 1963 pela fusão do Instituto de Engenheiros de Rádio (IRE) com o Instituto Americano de Engenheiros Eletricistas (AIEE). É a maior organização profissional do mundo dedicada ao avanço da tecnologia em benefício da humanidade.

Principais características do *IEEE*:

- **Missão:**
  - Promover a inovação tecnológica e buscar a excelência para o benefício da humanidade;
  - Organizar grupos de trabalhos com vistas à definição de padrões e especificações aplicáveis a diversas áreas da ciência e da indústria.

- **Iniciativas relacionadas à IoT:**
  - Definir padrões para comunicação sem fio;
  - Desenvolver o ecossistema de IoT por meio de grupos de trabalho.

- **Principais membros**: Aberto a profissionais e estudantes.

- **Página web**: https://www.ieee.org/index.html

6.2.2.5 ZigBee

A aliança Zigbee foi fundada em 2002, e colabora para criar e evoluir padrões abertos universais para os produtos que transformam a maneira como as pessoas vivem, trabalham e jogam. Zigbee designa um conjunto de especificação estabelecido na IEEE-802.15.4 para a comunicação sem fio entre dispositivos, caracterizado por baixa emissão de potência, baixa taxa de transmissão e baixo custo de operação.

Principais características do *ZigBee Alliance:*

- **Missão:**
  - Promover os produtos e serviços baseados nos padrões ZigBee;
  - Contribuir para o estabelecimento dos padrões da IoT;
  - Tornar-se uma entidade bem posicionada no ecossistema IoT.

- **Iniciativas relacionadas à IoT:**
  - Desenvolver padrões de conectividade sem fio para diversas aplicações, tais como: casas inteligentes, iluminação, saúde, indústrias, comércio varejista, etc.;
  - Elaborar programas de certificação de produtos;
  - Apoiar o desenvolvimento de produtos e serviços para IoT.

- **Principais membros**: COMCAST, HUAWEI, Itron, Kroger, Landis+Gyr, LEEDARSON, Legrand, Midea, NXP, Philips, Schneider Electric, Silicon Labs, SmartThings, Somfy, Texas Instruments, Wulian.

- **Página web**: http://www.zigbee.org/

6.2.2.6 OMA – Open Mobile Alliance

A *Open Mobile Alliance (OMA)* é uma organização sem fins lucrativos que desenvolve padrões abertos para a indústria de telefonia móvel. A OMA foi formada em 2002 por grandes operadores mundiais de dispositivos móveis, fornecedores de dispositivos e redes, empresas de tecnologia da informação e fornecedores de conteúdo como ponto focal da indústria para o desenvolvimento de especificações para fabricantes de serviços móveis.

Principais características da *OMA*:

- **Missão:**
  - Oferecer especificações abertas para a criação de serviços interoperáveis que funcionam em todos os limites geográficos, em qualquer rede. As especificações da OMA suportam bilhões de terminais fixos e móveis novos e existentes em uma variedade de redes móveis, incluindo redes de operadores celulares tradicionais e redes emergentes que suportam a comunicação de dispositivos máquina a máquina.

- **Iniciativa relacionada à IoT:**
  - MimOMNA Lightweight M2M (LWM2M).

- **Principais membros**: 101 membros distribuídos entre *Wireless Vendors*, Empresas de tecnologia de informação, operadores móveis e provedores de conteúdo e aplicação.

- **Página web**: http://openmobilealliance.org

6.2.2.7 Thread Group

O *Thread Group* foi criado em 2014 com o objetivo de criar a melhor maneira de conectar e controlar produtos em residências. O *Thread Group* usa o 6LoWPAN, que utiliza o protocolo sem fio IEEE 802.15.4 com malha de comunicação, como ZigBee e outros sistemas.

Principais características do *Thread Group*:

- **Missão:**
  - Oferecer uma rede *mesh* sem fio segura para casas e seus produtos conectados;
  - Focar na educação, marketing, promoção e garantia de uma grande experiência por meio de uma rigorosa e significativa certificação de produtos.

- **Iniciativas relacionadas à IoT:**
  - Endereçamento: DHCPv6;
  - Roteamento de Mensagens;
  - Segurança: Criptografia (AES128);
  - Suporte à camada de transporte: 6LoWPAN;
  - Suporte à camada de aplicação: CoAP e Smart Objects, Zigbee Smart Energy 2.0, Echonet Lite.

- **Principais membros:** Arm, Nest, Somfy, Big Ass Fans, Samsung, Tyco, Freescale, Silicon Labs, Yale.

- **Página web:** http://www.threadgroup.org

6.2.2.8 DASH7 Alliance

A *DASH7 Alliance (D7A)* foi criada em 2009 por um grupo de empresas e universidades. Os objetivos do grupo são gerenciar a evolução do protocolo Dash7, baseado na ISO 18000-7, e criar uma tecnologia completa e interoperável de RF para troca de dados entre a rede e dispositivos de sensores sem fio em uma escala de bloco (300m-1 km).

Principais características da *DASH7 Alliance:*

- **Missão:**
  - Coordenar, de forma colaborativa, a evolução das tecnologias aderentes aos protocolos DASH7, baseados nas especificações ISSO 18000-7;
  - Aprimorar a tecnologia DASH7 além das suas capacidades atuais, habilitando-a a participar em aplicação de segurança, automação e controle em diferentes ambientes.

- **Iniciativas relacionadas à IoT:**
  - Promover a utilização do padrão DASH7 em aplicações que requeiram sensores e atuadores de baixo consumo (Ultra Low Power);
  - Disponibilizar especificações e APIs para uso geral;
  - Estimular o uso do DASH7 em aplicações IoT em variados cenários.

- **Principais membros:** Arynga, Cortus, Institute of Logistics and Warehousing, Kawantech, Matrix, Normir, University of Antwerp, Wroclaw University of Technology, VISN, WizziLab S.A.S.

- **Página web**: http://www.dash7-alliance.org/

6.2.2.9 Wi-Sun

A *Wi-SUN Alliance* é uma associação global da indústria dedicada à conectividade. O foco da Wi-Sun é o desenvolvimento mundial de Redes de Comunicações Sem Fio para *utilities*, Cidades Inteligentes e IoT. Define padrões e certificados para sistemas sem fio, padroniza níveis de potência, taxas de dados, modulações e bandas de frequência, entre outras variáveis.

Principais características da *Wi-SUN Alliance:*

- **Missão:**
  - Promover o uso do padrão IEEE 802.15g™ para conectividade de dispositivos nos ambientes das *utilities* e cidades inteligentes.

- **Iniciativas relacionadas à IoT:**
  - IEEE 802.15g™: suportar os padrões definidos pela indústria e garantir interoperabilidade dos produtos por meio de programas de testes e certificação;
  - Forte atuação junto às empresas de *utilities*.

- **Principais membros:** Analog Devices, Cisco, muRata, NICT, OMRON, RENESAS, ROHM, Silver String Networks, Toshiba.

- **Página web**: https://www.wi-sun.org/index.php/en/

6.2.3 Alianças - Suporte a serviços e aplicações

Nesta seção, serão abordadas as alianças relativas à camada de Suporte a serviços e aplicações.

6.2.3.2 IPSO Alliance

A *IPSO Alliance* é uma organização sem fins lucrativos fundada em 2008 com membros das empresas de tecnologia, comunicações e energia. A IPSO Alliance promove o Protocolo de Internet (IP) com foco na comunicação com objetos inteligentes e provê dispositivos de rede IP em aplicações de energia, consumo, saúde e para soluções industriais.

Principais características da *IPSO Alliance:*

- **Missão:**
  - Permitir que dispositivos de IoT se comuniquem entre si, a partir da interoperabilidade global baseada em padrões abertos. Os membros da IPSO Alliance estão abertos a organizações que apoiam uma abordagem baseada em IP para conectar objetos inteligentes e interessados em definir o futuro da IoT.

- **Iniciativas relacionadas à IoT:**
  - *Framework*s para *gateway*s IoT/M2M: Kura (Java/OSGi-based), Mihini (roda sobre Linux);
  - Implementações Open Source para: MQTT, CoAP, OMA LWM2M, ETSI M2M etc.

- **Principais membros:** Arch Rock, Atmel, Cimetrics, Cisco, Duke Energy, Dust Networks, eka systems, EDF (Électricité de France) R&D, Emerson Climate Technologies, Ericsson, Freescale Semiconductor, Gainspan, IP Infusion, Jennic, Kinney Consulting, Nivis, PicosNet, Proto6, ROAM, SAP, Sensinode, SICS, Silver Spring Networks, Sun Microsystems, Tampere University, Watteco, Zensys.

- **Página web:** http://www.ipso-alliance.org

6.2.3.2 Eclipse Fundation IOT Alliance

O *Eclipse IoT Working Group* é uma aliança entre organizações e indivíduos que compartilham o objetivo de criar uma IoT baseada em padrões abertos. A aliança centra-se no desenvolvimento, promoção e adoção da tecnologia de código aberto de IoT da *Eclipse*.

Principais características da *Eclipse IoT Working Group:*

- **Missão:**
  - Estabelecer uma plataforma IOT/M2M aberta para ser utilizada por qualquer pessoa ou entidade.
- **Iniciativas relacionadas à IoT:**
  - Implementações Open Sourse para: CoAP, DTLS, IEC, 15118, IEC 61499, OMA LWM2M, MQTT, OGC SensorThings API, oneM2M, ETSI M2M, OPC UA, PPMP.

- **Principais membros:** Borland, IBM, MERANT, QNX *Software* Systems, Rational *Software*, Red Hat, SuSE, TogetherSoft, Webgain

- **Página web:** https://iot.eclipse.org

6.2.3.3 OASIS Alliance

A *Organization for the Advancement of Structured Information Standards* (*OASIS*) é uma aliança global sem fins lucrativos, fundada em 1993 (sob o nome *SGML Open*), que promove o consenso da indústria e propõe padrões mundiais de segurança, IoT, computação em nuvem, energia, tecnologias de conteúdo, gerenciamento de emergência e outras áreas. Os padrões abertos *OASIS* oferecem o potencial para reduzir custos, estimular a inovação, expandir os mercados globais e proteger o direito à livre escolha de tecnologia.

Principais características da *OASIS:*

- **Missão:**
  - Desenvolver um padrão aberto para passagem de mensagens de negócios entre aplicativos ou organizações. Conectando sistemas e alimentando processos de negócios com as informações necessárias e de forma confiável;

- **Iniciativas relacionadas à IoT:**
  - AMQP: Advanced Message Queuing Protocol;
  - MQTT: Message Queuing Telemetry Transport;
  - oBIX: Open Building Information Exchange.

- **Principais membros:** AIS, ArborText, Avalanche, Computer Task Group, Database Publishing Systems, EBT, Fulcrum, InfoDesign, Information Dimensions, Intergraph, Interleaf, Open Text, Object Design, Officesmith/CTMG, Oracle, SoftQuad, Xsoft.

- **Principais membros:** Organizações e membros individuais somam mais de 600 participantes.

- **Página web**: https://www.oasis-open.org

6.2.3.4 Object Management Group - OMG Alliance

O *Object Management Group* (*OMG)* é um consórcio internacional de associação aberta, sem fins lucrativos, fundado em 1989. Os padrões *OMG* são conduzidos por fornecedores, usuários finais, instituições acadêmicas e agências governamentais.

Os grupos de trabalho da *OMG* desenvolvem padrões de integração empresarial para uma ampla gama de tecnologias e de indústrias. Os padrões de modelagem da *OMG*, incluindo a *Unified Modeling Language - UML e a Model Driven Architecture (MDA)*, permitem um design visual, execução e manutenção de *software* entre outros processos. Além disso, o *OMG* hospeda organizações como o *Cloud Standards Customer Council (CSCC)* e o grupo de padronização de qualidade de *software* da indústria de TI, o *Consortium for IT Software Quality (CISQ).*

Principais características da *OMG*:

- **Missão:**
  - Desenvolver padrões de integração empresarial para uma ampla gama de tecnologias e uma gama ainda maior de indústrias.

- **Iniciativas relacionadas à IoT:**
  - Os padrões de modelagem da OMG incluem:
    - *Unified Modeling Language (UML);*
    - *Model Driven Architecture (MDA);*
  - *Consortium for IT Software Quality (CISQ).*
- **Principais membros:** OMG é composta de 101 membros (lista de membros não divulgada).

- **Página web:** http://www.omg.org

6.2.3.5 Hypercat Consortium

A *Hypercat Alliance*[311] está construindo um ecossistema para impulsionar a segurança e a interoperabilidade na internet das coisas para a indústria e cidades inteligentes. As principais características da *Hypercat Alliance* são:

- **Missão:**
  - O Consórcio HyperCat pretende criar um balcão único de melhores práticas de implementação de IoT por meio do compartilhamento de conhecimento de processos e aplicações.

- **Iniciativas relacionadas à IoT**:
  - HyperCat: serviço de catálogo baseado em JSON, leve, para ativos IoT na web.

- **Principais membros:** Device Pilot, Accenture, AIMES Grid Services, BAE System, BT, Cisco, Dartt, EDF Energy, Fujitsu, Huawei, IBM, INTEL, Symantec, University of Cambridge, entre outros.

- **Página web:** http://www.hypercat.io

311 Aliança originalmente formada por 40 empresas, instituições de ensino e autoridades locais do Reino Unido, apoiada pelo governo Britânico.

6.2.3.6 Allseen Alliance

A *AllSeen Alliance* dedica-se à adoção generalizada de produtos, sistemas e serviços que suportem a IoT baseadas em *AllJoyn*, um *framework* colaborativo de padrão aberto que permite que dispositivos próximos se comuniquem com outros.

Principais características da *AllSeen Alliance:*

- **Missão:**
  - Capacitar e impulsionar a adoção generalizada de produtos, sistemas e serviços que suportam a IoT com um *framework* de desenvolvimento aberto e universal.

- **Iniciativas relacionadas à IoT:**
  - Descoberta;
  - Roteamento de mensagens;
  - Segurança: Criptografia (AES128) e autenticação (PSK, ECDSA);
  - Interoperabilidade;
  - Suporte à camada de transporte: agnóstica – suporta camadas físicas que provêm pilha IP (WiFi, WiFi-Direct, Ethernet e Powerline). Suporte a Bluetooth LE, 6LowPan, ZigBee ou Z-Wave por meio de *gateway*.
  - API de referência.

- **Principais membros:** Mais de 100 membros entre eles, Electrolux, Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Sony, Technicolor, TP-Link;

- **Página web:** https://allseenalliance.org

6.2.3.7 Industrial Internet Consortium

O *Industrial Internet Consortium (IIC)* é uma organização global de associação aberta, criada em 2014 com o objetivo de acelerar o desenvolvimento, adoção e o uso generalizado de máquinas e dispositivos interligados e análises inteligentes.

O foco central da *IIC* é industrial, coordenando iniciativas de ecossistemas para conectar, controlar e integrar, de forma segura, ativos e sistemas de ativos com pessoas, processos e dados usando arquiteturas comuns, interoperabilidade e padrões abertos para entregar negócios transformacionais e resultados sociais para as indústrias e infraestrutura pública.

Principais características do *IIC:*

- **Missão:**
  - Promover o crescimento acelerado da IoT Industrial, coordenando iniciativas de ecossistemas para conectar, controlar e integrar de forma segura ativos e sistemas, com pessoas, processos e dados;
  - Realizar a integração com arquiteturas, interoperabilidade e padrões abertos.

- **Iniciativas relacionadas à IoT:**
  - Data Distribution Service (DDS);
  - Unified Component Model para sistemas distribuídos, em tempo real e embarcados;

- **Membros Fundadores**: Bosch, EMC2, GE, Huawei, Intel, IBM, SAP, Schneider Electric;

- **Página web**: http://www.iiconsortium.org/members.htm

6.2.3.8 The Connected Lighting Alliance

A *Connected Lighting Alliance* é a principal defensora da conectividade sem fio em aplicações de iluminação. Trata-se de uma organização sem fins lucrativos, constituída por empresas líderes na indústria de iluminação.

Principais características da *Connected Lighting Alliance:*

- **Missão:**
  - Promover a adoção e crescimento global de soluções de iluminação sem fio, apoiado em padrões abertos.

- **Iniciativas relacionadas à IoT:**
  - Suporte ao ZigBee 3.0 como padrão aberto de conectividade para aplicações em iluminação residencial;
  - Ampliação de escopo para o mercado de iluminação *indoor* profissional.

- **Principais membros:** GE, NXP, LG, Panasonic, Philips, Silicon Labs, Lutron.

- **Página web:** http://www.theconnectedlightingalliance.org

6.2.3.9 EnOcean Alliance

A *EnOcean Alliance* desenvolve e promove sistemas de monitoramento e controle sem fio autoalimentados para edifícios sustentáveis, formalizando o padrão interoperável sem fio. Módulos baseados na tecnologia EnOcean oferecem micro conversores de energia com consumo ultrabaixo, possibilitando comunicações sem fio e sem bateria entre sensores, switches, controladores e *gateway*s.

As principais características da *EnOcean Alliance* são:

- **Missão:**
  - Desenvolver e promover sistemas de monitoramento e controle sem fio autoalimentados para edifícios sustentáveis, formalizando o padrão interoperável sem fio.

- **Iniciativas relacionadas à IoT:**
  - Abrange as camadas de 1 a 3 do modelo OSI (Open Systems Interconnection);
  - EnOcean Wireless Standard ISO/IEC 14543-3-10.

