UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

ANTONIO FLÁVIO MONTEIRO PONTE NETO

COMPARATIVO DAS REDES DE ACESSO DE INTERNET INDUSTRIAL DAS COISAS LORAWAN, SIGFOX, ZIGBEE E 6LOWPAN PARA APLICAÇÃO EM REDES DE SENSORES PARA O MONITORAMENTO DE ATIVOS

VITÓRIA, ES
2019

ANTONIO FLÁVIO MONTEIRO PONTE NETO

COMPARATIVO DAS REDES DE ACESSO DE INTERNET INDUSTRIAL DAS COISAS LORAWAN, SIGFOX, ZIGBEE E 6LOWPAN PARA APLICAÇÃO EM REDES DE SENSORES PARA O MONITORAMENTO DE ATIVOS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica – PPGEE, do Centro Tecnológico da Universidade Federal do Espírito Santo - UFES, como requisito parcial para obtenção do Grau de Mestre em Engenharia Elétrica.

Orientador: Prof. Dr. Anilton Salles Garcia

VITÓRIA, ES
2019

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Ponte Neto, Antonio Flavio Monteiro, 1981-
P813c Comparativo das redes de acesso de internet industrial das coisas Lorawan, Sigfox, Zigbee e 6lowpan para aplicação em redes de sensores para o monitoramento de ativos / Antonio Flavio Monteiro Ponte Neto. - 2019.
102 f. : il.

Orientador: Anilton Salles Garcia.
Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Espírito Santo, Centro Tecnológico.

1. Internet das Coisas. 2. Engenharia Elétrica. 3. Tecnologia. 4. Redes de Computadores. I. Garcia, Anilton Salles. II. Universidade Federal do Espírito Santo. Centro Tecnológico. III. Título.

CDU: 621.3

Agradecimentos

A Deus, por me guiar e me acompanhar na minha jornada desde o nascimento até agora e por estar presente em todos os momentos da minha vida. Sem ele, não há nada.

A minha querida e linda esposa Alina, a minha “Zaya”, que sempre me impulsiona e me incentiva a buscar os meus objetivos e por ser um exemplo de determinação para mim.

Um agradecimento especial ao meu orientador o Prof. Dr. Anilton Salles Garcia por toda a sua dedicação, apoio e disponibilidade. Foram fatores importantes para que este trabalho fosse possível.

Resumo

A IIoT (*Industrial Internet of Things*), que é a aplicação da IoT na indústria, faz parte do conceito da indústria 4.0, que enfatiza a ideia de digitalização e conectividade de todas as unidades produtivas, combinando os pontos fortes da automação industrial tradicional com tecnologias da internet e de redes de sensores, notadamente sensores sem fio (BONAVOLONTÀ F. et al., 2017).

O grande número de dispositivos, juntamente com o volume, velocidade e estrutura de dados, apresenta desafios para a indústria, especialmente nas áreas de segurança, gestão de dados, armazenamento e rede. Confrontado com esses desafios, as indústrias estão imersas em um universo sem fim de opções tecnológicas, o que torna complexa a definição de um *roadmap*.

Quando confrontadas com tecnologias potencialmente inovadoras, muitas indústrias são cautelosas em sua adoção, pois quase invariavelmente envolvem a necessidade de investimento e, muitas vezes, mudanças organizacionais.

Aliado a isso, em um contexto no qual as indústrias estão passando por um processo de transformação digital, onde o monitoramento de ativos torna-se fundamental para alcançar melhores resultados de produção e menores custos de manutenção, este trabalho tem como objetivo auxiliar na escolha daquela tecnologia que mais se adequa à esta finalidade.

Portanto, através da análise comparativa dos protocolos de redes de acesso de IIoT mais utilizados atualmente no mundo, LoRaWAN, Sigfox, ZigBee e 6LoWPAN, foi possível concluir que 6LoWPAN é a tecnologia mais adequada para esta aplicação, levando em consideração os critérios de *throughput,* latência, topologia, *overhead,* segurança e consumo de energia.

Palavras-chave: Internet Industrial das Coisas, Indústria 4.0, LoRaWAN, Sigfox, ZigBee, 6LoWPAN.

Abstract

Industrial Internet of Things (IIoT), which is the application of IoT in the industry, is part of the Industry 4.0 concept, which emphasizes the idea of digitization and connectivity across all production facilities, combining the strengths of traditional industrial automation with internet and sensor networks technologies, notably wireless sensors (BONAVOLONTÀ F. et al., 2017).

The sheer number of devices, along with volume, speed and data structure, presents challenges for the industry, especially in the areas of security, data management, storage and networking. Faced with these challenges, industries are immersed in an endless universe of technological options, which makes defining a roadmap complex.

When confronted with potentially innovative technologies, many industries are cautious in their adoption as they almost invariably involve the need for investment and often organizational change.

Allied to this, in a context which industries are undergoing a digital transformation process, where asset monitoring becomes fundamental to achieve better production results and lower maintenance costs, this work aims to assist in choosing that technology. which best suits this purpose.

Therefore, through comparative analysis of the most commonly used IIoT access network protocols in the world today, LoRaWAN, Sigfox, ZigBee and 6LoWPAN, it was concluded that 6LoWPAN is the most suitable technology for this application, taking into account the throughput criteria, latency, topology, overhead, security and energy consumption.

Keywords: Industrial Internet of Things, Industry 4.0, LoRaWAN, Sigfox, ZigBee, 6LoWPAN.

Sumário

Sumário 8

Lista de Figuras 11

Lista de Tabelas 12

Lista de Abreviaturas 13

1. Introdução 14

1.1 Contextualização 14
1.2 Motivação do Trabalho 16
1.3 Justificativa do Trabalho 17
1.4 Objetivos 18
1.5 Metodologia de Desenvolvimento do Trabalho 18
1.6 Principais Resultados e Contribuições do Trabalho 19
1.7 Organização do Texto 20

2. Internet Industrial das Coisas 21

2.1 Características Principais 21
2.2 Vantagens da Internet Industrial das Coisas para o Negócio 22
2.3 Evolução do Conceito 23
2.3.1 Sistemas de automação industrial modernos 23
2.3.2 Ganhos com a introdução da IIoT nas empresas 24
2.3.3 Exemplos de implementação de sistemas industriais de IoT 25
2.4 Estado Atual do uso da Tecnologia 25
2.4.1 Aplicação da IIoT em várias indústrias 25
2.5 IIoT para o Monitoramento de Ativos 28
2.5.1 O desafio da manutenção 28
2.5.2 Manutenção Proativa (Preditiva) 29
2.5.3 Aplicação de IIoT na Manutenção Proativa 32
2.5.4 Características das redes IIoT *versus* Monitoramento de Ativos 34
2.6 Principais Desafios e Oportunidades 35

3. Fundamentos Teóricos 37

3.1 LoRaWAN 37
3.1.1 Arquitetura de redes LoRaWAN 39
3.1.2 Estrutura dos quadros da camada MAC 45
3.1.3 *Throughput* 47

3.1.4 Segurança 48
3.2 Sigfox 49
3.2.1 Arquitetura de redes Sigfox 50
3.2.2 Estrutura dos quadros da camada MAC 52
3.2.3 *Throughput* 53
3.2.4 Segurança 54
3.3 ZigBee 56
3.3.1 Arquitetura de redes ZigBee 58
3.3.2 Estrutura dos quadros da camada MAC 63
3.3.3 *Throughput* 65
3.3.4 Segurança 65
3.4 6LoWPAN 66
3.4.1 Arquitetura de redes 6LoWPAN 70
3.4.2 Estrutura dos quadros da camada MAC 73
3.4.3 *Throughput* 74
3.4.4 Segurança 75

4. Trabalhos Relacionados 77

5. Desenvolvimento da Proposta 80
5.1 *Throughput* 80
5.2 Latência 81
5.3 Topologia 82
5.4 *Overhead* 83
5.5 Segurança 84
5.6 Consumo de energia 85

6. Estudo de Caso 86
6.1 Comparativo LoRaWAN *versus* Sigfox 86
6.1.1 *Throughput* 87
6.1.2 Topologia 87
6.1.3 Latência 89
6.1.4 *Overhead* 89
6.1.5 Segurança 90
6.1.6 Consumo de energia 91
6.2 Comparativo 6LoWPAN *versus* ZigBee 91
6.2.1 *Throughput* 92
6.2.2 Topologia 92
6.2.3 Latência 93
6.2.4 *Overhead* 94
6.2.5 Segurança 94