- **Principais membros:** BSC Computer GmbH, Honeywell, Jäger Direkt, Pressac Communications, ROHM, Thermokon Sensortechnik.

- **Página web:** https://www.enocean-alliance.org/en/home/

6.2.3.10Internet of Things Consortium

O *Internet of Things Consortium (IoTC)* é uma associação comercial para o mercado de IoT. Fundada em 2012, busca constituir um ecossistema global de empresas líderes, para o desenvolvimento da IoT. Seu foco de atuação abrange automação residencial, cidades inteligentes, carros conectados, varejo conectado e *wearables*.

Principais características da *IoTC:*

- **Missão:**
  - Promover o crescimento da IoT por meio da facilitação de parcerias, compartilhamento de conhecimento e educação;
  - Conduzir a adoção de produtos e serviços IoT, ajudando a alcançar o potencial da IoT.

- **Iniciativas relacionadas à IoT:**
  - Rede IoT: empresas, executivos e recursos em IoT;
  - Comitês IoTC: representantes de cada membro que auxiliam na divulgação da visão do IoTC.

- **Principais membros:** Verizon, August, ABC, NXP, Homewell, Belkin, FOX, Nestle, Nielsen, UCIC, SKYBELL, ClearBlade. Plum.

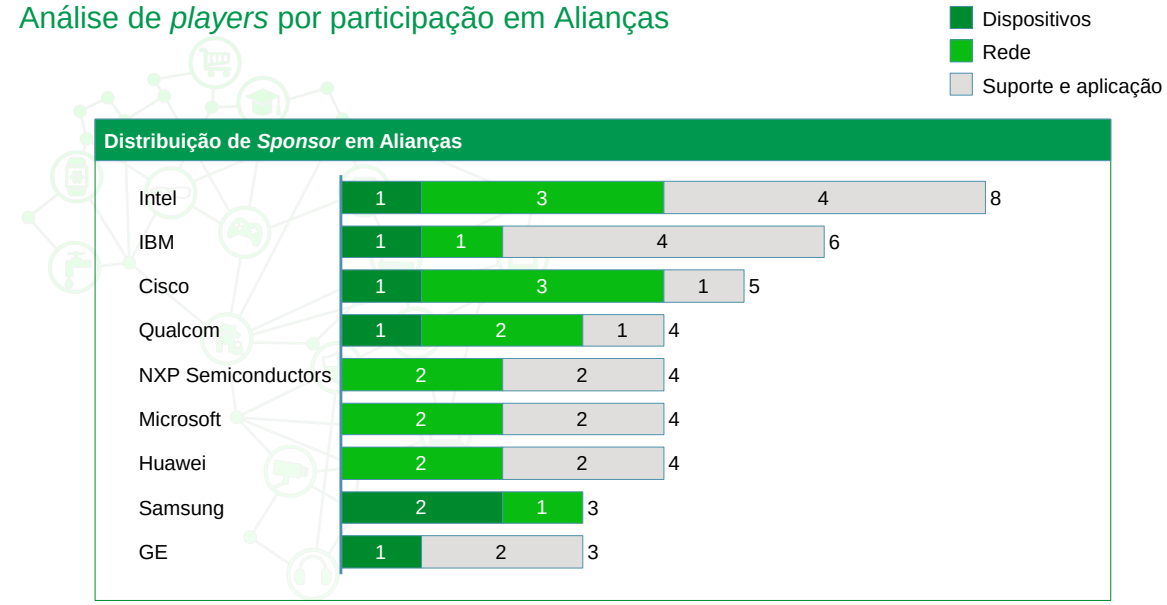
- **Página web:** http://iofthings.org

6.2.4 Participação de atores em alianças por camada

Posteriormente à segmentação das alianças por camada da IoT, realizou-se um cruzamento entre os *atores* que constam como patrocinadores nestas alianças e a relação dos principais *atores* anteriormente identificados. Assim, foi possível identificar o número de participações dos principais *atores*, em alianças, por camada, conforme mostra o QUADRO 57.

QUADRO 57

Análise de *players* por participação em Alianças



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Por meio do QUADRO 57, verifica-se que os principais *atores* fazem parte, principalmente, de alianças na camada de Suporte a serviços e aplicações. Especificamente, a Intel, cuja principal atuação se dá no setor de semicondutores, é patrocinador de quatro alianças focadas na camada de Suporte a serviços e aplicações. Movimentação semelhante é observada com os *atores* NXP e IBM.

6.2.4.1 Principais alianças comerciais entre atores por camada

Apresenta-se, nessa seção, a análise de alianças comerciais, entre os principais *atores*. O termo aliança comercial é entendido como parcerias firmadas entre duas ou mais empresas, com o objetivo de otimizar esforços de vendas, reduzir custos, ou identificar requisitos para evolução e desenvolvimento de produtos e serviços.

6.2.4.1.1 Método para seleção das alianças comerciais analisadas

O método para a identificação das alianças comerciais e respectivos *atores* participantes foi baseado no método de seleção de *atores* descrito no Capítulo 6.1.1.

Observou-se que grandes *atores* geralmente não referenciam seus parceiros, principalmente se estes forem pequenos. Contudo, *atores* menores são mais propensos a referenciar seus parceiros; assim, a busca de alianças comerciais partiu de *atores* com até 500 funcionários, dos quais 44 foram identificados e analisados quanto à formação de alianças comerciais. O QUADRO 58 sumariza esse método.

QUADRO 58

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.2.4.1.2 Seleção das empresas que possuem parcerias

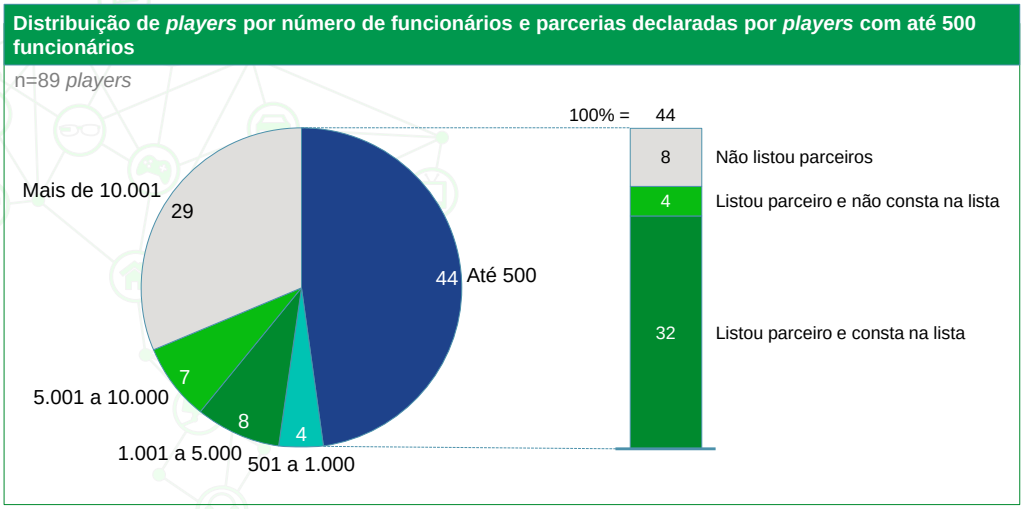
Dentre os 44 *atores* selecionados para a análise de parcerias comerciais, verificou-se que:

- Trinta e dois *atores* (73% do total) citam seus parceiros comerciais. Estes parceiros fazem parte da lista (conjunto dos 89 *atores* selecionados);
- Quatro *atores* (9% do total) citam seus parceiros comerciais, sendo que esses parceiros não fazem parte da lista;
- Oito *atores* (18% do total) não fazem citações à formação de parcerias comerciais.

O QUADRO 59 ilustra essa distribuição, em termos quantitativos.

QUADRO 59

Parcerias declaradas por *players* com até 500 funcionários



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

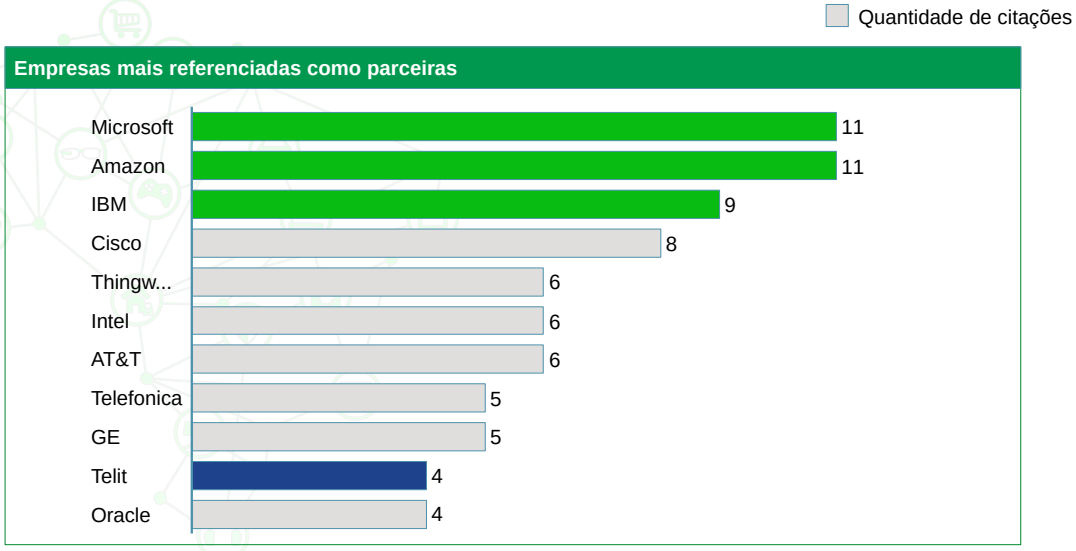
A busca de informações sobre as alianças comerciais dos 44 *atores* analisados foi realizada por meio das informações presentes na página *web* desses 44 *atores*. No caso de existência de alianças comerciais, buscou-se identificar os parceiros que as compunham e classificá-los por porte. Posteriormente, realizou-se o cruzamento destes parceiros com os *atores* selecionados no banco de dados da *IoT Analytics*.

6.2.4.1.3 Resultados da Análise das Alianças Comerciais

O resultado desse cruzamento é exibido nas figuras a seguir. O QUADRO 60 apresenta os *atores* presentes no banco de dados da *IoT Analytics* (lista dos 89 *atores* selecionados) que mais foram referenciados como parceiros em alianças comerciais, independente de porte. Observa-se que, em geral, os parceiros mais citados são gigantes do setor, com clara atuação internacional, com exceção da Telit, uma empresa com menos de 1000 funcionários. O QUADRO 61 apresenta os parceiros mais citados, com menos de 500 funcionários.

QUADRO 60

Análise das Alianças Comerciais – Resultados



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

QUADRO 61

Análise das Alianças Comerciais – Resultados

FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

O QUADRO 62 apresenta os três parceiros comerciais mais citados, por camada, e as empresas que os apontaram. Por exemplo, na camada de Suporte a serviços e aplicações, observa-se que os parceiros comerciais mais citados são a Amazon, Microsoft e IBM. Abaixo de cada um desses parceiros, encontram-se as empresas que as apontaram.

QUADRO 62

Players mais citados como parceiros por camada e apontamentos

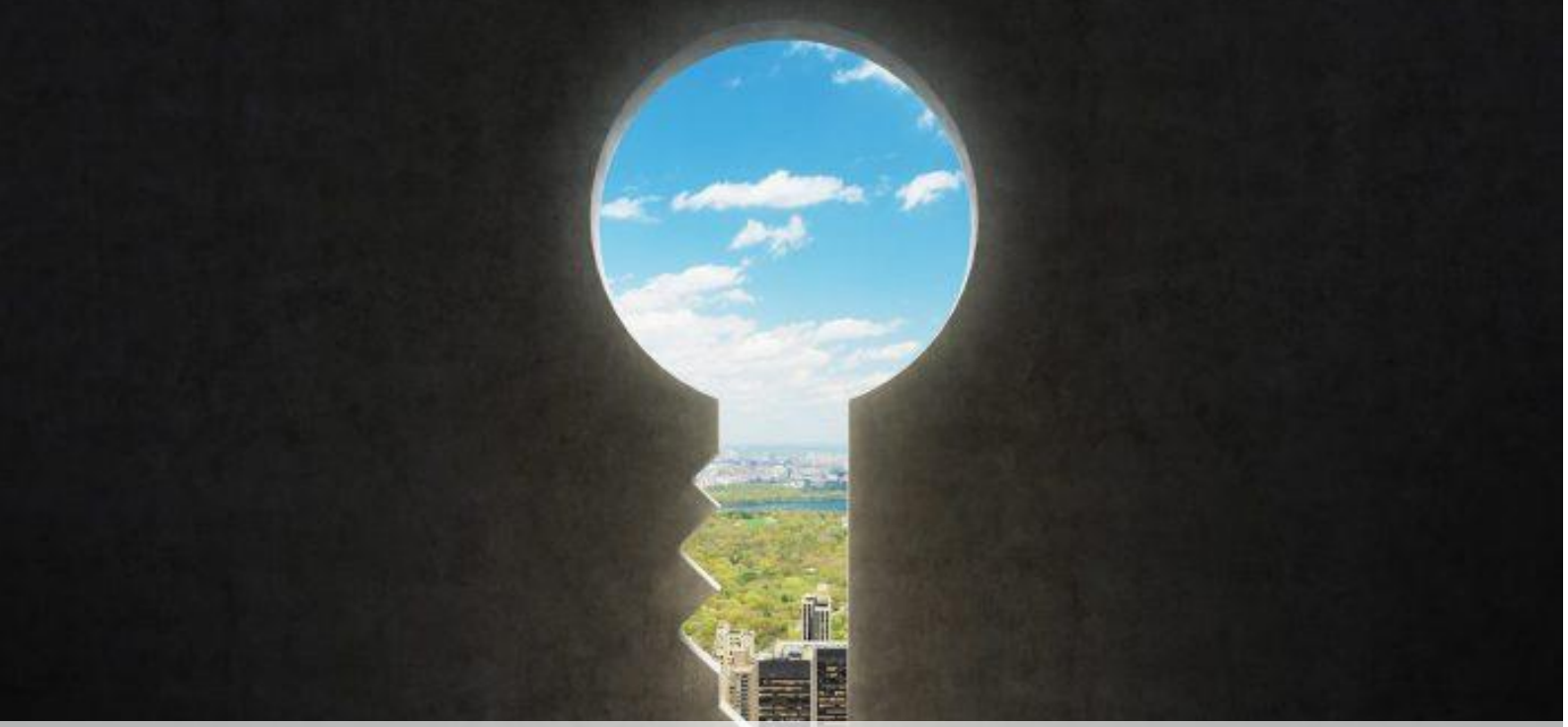
Camada tecnológica	Dispositivos e gateways			Camada de rede			Suporte à aplicação		
***Players* mais citados como parceiros comerciais**	**Intel**	**Arrow electronics**	**Gemalto**	**Cisco**	**AT&T**	**Telefonica**	**Amazon**	**Microsoft**	**IBM**
Empresas que apontaram os *players* mais citados	▪ Altiux ▪ Bitstew Systems ▪ Eurotech ▪ Evrythng ▪ M2Mi ▪ Ntels	▪ Ingeny ▪ KORE ▪ Telematics ▪ Wyless	▪ Kore ▪ Telematics ▪ Numeres ▪ Wyless	▪ Aeroscout ▪ Bitstew Systems ▪ Carriots ▪ Eurotech ▪ Evrythng ▪ Jasper ▪ M2Mi ▪ Numerex	▪ C3 IoT ▪ Jasper ▪ Kore ▪ Telematics ▪ Mesh Systems ▪ Numerex ▪ Wyless	▪ Jasper ▪ Kore ▪ Telematics ▪ Libeloim ▪ Numerex ▪ Wyless	▪ Altizom Systems ▪ Ayla Networks ▪ Bitstew Systems ▪ Bright Wolf ▪ Bsquare ▪ C3 IoT ▪ Electric Imp ▪ Green City Solutions ▪ Libelium ▪ Numerex ▪ SIGFOX	▪ Altizom Systems ▪ Bsquare ▪ Carriots ▪ Electric Imp ▪ Eurotech ▪ Green City Solutions ▪ Libelium ▪ Mesh Systems ▪ Numerex ▪ SIGFOX ▪ Solair	▪ Axeda ▪ Cariots ▪ Electric Imp ▪ Eurotech ▪ Libelium ▪ M2Mi ▪ Ntels ▪ SIGFOX ▪ Wi-NEXT

FONTE: Análise do consórcio

6.2.4.2 Conclusões

As camadas de Rede e de Suporte a Serviços e Aplicações apresentam o maior número de alianças. *Atores* com notória participação em algumas camadas da arquitetura de IoT também se apresentam como patrocinadores de alianças em outras camadas, com destaque para a camada de Suporte a serviços e aplicações (por exemplo, Intel e NXP).

Em relação às alianças comerciais, observou-se que as empresas mais apontadas são grandes *atores*, com notória participação internacional, como por exemplo Intel, Arrow Electronics e Gemalto na camada de Dispositivos; Cisco, AT&T e Telefonica na camada de Rede; e Amazon, Microsoft e IBM na camada de Suporte a serviços e aplicações.



6.3 Oportunidades de Nicho

Uma decisão central na estratégia competitiva dos *atores* de IoT consiste em criar proposições de valor focadas em nichos[312], sejam esses de verticais de mercado, ou de soluções horizontais, isto é, aplicáveis em diversas verticais.

Nota-se que soluções verticais, que são mais especializadas, requerem maior conhecimento dos negócios, e, portanto, da cadeia de valor associada. Em princípio, o desenvolvimento de soluções em verticais específicas precede o desenvolvimento de soluções horizontais. Ou seja, a capacidade de desenvolvimento de soluções de nicho guarda relação com a habilidade de se desenvolver estratégias competitivas.

6.3.1 Contabilização das oportunidades por vertical

Essa análise também foi desenvolvida sobre a base de dados de 643 iniciativas internacionais em IoT da IoT Analytics[313]. O primeiro passo foi filtrar, dentre todas as iniciativas, aquelas que se enquadravam nas 12 principais verticais selecionadas nesse projeto, o que resultou em 553 iniciativas.

No passo seguinte, foram analisadas as iniciativas consideradas como oportunidades de nicho, obtendo-se uma amostra de 314 iniciativas. Considerou-se como oportunidade de nicho aquelas iniciativas que contemplaram soluções para nichos de mercado, ou seja, segmentos públicos ou privados de mercado, cujas necessidades particulares são pouco

312 O termo nicho utilizado nesta análise representa segmentos privados ou públicos cujas necessidades particulares são pouco exploradas ou inexistentes.

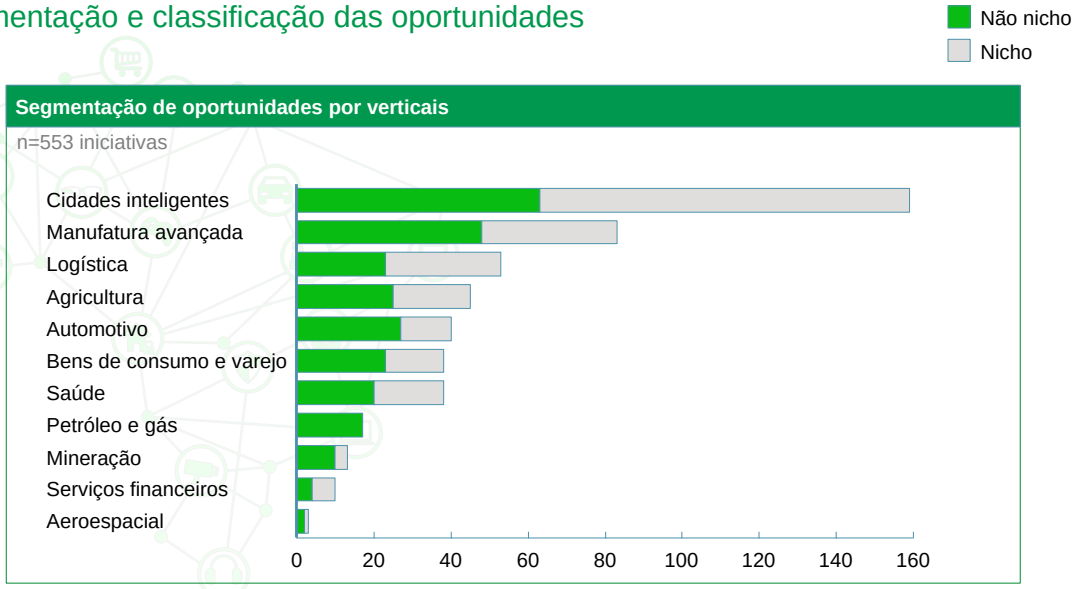
313 McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

exploradas ou inexistentes. Essa seleção foi realizada por meio da opinião de especialistas da equipe do CPqD.

As 553 iniciativas foram contabilizadas em cada vertical, conforme mostra o QUADRO 63. Optou-se por analisar as iniciativas e soluções com base nas verticais, por considerar que muitas das oportunidades de nicho surgem em verticais específicas. Verificou-se que, em diversas verticais, por exemplo, Cidades inteligentes, a maioria das oportunidades foi considerada como sendo de nicho.

QUADRO 63

Segmentação e classificação das oportunidades

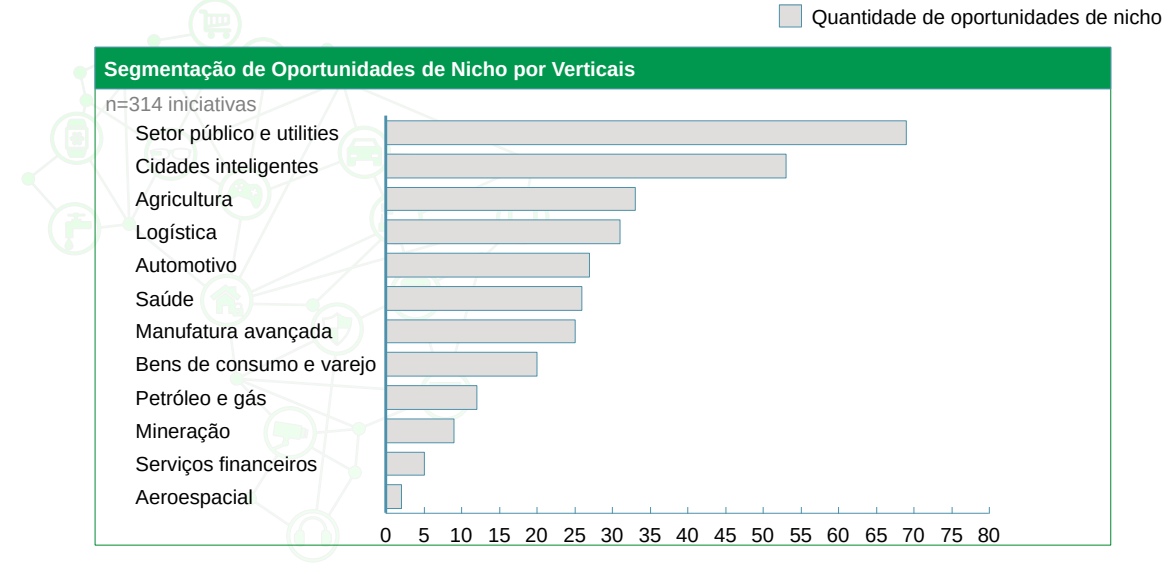


FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

Conforme mostra o QUADRO 64, entre as 314 iniciativas consideradas de nicho, o maior número de ocorrências se verificou no Setor público e *utilities*, seguido de Cidades inteligentes.

QUADRO 64

Segmentação e classificação das oportunidades



FONTE: Banco de dados Enterprise IoT Projects da IoT Analytics (Agosto 2016), Análise do consórcio

6.3.1.1 Categorização das oportunidades por vertical

Além da contabilização das oportunidades, por vertical, as iniciativas e soluções consideradas oportunidades de nicho foram analisadas caso a caso, o que resultou na constatação que poderiam ser categorizadas no âmbito de cada vertical. Buscou-se apresentar aquelas que se destacavam pelo seu caráter inovador.

6.3.1.1.1 Oportunidades na vertical Agricultura

Nessa vertical, foram examinadas as soluções tecnológicas de 47 iniciativas descritas na base de dados de iniciativas[314], dentre as quais, 34 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Gestão de equipamentos agrícolas (12)**: soluções que atuam na gestão de máquinas automáticas, baseadas em dados de telemetria desses equipamentos. Estas soluções demandam conectividade no Campo para transmissão dos dados e gerenciamento centralizado;
- **Telemetria e sensoriamento avançado em veículos agrícolas autônomos (1)**: soluções que atuam na operação de veículos e máquinas autônomos, por exemplo, no controle de consumo combustível. Estas soluções também demandam conectividade no campo para transmissão dos dados e gerenciamento centralizado;
- **Controle de pragas (5)**: soluções específicas de sensoriamento de variáveis e de alterações meteorológicas para controle específico e preciso de pragas nas plantações;
- **Controle da flora local em florestas (2)**: soluções específicas de sensoriamento de variáveis do ambiente de florestas, visando, por exemplo, prevenir roubo de madeiras e plantas da flora local;
- **Controle do ambiente de cultivo (14)**: soluções específicas de sensoriamento de variáveis do ambiente de cultivo e de alterações meteorológicas para melhoria da produtividade e assertividade no plantio e colheita.

Dentre as iniciativas da vertical, considerou-se destaque a iniciativa *Connected Olive Fields*. Neste projeto, a solução proporciona a integração de distintas variáveis monitoradas, tais como, informações meteorológicas e do ambiente da plantação, com vistas à criação de modelos de predição sobre a difusão de moscas que causam problemas para o plantio de oliveiras.

[314] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

6.3.1.1.2 Oportunidades na vertical Cidades Inteligentes

Foram examinadas as soluções tecnológicas de 84 iniciativas descritas na base de dados de iniciativas[315], dentre as quais, 53 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Construções inteligentes (4)**: soluções que atuam na gestão de prédios e construção, comerciais ou residenciais, no intuito de melhorar a eficiência no uso de recursos como energia, água e vagas de estacionamento. Atuam, também, na automatização de funções no âmbito de sua construção, como a refrigeração de ar. Estas soluções demandam conectividade para transmissão dos dados e gerenciamento centralizado;
- **Gerenciamento de frotas (6)**: soluções voltadas para o aumento da eficiência no uso de veículos de frota, como caminhões, ônibus ou automóveis particulares. Atendem veículos autônomos, ou não, e são baseadas em dados de telemetria e sensoriamento enviados por redes sem fio. Estas soluções demandam conectividade nas cidades, estradas ou a utilização de transmissores nos veículos para transmissão dos dados e gerenciamento centralizado;
- **Gestão de infraestruturas municipais** (7): soluções de telemetria e sensoriamento de infraestrutura das cidades, tais como rede de água, rede de esgoto, energia para centralizar o gerenciamento destas estruturas e gerar análises preditivas de falhas;
- **Gestão de serviços e meio ambiente no município (15)**: soluções específicas de sensoriamento de variáveis associadas à prestação de serviços no âmbito municipal e do controle do meio ambiente. Alguns exemplos são o controle de veículos de distintas frotas de transporte público, com vistas à melhoria da eficiência do sistema de transporte público como um todo, gestão da iluminação pública e monitoramento de condições críticas de poluição;
- **Gestão da segurança pública e patrimonial (2)**: soluções de vigilância patrimonial, de edificações públicas ou privadas, e soluções de vigilância de espaços públicos (ruas, praças, etc.) que detectam situações de ameaças por meio da análise de sons (disparos de armas), imagens, vibrações;
- **Serviços avançados à população (19)**: soluções para uso pelos cidadãos por meio de seus aparelhos portáteis móveis (celulares, *tablets*), baseadas na captura de informações de sensores trânsito; rotas e localização de ônibus e trens; previsão de tempo; turismo e outras.

Dentre as iniciativas da vertical, considerou-se destaque a iniciativa *San Francisco Parking*, projeto de gerenciamento de vagas de estacionamento na cidade Em que os dados são enviados e trabalhados pelas autoridades para calcular o valor do estacionamento, baseado na sua taxa de ocupação.

[315] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

6.3.1.1.3 Oportunidades na vertical Petróleo e Gás

Foram examinadas as soluções tecnológicas de 13 iniciativas descritas na base de dados de iniciativas[316], sendo que todas foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Gestão de equipamentos e infraestrutura (12):** soluções que atuam na gestão de oleodutos, gasodutos ou maquinário de exploração de petróleo e gás por meio de sensores e sistemas preditivos visando minimizar falhas, fadigas e vazamentos;
- **Gestão de equipamentos e infraestrutura com interação avançada (1):** solução de gestão de equipamentos e infraestrutura de óleo e gás, que incorporam recursos avançados de interação homem-máquina (fala, anotações), inclusive técnicas de aprendizagem por máquina (*machine-learning*).

Dentre as iniciativas dessa vertical, considerou-se destaque a *Connected Wells*, que utiliza algoritmos baseados na aprendizagem de máquinas para melhorar as capacidades de previsão de falhas e diagnóstico, a partir de leituras diárias de sensores integrados aos equipamentos em campo e dados não estruturados (por exemplo, notas de campo e comentários de operadores) de ordens de serviço de manutenção.

6.3.1.1.4 Oportunidades na vertical Bens de Consumo e Varejo

Foram examinadas as soluções tecnológicas de 36 iniciativas descritas na base de dados de iniciativas[317], dentre as quais, 20 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Gestão (9):** soluções que atuam na gestão de máquinas automáticas, controle de estoque, otimização de rotas de entrega e reposição de produtos, bem como, no controle de consumo de água, gás, eletricidade;
- **Interação com o consumidor (4):** soluções com interação com o consumidor a fim de auxiliá-lo nos processos de compra de produtos ou fruição de serviços;
- **Padrões de comportamento (4):** soluções de coleta de dados comportamentais de grupos de consumidores, a fim de oferecer produtos e promoções de forma direcionada, com maior assertividade;
- **Outros** (3).

Dentre as iniciativas da vertical, considerou-se destaque a *Supermarket of the future*, em que sensores acompanham o movimento dos olhos dos consumidores sobre telas que apresentam o produto, visando capturar informações sobre seus interesses e auxiliá-los na sua busca por produtos específicos, além de oferecer promoções baseadas em hábitos de compra.

316 McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.
317 Idem.

6.3.1.1.5 Oportunidades na vertical Logística

Foram examinadas as soluções tecnológicas de 43 iniciativas descritas na base de dados de iniciativas[318], dentre as quais, 31 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Gestão de Frota (15):** soluções focadas no gerenciamento de frotas privadas, que englobam o rastreio, otimização de rotas, controle do ciclo de manutenção preventiva de veículos, gestão da carga de trabalho etc;
- **Gestão de Carga (7):** compreende soluções de gerenciamento e rastreio de cargas, engloba rastreio e monitoração das condições de armazenagem da carga como temperatura, humidade, etc. Em geral a gestão ocorre em tempo real;
- **Automação de transporte de mercadorias (4):** compreende soluções que utilizam de robótica avançada, *machine learning* e sensoriamento para substituir a ativada humana;
- **Outros (5).**

Dentre as iniciativas da vertical, considerou-se destaque a *Connected Robots Still*, que consiste em um robô equipado com sensores e tecnologia de varredura que permite identificar, transportar e empilhar, de forma independente, mercadorias em um armazém.

6.3.1.1.6 Oportunidades na vertical Aeroespacial

Foram examinadas as soluções tecnológicas de 4 iniciativas descritas na base de dados de iniciativas[319], dentre as quais, duas foram classificadas como oportunidades de nicho. A análise dessas soluções permitiu sua classificação nas seguintes categorias:

- **Modelo de Negócios (1):** solução que viabiliza um modelo de negócios inovador, para turbinas de aviões. Em relação ao tradicional modelo de aquisição de turbinas de aviões, o monitoramento do tempo de uso das turbinas permite o pagamento de um menor valor de aquisição, que é complementado por valores que variam em função do uso;
- **Operação aeroportuária (1):** solução de IoT para degelo das asas das aeronaves comerciais. A partir na medição do acúmulo de gelo, a solução alerta a equipe de manutenção sobre a necessidade de realização do degelo.

Dentre as iniciativas da vertical, considerou-se destaque a *Connected Aircraft Engines*, que busca alterar o modelo de venda de motores (turbinas) de aeronaves. Consiste na instalação de sensores nos propulsores das aeronaves, possibilitando precificação baseada

[318] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.
[319] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

em um valor inicial (*upfront fee*) somado a pagamentos periódicos, baseados em horas de uso.

6.3.1.1.7 Oportunidades na vertical Automotivo

Foram examinadas as soluções tecnológicas de 40 iniciativas descritas na base de dados de iniciativas[320], dentre as quais, 28 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Compartilhamento de veículos e otimização no uso de frotas (2):** soluções que viabilizam novos modelos de compartilhamento de veículos diretamente para o usuário final, ou no uso de frotas empresariais. Utilizam dados de localização, rotas percorridas e aplicativos que facilitam a localização, reserva e uso dos veículos**;**
- **Veículos conectados (21):** soluções predominantes nesta vertical. Grande parte dessas soluções provém informação e serviços de entretenimento (*infotainement*) para os ocupantes de um veículo, bem como, dados técnicos para análise dos fabricantes;
- **Identificação de veículos (2):** soluções de RFID para identificação de veículos em pontos de checagem, por exemplo, em pedágios;
- **Veículo-Veículo V2V e Veículo-Infraestrutura (V2I) (3):** soluções que visam melhorar o tráfego nas vias, por meio da comunicação entre veículos, ou entre esses e infraestruturas inteligentes.

Nesta vertical, o destaque foi dado não uma iniciativa específica, mas ao conjunto de soluções de veículos conectados.

6.3.1.1.8 Oportunidades na vertical Mineração

Foram examinadas as soluções tecnológicas de 12 iniciativas descritas na base de dados de iniciativas[321], dentre as quais, 9 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Monitoramento dos sítios de mineração (8):** soluções de monitoramento de indicadores ambientais e operacionais nos ambientes das minas de extração de minérios. O objetivo é desenvolver ações de curto, médio e longo prazo para assegurar a segurança dos trabalhos e aumentar a eficiência operacional das atividades desenvolvidas;

[320] Idem.

[321] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

- **Estações meteorológicas (1):** solução de monitoramento ambiental associadas às atividades de mineração. A solução monitora dados meteorológicos, por meio de estações com sensores e bases de análises, e são conectadas aos centros de operação de empresas mineradoras.