6.2.6 Consumo de energia..... 95
6.3 Resumo da análise comparativa..... 95

7. Conclusão..... 98

Referências Bibliográficas..... 99

Lista de Figuras

Figura 1 – Exemplos de aplicação de Internet das Coisas 16
Figura 2 – níveis de sistemas de automação industrial.....24
Figura 3a – motor elétrico de correia transportadora oscilatória.....31
Figura 3b – motor elétrico de ventilador da torre de resfriamento.....32
Figura 4 – Manutenção preditiva dividida em níveis. 34
Figura 5 – Arquitetura de rede LoRaWAN. 39
Figura 6 – Classes de dispositivos LoRaWAN. 42
Figura 7 – Procedimento de ativação do terminal do "assinante" (*end node*) via rádio. 45
Figura 8 – Formato da mensagem da camada MAC LoRaWAN. 46
Figura 9 – Encapsulamento da mensagem da camada MAC LoRaWAN. 47
Figura 10 – Arquitetura da rede Sigfox. 51
Figura 11 – Arquitetura plana da rede Sigfox. 52
Figura 12 – Estrutura dos quadros de *uplink* e *downlink* da camada MAC Sigfox. 53
Figura 13 – Esquemas de segurança dos dispositivos Sigfox. 55
Figura 14 – Tipos de dispositivos de redes ZigBee. 58
Figura 15 – (a) topologia em estrela; (b) topologia *peer-to-peer*. Círculo roxo – dispositivo com funcionalidade completa (FFD); Círculo verde – dispositivo com funcionalidade reduzida (RFD). 60
Figura 16 – Exemplo de rede com topologia em árvore de *cluster*. (CID = *Cluster* ID; CLH = *Cluster Head*). 62
Figura 17 – Estrutura de *superframe* com intervalos de tempo definidos. 63
Figura 18 – O formato do quadro de dados de acordo com o IEEE 802.15.4. 65
Figura 19 – Comparativo de áreas de aplicação e possibilidade de cobertura dos serviços ZigBee e 6LoWPAN.....68
Figura 20 – Exemplo de rede IPv6 com uma rede de malha 6LoWPAN. 70
Figura 21 – Arquitetura de redes 6LoWPAN. 72
Figura 22 – Pilha de cabeçalhos 6LoWPAN. 74
Figura 23 – Gráficos resumo da análise comparativa entre as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN. ..96
Figura 24 – Gráfico de radar da análise comparativa entre as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN. ..97

Lista de Tabelas

Tabela 1 - Acrônimos, descrição e comprimento dos campos das mensagens da camada MAC LoRaWAN.....47
Tabela 2 – Exemplos de mensagens Sigfox 52
Tabela 3 – Níveis do modelo OSI da rede ZigBee / IEEE 802.15.4.....57
Tabela 4 – Quadro resumo da bibliografia estudada.....79
Tabela 5 – Comparação das características técnicas das redes de longo alcance LPWAN 87
Tabela 6 – Comparação das características técnicas das redes WPAN. 92
Tabela 7 – *Overhead:* Comparação entre protocolos.....94

Lista de Abreviaturas

6LoWPAN – IPv6 over Low power Wireless Personal Area Networks
AMQP – Advanced Message Queuing Protocol
ANSI – American National Standards Institute
CAPEX – Capital Expenditure
CIoT – Customer Internet Of things
CoAP – Constrained Application Protocol
CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance
ERP – Enterprise Resource Planning
FOTA – Firmware Over The Air
GLONASS – Global Satellite Navigation System
GPS – Global positioning Sysytem
HAN – Home Area Network
HTTP – Hyper Text Transfer Protocol
IIoT – Industrial Internet Of Things
ISA – International Society for Automation
JSON – Java Script Object Notation
LAN – Local Area Network
LoRaWAN – Long Range Wide Area Network
LPWA – Low Power, Wide Area
LPWAN – Low Power Wide Area Network
LTE – Long Term Evolution
M2M – Machine to Machine
MAN – Metropolitan Area Network
MES – Manufacturing Execution System
MQTT – Message Queuing Telemetry Transport
MTBF – Mean Time Between Failures
MTTR – Mean Time To Repair
OPEX – Operational Expenditures
OSI – Open System Interconnection
PAN – Personal Area Network
PLC – Programmable Logic Controller
QoS – Quality of Service
RFID – Radio Frequency Identification
SCADA – Supervisory Control and Data Acquisition
TCP/IP – Transmission Control Protocol/Internet Protocol
UDP – User Datagram Protocol
WAN – Wide Area Network
WPAN – Wireless Personal Area Network
XMPP – Extensible Messaging and Presence Protocol

1. Introdução

1.1 Contextualização

Atualmente a Internet das Coisas (IoT – *Internet of Things*) é o ramo da tecnologia da informação que mais se desenvolve e está em constante atualização. É a combinação de uma variedade de dispositivos, sensores, atuadores, etc., que anteriormente eram utilizados localmente e de forma autônoma, mas que agora possuem conexão com a internet. Portanto, atualmente, a Internet vem desempenhando o papel de uma rede global para a Internet das Coisas através do protocolo IP.

De acordo com um estudo realizado pela Cisco (EVANS, 2011), a mudança para a Internet das Coisas ocorreu aproximadamente entre 2008 e 2009. Desde aquela época, o número de dispositivos conectados à internet é maior do que a população da terra e o número de inovações neste campo é continuamente crescente, indicando o desenvolvimento ativo da Internet das Coisas.

Em linhas gerais, "Coisas" (dispositivos que compõem a Internet das Coisas) devem possuir as seguintes características:

- Ter acesso à Internet com a finalidade de transmitir ou solicitar quaisquer dados;
- Ter um endereço específico na WAN ou identificador que pode ser usado para *feedback*;
- Possuir uma interface para a interação com o usuário.

"Coisas" na Internet das Coisas podem formar redes locais (LAN – *Local Area Networks*) unidas por uma área de serviço ou função. Por exemplo, uma rede de *Smart Home*, consistindo de diferentes sensores, pode ter acesso à Internet e tem a capacidade de gerenciamento através de uma interface *Web*. Ao mesmo tempo, várias "redes inteligentes" podem ser mescladas em uma rede interconectada de monitoramento. Por exemplo, a gestão dos sistemas de combate a incêndios de uma cidade e as redes de área metropolitana (MAN – *Metropolitan Area Networks*) podem ser combinadas para formar uma rede para compartilhar informações sobre índices de incêndios e dados de segurança em qualquer cidade do país. Este exemplo é um caso especial de redes distribuídas geograficamente, cujo desenvolvimento levou a uma ativa inovação em redes de sensores sem fio na última década.

Redes de sensores sem fio são uma das áreas mais ativas no campo de sistemas de monitoramento e são desenvolvidas a partir das redes locais de sensores distribuídos

geograficamente, conectados a redes globais de Internet. Com o advento da Internet das Coisas, todas as "Coisas" inteligentes com acesso à Internet passaram a ser chamadas de Internet das Coisas.

O principal objetivo de aplicações de IoT é a coleta de informações (sobre o ambiente urbano, sobre a saúde humana, sobre o estado dos equipamentos na fábrica) através de redes de sensores – pressão, umidade, luz, movimento, fluxo de calor, nível, etc. Graças à comunicação sem fio e vários protocolos, eles são capazes de interagir entre si, e enviar as informações coletadas para sua posterior análise por uma pessoa ou inteligência artificial.

Centros de dados, tecnologias de nuvem e *Big Data* são usados para armazenar e processar os dados recebidos. Hoje, a Internet das Coisas não possui um único padrão ou protocolo, mas há uma coleção de muitos tipos de comunicações sem fio disponíveis. Em vários projetos de IoT, uma conexão pode ser construída com base em tecnologias como Wi-Fi, Bluetooth, RFID (*Radio Frequency Identification*), LPWAN (*Low Power Wide Area Network*), LTE (*Long Term Evolution*), 3G, ZigBee, LoRaWAN (*Long Range Wide Area Network*), etc.

Além disso, as aplicações de IoT são extremamente diversificadas e podem ser divididas em dois grupos – CIoT (*Costumer Internet of Things* – Internet das Coisas do Consumidor) e IIoT (*Industrial Internet of Things* – Internet das Coisas Industrial). CIoT é destinado ao usuário final, a Internet das coisas é usada em produtos como eletrodomésticos inteligentes, eletrônicos *wearables* (rastreadores de *fitness*, relógios inteligentes) e outros aparelhos inteligentes. Já os projetos de IIoT são implementados em vários setores da economia (indústria, agricultura, saúde, etc.) e têm um consumidor corporativo, ou a sociedade como um todo age como um consumidor. Exemplos incluem casas inteligentes, cidades inteligentes, setor de transportes, automação e monitoramento de ativos de produção, etc.

A Figura 1 ilustra mais exemplos de aplicações de IoT como soluções para pessoas, cidades e indústrias.

Figura 1 – Exemplos de aplicação de Internet das Coisas

Fonte: https://portal.tcu.gov.br/inovatcu/noticias/internet-das-coisas-de-objetos-a-cidades-inteligentes.htm

Ainda sobre as redes de sensores, mais um passo importante para a viabilização da ideia de Internet das Coisas é a tecnologia M2M (*Machine to Machine*). M2M é um nome genérico para tecnologias que permitem que os instrumentos e sensores troquem informações entre si. Estes são sistemas de sensores com e sem fio que transmitem informações de um dispositivo para outro. Considera-se que esta tecnologia deu origem ao termo Internet das Coisas, o que significa um ambiente computacional discreto, que consiste em dispositivos que comunicam entre si de forma independente e fornecem ao usuário os resultados das suas atividades.