Nessa vertical, não foram encontradas iniciativas que pudessem ser consideradas de destaque. Cabe ressaltar que as oito iniciativas relacionados ao monitoramento dos sítios de operação e de monitoramento ambiental são semelhantes a muitas outras verificadas.

6.3.1.1.9 Oportunidades na vertical Setor Público e Utilities

Foram examinadas as soluções tecnológicas de 157 iniciativas descritas na base de dados de iniciativas[322], dentre as quais, 67 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Eficiência energética e SmartGrids (25):** soluções relacionadas ao uso de IoT para soluções de eficiência energética em diversos ambientes. Contempla, também, aplicações da IoT no âmbito das redes elétricas inteligentes, endereçando aspectos para melhoria de sua eficiência operacional;
- **Meio ambiente (8):** soluções para monitoramento de indicadores e controle ambiental, orientadas para órgãos públicos que atuam no controle de emissões e a presença de elementos poluentes. Aplicáveis ao monitoramento da qualidade do ar, água e de áreas de risco e de preservação ambiental;
- **Serviços públicos e concessões (27):** soluções voltadas a melhoria da eficiência de serviços públicos em geral, orientadas, principalmente, a empresas concessionárias de serviços públicos;
- **Transportes (4):** soluções customizadas para órgãos e empresas que têm a missão de controlar o tráfego de veículos e para usos especiais;
- **Outras (3).**

Dentre as iniciativas da vertical, considerou-se destaque a *Crime prevention system*, um projeto piloto de sistema de prevenção de crimes, que permite que o Ministério da Justiça estabeleça modelos de prevenção de crimes baseados em informações sobre criminosos que utilizam uma tornozeleira eletrônica, incluindo o local em tempo real e perfis criminais.

[322] Idem.

6.3.1.1.10 Oportunidades na vertical Saúde

Foram examinadas as soluções tecnológicas de 35 iniciativas descritas na base de dados de iniciativas[323], dentre as quais, 27 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Monitoramento remoto de pacientes e debilitados (14):** soluções para o monitoramento remoto de pacientes (cardíacos, apneia, etc.), idosos e debilitados (pacientes com doença de *alzhaimer*, etc.);
- **Facilitação de tratamentos (5):** soluções que facilitam a realização de tratamentos médicos, dentre essas, atendimento em ambulância, transmissão e análise de imagens, controle de ingestão de medicamentos prescritos e terapia anticoagulante;
- **Rastreio em ambientes clínicos (3):** soluções para a localização de pessoal, equipamentos médicos, amostras e medicamentos, em hospitais e laboratórios;
- **Monitoramento de equipamento médico (3):** supervisão de equipamentos de uso clínico, como o status de funcionamento, temperatura e uso de refrigeradores médicos; e equipamentos de uso no tratamento de câncer;
- **Instrumentação médica (2):** soluções para instrumentação médica, como de análise do uso cateteres e sistemas para autodiagnostico e diagnóstico remoto.

Dentre as iniciativas da vertical, considerou-se destaque a *Wearables for Patients*, baseada em dispositivos *wearables* (utensílios e vestimentas conectadas) para acompanhamento e localização de pessoas por cuidadores ou familiares.

6.3.1.1.11 Oportunidades na vertical Manufatura Avançada

Foram examinadas as soluções tecnológicas de 63 iniciativas descritas em IoT Analytics (2015), dentre as quais, 26 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Operação Inteligente (15):** soluções que atuam no monitoramento e supervisão eficiente de processos, equipamentos, pessoas e instalações, em ambientes de produção, visando torná-los mais eficientes e autônomos;
- **Manutenção Inteligente (5):** soluções de otimização de processos de manutenção, baseadas, principalmente, no uso de sensores acoplados a equipamentos do processo produtivo e *software* com capacidade preditiva, que permitem mitigar ou diminuir falhas que prejudicam o processo produtivo e de distribuição de materiais;
- **Gerenciamento Energia (3):** soluções que monitoram e controlam o uso de energia em postos e equipamentos de linhas de produção;

[323] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

- ***Supply Chain* (1):** solução de rastreio de pessoas e mercadorias na cadeia produtiva;
- **Segurança na produção (1):** solução que aprimoram a segurança de pessoas e dos processos produtivos**.**

Dentre as iniciativas da vertical, considerou-se destaque a *Plant Data Services*, solução de Operação Inteligente, que habilita serviços baseados em plataforma com dados abertos para uso por diferentes indústrias.

6.3.1.1.12 Oportunidades na vertical Serviços Financeiros

Foram examinadas as soluções tecnológicas de 9 iniciativas descritas na base de dados de iniciativas[324], dentre as quais, 4 foram classificadas como oportunidades de nicho. A análise de cada uma dessas soluções permitiu sua classificação e contabilização (quantidades entre parênteses) nas categorias, descritas a seguir:

- **Financiamento e Seguro (3):** soluções para melhor precificação de seguros e financiamentos, por meio de monitoramento do padrão de comportamento do motorista e rastreio de veículos;
- **Ponto de Venda Inteligente (1):** solução para terminal de ponto de venda (*POS*), baseada em nuvem e com integração em tempo real com sistemas legados de estoque, precificação e *supply-chain*.

Dentre as iniciativas da vertical, considerou-se destaque a *Connected vehicles CallPass Tech*, solução de habilitação de crédito facilitada via rastreio, que possibilita que usuários de financiamento de veículos, de elevado risco, obtenham financiamento com taxas reduzidas.

6.3.1.2 Conclusões

Foram identificadas 553 oportunidades em linha com as principais verticais de mercado consideradas neste projeto; dessas, 314 foram consideradas ofertas de nicho.

Verificou-se que em várias verticais a maioria das oportunidades foi considerada de nicho: Setor Público e Utilities; Cidades Inteligentes; Agricultura; Logística; Automotivo. Foram identificadas subcategorias de oportunidades de nicho em cada vertical.

Oportunidades de nicho consideradas destaques são: Connected Olive Fields, San Francisco Parking, Connected Wells, Supermarket of the future, Connected Robots Still, Connected Aircraft Engines, Veículos conectados, Crime prevention system, Wearables for Patients, Plant Data Services, Connected vehicles CallPass Tech.

[324] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

A análise de oportunidades de nicho realizada para as iniciativas internacionais de IoT, em curso, demonstram um ecossistema emergente. Um número relativamente elevado de *atores* busca um posicionamento estratégico favorável, explorando soluções que poderão, eventualmente, atingir mercados amplos (*mainstream*), seja em verticais específicas ou em um conjunto de verticais.

6.4 Cadeia de valor para IoT

Nessa seção descrevem-se as relações de produção e consumo entre *atores* dos elos que caracterizam a cadeia de valor da IoT. Busca-se, a partir dessa caracterização, identificar os elos com maior valor agregado, ou seja, com maior potencial de geração de valor. A geração de valor é entendida como uma estimativa sobre o montante de gastos para aquisição e disponibilização das soluções tecnológicas de IoT.

6.4.1 Elos da cadeia de valor de IoT

A descrição dos elos da cadeia visa definir os principais papéis ou atividades que precisam ser desempenhados para a entrega de valor (produtos ou serviços de IoT) aos clientes e usuários.

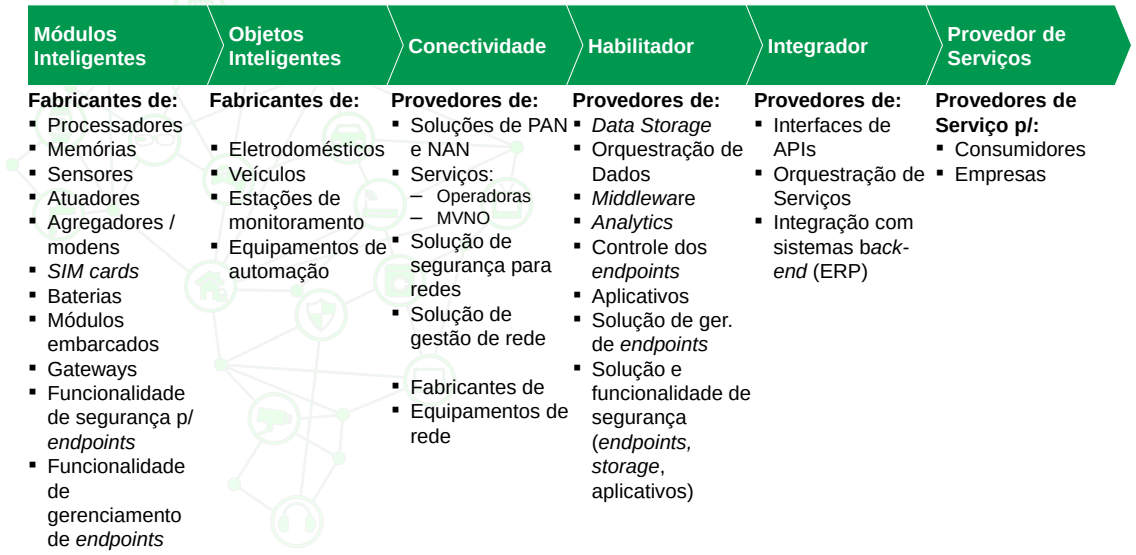
O método empregado para essa definição partiu da prospecção da literatura especializada, selecionando-se um conjunto de estudos (científicos e de mercado) que discutem o tema. A análise desses estudos por especialistas permitiu a formação de um consenso sobre como se poderia adaptar aquelas que foram consideradas as melhores propostas[325,326], tendo em conta a entendimento adquirido por meio das análises realizadas sobre *atores* e oportunidades em IoT. Resultou dessa análise a definição dos elos da cadeia IoT, conforme apresentada no QUADRO 65.

[325] Arthur D. Little. Smart market-makers for the "Internet of Things". 2011.

[326] McKinsey & Company. Internet of Things (IoT) technology stack. 2015 (update 2016).

QUADRO 65

Cadeia de Valor de IoT



FONTE: Análise do consórcio

A seguir, detalham-se cada um dos elos dessa cadeia de valor.

6.4.1.1 Módulos Inteligentes

Os principais papéis ou atividades desse elo são o desenvolvimento e provimento dos *building blocks* que constituem os objetos inteligentes, que formam o universo da IoT. Módulos inteligentes compreendem desde componentes básicos, tais como os processadores, sensores, atuadores, memórias, modens e baterias, até dispositivos mais complexos na forma de arranjos de *hardware* e *software* embarcados. Em algumas aplicações, os módulos podem atuar como *gateways* de dispositivos com limitada capacidade de processamento e comunicação.

Dentre os *atores* desse elo, encontram-se fabricantes de:

- Processadores;
- Memórias;
- Sensores;
- Atuadores;
- Agregadores / modems;
- SIM *cards;*
- Baterias;
- Módulos embarcados;
- *Gateways*;
- Funcionalidade de segurança p/ *endpoints;*
- Funcionalidade de gerenciamento de *endpoints.*

6.4.1.2 Objetos Inteligentes

O papel dos principais *atores* desse elo é fabricação e comercialização de objetos inteligentes, ou seja, dos elementos tangíveis com os quais interagimos no universo da IoT. Eles são formados pelos módulos fornecidos por *atores* do elo anterior da cadeia (seção 5.5.1) e dentre suas principais funcionalidades encontram-se: atuação, processamento, armazenamento de energia e comunicação, além de funções intrínsecas a sua concepção.

Como exemplos de objetos inteligentes, podem-se citar eletrodomésticos, veículos, medidores de energia, câmeras de vídeo, estações meteorológicas, etc. *Atores* atuantes neste elo compreendem empresas fabricantes de sistemas embarcados, eletrodomésticos, equipamentos para *utilities*, automação industrial, etc.

6.4.1.3 Conectividade

Neste elo estão os fornecedores de equipamentos de telecomunicações e os provedores de serviços de comunicação (operadores de telecomunicações, operadores virtuais de rede celular, etc.). Sua função é prover os meios para comunicação entre os elementos que compõem as soluções, permitindo a interação entre os diversos elementos localizados nas camadas do modelo de referência da IoT. Os operadores de telecomunicações atuam principalmente no provimento de serviços, enquanto que fornecedores de equipamentos atendem, inclusive, necessidades de comunicação privada, como, por exemplo, de um *Home Office*. Via de regra, os produtos e serviços ofertados buscam soluções de compromisso para atender os requisitos das distintas aplicações, tais como, cobertura, latência, taxa de transmissão e consumo, bem como os limitantes financeiros (*Capex*/*Opex*) e a complexidade de implantação e manutenção da infraestrutura implantada.

Dentre *os atores* do elo encontram-se:

- Operadores de Telecom;
- Solução de segurança para redes;
- Solução de gestão de rede;
- Fabricantes de equipamentos de rede.

6.4.1.4 Habilitador

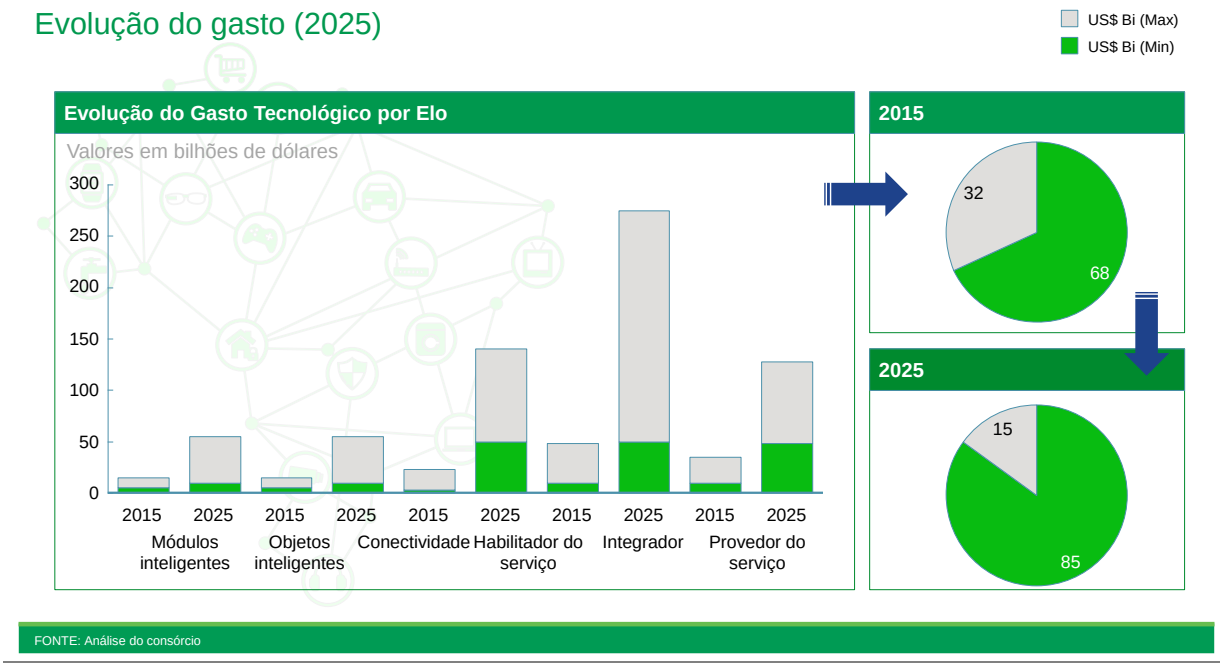
Considerado como um dos elos de maior potencial de geração de valor na cadeia; seus *atores* desenvolvem e provêm soluções de armazenamento (*storage*), orquestração (articulação) de dados, *middleware*, processamento analítico, aplicações e as soluções de controle e gerenciamento de objetos. Tais soluções possibilitam a transformação dos dados em valor.

As análises aqui desenvolvidas evidenciaram que este é o elo com a maior quantidade de novos entrantes, isto é, *atores* de pequeno porte (até 200 funcionários) e ativos no mercado

há menos de 10 anos. Adicionalmente, se verificou que a atuação destas empresas segue, principalmente, duas estratégias: i) concentrar seus esforços em até 3 verticais; e ii) ofertar uma solução horizontal, customizável para necessidades específicas.

O QUADRO 66 a seguir apresenta estas evidências com dados quantitativos.

QUADRO 66



6.4.1.5 Integrador

O papel dos *atores* do elo Integrador é o de combinar diferentes sistemas, processos e objetos na formação das soluções IoT. Na maioria dos casos, essa integração é realizada por meio de interfaces padronizadas de programação de aplicativo (APIs), devendo a composição final atuar conforme as regras de negócio estabelecidas pelo cliente. Desta forma, o integrador garante a interação e interoperabilidade entre os objetos inteligentes e as plataformas que dão corpo às soluções IoT.

Em síntese, a integração ocorre: (i) entre o módulo e objeto inteligente; (ii) entre os objetos inteligentes e as plataformas de *software*. Em muitos casos, a integração é realizada na nuvem (*cloud*), o que requer que os *atores* do elo Habilitador façam uso de plataformas que suportem APIs padronizadas.

Uma característica deste elo é a presença cada vez maior de empresas de grande porte. Neste cenário, empresas, como IBM, SAP e Oracle, exploram o segmento de integrador oferecendo soluções para conectar módulos e objetos inteligentes.

6.4.1.6 Provedor de Serviços

Atores desse elo realizam o empacotamento de soluções, atribuindo tarifas para os serviços, faturando e oferecendo suporte e relacionamento aos clientes e usuários finais das soluções. De modo geral, prestam um serviço baseado em uma ou mais soluções fim-a-fim, que por sua vez são compostas por *hardware*, *software* e conectividade. Adicionalmente, os provedores gerenciam os dados de clientes e o ciclo de vida da solução implantada, provendo inclusive a visualização e o gerenciamento dos objetos inteligentes, *software*s e sua integração conforme as regras de negócio do cliente.