No futuro, a Internet das Coisas atingirá um grande número de dispositivos. De acordo com o mesmo estudo realizado pela Cisco (EVANS, 2011), até 2020, o número total de dispositivos conectados à rede será de 12 a 50 bilhões de unidades. Além disso, a cada dia surgem novas tecnologias de IoT para diversas aplicações. Portanto, neste contexto, torna-se cada vez mais importante a elaboração de requisitos de desempenho e critérios de comparação para auxiliar na escolha da solução mais adequada para uma determinada aplicação.

1.2 Motivação do Trabalho

Em um momento onde a Internet das Coisas vem cada vez mais inserindo-se nos mais variados ambientes industriais, diferentes requisitos para os dispositivos pertencentes às redes de acesso podem ser exigidos dependendo da aplicação e ramo de negócio.

Um dos desafios enfrentados hoje pela Internet das Coisas (IoT) é suportar de forma eficiente a comunicação máquina-a-máquina, dado que os sensores remotos e os dispositivos de *gateway* são conectados na sua grande maioria através de *links* de comunicação sem fio não confiáveis, de baixa largura de banda ou intermitentes.

Já existem comercialmente muitos protocolos de IIoT para os dispositivos na camada de conectividade. Entretanto, ainda não há critérios bem definidos para a escolha de um protocolo para aplicação em monitoramento de ativos e manutenção preditiva.

Neste trabalho, são comparados qualitativamente o desempenho em *throughput*, latência, topologia, *overhead*, segurança e consumo de energia dos protocolos de IIoT LoRaWAN (*Low Power WAN Protocol for Internet of Things*), ZigBee, Sigfox e 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*), aplicados ao monitoramento de ativos. Primeiramente são comparados dois a dois os protocolos com características semelhantes (LoRaWAN *vs* Sigfox e ZigBee *vs* 6LoWPAN) e, em seguida, são consolidados os desempenhos das quatro tecnologias de forma a concluir a análise comparativa.

1.3 Justificativa do Trabalho

Atualmente existem inúmeros protocolos de rede de acesso de IIoT, licenciados e não licenciados, que podem ser aplicados a diversos segmentos, tais como cidades inteligentes, agricultura moderna, medicina, cuidado em saúde, dispositivos *wearables* e indústria 4.0. Neste último, e mais especificamente na aplicação em monitoramento remoto de ativos e manutenção preditiva, algumas características dos protocolos de rede de IIoT são mais preponderantes, por exemplo, consumo da largura de banda, latência, vida útil da bateria, segurança, topologia e relação entre *overhead* de controle e *payload*. Escolher o tipo apropriado de conectividade é uma parte importante de qualquer projeto de IIoT.

Portanto, uma base comparativa onde os principais protocolos de redes de acesso de IIoT sejam comparados e classificados, tomando como base os critérios mencionados anteriormente, é essencial para aquele que pretende aplicar IIoT como uma solução para a implantação de monitoramento preditivo de ativos como estratégia de manutenção.

1.4 Objetivos

O objetivo geral deste trabalho é elencar os principais protocolos de rede de acesso de IoT na atualidade, destacando e comparando as características mais relevantes para a aplicação em redes de sensores para o monitoramento de ativos industriais. Este comparativo deverá guiar os engenheiros de aplicação na escolha do protocolo mais adequado para a utilização desejada.

Os objetivos podem ser divididos em estratégicos e específicos, os quais foram executados como tarefas durante o desenvolvimento do trabalho. Os objetivos estratégicos são:

- Pesquisar e definir protocolos de rede de acesso de IoT para determinadas aplicações industriais;
- Definir critérios de comparação entre esses protocolos.

Os objetivos específicos são:

- Apresentar aplicações que utilizam ou podem utilizar redes de IIoT;
- Contextualizar a importância e necessidade de redes de IIoT para aplicações industriais, tais como monitoramento de ativos e manutenção preditiva;
- Analisar e descrever as diferenças entre os protocolos de IIoT selecionados, baseado nos critérios de latência, *throughput*, topologia, *overhead* de controle, segurança e consumo de energia;
- Realizar comparações qualitativas baseadas nas bibliografias selecionadas;
- Propor uma base comparativa para auxiliar na escolha de protocolos de redes de acesso de IoT para aplicação em monitoramento de ativos e manutenção preditiva.

1.5 Metodologia de Desenvolvimento do Trabalho

O método de pesquisa utilizado é a análise qualitativa dos critérios de comparação entre os protocolos de redes de acesso de IoT, definidos no capítulo 2.

O estudo é desenvolvido a partir de pesquisa bibliográfica de artigos recentes relacionados ao tema “Redes de Acesso de IoT”, “Monitoramento de Ativos Utilizando IoT”, “Avaliação de Desempenho de Protocolos de Redes de IoT” e “Comparativo entre Protocolos de Rede de IoT”.

Neste trabalho são analisados os conceitos mais relevantes para a aplicação de tecnologias de IIoT no monitoramento de ativos, pois podem ser decisivos para a sua implementação.

Os conceitos analisados são:

- *Throughput*;
- Latência;
- Topologia;
- Relação entre *Overhead* de Controle e *Payload*;
- Segurança;
- Consumo de energia.

Throughput e latência normalmente são requisitos de QoS (*Quality of Service*) utilizados para definir regras de roteamento em redes de IIoT. Baixos *throughputs* e elevadas latências observadas em tais redes são indícios de sobrecarga e podem comprometer o funcionamento, causando indisponibilidades.

A análise da topologia das tecnologias selecionadas deu informações importantes quanto à escalabilidade das redes e restrições para futuras ampliações.

Ao comparar o *overhead* de controle entre as diferentes tecnologias, foi possível concluir qual aquela que menos exige recursos da rede para o envio de dados.

Já a segurança dos dados que circulam nas redes e a segurança contra ataques externos vem se tornando uma preocupação cada vez maior em aplicações de tecnologias de IIoT em ambientes industriais.

Finalmente, o consumo de energia pode ser decisivo na implementação de tecnologias de IIoT, uma vez que essas diferem das tecnologias tradicionais de automação industrial pela autonomia dos dispositivos e facilidade de mobilidade.

Os principais autores cujas publicações contribuíram para o desenvolvimento da dissertação foram: C. Burati et al. (2016), J. Kaur et al. (2016), F. Bonavolontà et al. (2017), M. Iglesias-Urkia et al. (2017), S. Al-Sarawi et al. (2017) e A. Gloria et al. (2017).

1.6 Principais Resultados e Contribuições do Trabalho

A contribuição efetiva deste trabalho é a apresentação de uma base comparativa entre os protocolos de IIoT: LoRaWAN, Sigfox, ZigBee e 6LoWPAN, utilizando os critérios mais

relevantes para o monitoramento de ativos industriais (*throughput*, latência, topologia, *overhead*, segurança e consumo de energia).

O resultado desta comparação mostrou a tecnologia 6LoWPAN como sendo aquela que apresenta o melhor desempenho na maoiria dos critérios de comparação definidos neste trabalho, sendo portanto a mais favorável para a aplicação em monitoramento de ativos.

Semelhantemente, como parte da pesquisa deste trabalho, também foi publicado um artigo que apresenta critérios para comparação entre redes industriais legadas (Ethernet, Controlnet e Devicenet) (PONTE F. e LIM G. F., 2019). Entretanto, as redes tradicionais de automação foram comparadas segundo os critérios de tempo total de atraso, utilização do meio de transmissão, taxa de descarte de pacotes e eficácia da rede, mais relevantes para redes de controle.

1.7 Organização do Texto

Este trabalho está estruturado em sete capítulos. No Capítulo 1, em uma breve introdução, são apresentados os aspectos da realidade atual da Internet das Coisas e os desafios que as indústrias de hoje enfrentam para a escolha de soluções e IIoT para as aplicações pretendidas, dentro de uma variedade de protocolos que aumenta a cada dia. Esses desafios motivaram a elaboração deste trabalho e, ainda no Capítulo 1, são descritos os objetivos gerais e específicos que definiram o escopo e a abordagem escolhidos para o preenchimento dos *gaps* identificados a partir da revisão da bibliografia disponível, relacionada ao tema.

O restante deste trabalho está organizado da seguinte forma: no Capítulo 2 são apresentados o conceito da Internet Industrial das Coisas e como ela se insere no contexto do monitoramento de ativos. Os protocolos de redes de acesso de IoT, objetos deste estudo, estão descritos no Capítulo 3, seguidos por um breve levantamento de trabalhos relacionados no Capítulo 4. No Capítulo 5, é descrita a abordagem proposta. O Capítulo 6 apresenta e analisa os resultados da revisão bibliográfica. E, finalmente, as conclusões são apresentadas e trabalhos futuros são identificados no Capítulo 7.

2. Internet Industrial das Coisas

2.1 Características Principais

Internet das Coisas na Indústria ou Internet das Coisas em Ambiente Industrial (*Industrial Internet of Things*, IIoT) é um conceito em que uma variedade de dispositivos industriais como sensores, ou equipamentos e dispositivos diversos, conectam-se em rede. O termo "Internet Industrial das Coisas" foi primeiramente usado pela *General Electric* no final do ano de 2012.