Desta forma, os *atores* desse elo oferecem soluções completas e prontas para entrada em produção, aos clientes finais, facilitando a difusão da IoT. Como parte das soluções ofertadas, toda a informação coletada é armazenada, tratada e transformada em valor para cada negócio, em geral, sendo fornecida como serviço aos clientes. Em alguns casos, *atores* neste elo possuem conhecimento dos produtos e serviços providos pelos elos anteriores e chegam a ofertar produtos destes elos.

Já se considera que o aumento de dispositivos conectados ampliará as ameaças de Segurança de Informação. Por se tratar-se de um elo que requer elevada disponibilidade, integridade e confidencialidade, se antevê a crescente necessidade de soluções robustas de gestão e Segurança da Informação agregadas ao serviço prestado. Quando os *atores* deste elo se configuram como "provedores da solução fim a fim", torna-se ainda mais importante que os dados do cliente sejam mantidos seguros, seja no armazenamento ou tráfego, de modo que esses *atores* não tenham que responder às quebras de sigilo. Desse modo, há uma expectativa de oportunidades crescente de negócio para empresas de Segurança da Informação, cujas soluções atendam às necessidades dos *atores* desse elo.

6.4.2 Distribuição do valor pelos elos da cadeia

Tão importante quanto se caracterizar os principais papéis, atividades e *atores* de cada elo, é importante avaliar quais elos apresentam maior potencial de negócios (geração de valor). Esse cálculo foi realizado a partir de dois estudos. O primeiro estudo[327], da McKinsey, avaliou o potencial de vendas de soluções em cada elo, a partir da análise dos principais caso de uso no mundo, em 2015. Estimou-se que os gastos com tecnologia de IoT para atender àquelas necessidades estariam entre 45 e 135 bilhões de dólares. Esse montante de gastos foi distribuído em percentuais médios para cada elo da cadeia de valor de IoT, segundo as proporções mostradas a seguir, adaptadas a partir de outro estudo referencial[328]:

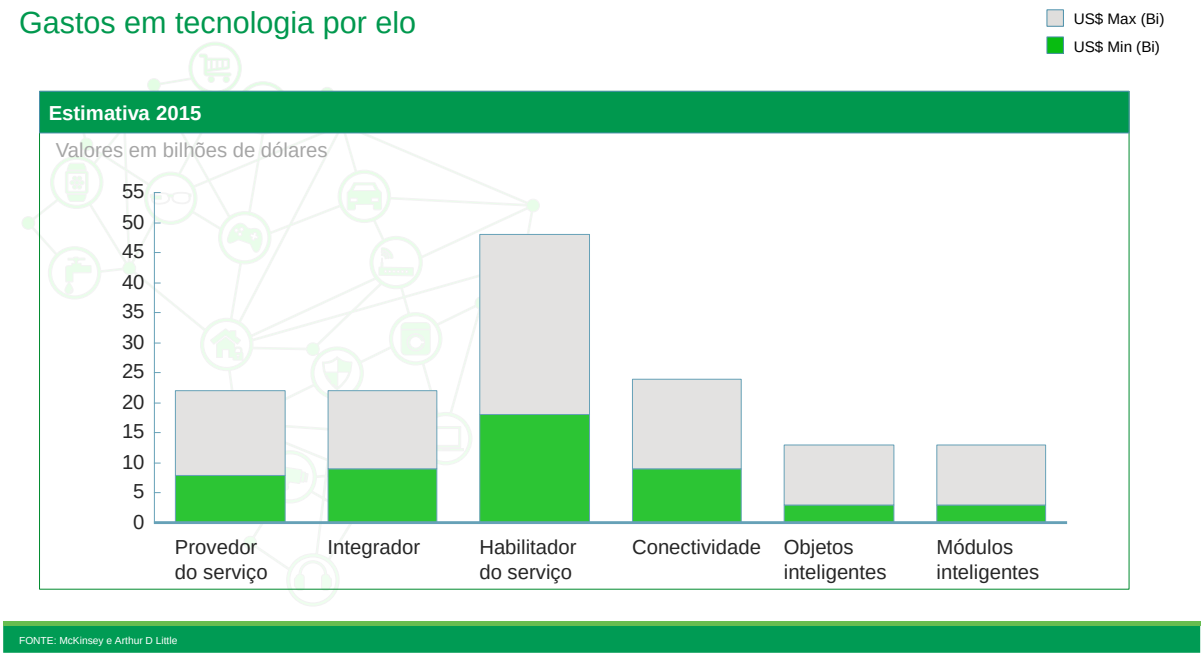
[327] McKinsey & Company. Internet of Things (IoT) technology stack. 2015 (update 2016).

[328] Arthur D. Little. Smart market-makers for the "Internet of Things". 2011.

- Módulos Inteligentes: 7,5%;
- Objetos Inteligentes: 7,5%;
- Conectividade: 17,5%;
- Habilitador de Serviço: 35%;
- Integrador: 17,5%;
- Provedor de Serviço: 15%.

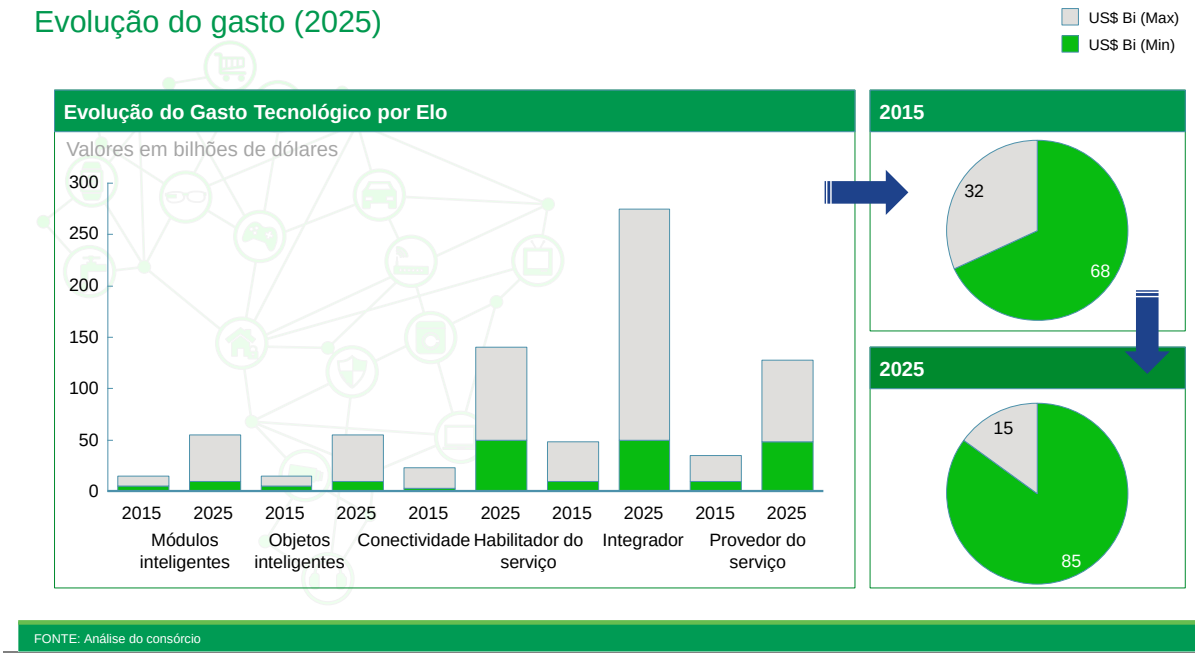
O QUADRO 67 apresenta os valores máximos e mínimos calculados para cada elo, em valores de 2015.

QUADRO 67



Nota-se que o maior valor se encontra nos elos Conectividade, Habilitador, Integrador e Provedor de Serviços. Como o estudo da McKinsey apresenta uma estimativa de evolução do percentual de valor, para 2025, em valores atribuíveis aos três últimos elos, buscou-se comparar esses valores, obtendo-se, assim, a perspectiva de evolução da distribuição de valores entre esses elos, em dois momentos: 2015 e 2025. O QUADRO 68 apresenta esta distribuição de valores máximos para 2015 na cadeia e a evolução prevista para 2025. Estimou-se para 2015, um valor total da cadeia de oferta tecnológica global entre 45 e 135 bilhões de dólares. Os três últimos elos concentram 68% do valor. Em 2025, espera-se que os valores totais se situem entre 273 a 777 bilhões de dólares, representando 85% do valor total da cadeia, comparado com 68% em 2015.

QUADRO 68



FONTE: Análise do consórcio

Como o Habilitador, Integrador e Provedor de Serviço estão entre os elos com maior valor estimado em 2025, é possível que o número de soluções vendidas ou seu preço se elevem, ou que novas alianças comerciais se consolidem para a exploração dos negócios, trazendo considerável valor agregado para os clientes destes elos.

Por outro lado, para os demais elos (Módulos Inteligentes, Objetos Inteligentes e Conectividade) provavelmente ocorrerá uma perda na participação no valor total da cadeia, de 32% para 15%. Entretanto, como provavelmente ocorrerá um crescimento significativo na escala de venda das soluções desses três elos, essa redução na participação do valor da cadeia poderá ocorrer à custa de uma pressão sobre seus preços unitários.

6.4.3 Conclusões

Os elos, ou papéis definidos para a cadeia de valor de IoT são: Módulos Inteligentes, Objetos Inteligentes, Conectividade, Habilitador, Integrador, e Provedor de Serviços.

Estima-se que, em 2015, os elos Habilitador, Integrador e Provedor de Serviços foram responsáveis por 66% do valor gerado na cadeia de IoT (oferta tecnológica). Já, em 2025, estima-se que a concentração também ocorrerá nesses elos, elevando esse percentual para 85%. Observa-se que o elo Habilitador é que apresenta maior quantidade de novos entrantes. Outrossim, *atores* de grande porte e consolidados no seu elo principal estão buscando oportunidades de negócio em outros elos da cadeia.

Os aspectos de Segurança de Informação e Gestão de terminais (*endpoints*) tendem a estar cada vez mais presentes nas soluções dos diversos elos, principalmente de Conectividade, Habilitador, Integrador e Provedor de Serviços. O principal aspecto capturado nessa análise foi a concentração atual de valor nos elos finais da cadeia, bem como a previsão de sua ampliação nos próximos anos. Essa perspectiva permitiu compreender boa parte das estratégias competitivas que estão em curso no ecossistema de IoT.

6.5. Evolução do quadro competitivo

A análise da evolução do quadro competitivo na cadeia de valor de IoT visou compreender como as estratégias competitivas estão se desenvolvendo, desde uma visão macro sobre seus principais vetores, bem como o entendimento da dinâmica atual e estratégias utilizadas pelos *atores*, nos elos cadeia de IoT. Além disso, a análise consolidou aspectos centrais sobre as tendências na atuação dos *atores*, que auxiliam na compreensão da evolução dessa cadeia.

6.5.1 Vetores da transformação do quadro competitivo

A dinâmica dessa evolução do quadro competitivo em IoT encontra paralelos em trajetórias seguidas por ondas tecnológicas anteriores à Internet e a indústria computacional, conforme estudo desenvolvido pelo Mckinsey Global Institute[329], que mapeou o potencial de geração de valor da IoT a partir da análise de um conjunto de casos de uso relacionados a vários ramos de negócio. O QUADRO 69, adaptado do referido

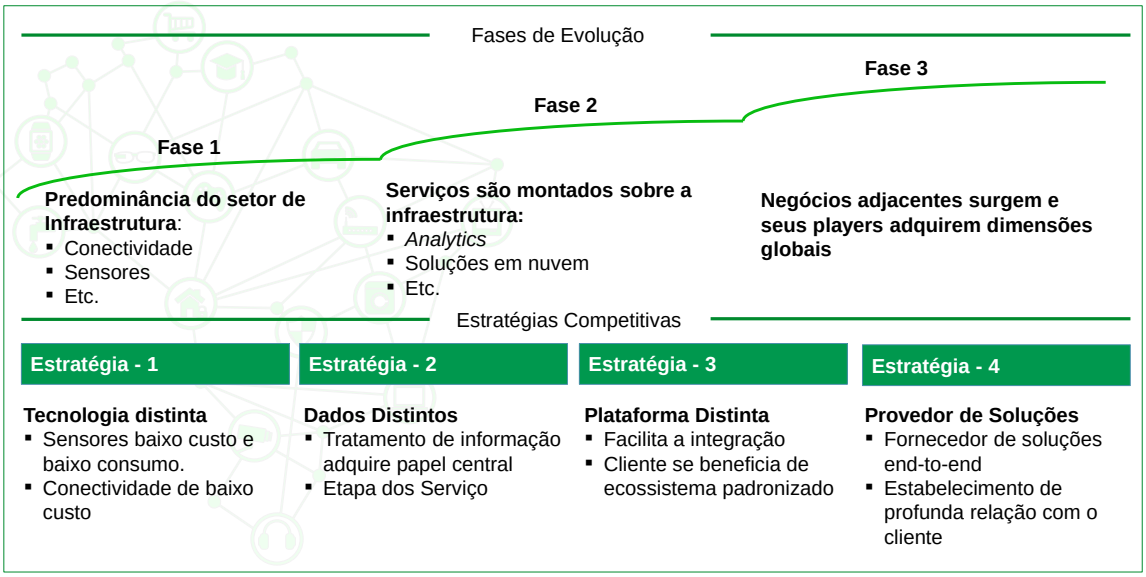
[329] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", Junho/2015.

estudo, ilustra a provável evolução tecnológica da indústria da IoT, que deve ocorrer em três fases:

- **Fase 1**: caracteriza-se pelo predomínio do fornecimento de infraestrutura, contemplando os dispositivos de *hardware/software* que proveem as funções de sensoriamento e conectividade, e os serviços associados a instalações e comissionamento de infraestrutura;
- **Fase 2**: *atores* constroem aplicações e serviços baseados em processamento analítico, *software*, plataformas e soluções em nuvem. Em conjunto, esses elementos proporcionam uma maior geração de valor;
- **Fase 3:** contempla o surgimento de novos modelos de negócio e *atores* com uma atuação mais global.

QUADRO 69

Dinâmica da evolução do mercado IoT



FONTE: Análise do consórcio

Ainda segundo o Mckinsey Global Institute[330], atualmente a IoT está entre as fases 1 e 2; existem empresas atuando como fornecedoras dos *building blocks* das soluções, tais como conectividade, sensoriamento, etc., e outras empresas se especializando em *software*, processamento analítico e soluções mais completas. Para *atores* em ambos as fases, observa-se uma tendência de expansão da atuação dentro da cadeia de valor, conforme apontado adiante.

330 Idem.

Em relação à forma de atuação nestas fases, o estudo mostra um conjunto de quatro possíveis estratégias que os *atores* podem adotar para se posicionar estrategicamente neste mercado. Estas estratégias estão descritas a seguir:

- **Tecnologia distinta**

  Aplicável a *atores* que possuem propriedade intelectual em tecnologias básicas, tais como sensores e módulos de comunicação de baixa potência. De modo geral, *atores* com tecnologias distintas e de alta aplicabilidade à IoT tendem a ter uma relativa facilidade para obter um bom posicionamento no quadro competitivo.

- **Dados Distintos**

  Atores proprietários de dados coletados pelos dispositivos da IoT podem ter uma vantagem competitiva, uma vez que o tratamento das informações brutas e a disponibilização de forma agregada podem ter um valor expressivo para a melhoria de serviços e produtos, bem como para alimentar sistemas de processamento analítico e *big data*. De modo particular, os dados podem ajudar os fornecedores de equipamentos e os provedores de serviços a expandir e melhorar sua atuação em IoT.

- **Fornecedores de Plataformas**

  De modo geral, as plataformas são sistemas de *software* que permitem a construção de aplicações e habilitam a interoperabilidade no acesso aos dados e serviços, facilitando a integração com as aplicações utilizadas pelo cliente final. *Atores* que adotam esta estratégia podem alcançar um bom posicionamento no ecossistema por meio da oferta de plataformas de amplo uso ou orientadas para determinados segmentos de negócio.

- **Provedor de Soluções Fim-a-Fim**

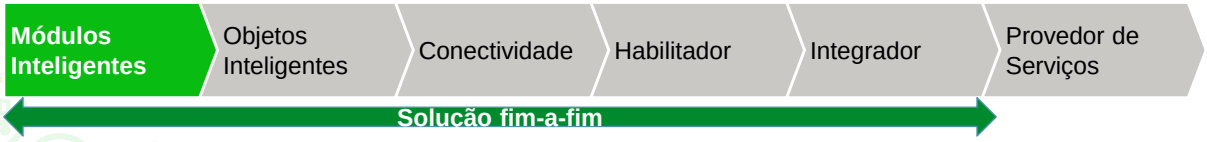
  Esta estratégia é aplicável aos *atores* que desenvolvem soluções completas para os clientes, envolvendo os componentes básicos, como *hardware* e *software*, as aplicações e os serviços de instalação e operação. Esta estratégia permite atuar mais próximo dos clientes.

A análise das ofertas dos *atores* bem posicionados e da sua forma de atuação na cadeia de valor mostrou que as fases indicadas no QUADRO 69 representam adequadamente a maneira como empresas incumbentes e novos entrantes estão se posicionando no ecossistema da IoT. De forma análoga, a análise mostrou que *atores* buscam criar diferenciais por meio da adoção de uma ou mais estratégias, entre as quatro estratégias apresentadas. Seguindo essa linha analítica, as próximas seções apresentam a situação atual em cada elo da cadeia, as estratégias de posicionamento adotadas e um compêndio de algumas das tendências observadas.

6.5.2 Evolução da Dinâmica no Elo Módulos Inteligentes

A situação atual dos *atores* atuantes neste elo está representada no diagrama do QUADRO 70. Como indicado, há uma busca pela expansão da atuação para praticamente todos os elos da cadeia, como forma de garantir uma maior presença no mercado e aumentar a geração de valor.

QUADRO 70



Em relação aos *atores*, estes se dividem entre os que proveem componentes básicos e os que fornecem dispositivos formados por *hardware* e *software* embarcados. Alguns exemplos de *atores* bem posicionados neste elo estão apresentados no QUADRO 71.

QUADRO 71

Dentre as estratégias competitivas mais utilizadas, destacam-se as seguintes:

- **Plataformas Comuns:**

  A oferta de plataformas comuns a várias verticais é uma forma dos *atores* viabilizarem a atuação em mercados fragmentados. Com isto, os investimentos são otimizados e as oportunidades de expandir a atuação na cadeia são maiores por conta da aplicabilidade a vários segmentos de mercado.

- **Expansão na Cadeia:**

  Esta estratégia demanda que os *atores* atuem de forma diversificada, pois requer que saiam do seu elo de origem e avancem em direção aos demais elos da cadeia.

  Novamente, o principal motivador é fortalecer a presença no ecossistema da IoT, expandindo a atuação aos elos com maior potencial de geração de valor. A análise da atuação de alguns dos *atores* mais bem posicionados mostrou que a movimentação mais comum ocorre em direção aos elos de Habilitador e Conectividade.

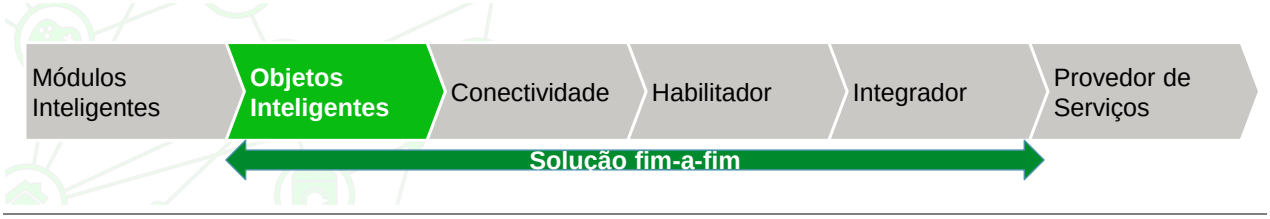
Como tendência para *atores* atuantes neste elo, cabe destacar:

- Alguns fabricantes de semicondutores têm se reorganizado para capturar oportunidades em outros elos, inclusive através de aquisições, como, por exemplo, a iniciativa de aquisição da NXP pela Qualcomm. Estas reorganizações devem buscar condições mais propícias para a construção de um portfólio completo de produtos e serviços, com diferenciais em conectividade, processamento, sensoriamento e atuação. Fazem parte, portanto, do leque de alternativas para encontrar os nichos mais adequados para suas áreas de *expertise* e desenvolver uma estratégia de posicionamento em IoT que esteja além do fornecimento de módulos básicos;
- Comunidades já estabelecidas e autossustentáveis, como Arduino e Raspberry Pi, devem se consolidar como uma excelente forma de inserção de novos *atores*, o que deve estimular a criação de produtos e soluções para uma variedade de aplicações.

6.5.3 Evolução da Dinâmica no Elo Objetos Inteligentes

A situação atual neste elo está representada no diagrama do QUADRO 72. Assim como no elo anterior, existe uma busca pela expansão da atuação para os outros elos da cadeia como forma de garantir uma maior presença no mercado e aumentar a geração de valor.

QUADRO 72



Neste elo, os *atores* podem ser mais bem visualizados a partir da sua área de atuação, conforme mostrado no QUADRO 73, que apresenta exemplos de *atores* atuantes nos segmentos das *utilities* de energia, casas e escritórios inteligentes, manufatura avançada e cidades inteligentes.

QUADRO 73

Players – Objetos inteligentes

FONTE: Fonte

Um dos grupos de destaque é formado pelos fabricantes de equipamentos para o setor elétrico. Motivados pelo advento das redes inteligentes de energia, esses fabricantes têm fornecido uma ampla gama de produtos de medição, sensoriamento e automação para a operação das *utilities* de energia. A estratégia utilizada tem sido posicionar estes produtos no contexto da IoT, por meio de soluções de conectividade geralmente fornecidas por terceiros. Com isto, é possível expandir a atuação para o elo de conectividade. Ainda por conta da presença forte no setor de energia, a atuação se expande também em direção aos demais elos da cadeia. Alguns *atores* atuam no elo de módulos inteligentes, desenvolvendo produtos para uso próprio ou para outros fabricantes.

No segmento de eletrodomésticos e automação residencial, a análise apontou a relevância dos aspectos de conectividade em adição às funcionalidades intrínsecas dos objetos. Neste caso, o objetivo é habilitar a integração com soluções fornecidas por outros *atores* atuantes na IoT e aumentar o valor percebido pelos clientes. Dentre as estratégias competitivas mais utilizadas neste elo, destacam-se:

- **Verticais de mercado**

  São adotadas por fabricantes de sistemas embarcados, eletrodomésticos e módulos para ambientes inteligentes, indústrias, uso pessoal, *utilities*, etc.

- **Expansão na cadeia**

  Como apontado no QUADRO 72, *atores* têm procurado expandir sua atuação nos outros elos da cadeia. No caso de novos entrantes, a formação de parcerias é uma das estratégias adotadas.

- **Integração de soluções**

  Além de incorporar funções específicas dos objetos, alguns *atores* têm focado na integração de soluções, explorando os recursos da conectividade, buscando assim um melhor posicionamento na cadeia.

Como tendências para *atores* atuantes neste elo, cabe citar:

- *Connected Home* e *Connected Office* devem gerar oportunidades para novos objetos inteligentes, aplicações de automação e monitoramento desses ambientes, devendo contribuir também para a otimização do uso da energia e de outros recursos naturais;
- Aspectos relacionados à preservação ambiental, à qualidade de vida nos centros urbanos e ao desenvolvimento sustentável devem fortalecer iniciativas de Cidades inteligentes, o que demandará objetos inteligentes e soluções voltados para essas iniciativas;
- *Atores* tradicionais e com forte presença em aplicações baseadas em M2M tendem a posicionar seus produtos e serviços no ecossistema da IoT, incorporando gradativamente os avanços tecnológicos e aproveitando as novas oportunidades de negócio.

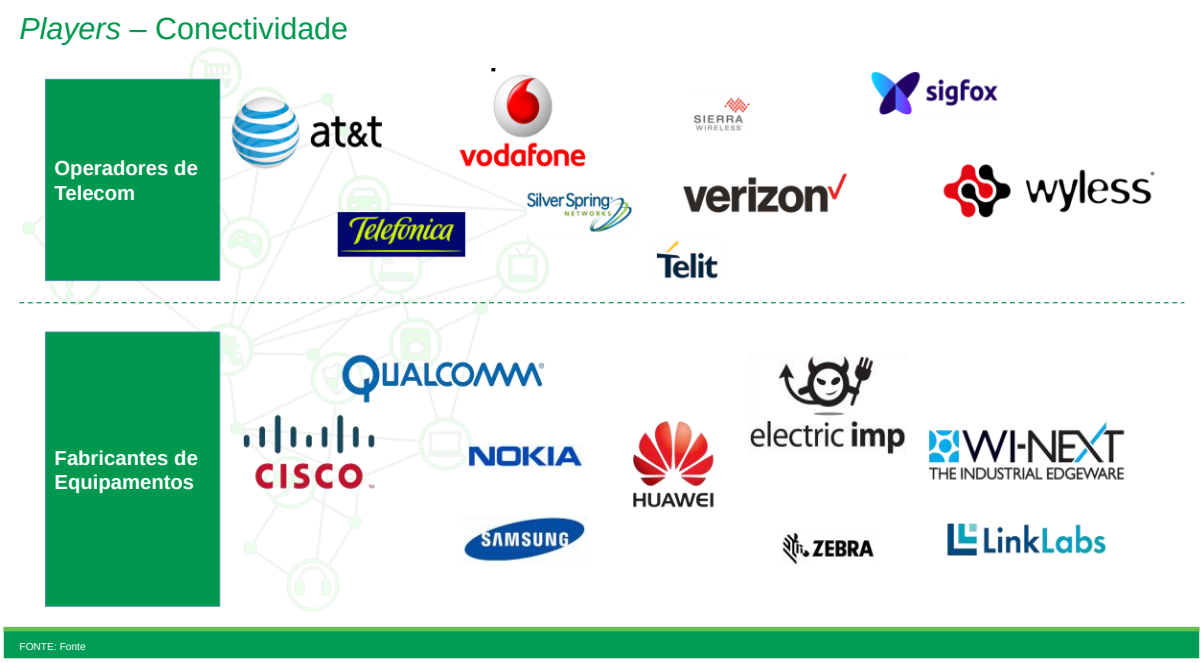
6.5.4 Evolução da Dinâmica no Elo Conectividade

Devido à elevada competição e às pequenas margens nesse elo, seus *atores* têm buscado ampliar a atuação por meio de diferentes estratégias competitivas, como mostrado no QUADRO 74. Observam-se ações claras no sentido de atuar em praticamente todos os elos da cadeia, com destaque para o desenvolvimento de plataformas horizontais e verticais que permitem um melhor posicionamento no elo de habilitador de serviço, no qual existe um maior potencial de obtenção de ganhos.

QUADRO 74

Os *atores* se dividem entre os operadores dos serviços de telecomunicações e os fabricantes de equipamentos. Alguns exemplos estão mostrados no QUADRO 75.

QUADRO 75



Como exemplo dessa dinâmica, pode-se citar o caso do operador de telecomunicações Vodafone que oferece uma plataforma de gestão de ativos móveis (*Mobile Asset Tracking*). Com esta oferta, este *player* expandiu sua atuação para o elo Habilitador, por meio de uma plataforma para uma vertical específica.

Dentre as estratégias competitivas mais utilizadas, destacam-se as seguintes:

- **Conectividade**

  Buscam oferecer a maior gama de opções de conectividade, tanto com tecnologias abertas operando em redes públicas (NB-IoT, eMTC, etc.) ou soluções proprietárias em faixas de frequência não licenciadas (LoRa, SigFox, Ingenu, etc.);

- **Plataforma horizontal**

  Compreendem plataformas para desenvolvimento de aplicações de uso comum a várias verticais.

- **Plataforma vertical**

  Compreendem plataformas para desenvolvimento de aplicações orientadas a vertical específica.

- **Solução fim-a-fim**

  Oferecem uma solução completa, abarcando todos os elos da cadeia de valor.

Como tendências para *atores* atuantes neste elo, cabe citar:

- Provável queda nos preços da conectividade devido ao aumento significativo do volume de dados transportados pelas redes;
- Redes celulares 4G/5G para IoT serão disponibilizadas por operadores, como a AT&T, devendo atender aplicações que requerem maior capacidade de transporte de dados (até 1 Gb/s);
- Módulos equipados com terminais para acesso a redes LPWAN proprietárias, como INGENU, LoRaWan, SIGFOX, Sensus e Telensa, tendem a se firmar como alternativa às redes públicas operando em espectro licenciado;
- Soluções baseadas em tecnologia 3GPP LPWAN (NB-IoT e LTE-M) terão uma participação crescente no mercado em função de atualizações nas redes de operadores de telecomunicações;
- Diversificação do portfólio de fabricantes de equipamentos de telecomunicações, tanto para o espectro das redes celulares (NB-IoT, eMTC) como para o espectro não licenciado (LoRaWan, WiFi, etc).

6.5.5 Evolução da Dinâmica no Elo Habilitador

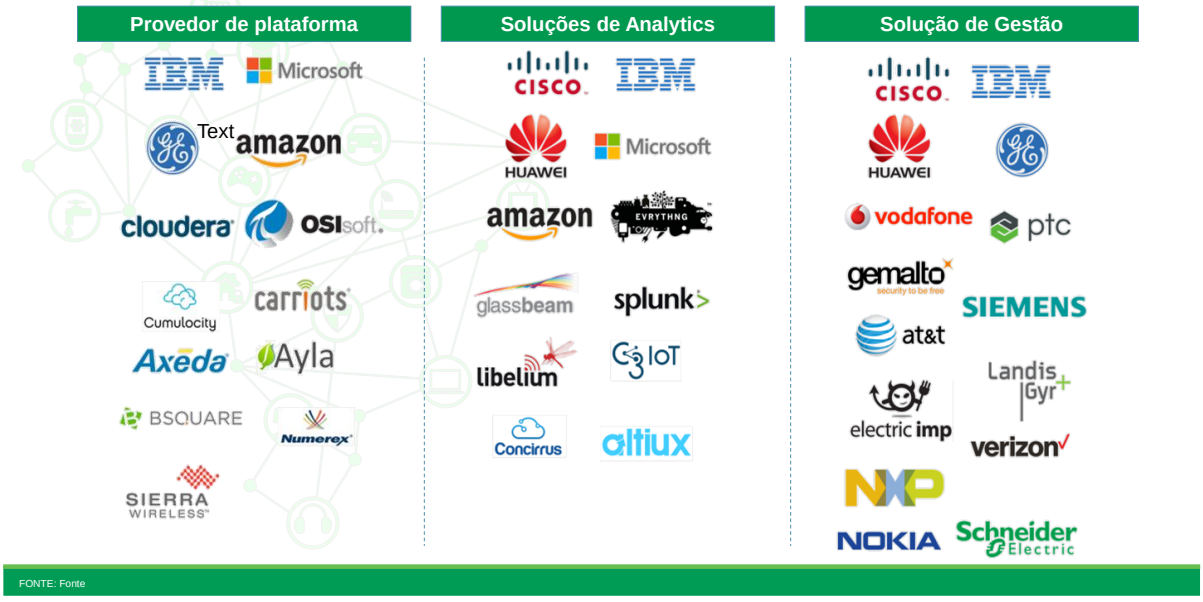
Observam-se *atores* consolidados em outros elos ofertando produtos e serviços próprios dos habilitadores, com vistas a prover soluções de maior valor agregado e obter um melhor posicionamento na cadeia de valor. Como exemplo, pode-se citar alguns operadores de telecomunicações, que em adição à oferta de conectividade, passaram a prover soluções de *analytics* ou de gestão de *endpoints*, que tipicamente pertenceriam ao elo de habilitação de serviços. Esta movimentação está indicada na situação atual deste elo, representada no QUADRO 76.

QUADRO 76

Em geral, estão presentes neste elo grandes *atores* de *software*, como Microsoft, IBM, Oracle, Amazon, entre outros. Os *atores* se dividem de acordo com o papel executado, e conforme apresentado no QUADRO 77, é comum alguns deles proverem mais de uma funcionalidade. Observa-se também a presença de novos entrantes, o que pode se configurar como um elo de oportunidade para inserção na cadeia de IoT.

QUADRO 77

Players – Habilitador



FONTE: Fonte

Dentre as estratégias competitivas mais utilizadas, destacam-se as seguintes:

- **Expansão na Cadeia**

  Alguns provedores de plataformas têm passado a atuar como integradores, oferecendo assim soluções de maior valor agregado.

- **Novos Competidores**

  Atores de atuação mais tradicional em outros elos estão migrando para o elo de Habilitador, oferecendo serviços e concentrando suas ofertas principalmente na gestão de *endpoints*.

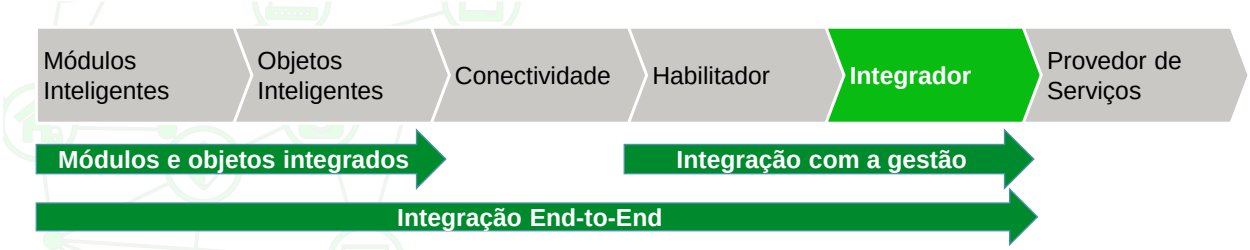
Como tendências para *atores* atuantes neste elo, cabe citar:

- Soluções de processamento analítico tendem a se sofisticar e ganhar espaço;
- Investimentos no desenvolvimento de plataformas devem aumentar, gerando soluções mais refinadas;
- O elo habilitador de serviço provavelmente permanecerá como uma das principais portas de entrada para novos *atores*;
- O preço de soluções baseadas em nuvem provavelmente cairá com a comoditização da infraestrutura.