Sensores, atuadores, controladores e interfaces homem-máquina são instalados em diversos equipamentos críticos para o processo, com o objetivo de monitorar e/ou controlar parâmetros que traduzem a condição de funcionamento (temperatura, vibração, pressão, vazão, etc.).

Em seguida, os dados coletados (vibração, temperatura, produção, etc.) permitem que as empresas possam diagnosticar falhas antes que elas ocorram, obter informações de produção em tempo real e até mesmo obter um banco de dados que pode ser utilizado para definir tempos ótimos para manutenção.

As informações obtidas podem ser usadas para evitar paralisações não programadas, interrupções de equipamentos, reduzir a manutenção não programada e falhas no gerenciamento da cadeia de suprimentos, permitindo assim que a empresa funcione com mais eficiência.

A fim de evitar paralisações e manter a segurança na empresa, é necessário introduzir tecnologias para detectar e prever riscos. O monitoramento proativo contínuo dos principais indicadores permite identificar o problema e tomar as medidas necessárias para resolvê-lo. Para a conveniência dos operadores, os sistemas modernos permitem que se visualize as condições do fluxo de processos tecnológicos e identifique os fatores que os afetam através de qualquer navegador da *web*. A análise *online* ajuda os usuários a encontrar a causa raiz do problema mais rapidamente.

Graças a tais soluções, os dados de produção são transformados em informações úteis, necessárias para o gerenciamento seguro e racional de uma empresa.

A introdução de tais tecnologias permite que empresas de diferentes setores da economia obtenham certas vantagens: aumentar a eficiência do uso de ativos de produção, reduzindo o número de paradas não planejadas; reduzir os custos de manutenção; melhorar os

procedimentos de previsão e prevenção de falhas catastróficas de equipamentos e identificar operações ineficientes.

A Internet industrial das Coisas está mudando fundamentalmente todo o modelo econômico de interação fornecedor-consumidor. Isso permite:

- Automatizar o processo de monitoramento e gerenciamento do ciclo de vida dos equipamentos;
- Organizar cadeias auto-otimizadoras efetivas de empresas - fornecedores para empresas - consumidores finais.

Nos casos mais avançados, a Internet industrial das Coisas permite não só melhorar a qualidade do suporte técnico de equipamentos utilizando ferramentas avançadas de telemetria, mas também proporcionar uma transição para um novo modelo de negócio de sua operação, quando o equipamento é pago pelo cliente mediante o uso de suas funções.

A introdução de redes entre máquinas, equipamentos, edifícios e sistemas de informação, a capacidade de monitorar e analisar o ambiente, o processo de produção e seu próprio estado em tempo real, transferindo funções de gerenciamento e tomada de decisão para sistemas inteligentes levam a uma mudança no “paradigma” do desenvolvimento tecnológico. "A quarta revolução industrial".

Especialistas reconhecem a Internet das Coisas como uma tecnologia que introduz uma transformação irreversível na organização de processos modernos de produção e negócios e gera novos modelos de negócios.

Essa abordagem permite implementar no espaço virtual processos de negócios *end-to-end* arbitrariamente complexos que são capazes de executar automaticamente o gerenciamento de otimização de vários tipos de recursos através de toda a cadeia de suprimentos e criação de valor de produtos - desde o desenvolvimento de ideias, *design*, produção e operação.

Assim, pode-se dizer que a Internet Industrial das Coisas é uma transformação organizacional e tecnológica da produção baseada nos princípios da “economia digital”, que permite, no nível gerencial, combinar produção real, transporte, recursos humanos, engenharia e outros recursos virtuais praticamente controláveis por *software*.

2.2 Vantagens da Internet Industrial das Coisas para o Negócio

- Dados que anteriormente não estavam disponíveis, com a penetração crescente de sistemas embarcados são transformados em informações valiosas sobre a natureza do uso de produtos e equipamentos para todos os participantes do ciclo

de produção, são fundamentais para a formação de novos modelos de negócios e proporcionam receita adicional de novos serviços, como: contrato de ciclo de vida para equipamentos industriais, contrato de fabricação como serviço, transporte como serviço, segurança como serviço e outros;

- Modelagem de processos tecnológicos, *design end-to-end* e, como resultado, otimização da cadeia de valor em todas as fases do ciclo de vida do produto em tempo real;
- O funcionamento de vários setores da economia se torna continuamente mais complexo devido ao desenvolvimento de tecnologias e cada vez mais pela tomada automática de decisões pelas próprias máquinas com base na análise de grandes quantidades de dados de dispositivos conectados, o que gradualmente reduz o papel do pessoal de produção, inclusive qualificados. Educação profissional de alta qualidade, incluindo engenharia, programas especiais de treinamento para funcionários e treinamento são necessários.

2.3 Evolução do Conceito

2.3.1 Sistemas de automação industrial modernos

Sistemas de automação industrial tradicionais (que não usam os princípios da Indústria 4.0) podem ser divididos, de acordo com a norma americana ANSI/ISA-95, em vários níveis (Figura 2). O primeiro – equipamentos de "campo", por exemplo, no *site* tecnológico da empresa ou na loja: vários sensores e atuadores. O segundo nível de controle – controladores lógicos programáveis (em inglês, PLC – *Programmable Logic Controller*), coletando informações dos sensores e controlando os atuadores. Os sistemas de controle de processo de terceiro nível são classe SCADA (Controle de Supervisão e Aquisição de Dados). No quarto nível, encontram-se os sistemas de planejamento de produção ou MES (*Manufacturing Execution System*). Finalmente, no topo, no quinto nível, está o sistema de planejamento dos recursos corporativos (*Enterprise Resource Planning*, ERP) que geralmente são executados em servidores localizados em *datacenters* corporativos.

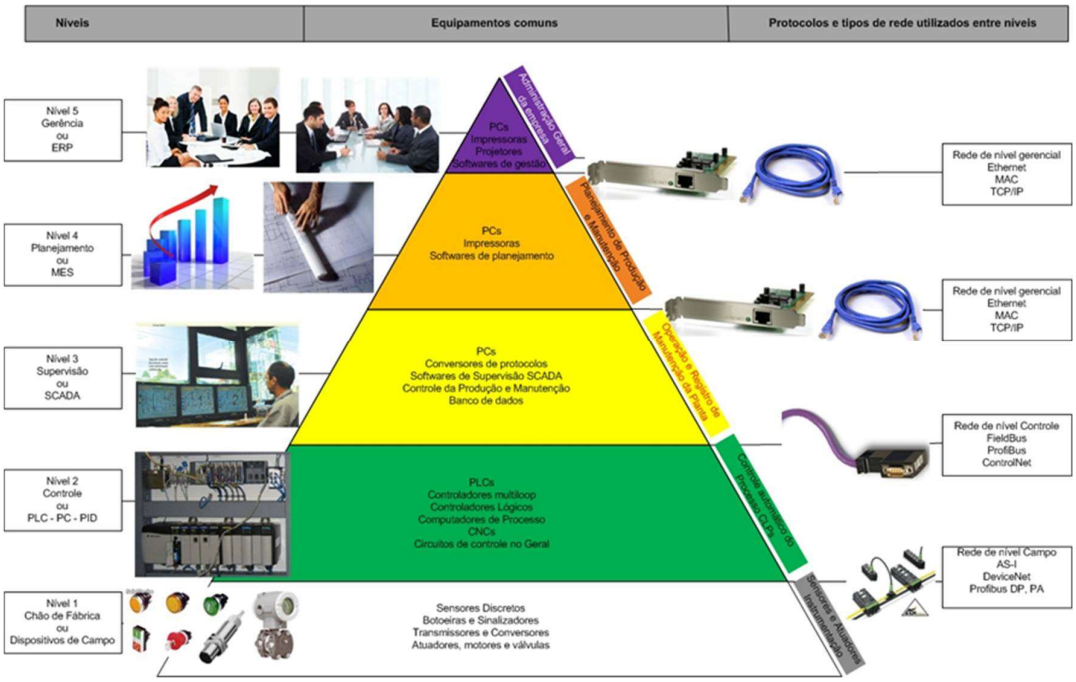

Figura 2 – níveis de sistemas de automação industrial.

Fonte: http://kleberautomation.blogspot.com/2012/01/piramide-da-automacao.html

A implementação do conceito de indústria 4.0 e IIoT, no futuro próximo, poderá implicar em uma mudança na pirâmide da automação tradicional (Figura 2). O nível inferior permanecerá, mas o número de dispositivos neste nível aumentará significativamente e estes serão mais inteligentes. Eles se tornarão parte de sistemas cyber-físicos e serão capazes de desempenhar autonomamente muitas funções de coleta inteligente de dados e mecanismos de controle. A maioria dos recursos dos sistemas *upstream* existentes será migrada para servidores de alto desempenho que serão localizados em *data centers*. As tecnologias de virtualização usadas no campo da tecnologia da informação penetram nos sistemas de automação industrial. O número total de sistemas de controle será reduzido e a produtividade do trabalho, a eficiência de recursos aumentará, enquanto os custos de produção diminuirão.