6.5.6 Evolução da Dinâmica no Elo Integrador

Considerado um elo de alto valor na cadeia de IoT, o Integrador provê a possibilidade de orquestração de serviços e a Integração com sistemas *backend* dos clientes, como por exemplo, ERPs. As movimentações na cadeia de valor em torno do elo Integrador são mostradas no QUADRO 78.

QUADRO78

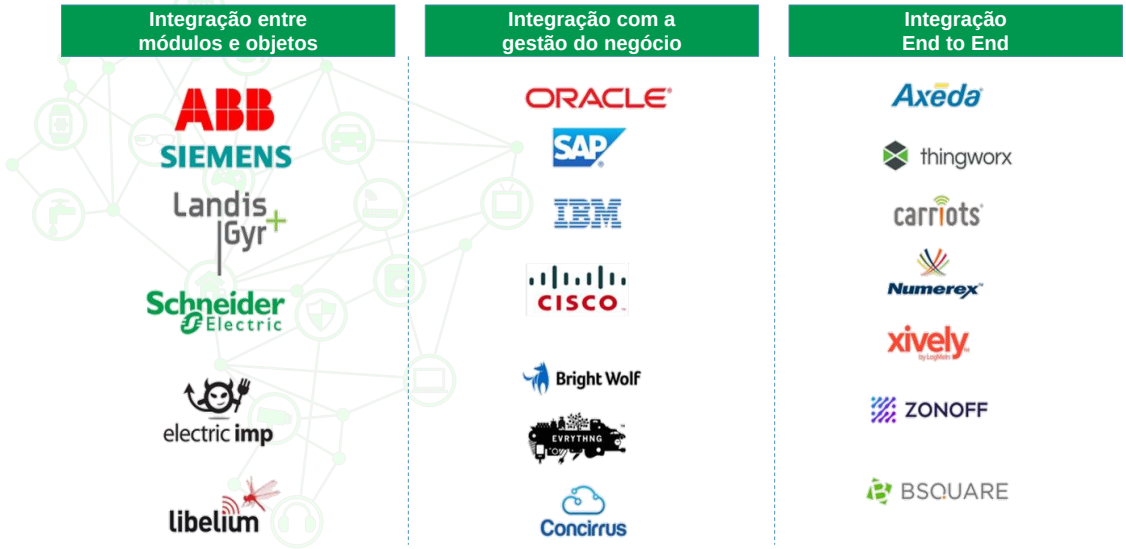


Grandes integradores de sistemas estão entrando neste território, tradicionalmente dominado por pequenos *atores* regionais, como a Axeda nos Estados Unidos. Assim, este elo começa a ser caracterizado pela presença de integradores de sistemas tradicionais e de grande porte nesse mercado. Entretanto, há também oportunidades para novos entrantes.

Os *atores* se dividem de acordo com o papel executado, e podem atuar desde a integração entre módulos e objetos até uma abordagem fim a fim, conforme mostrado no QUADRO 79.

QUADRO 79

Players – Integrador



FONTE: Fonte

Dentre as estratégias competitivas mais utilizadas, destacam-se as seguintes:

- Ofertas para integração entre módulos e dispositivos;
- Ofertas para integração da plataforma de gestão com as regras do negócio;
- Ofertas de integração fim a fim.

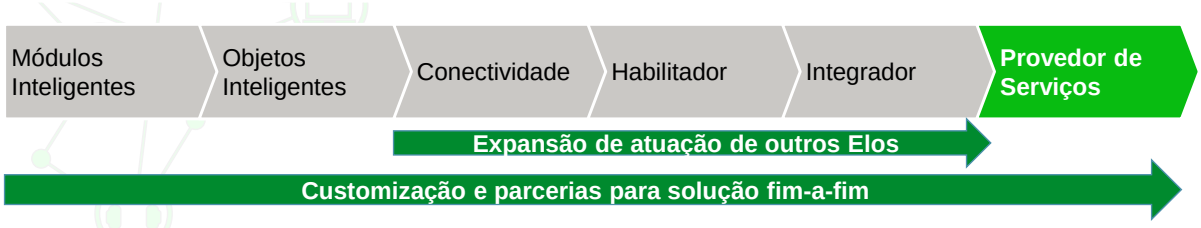
Como tendências para *atores* atuantes neste elo, cabe citar:

- Integradores que oferecem soluções fim a fim tendem a ganhar espaço no ecossistema IoT;
- A demanda por soluções de integração continuará alta devido à relevância do papel do Integrador no contexto da IoT. Embora existam desafios complexos e questões de interoperabilidade a resolver, o provável é que o elo do Integrador mantenha a sua importância;
- Grandes *atores* de integração de sistemas deverão se consolidar como integradores de soluções IoT.

6.5.7 Evolução da Dinâmica no Elo Provedor de Serviços

Por ser um dos elos com grande potencial de geração de valor, observa-se a movimentação de *atores* consolidados em outros elos ou em outros mercados, que passam a atuar nesse elo, provendo assim, soluções de maior valor agregado. As movimentações na cadeia de valor em torno do elo Provedor de Serviços são mostradas no QUADRO 80.

QUADRO 80



Como provedores de serviços, podem-se citar grandes *atores* do setor de *software* como Microsoft, Amazon, GE, entre outros. O QUADRO 81 apresenta alguns *atores* típicos atuando neste elo.

QUADRO 81

Players – Provedor de Serviços

FONTE: Fonte

Dentre as estratégias competitivas mais utilizadas, destacam-se as seguintes:

- **"As a Service"**

  Compreende ofertas baseadas no provimento de plataformas, *software*s e infraestrutura como serviço. Os principais benefícios para os clientes são custos reduzidos, a maior escalabilidade, integração e disponibilidade e agilidade na implementação de soluções customizadas para o cliente final.

- **Verticais de Mercado**

  Ao evoluir as soluções ofertadas como serviços, os provedores de procuram escolher verticais com maior potencial de geração de valor, atuando com produtos e serviços especializados para estes segmentos.

- **Customização e parcerias**

  Neste caso, o provedor de serviço oferece a visualização e o gerenciamento dos objetos inteligentes, *software*s, além dos serviços de integração destes com a aplicação.

Sobre as tendências para *atores* atuantes neste elo, cabe citar:

- Empresas com ofertas fim a fim devem agir no intuito de facilitar e diminuir os esforços em implantações robustas, para os clientes;
- Aspectos de segurança da informação (como confidencialidade, integridade autenticidade) deverão ser incorporados cada vez mais na oferta de Provedores de Serviço IoT;
- Espera-se um crescimento da base de provedores locais para prestação desses serviços, o que se configurará como oportunidades de entrada no mercado de IoT.

6.5.8 Conclusões

Alguns fabricantes de semicondutores têm se reorganizado para capturar oportunidades em outros elos, posicionando-se além do fornecimento de módulos básicos. Além disso, observa-se que o elo habilitador de serviço provavelmente permanecerá como uma das principais portas de entrada para novos *atores*. Adicionalmente, a oferta de soluções fim a fim tende a ganhar espaço.

Esses movimentos ilustram a tendência geral de reposicionamento estratégico dos *atores*, que consiste na busca pela atuação em elos e por meio de ofertas, de maior valor agregado. Para isso, as estratégias competitivas identificadas nos elos da cadeia de IoT foram: uso de plataformas comuns; expansão na cadeia; foco em algumas verticais de mercado; integração de soluções; ampliação das ofertas de conectividade; plataforma horizontal (qualquer vertical); plataformas para várias verticais específicas; solução fim-a-fim; migração para outros elos da cadeia; ofertas para integração entre módulos e dispositivos; ofertas para integração da plataforma de negócio; ofertas de integração fim a fim; ofertas "as a service"; customização e parcerias.

REFERÊNCIAS

Dispositivos

Any Silicon: http://anysilicon.com/semiconductor-technology-nodes/

ARM: https://www.arm.com/products/processors/cortex-m/cortex-m0.php

ARM: https://www.arm.com/products/processors/cortex-m/cortex-m4-processor.php

Armutlulu: Armutlulu, Y Fang, S H Kim, C H J, S A Bidstrup Allen and M G Allen, "A MEMS-enabled 3D zinc–air microbattery with improved discharge characteristics based on a multilayer metallic substructure" Journal Of Micromechanics and Microengineering, 2011.

ASUS: https://www.asus.com/News/uCgzySroxaAEOlam

Battery Power Online: http://www.batterypoweronline.com/main/articles/energy-density-comparison-of-silver-zinc-button-cells-with-rechargeable-li-ion-and-li-polymer-coin-and-miniature-prismatic-cells/

BITAG: “Internet of Things (IoT) Security and Privacy Recommendations”. 2016.

Brasil RFID: http://brasil.rfidjournal.com/noticias/vision?15145/2

Chamran: Fardad Chamran, Hong-Seok Min, Bruce Dunn and Chang-Jin “CJ” Kim, "Zinc-Air Microbattery With Electrode Array of Zinc Microposts", MEMS 2007.

Cisco: http://www.cisco.com/c/pt_br/services/overview.html

Communications and Network: http://file.scirp.org/pdf/CN_2016022517010096.pdf

Cryptec: Cryptography Research and Evaluation Committees (CRYPTREC). http://www.cryptrec.go.jp/english. Acessado em janeiro de 2017.

EBC: http://www.ebc.com.br/tecnologia/2015/07/entenda-por-que-*software*-livre-e-mais-seguro-que-*software*-proprietario

Embarcados: https://www.embarcados.com.br/pulpino

ENISA: “Cyber Security and Resilience of smart cars”. 2017.

ENISA: “Cyber security for Smart Cities - An architecture model for public transport”. 2015.

ENISA: “Securing Smart Airports”. 2016.

ENISA: “Security and Resilience of Smart Home Environments - Good practices and recommendations”. 2015.

eSTREAM: eSTREAM competition. European Network of Excellence for Cryptology. http://www.ecrypt.eu.org/stream. Acessado em janeiro de 2017.

Ferrari: Stefania Ferrari, Melanie Loveridge, Shane D. Beattie, Marcus Jahn, Richard J. Dashwood, Rohit Bhagat," Latest advances in the manufacturing of 3D rechargeable lithium microbatteries", Journal of Power Sources, 286, 2015.

Fujitsu: http://www.fujitsu.com/global/documents/products/network/solutions/nw-virtualization-6/WhitePaper-SDN-NFV-HG1064-1.pdf

GlobalPlatform: “The standard for managing applications on secure chip technology”. http://globalplatform.org.

Heer: T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, K. Wehrle, “Security challenges in the IP-based internet of things,” Wireless Personal Communications. 2011.

Huwaei: http://pr.huawei.com/en/news/hw-432402-agilenetwork3.0.htm

Huwaei: http://pr.huawei.com/en/news/hw-432402-agilenetwork3.0.htm

IEEE: Cybersecurity. http://cybersecurity.ieee.org. Acessado em fevereiro de 2017.

IEEE: http://spectrum.ieee.org/semiconductors/devices/leading-chipmakers-eye-euv-lithography-to-save-moores-law

Intel: http://www.intel.com.br/content/www/br/pt/internet-of-things/iot-platform.html

Intel: http://www.intel.com/content/www/us/en/internet-of-things/products-and-solutions.html

IoT Analytics: https://iot-analytics.com/5-things-know-about-iot-platform/

ISO: ISO/IEC 19790:2012. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52906. Acessado em fevereiro de 2017.

ISO: ISO/IEC 29167-1:2014. “Information technology Automatic identification and data capture techniques Part 1: Security services for RFID air interfaces”.

ISO: ISO/IEC 29167-10:2015. “Information technology Automatic identification and data capture techniques Part 10: Crypto suite AES-128 security services for air interface communications”.

ISO: ISO/IEC 29167-11:2014. “Information technology Automatic identification and data capture techniques Part 11: Crypto suite PRESENT-80 security services for air interface communications”.

ISO: ISO/IEC 29167-12:2015. “Information technology Automatic identification and data capture techniques Part 12: Crypto suite ECC-DH security services for air interface communications”.

ISO: ISO/IEC 29167-13:2015. “Information technology Automatic identification and data capture techniques Part 13: Crypto suite Grain-128A security services for air interface communications”.

ISO: ISO/IEC 29167-14:2015. “Information technology Automatic identification and data capture techniques Part 14: Crypto suite AES OFB security services for air interface communications”.

ISO: ISO/IEC 29167-16:2015. “Information technology Automatic identification and data capture techniques Part 16: Crypto suite ECDSA-ECDH security services for air interface communications”.

ISO: ISO/IEC 29167-19:2016. “Information technology Automatic identification and data capture techniques Part 19: Crypto suite RAMON security services for air interface communications”.

ISO: ISO/IEC 29192-1:2012. “Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General”.

ISO: ISO/IEC 29192-2:2012. “Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers”.

ISO: ISO/IEC 29192-3:2012. “Information technology -- Security techniques -- Lightweight cryptography -- Part 3: Stream ciphers”.

ISO: ISO/IEC 29192-4:2013. “Information technology -- Security techniques -- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques”.

ISO: ISO/IEC PDTS 29167-15. “Information technology Automatic identification and data capture techniques Part 15: Crypto suite XOR security services for air interface communications”.

IT Channel: http://www.itchannel.pt/news/*hardware*/novo-processador-intel-atom-e3900-dedicado-a-iot

ITU, “Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things”. Disponível em https://www.itu.int/rec/T-REC-Y.2060. Acesso em janeiro de 2017

ITU: “The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things”. 2016.

Kithion: Brucelin Kithion, disponível em: https://www.linkedin.com/pulse/iot-devices-arduino-vs-raspberry-pi-beaglebone-which-kithion, acesso em maio de 2017.

Kraytsberg: Alexander Kraytsberg, Yair Ein-Eli, Review on Li–air batteries-Opportunities, limitations and perspective, Journal of Power Sources 196, 2011.

Laboratório Mobilis: http://www.decom.ufop.br/imobilis/o-risc-v

Libelium: Disponível em: http://www.libelium.com/development/waspmote/documentation/waspmote-lorawan-networking-guide/].

Mais Tecnologia: https://www.maistecnologia.com/ces-2016-mediatek-lanca-tres-novos-processadores-wearables-iot

MBED: https://developer.mbed.org/

MBED: https://www.mbed.com/en/development/mbed-os

McKinsey & Company: “Semiconductor 2.0 – The next wave: Where to play? How to play? When to play?”, Discussion document 2015 T-30.

McKinsey & Company: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity

McKinsey & Company: http://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies

Mediatek: http://www.mediatek.com/products/smartHome/mt7697

Mediatek: http://www.mediatek.com/products/wearables/mt2523g

Micrium: https://www.micrium.com/rtos/

Microchip: Disponível em: http://www.microchip.com/wwwproducts/en/en027752

Microchip: Disponível em: http://www.microchip.com/wwwproducts/en/RN2483

My Evolution: http://www.myevolution.my/wp-content/uploads/2015/09/20150716-GSMA-Shanghai-International-MVNO-Summit-On.pdf

NIST FIPS: http://csrc.nist.gov/groups/STM/cmvp/standards.html. Acessado em fevereiro de 2017.

NXP: Disponível em: http://www.nxp.com/products/microcontrollers-and-processors/more-processors/application-specific-mcus-mpus/ieee-802.15.4-wireless-mcus:IEEE-802.15.4

NXP: Disponível em: http://www.nxp.com/products/microcontrollers-and-processors/more-processors/application-specific-mcus-mpus/ieee-802.15.4-wireless-mcus/zigbee-pro-and-ieee802.15.4-module:JN5168-001-M00#featuresExpand

Open Silicon: http://www.open-silicon.com/

Open Silicon: http://www.open-silicon.com/custom-soc-revolutionise-iot-product/

Open-TEE: Open source project for a "virtual TEE based on *software*". https://open-tee.github.io. Acessado em janeiro de 2017.

Oracle: http://www.oracle.com/technetwork/articles/java/afterglow2013-2030343.html

Pervices: https://pervices.com/wp-content/uploads/2016/10/rtc1607.pdf

RISC: https://riscv.org

Rocket: https://github.com/ucb-bar/rocket

Rocket: https://github.com/ucb-bar/rocket-chip

Rose: K. Rose, S. Eldridge, e C. Lyman. "The internet of things: an overview". Internet Society. 2015.

Semiconductor Engineering: http://semiengineering.com/iot-will-force-new-memory-paradigm/

Semtech: Disponível em: http://www.semtech.com/wireless-rf/lora.html

Sergio Prado: https://sergioprado.org/sistemas-operacionais-com-foco-na-internet-das-coisas

Subramanian: Vivek Subramanian, disponível em: https://www.youtube.com/watch?v=806JGh4LPSM&feature=youtu.be, acesso em maio de 2017.

Synopsys: https://www.synopsys.com/designware-ip/newsletters/technical-bulletin/advantages-of-mtv.html

T. Haigh, C. Landwehr. "Building Code for Medical Device *Software* Security". 2015.

The Guardian: https://www.theguardian.com/technology/2017/jan/26/vanishing-point-rise-invisible-computer?CMP=Share_iOSApp_Other

TI: Disponível em: http://www.ti.com/lsds/ti/wireless-connectivity/wi-fi/wilink-wl18xx/products.page

TI: Disponível em: http://www.ti.com/lsds/ti/wireless-connectivity/nfc-rfid/overview.page

TSMC: http://www.tsmc.com/english/dedicatedFoundry/technology/16nm.htm

U-blox: Disponível em: https://www.u-blox.com/en/product/sara-n2-series

UBM: "2015 Embedded Markets Study – Changes in Today's Design, Development & Processing Environments", April 2015

University of Michigan: http://www-personal.umich.edu/~adriaens/Site/UM_CleanTech_files/Sastry.pdf

VDC Research: http://www.slideshare.net/vdcresearch/searching-for-the-total-size-of-the-embedded-*software*-engineering-market

Voas: J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

Wang: Y. Wang et al., "Lithium and lithium ion batteries for applications in microelectronic devices: A review",Journal of Power Sources, 286, 2015.