2.3.2 Ganhos com a introdução da IIoT nas empresas

A introdução da Internet Industrial das Coisas (IIoT) nas empresas pode ajudar a economizar grandes quantias ao assegurar confiabilidade e bom funcionamento. Por exemplo, a empresa de energia *Salt River Project* economiza cerca de US$ 5 milhões por ano usando uma solução de *software* da *General Electric Digital* para gerenciamento de eficiência de recursos baseado em IIoT. Outra empresa de energia, a *Scottish and Southern Energy*, utiliza a

confiabilidade do sistema de controle 365 dias por ano e poupa cerca de 3 milhões de euros por ano (GENERAL ELECTRICS DIGITAL, 2016). Alguns especialistas do setor estimam o lucro total da Internet das Coisas (IoT) até 2020 em US$ 1,9 trilhão.

Na China, um tópico importante é a aplicação dos princípios da Internet das Coisas na agricultura, por exemplo, ao rastrear toda a cadeia de vendas de pepinos, desde o cultivo até a entrega ao ponto de venda ao consumidor final (QU et al., 2011 e HONG et al., 2011 e ZHOU et al., 2013).

2.3.3 Exemplos de implementação de sistemas industriais de IoT

Na Rússia, os especialistas da *Yandex Data Factory* desenvolveram e implementaram uma solução baseada nas tecnologias da Yandex na área de aprendizado de máquina e análise de *Big Data* na *Magnitogorsk Iron and Steel Works* (MMK). É utilizado para otimizar o consumo de materiais adicionais e ferroligas na produção de aço. O serviço desenvolvido prevê a composição química do aço, com base em dados históricos sobre o uso de ferro-ligas em pré-fundidos (usando dados de mais de 200 mil aquecedores nos últimos sete anos). Então, o conjunto ótimo e o número de ferroligas para fusão do aço é calculado com base nas previsões do modelo de processo, que o sistema fornece ao operador em tempo real na forma de recomendações apropriadas. Testes e validação do processo mostraram que o consumo de ferroligas usando essa solução é reduzido em uma média de 5%, e a economia anual pode exceder 275 milhões de rublos (BARSKOV, 2016).

A Internet das Coisas abrange uma enorme variedade de setores e casos de uso que variam de um único dispositivo a implementações em massa de plataformas cruzadas de tecnologias incorporadas e sistemas em nuvem que se conectam em tempo real.

Juntando tudo isso existem inúmeros protocolos de comunicação legados e emergentes que permitem que dispositivos e servidores conversem entre si de maneiras novas e mais interconectadas.

Ao mesmo tempo, dezenas de alianças e coalizões estão se formando na esperança de unificar o cenário de IoT.

2.4 Estado Atual do uso da Tecnologia

2.4.1 Aplicação da IIoT em várias indústrias

2.4.1.1 Sistemas de fornecimento de energia

Na indústria de energia elétrica, o termo “redes inteligentes” e medidores inteligentes geralmente se enquadram na definição de “Internet Industrial das Coisas”.

No nível de gerenciamento do sistema, balanços e modos no setor de energia, um passo em direção à transformação digital de ativos pode dar uma oportunidade de planejar melhor o carregamento das capacidades de geração e, mais importante, seu volume. Como o sistema de energia brasileiro é construído sobre redundância, a criação de um modelo de distribuição inteligente removeria parte da geração ineficiente da operação e resolveria parcialmente a superprodução de capacidade de geração. Ao mesmo tempo, isso permitiria uma introdução mais generalizada de incentivos modernos para reduzir o consumo de eletricidade: por exemplo, a resposta à demanda.

No setor de redes elétricas, uma introdução mais ampla de tecnologias inteligentes, especialmente dada a extensão de instalações lineares, poderia levar a uma maior confiabilidade e menores custos operacionais. Isso permitiria, finalmente, passar para a gestão da rede “por estado” (preditivo), e não para realizar reparos de acordo com prazos regulamentares rigorosos (reativo).

Na América do Norte e na Europa Ocidental, as “redes inteligentes” também possibilitam organizar o movimento da eletricidade em duas direções, possibilitando a venda do excedente de eletricidade produzida pelas residências (principalmente painéis solares nos telhados das casas).

Na geração, também são usados elementos da “Internet das coisas” - estes são sistemas de gerenciamento de ativos da classe de sistemas automatizados de controle de processos. Eles são instalados em várias combinações em todas as usinas de energia e permitem receber informações remotamente sobre a operação dos principais sistemas.

É claro que uma indústria de energia mais inteligente traria benefícios óbvios tanto para os consumidores e produtores de eletricidade quanto para a economia como um todo.

A União Europeia, por exemplo, pretende alcançar 80% dos consumidores com medidores inteligentes até 2020 (200 milhões de medidores elétricos e 45 milhões de medidores de gás). Nos EUA, cada estado determina, de forma independente, a política para sua implementação, no entanto, o número de “medidores inteligentes” em todo o país já está próximo de 50% do total (em seis estados a participação de “medidores inteligentes” é superior a 80%).

2.4.1.2 Setor de Transportes

No mundo, a Internet das Coisas penetrou muito mais fundo no setor de transportes. Em países como a Rússia, onde o comprimento de vários tipos de vias excede 1,6 milhões de km, e o número de veículos de transporte de carga (rodoviário, ferroviário e outros) é de 7 milhões de unidades, em princípio, é uma tarefa difícil fazer sem sistemas de monitoramento remoto.

A IoT se desenvolveu de forma mais expressiva no setor de automóveis devido à proliferação dos mesmos *smartphones* que os motoristas levam consigo na estrada e cuja participação é próxima de 50% dos dispositivos celulares. Graças a eles, os sistemas de monitoramento de congestionamentos rodoviários foram construídos sobre o Waze, o Google e outros mapas. Os *smartphones* do carro são um ecossistema completo de soluções de *software* (por exemplo, Uber, 99 Pop, etc.).

Essas soluções mudaram completamente o mercado de táxis nas grandes cidades. Tais serviços não estão mais limitados à esfera dos táxis e penetram na esfera da logística, alimentação e lazer: como a Uber Cargo, IFood e Yellow, que surgiram com base no uso da IoT.

Sistemas mais profissionais de monitoramento inteligente de veículos estão sendo introduzidos graças à instalação de sistemas remotos de monitoramento de movimento baseados em sensores GLONASS/GPS em carros e sistemas de controle para consumo de combustível. Tais dispositivos podem reduzir significativamente os custos e controlar o uso direcionado de transporte, analisar e otimizar as rotas de tráfego, o que é muito importante para a logística. Provavelmente, nenhuma empresa de transporte de médio ou grande porte pode dispensar tais dispositivos. Ao mesmo tempo, eles são usados não apenas para o transporte externo, mas também dentro das empresas: algumas empresas de mineração e produção de aço, por exemplo Severstal, rastreia o peso e o movimento das mercadorias e as rotas das carregadeiras em suas plantas. Existem também muitos produtos de *software* no mercado que permitem analisar os dados recebidos e otimizar custos e processos.

2.4.1.3 Produção

Primeiramente, o uso de sensores controlando a operação do equipamento com acesso à rede permite que o fabricante monitore remotamente seu trabalho, realize a manutenção de rotina, preveja acidentes e realize manutenções preventivas ou prepare os detalhes necessários com antecedência para substituição, etc.

Em segundo lugar, o conhecimento do carregamento real e planejado do equipamento de produção conectado à rede permite que a organização de uma rede automática de pedidos

entre diferentes indústrias em uma longa cadeia de fornecedores de materiais para consumidores de produtos finais. Isso é alcançado conectando todos os *sites* de produção a uma única plataforma de *software* e seus participantes podem ser empresas diferentes.

Tal modelo otimiza consideravelmente os custos de transação em cadeias cooperativas que adquirem a capacidade de auto otimização. Em outras palavras, o uso do conceito da Internet das Coisas torna possível otimizar ao máximo os laços de cooperação para toda a cadeia de empresas participantes, a fim de alcançar o resultado de melhor custo-efetivo para o usuário final.

Assim, nos casos mais avançados, pode não ser apenas uma nova qualidade de suporte técnico para equipamentos (usando ferramentas avançadas de telemetria), mas também um modelo de negócios diferente de sua operação, quando o equipamento não é transferido para a propriedade do cliente, mas é pago pelo uso de suas funções.

2.5 IIoT para o Monitoramento de Ativos

2.5.1 O desafio da manutenção

Indústrias intensivas em ativos enfrentam uma série de desafios quando se trata de garantir que plantas e equipamentos de missão crítica operem com eficiência e tempo de operação máximos, e os compromissos de atendimento ao cliente sejam atendidos, pois até mesmo a menor interrupção pode levar a penalidades, ou ainda, à escolha de outro fornecedor por parte do cliente. As empresas precisam entender como seus produtos e ativos estão executando suas funções para que eles possam otimizar seu uso e antecipar melhor os problemas e fracassos.

Entretanto, a manutenção reativa (ou corretiva) não é a solução transformacional que as empresas exigem no ambiente competitivo. Os custos associados à manutenção reativa são proibitivos e, no mundo cada vez mais competitivo, grandes indisponibilidades podem causar o descumprimento de prazos e compromissos com clientes, fazendo com que estes busquem novos fornecedores, o que pode ser prejudicial para o negócio.

O monitoramento remoto e a manutenção preditiva fornecem uma solução para esses desafios e é um dos principais recursos habilitados pela IIoT. O mercado oferece uma muitos dispositivos potentes e conectados a baixo custo, que podem ser usados para fornecer dados em tempo real sobre o desempenho dos ativos. Se integrado com os sistemas corporativos, associados a modelos de atendimento ao cliente, esses dados podem aumentar seu valor para os

negócios. Quando se trata de monitoramento e manutenção remotos, por exemplo, a integração de dados da IIoT permite redução de custos, redução do tempo de reparo e até modelos de negócio completamente novos – ideal para enfrentar os desafios competitivos da era digital.

O monitoramento remoto permite que as empresas atualizem e controlem produtos no campo.

2.5.2 Manutenção Proativa (Preditiva)

A fim de garantir o alto desempenho dos equipamentos industriais, uma estratégia proativa de manutenção e reparo vem se tornando cada vez mais popular.

A essência da estratégia proativa de manutenção é realizar as ações de reparo necessárias visando reduzir o *downtime* (tempo de indisponibilidade) e MTTR (*Mean Time To Repair*) e aumentar o MTBF (*Mean Time Between Failures*) dos ativos, os quais são identificados com base em informações sobre as condições (temperatura, vibração, pressão, alinhamento, etc.) dos equipamentos.

Vários fatores que acompanham a operação (*design* e cargas não planejados, o impacto de fatores ambientais e equipamentos próximos, condições de operação, manutenção e reparo, entre outros), de certa forma levam ao desenvolvimento de vários tipos de falhas. O efeito determinante de uma combinação de fatores provoca um desenvolvimento acelerado de uma ou mais falhas, que se tornam determinantes em relação à operacionalidade da máquina. Escolhendo os efeitos de reparo de forma a reduzir a influência dos fatores determinantes, é possível reduzir a taxa de desenvolvimento de avarias, mantendo a máquina em condições de funcionamento (BOBROVITSKY, 2011).

A estratégia proativa de manutenção e reparo é baseada em uma avaliação da condição do equipamento, que pode ser realizada usando os seguintes métodos:

- Monitoramento de parâmetros;
- Inspeção visual;
- Controle de temperatura;
- Diagnósticos acústicos e de vibração;
- Levantamento usando testes não destrutivos (magnético, elétrico, corrente parasita, onda de rádio, térmica, óptica, radiação, ultrassom, teste penetrante).

A utilização destes métodos permite:

- Aumentar a vida útil do equipamento, eliminando as falhas na fase inicial de sua ocorrência;
- Reduzir o custo de manutenção, devido a mudanças nas abordagens de manutenção e reparo em favor do aumento de reparos de baixo custo em vez de operações de reparo dispendiosas (substituição, restauração);
- Escolher os intervalos "ótimos" para as manutenções, baseado no histórico de falhas ou por meio de diagnósticos;
- Aumentar a disponibilidade dos equipamentos, o que permite aumentar os volumes de produção e reduzir os custos de produção.

Entretanto, muitas vezes não é possível realizar a coleta de dados (medições) de forma manual por motivos de segurança (Figura 3a), pois isso poderia colocar os inspetores de manutenção em risco, ou simplesmente por não ser possível acessar os equipamentos a serem medidos (Figura 3b).

A figura 3a mostra um transportador de correia que possui movimento transversal oscilatório, crítico para o processo. Falhas neste equipamento causam parada imediata da planta. Portanto, o monitoramento de vibração e temperatura do motor elétrico foi uma das estratégias de manutenção adotadas para identificar tendências de falha e evitar paradas não programadas deste equipamento. Entretanto, devido ao movimento transversal oscilatório do carrinho onde o moto redutor esta montado, a coleta manual de dados (vibração e temperatura) colocaria em risco os inspetores de manutenção. Neste caso, foram instalados sensores de vibração e temperatura sem fio que fazem a coleta de dados e os enviam através de uma rede de automação para um sistema especialista, que fará o tratamento.

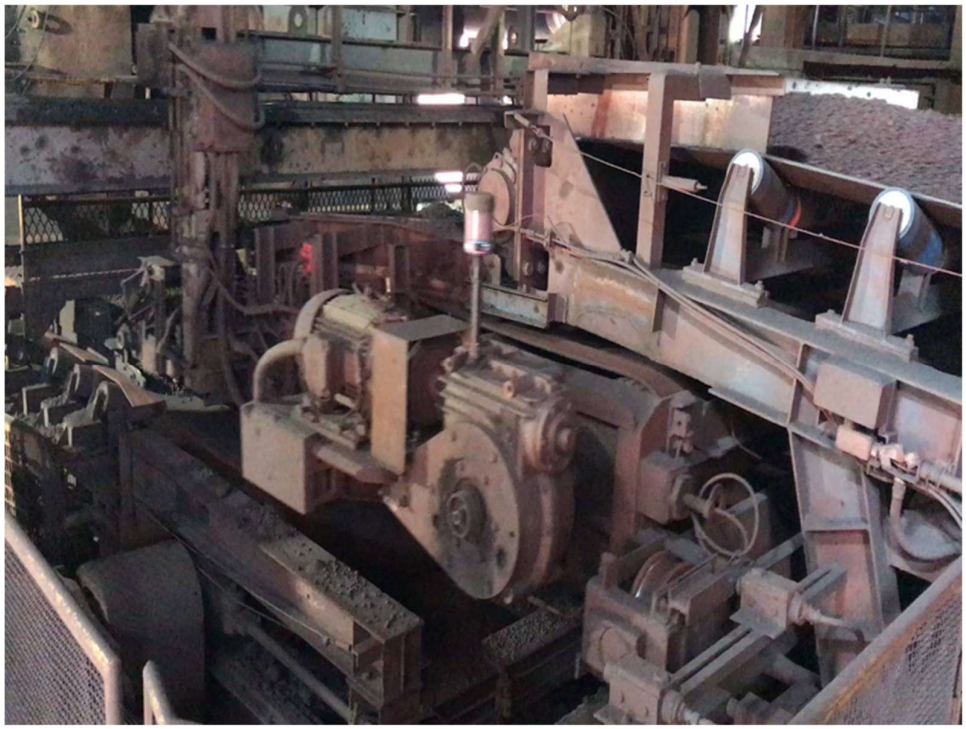

Figura 3a – motor elétrico de correia transportadora oscilatória.

Fonte: autor

A figura 3b mostra o topo de uma torre de resfriamento, responsável pela refrigeração de equipamentos críticos para o processo. Portanto, falhas neste equipamento também causam parada imediata da planta. Semelhantemente ao equipamento mostrado na figura3a, o monitoramento de vibração e temperatura do motor elétrico foi uma das estratégias de manutenção adotadas para identificar tendências de falha e evitar paradas não programadas deste equipamento. Entretanto, não há acesso de pessoas ao motor elétrico devido a altura do equipamento, impossibilitando a coleta manual de dados (vibração e temperatura). Neste caso, também foram instalados sensores de vibração e temperatura sem fio que fazem a coleta de dados e os enviam através de uma rede de automação para um sistema especialista, que fará o tratamento.

Figura 3b – motor elétrico de ventilador da torre de resfriamento.

Fonte: autor

2.5.3 Aplicação de IIoT na Manutenção Proativa

A aplicação de IIoT, assim como mostrado nas Figuras 3a e 3b, ao invés das tecnologias tradicionais de automação é justificada pelo baixo custo dos dispositivos, escalabilidade, interoperabilidade e principalmente pela ausência de legado, pois as tecnologias de IIoT são comumente intercomunicáveis. Dessa forma, a utilização de tecnologias de IIoT para o monitoramento remoto da utilização, desempenho e manutenção de equipamentos permite que as empresas monitorem o *status* e atualizem equipamentos "no campo" em tempo real.

O monitoramento remoto, juntamente com a análise preditiva, pode reduzir as interrupções e melhorar o tempo de atividade.

Conectar dispositivos dessa forma permite o monitoramento quase em tempo real do equipamento, o que significa que os engenheiros e as equipes de manutenção podem identificar remotamente falhas mais rapidamente e reduzir o tempo de reparo ou eliminá-las completamente.

Os dados adquiridos dos sensores, por meio de monitoramento remoto, podem ser aproveitados para a geração de modelos para fornecer previsões sobre falhas iminentes de ativos e identificar as causas raízes dos problemas.

Os "equipamentos inteligentes" conectados podem ser atualizados (adicionar novos recursos) sem a participação direta de especialistas ou alterar os parâmetros operacionais para obter um melhor desempenho.