Redes

BITAG: "Internet of Things (IoT) Security and Privacy Recommendations". 2016.

Cheng: Y. Cheng, J. Chu, S. Radhakrishnan, A. Jain. "TCP Fast Open", draft-ietf-tcpm-fastopen-10, September 2014.

Clausen: T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR), "RFC 3626, IETF, October 2003

DYN Corp: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/. Acessado em fevereiro de 2017.

ENISA: "Cyber Security and Resilience of smart cars". 2017.

ENISA: "Securing Smart Airports". 2016.

ENISA: "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

Forbes: http://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#4f68e31b3046. Acessado em fevereiro de 2017.

Geer: David Geer. SDN to support Internet of Things devices. http://internetofthingsagenda.techtarget.com/feature/SDN-to-support-Internet-of-Things-devices

Granjal: J. Granjal, E. Monteiro, J.Silva. "Security for the internet of things: A survey of existing protocols and open research issues". IEEE Communications Surveys and Tutorials.

Hui: J. Hui, Ed., P. Thubert. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, 2011.

ITU: "Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things". https://www.itu.int/rec/T-REC-Y.2060. Acessado em janeiro de 2017.

ITU: TMN recommendation on Management Functions - M.3400, disponível em https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-M.3400-200002-I!!PDF-E&type=items, acesso em maio de 2017.

Kaspersky Lab: https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/. Acessado em fevereiro de 2017.

Kreutz: D. Kreutz et al., “Software-defined networking: A comprehensive survey,” Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

Legare: Christian Legare, Micrium. Reworking the TCP/IP stack for use on embedded IoT devices. http://www.embedded.com/design/connectivity/4429865/Reworking-the-TCP-IP-stack-for-use-on-embedded-IoT-devices. Acessado em fevereiro de 2017.

Magalhaes: G. Magalhaes. “Estudo de segurança nos principais protocolos da Internet das Coisas, Universidade de Brasília”. Instituto de Ciências Exatas Departamento de Ciência da Computação. 2016.

Mijumbi: R. Mijumbi et al., “Network function virtualization: State-of-the-art and research challenges,” IEEE Commun. Surveys Tuts. vol. 18, no. 1, pp. 236–262, 1st Quart. 2016.

Montenegro: G. Montenegro, N. Kushalnagar, , J. Hui, D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007.

Nikaein: Navid Nikaein, Eryk Schiller, Romain Favraud, Kostas Katsalis, Donatos Stavropoulos, Islam Alyafawi, Zhongliang Zhao, Torsten Braun and Thanasis Korakis. Network Store: Exploring Slicing in Future 5G Networks. http://www.eurecom.fr/en/publication/4641/download/cm-publi-4641.pdf. Acessado em fevereiro de 2017.

Omnes: N. Omnes, M. Bouillon, G. Fromentoux and O. L. Grand, "A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges," 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, 2015, pp. 64-69.

Open Networking Foundation: https://www.opennetworking.org/sdn-resources/sdn-definition. Acessado em fevereiro de 2017.

Qian: Qian (Clara) Li, Geng Wu, Apostolos (Tolis) Papathanassiou, Udayan Mukherjee. An end-to-end network slicing framework for 5G wireless communication systems. https://arxiv.org/pdf/1608.00572.pdfeiro de 2017.

Raza: U. Raza, P. Kulkarni, M. Sooriyabandar, “Low Power Wide Area Networks: An Overview”, IEEE Communications Surveys & Tutorials · January 2017.

Schneier: Schneier, B., https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html. Acessado em fevereiro de 2017.

SearchSecurity: http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet. Acessado em fevereiro de 2017.

Shang: Wentao Shang, Yingdi Yu, Ralph Droms, Lixia Zhang. Challenges in IoT Networking via TCP/IP Architecture. NDN, Technical Report NDN-0038, February 10, 2016.

Sharma: Anamika Sharma, Er. Sonia Saini, Energy Efficient AODV Protocol for Internet of Things. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 5, Issue 8, August 2016

Sreekanth: Sreekanth. S.S. Software-Defined Networking -A Critical Enabler of IoT. https://medium.com/@Infosys/software-defined-networking-a-critical-enabler-of-iot-eb4e6e4b411f#.lg4p89kli

Steenbrink: Lotte Steenbrink, Routing in the Internet of Things, Hamburg University of Applied Sciences, 2014. http://www.inet.haw-hamburg.de/teaching/ss-2014/master-projekt/aw1_lotte_steenbrink.pdf

Vitkowsky: Vitkowsky, V., https://litigationconferences.com/wp-content/uploads/1955/12/Are-You-and-Your-Insurer-The-Internet-of-Things.pdf. Acessado em fevereiro de 2017.

Voas: J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

Warner: Warner, M. R., http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CD1BBB25-83E0-494D-B7E1-1C350A7CFCCA. Acessado em fevereiro de 2017.

Suporte e serviços e aplicações

Amazon AWS IoT: https://aws.amazon.com/iot/. Acessado em fevereiro de 2017.

AMQP: https://www.amqp.org/. Acessado em fevereiro de 2017.

Bandyopadhyay: Soma Bandyopadhyay, Munmun Sengupta, Souvik Maiti, Subhajit Dutta. Role of *Middleware* for Internet of things: A Study. International Journal of Computer Science & Engineering Survey (IJCSES). 2011

Berthelsen: Emil Berthelsen. Why nosql databases are needed for the internet of things. Research Note, Machina Research (Apr 2014), https://machinaresearch.com/report/research-note-why-nosql-databases-are-needed-for-the-internet-of-things/. Acessado em fevereiro de 2017.

Buyya: Buyya R.. Internet of Things Principles and Paradigms. 2016. Elsevier.

Cassandra: http://cassandra.apache.org/. Acessado em fevereiro de 2017.

Cisco IOx: http://www.cisco.com/c/en/us/products/cloud-systems-management/iox/index.html. Acessado em fevereiro de 2017.

CoAP: http://coap.technology/. Acessado em fevereiro de 2017.

DDS: https://xmpp.org/. Acessado em fevereiro de 2017.

Derhamy: Hasan Derhamy, Jens Eliasson, Jerker Delsing, Peter Priller. A survey of commercial frameworks for the Internet of Things. 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). 2015.

Electronicdesign: Understanding The Protocols Behind The Internet Of Things. http://electronicdesign.com/iot/understanding-protocols-behind-internet-things. Acessado em fevereiro de 2017.

eSTREAM: eSTREAM competition. European Network of Excellence for Cryptology. http://www.ecrypt.eu.org/stream. Acessado em janeiro de 2017.

Fiware: https://www.fiware.org/ . Acessado em fevereiro de 2017.

GlobalPlatform: "The standard for managing applications on secure chip technology". http://globalplatform.org.

Hadoop/HBase: http://hbase.apache.org/. Acessado em fevereiro de 2017.

IBM Watson IoT: https://www.ibm.com/internet-of-things/iot-solutions/watson-iot-platform/. Acessado em fevereiro de 2017.

Kaa: https://www.kaaproject.org/. Acessado em fevereiro de 2017.

Melanie: Swan, Melanie. "Blockchain: Blueprint for a new economy", 2015.

Microsoft Azure IoT Suite: https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suitehttps://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite. Acessado em fevereiro de 2017.

MongoDB: https://www.mongodb.com/. Acessado em fevereiro de 2017.

MQTT: http://mqtt.org/. Acessado em fevereiro de 2017.

Nakhuva: Bhumi Nakhuva, Tushar Champaneria. Study of Various Internet of Things Platforms. International Journal of Computer Science & Engineering Survey (IJCSES). 2016.

Newcomer: Eric Newcomer. Understanding Web Services: XML, WSDL, SOAP, and UDDI. 2002. Primeira Edição. Addison-Wesley Professional.

Ngu: Anne H. H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, Michael Z. Sheng. IoT *Middleware*: A Survey on Issues and Enabling technologies. IEEE Internet of Things Journal. 2016.

Oliveira: Artur Oliveira, Daniel Melo, Geiziany Silva, Thiago Gregório. Comparing IoT Platforms under *Middleware* Requirements in an IoT Perspective. UBICOMM 2016: The Tenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. 2016.

OMA: Device Management Overview http://www.openmobilealliance.org/wp/overviews/dm_overview.html. Acessado em feveiro de 2017.

OMA: LightweightM2M V1.0 Overview. http://www.openmobilealliance.org/wp/Overviews/lightweightm2m_overview.html. Acessado em fevereiro de 2017.

Open-TEE: Open source project for a "virtual TEE based on *software*". https://open-tee.github.io. Acessado em janeiro de 2017.

Oracle IoT Cloud Service: https://cloud.oracle.com/iot. Acessado em fevereiro de 2017.

Razzaque: Mohammad A. Razzaque, Marija Milojevic-Jevric, Andrei Palade, Siobhán Clarke. *Middleware* for Internet of Things: A Survey. IEEE Internet of Things Journal. 2016.

Redbend: "Making Sense of IoT Standards". http://www.redbend.com/data/upl/whitepapers/Making%20Sense%20of%20IoT%20Whitepaper.pdf. Acessado em fevereiro de 2017.

Richardson: Leonard Richardson, Sam Ruby. RESTful Web Services. 2007. Primeira Edição. O'Reilly Media.

Tesla: Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/. Acessado em fevereiro de 2017.

ThingWorx: https://www.thingworx.com/. Acessado em fevereiro de 2017.

Voas: J. Voas, "NIST Special Publication 800-183 Networks of 'Things'". 2016.

Xively IoT Platform: https://www.xively.com/. Acessado em fevereiro de 2017.

XMPP: https://xmpp.org/. Acessado em fevereiro de 2017.

Segurança da informação

AIOTI: WG04. https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-20-0. Acessado em fevereiro de 2017.

Atzori: L. Atzori, A. Iera, G. Morabito, "The internet of things: A survey" Computer Networks. 2010.

BITAG: Broadband Internet Technical Advisory Group. http://www.bitag.org. Acessado em fevereiro de 2017.

Caron: X. Caron, R. Bosua, S. Maynard, A. Ahmad. "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective". Computer Law & Security Review.

Dorri: Dorri A.; Kanhere S.; Jurdak R.; Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. IEEE, http://ieeexplore.ieee.org/abstract/document/7917634. Acessado em maio de 2017.

ENISA: "Cyber security and resilience for Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures". 2016.

ENISA: "Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations". 2015.

ENISA: "Cyber Security and Resilience of smart cars". 2017.

ENISA: "Cyber security for Smart Cities - An architecture model for public transport". 2015.

ENISA: "Securing Smart Airports". 2016.

ENISA: "Security and Resilience of Smart Home Environments - Good practices and recommendations". 2015.

ENISA: https://www.enisa.europa.eu. Acessado em fevereiro de 2017.

European Comission: 7 th Framework Programme for Research and Technological - FP7. https://ec.europa.eu/research/fp7/index_en.cfm. Acessado em fevereiro de 2017.

European Comission: Horizon 2020 Work Programme 2016-2017: Internet Of Things Large Scale Pilots. https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots. Acessado em janeiro de 2017.

Forbes: http://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#4f68e31b3046. Acessado em fevereiro de 2017.

Fremantle: Fremantle P.; Aziz B.; Kirkham T. Enhancing IoT Security and Privacy with Distributed Ledgers - a Position Paper. Abril de 2017.

IBM Institute of Business Value: Device democracy: Saving the future of the Internet of Things. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF. Acessado em maio de 2017.

IBM Institute of Business Value: Fast forward: Rethinking enterprises, ecosystems and economies with blockchains. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03757usen/GBE03757USEN.PDF. Acessado em maio de 2017.

IERC: http://www.internet-of-things-research.eu. Acessado em fevereiro de 2017.

IERC: Internet of Things Applications. AIOTI WG01 – IERC. http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG01Report2015.pdf. Acessado em janeiro de 2017.

ISO: ISO/IEC 27001:2005. Tecnologia da informação – Sistema de gestão de segurança da informação.

ITU: "Global information infraestructure, internet protocol - Aspects and next-generation networks – Frameworks and functional architecture models – Overview of internet of things". https://www.itu.int/rec/T-REC-Y.2060. Acessado em janeiro de 2017.

ITU: "The 3rd revised text for ITU-T X.iotsec-2, security framework for Internet of Things". 2016.

Kaspersky Lab: https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/. Acessado em fevereiro de 2017.

Magalhaes: G. Magalhaes. "Estudo de segurança nos principais protocolos da Internet das Coisas, Universidade de Brasília". Instituto de Ciências Exatas Departamento de Ciência da Computação. 2016.

McKay: K. A. McKay, L. Bassham, M. S. Turan, N. Mouha, "DRAFT NISTIR 8114 Report on Lightweight Cryptography". 2016.

McKinsey: The IoT the value of digitalizing the physical world. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Acessado em maio de 2017.

Miorandi: D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges". Ad Hoc Networks. 2012.

NIST: NIST SP 800-162, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", 2014. http://dx.doi.org/10.6028/NIST.SP.800-162.

NIST: NIST-CSRC. http://csrc.nist.gov. Acessado em fevereiro de 2017.

OWASP: https://www.owasp.org. Acessado em janeiro de 2017.

Ross: R. Ross, M. McEvilley, J. C. Oren, "NIST Special Publication 800-160 - Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems". 2016.

SearchSecurity: http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet. Acessado em fevereiro de 2017.

Stanford: “Rethinking a Secure Internet of Things”. http://iot.stanford.edu/doc/SITP-summary-2016-project.pdf. Acessado em janeiro de 2017.

Suo: H. Suo, J. Wan, C. Zou, J. Liu, “Security in the internet of things: A review”. International Conference on Computer Science and Electronics Engineering (ICCSEE). 2012.

Tapscott: Tapscott, D.; Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Maio de 2016.

TechTarget: Details emerging on Dyn DNS DDoS attack, Mirai IoT botnet. http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet. Acessado em maio de 2017.

Voas: J. Voas, “NIST Special Publication 800-183 Networks of ‘Things’”. 2016.

World Economic Forum: The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. Agosto de 2016.

Zhou: Jun Zhou J.; Cao Z., Dong X.; Vasilakos A. Security and Privacy for Cloud-Based IoT: Challenges. IEEE, http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=7823317. Acessado em maio de 2017.

6.1 Atores

Arthur D. Little: Smart market-makers for the “Internet of Things”. 2011.

McKinsey & Company: Internet of Things (IoT) technology stack. 2015 (update 2016).

MGI: McKinsey Global Institute, “The Internet of Things: Mapping the Value Beyond the Hype”, Junho/2015.

Postscapes: Handbook. Internet of Things Alliances and Consortia. Disponível em: http://www.postscapes.com/internet-of-things-alliances-roundup/. Acesso em 21/02/2017.

Agradecimentos

Gostaríamos de agradecer aos seguintes pesquisadores e profissionais que contribuíram por meio de sua participação no Workshop Tendências Tecnológicas de IoT e entrevistas individuais:

Amanda Remes Mattiuz (VENTURUS) • André Santos (FIT) • Antônio Alberti (INATEL) •Antonio Alfredo Ferreira Loureiro (FCO/UFMG) • Arthur Henrique César de Oliveira (VON BRAUN) • Átila Xavier (CETUC) • Bruno Herrera (CERTI) • Carlos Rodrigues (CETUC) • Daniel Pereira (CESAR) • Eduardo Peixoto (CESAR) • Fabio Lima (FEI) • Felipe Cury (PARQUE TECNOLÓGICO DE SJC) • Fredy João Valente (UFSCAR) • Giordano Cabral (CESAR) • Guilherme Travassos (COPPETEC) • João Paulo Cruz Lopes Miranda (VENTURUS) • José Scodiero (SBMICRO) • Kiev Gama (CESAR) • Laisa Costa (LSITEC) • Lauzier Pereira de Araújo (VENTURUS) • Leandro Augusto da Silva (MACKENZIE) • Leandro Castro Nunes (MACKENZIE) • Leonardo Moreira Resende (FITEC) • Luciano Roncalio (CERTI) • Marcelo Abreu (VENTURUS) • Marcelo Nunes (PARQUE TECNOLÓGICO DE SJC) • Marcelo Sáfadi (PARQUE TECNOLÓGICO DE SJC) • Marlene Pontes (CETUC) • Marta Pudwell Almeida (CETUC) • Matheus Jacon Pereira (IPT) • Mauro Kendi Noda (IPT) • Mauro Miyashiro (ELDORADO) • Moacyr Martucci Jr. (USP) • Nilton I. Morimoto (LSITEC) • Paula Valeiro (FIT) • Renato Franzin (LSITEC) • Rodrigo da Rosa Righi (UNISINOS) • Rodrigo Filev Maia (FEI) • Rodrigo Goncalves Vaz (VAN BRAUN) • Sergio Soares (PORTO DIGITAL) • Tiagos Barros (CESAR) • Werter Padilha (Conselho Consultivo) • Wilhelmus van Noije (LSITEC).

Nossos sinceros agradecimentos também a todos que participaram enviando valiosas contribuições na Consulta Pública para “Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil”.