Além disso, o monitoramento remoto utilizando IIoT, juntamente com a previsão analítica reduz o número de falhas e aumenta os períodos de operação sem problemas, fazendo com que as empresas, cada vez mais, deixem as abordagens de manutenção baseadas em intervalos de tempo (Preventiva) e façam a transição para serviços de manutenção proativos (Preditiva), baseados na condição do equipamento, com detecção precoce de um problema.

O processamento e análise de dados coletados no âmbito da IIoT usando modernas técnicas de análise preditiva permitirá:

- Manter equipamentos baseados em controle de sua condição (a chamada manutenção Preditiva);
- Garantir confiabilidade e eficiência de sistemas e equipamentos complexos (aviões, navios, foguetes, centrais nucleares, etc.);
- Conduzir o controle automático de qualidade dos produtos, etc.

Muitas vezes, ao escolher uma estratégia de manutenção, é necessário otimizar vários indicadores de metas de uma só vez. Por exemplo, na aviação é necessário, por um lado, garantir a segurança e confiabilidade do transporte (segurança e confiabilidade), por outro, aumentar a disponibilidade da aeronave (disponibilidade), reduzir custos de manutenção (custos de manutenção) e minimizar o número de quebras em operação (interrupções operacionais).

O esquema de alto nível do sistema de Manutenção Preditiva é mostrado na Figura 3.

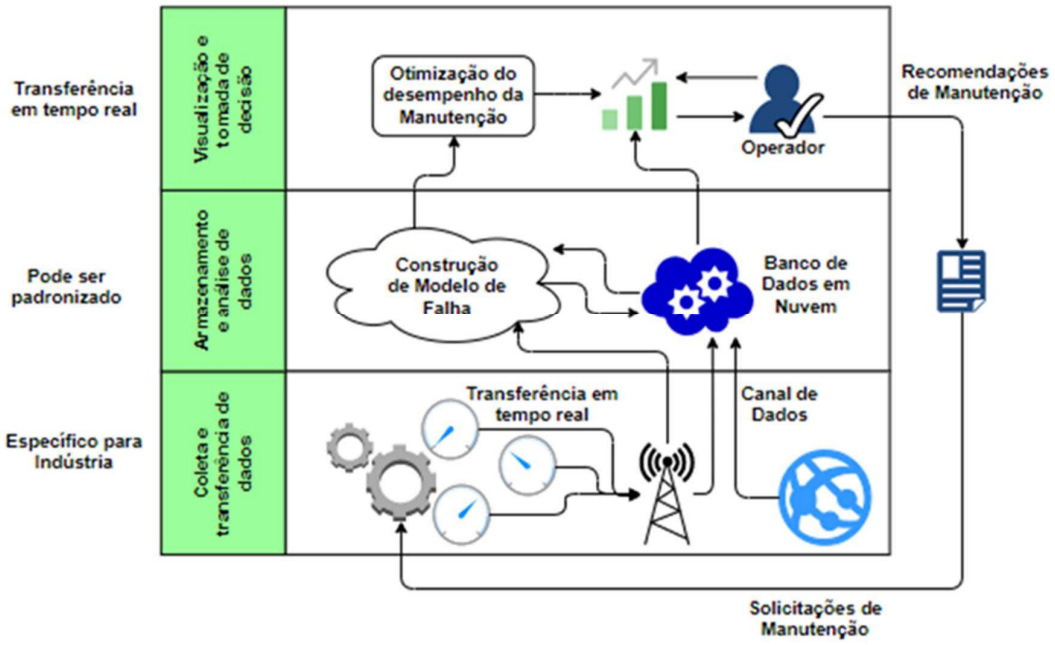

Figura 4 – Manutenção preditiva dividida em níveis.

Fonte: Autor.

No nível inferior, os dados são coletados e transmitidos com sistemas de engenharia. O *hardware* e o *software* adequados são específicos para o setor em questão, pois exigem a interface com equipamentos (máquinas, turbinas, etc.).

No próximo nível, os dados são armazenados e pré-processados e convertidos para um formato uniforme, construindo modelos preditivos. Nesse caso, o *software* apropriado e um conjunto de métodos de mineração de dados necessários para resolver problemas dependerão pouco das especificidades da aplicação industrial, uma vez que os requisitos para implementar os algoritmos correspondentes de análise preditiva nesse caso podem ser amplamente unificados.

O terceiro nível do sistema Manutenção Preditiva fornece a visualização dos resultados da análise preditiva e aumenta a eficiência da tomada de decisões pelo operador do sistema. Nesse caso, a implementação do *software* pode depender muito das especificidades do sistema de gerenciamento do ciclo de vida do equipamento.

2.5.4 Características das redes IIoT *versus* Monitoramento de Ativos

Para a implementação de tecnologias de IIoT em redes de sensores para o monitoramento de ativos industriais, algumas características são mais relevantes do que outras. Neste contexto, de forma a garantir a máxima disponibilidade das redes de monitoramento, limites (mínimo/máximo) de *throughput, overhead* e latência devem ser definidos durante a escolha da tecnologia a ser aplicada. Pois baixos *throughputs* e elevadas latência e *overhead* podem causar sobrecarga e comprometer o funcionamento ou até mesmo provocar indisponibilidades.

Outro aspecto a ser observado é a possibilidade para ampliações e escalabilidade das redes de sensores para o monitoramento de ativos. Pois o número de ativos críticos a serem monitorados varia também de acordo com expansões das plantas industriais e necessidades das unidades de negócio. Portanto, é muito importante para a escolha da tecnologia a ser aplicada o tipo de topologia suportado e as restrições para futuras ampliações.

A criptografia e segurança dos dados fornecidas pelas tecnologias de IIoT também devem ser criteriosamente analisadas antes de sua implementação no monitoramento de ativos, pois ataques externos podem causar indisponibilidades, roubo de dados de comportamento dos ativos ou até mesmo acesso a redes de controle, caso estas e as redes de monitoramento estejam conectadas.

E, finalmente, o consumo de energia destas tecnologias de IIoT também deve ser observado, principalmente quando as redes de monitoramento de ativos são implantadas em grandes áreas externas (pátios de estocagem, sistemas remotos de captação de água, etc.) ou quando os sensores são instalados em partes de difícil acesso dos equipamentos.

2.6 Principais Desafios e Oportunidades

A aplicação de redes de sensores e protocolos de comunicação de IoT para o monitoramento de ativos na indústria requer uma série de especificações mínimas, com o objetivo de garantir a confiabilidade dos dados que estão sendo obtidos, de forma que a tomada de decisão seja assertiva.

Esses requisitos podem variar, dependendo da quantidade de sensores, da área de cobertura, da agressividade do ambiente, do nível de segurança exigido, etc. Algumas tecnologias possuem limitação de quantidade de nós, por exemplo, somente é possível conectar 255 dispositivos a um mesmo roteador ou *access point* de Wi-Fi (*Wireless Fidelity*). A área de cobertura também pode ser um limitador para a utilização de algumas soluções. Por exemplo, em uma mina a céu aberto, os equipamentos muitas vezes ficam a quilômetros de distância uns

dos outros ou de salas de controle. Portanto, tecnologias de curto alcance como Bluetooth, que possui alcance máximo de algumas dezenas de metros, tornam-se inviáveis para essas aplicações.

Como existem muitas tecnologias sem fio nas redes de IoT, cada uma tendo certas vantagens e desvantagens, é muito difícil concluir qual delas é a melhor. Portanto, a pergunta que deve ser feita é: "qual tecnologia é a melhor para a minha aplicação?". No intuito de viabilizar uma boa resposta a essa pergunta, este trabalho apresenta uma base comparativa das tecnologias LoRaWAN, Sigfox, 6LoWPAN e ZigBee para aplicação em monitoramento de ativos na indústria. Para esta comparação, foram utilizados os critérios mais relevantes para a aplicação de redes de sensores para o monitoramento de ativos: *throughput*, latência, topologia, *overhead*, segurança e consumo de energia. Entretanto, trabalhos futuros podem utilizar critérios diferentes para comparar esses protocolos de comunicação. Tais critérios incluem potência, alcance, tipo de criptografia, espalhamento, tipo de modulação, coexistência com outros protocolos e dispositivos.

3. Fundamentos Teóricos

3.1 LoRaWAN

A especificação LoRaWAN é um protocolo de rede LPWA (*Low Power, Wide Area*) projetado para conectar sem fio "coisas" operadas por bateria à Internet em redes regionais, nacionais ou globais, e tem como alvo os principais requisitos da Internet das Coisas (IoT), como serviços de comunicação bidirecional, segurança *end-to-end*, mobilidade e localização (LORA-ALLIANCE, 2019).

Em janeiro de 2015, a organização sem fins lucrativos LoRa Alliance foi criada para adotar e promover o protocolo LoRaWAN como um padrão único para redes globais de baixa potência (LPWAN). Participantes de diferentes níveis da LoRa Alliance são fabricantes de *software*, microeletrônica, operadores de comunicação, etc. Por exemplo IBM, Semtech, Cisco, Inmarsat, Swisscom, dentre outros.

Se a modulação LoRa for uma camada física (camada 1 do modelo OSI), então LoRaWAN é um protocolo de camada de *link* MAC (camada 2 do modelo OSI) para redes com muitos nós com um grande intervalo e baixo consumo de energia. A rede LoRaWAN possui uma arquitetura simples tipo "estrela" sem repetidores e *links* de malha. Os nós da rede são caracterizados por baixo consumo de energia (até 10 anos de operação de baterias AA convencionais), baixas taxas de troca de dados, grande alcance de comunicação (15 km em áreas rurais e 5 km em áreas urbanas densas) e baixo custo de equipamentos terminais.

A especificação define os parâmetros e o protocolo (LoRaWAN) da camada física do dispositivo para a infraestrutura (LoRa®) e, portanto, fornece interoperabilidade contínua entre os fabricantes, conforme demonstrado pelo programa de certificação de dispositivos.

O protocolo LoRaWAN é otimizado para terminais alimentados por bateria e inclui várias classes de nós, fornecendo uma compensação entre a velocidade de entrega de informações e o tempo de operação do dispositivo ao usar a energia da bateria (baterias). O protocolo fornece comunicação bidirecional completa e a arquitetura, usando métodos especiais de criptografia, garante a confiabilidade e a segurança geral de todo o sistema. A arquitetura LoRaWAN foi projetada com vistas à possibilidade de trabalho ativo com dispositivos finais móveis, que é uma das áreas de crescimento mais rápido da Internet das Coisas.

Em uma rede LoRaWAN típica, os *gateways* transmitem dados criptografados recebidos de dispositivos finais (*End Nodes*) para o servidor de rede central do provedor (*Network Server*)

e depois para o servidor de aplicativos (*App Server*) do provedor de serviços do qual os dados são enviados ao usuário final.

Em redes LoRaWAN, em contraste, por exemplo, com a Ethernet, os *gateways* também são chamados de *hubs*. Os dispositivos finais são chamados nós finais (*End Nodes*) ou simplesmente nós. A pilha de rede do LoRaWAN às vezes também é chamada de LoRaMAC, para enfatizar que ele funciona no segundo nível do modelo de camada OSI.

A arquitetura de rede LoRaWAN é implantada em uma topologia de estrela em que os *gateways* transmitem mensagens entre os dispositivos finais e um servidor de rede central. Os *gateways* são conectados ao servidor de rede por meio de conexões IP padrão e atuam como uma ponte transparente, simplesmente convertendo pacotes RF (Rádio Frequência) em pacotes IP e vice-versa. A comunicação sem fio aproveita as características de longo alcance da camada física LoRa®, permitindo um *link* de um único salto entre o dispositivo final e um ou vários *gateways*. Todos os modos são capazes de comunicação bidirecional, e há suporte para grupos de endereçamento *multicast* para fazer uso eficiente do espectro durante tarefas como atualizações de *Firmware Over-The-Air* (FOTA) ou outras mensagens de distribuição em massa (LORA-ALLIANCE, 2019).

Embora a especificação defina a implementação técnica, ela não define nenhum modelo comercial ou tipo de implantação (pública, compartilhada, privada, empresarial) e oferece ao setor a liberdade de inovar e diferenciar como ela é usada (LORA-ALLIANCE, 2019).

Características do LoRaWAN:

- Longo alcance – vários quilômetros;
- Baixa potência – pode durar anos em uma bateria;
- Baixo custo – menos de 20 € CAPEX por nó, quase sem OPEX;
- Largura de banda baixa – entre 250bit/s e 11kbit/s na Europa usando a modulação LoRa;
- Seguro – criptografia de ponta a ponta de 128 bits

Entretanto, o LoRaWAN não é adequado para as seguintes aplicações:

- Dados em tempo real – é possível enviar apenas pacotes pequenos a cada dois minutos;
- Ligações/áudio;
- Envio de fotos ou vídeos.

O *payload* (dado útil) deve ser o menor possível. Isso significa que não é recomendado o envio de textos JSON ou simples (ASCII), é necessário codificar os dados como dados binários.

O intervalo entre as mensagens deve estar no intervalo de vários minutos, portanto, a taxa de dados deve ser a mais rápida possível para minimizar o tempo de transmissão.

3.1.1 Arquitetura de redes LoRaWAN

Uma típica rede LoRaWAN consiste nos seguintes elementos: nós finais (*End Nodes*), *gateways* (ou *Hubs*), servidor de rede (*Network Server*) e servidor de aplicação (*Application Server*) (Figura 5).

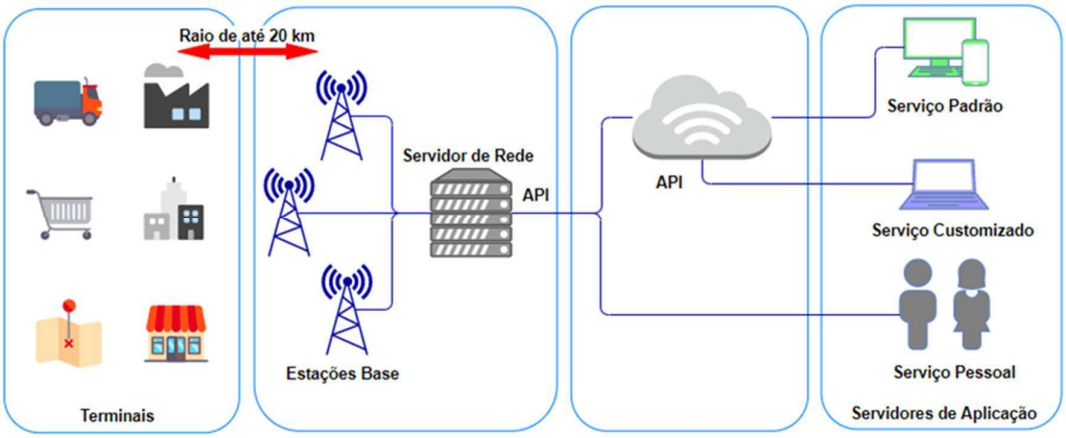

Figura 5 – Arquitetura de rede LoRaWAN.

Fonte: Autor.

3.1.1.1 *End Nodes*

End nodes (ou nós finais) em uma rede LoRaWAN podem ser sensores, atuadores e módulos de rádio IoT instalados no lado do usuário, projetados para implementar funções de controle ou medição e contém um conjunto de sensores e elementos de controle necessários. Podem trabalhar em dois modos:

- Ponto-a-ponto (do inglês *peer-to-peer* P2P) – quando a troca ocorre entre o dispositivo final e o *gateway* ou apenas entre dois nós sem usar *hubs*;
- Modo híbrido – quando um dos nós está conectado, por um lado, a outros nós através de um canal de rádio e por outro há uma conexão de rede com fio via

TCP/IP e atua como um *gateway* (usando *software packet-forwarder*). Um *mini-gateway* de um único canal pode servir de uma a várias dezenas de terminais, que competirão entre si por intervalos de tempo livres do *mini-gateway* para receber e transmitir dados.

O padrão LoRaWAN define três classes de dispositivos para resolver vários problemas e aplicações diferentes.

Classe A – dispositivos finais bidirecionais com a menor potência:

Eles são usados quando o consumo mínimo de energia é necessário quando a transmissão de dados para o servidor prevalece. O iniciador da sessão de comunicação é o nó final, enviando um pacote com os dados necessários e, em seguida, seleciona duas janelas durante as quais aguarda os dados do servidor. Então a transferência de dados do servidor só é possível após entrar em contato com o dispositivo final.

A classe A deve ser suportada por todos os dispositivos finais LoRaWAN por padrão. Uma transferência é sempre iniciada pelo dispositivo final e é completamente assíncrona. Cada transmissão de ligação ascendente pode ser enviada a qualquer momento e é seguida por duas janelas curtas de *downlink*, que permitem a comunicação bidirecional ou comandos de controle de rede, se necessário. Este é um protocolo do tipo ALOHA – protocolo de acesso múltiplo da subcamada MAC. O Protocolo ALOHA permite que um *host* utilize o meio de transmissão sempre que tiver necessidade de enviar um *frame* pela rede. Uma vez que o meio é compartilhado podem ocorrer colisões e o *frame* é perdido

O dispositivo final pode entrar no modo de baixa energia dependendo de suas configurações individuais. Isso torna a classe A a mais eficiente em termos energéticos e a vida útil do sensor é de 5 anos ou mais, enquanto ao mesmo tempo permite a comunicação no *uplink* a qualquer momento.

Como a comunicação de *downlink* deve sempre seguir uma transmissão de *uplink* com a programação definida pelo aplicativo do dispositivo final, a comunicação de *downlink* deve ser armazenada em *buffer* no servidor de rede até o próximo evento de *uplink*.

Classe B – dispositivos finais bidirecionais com latência a jusante definida:

Eles diferem dos dispositivos “Classe A” pela alocação de uma janela de recepção adicional, que o dispositivo abre em um agendamento. Para o agendamento, o dispositivo final

é sincronizado com um sinal especial do *gateway*. Graças a essa janela adicional, o servidor pode iniciar a transferência de dados em um tempo conhecido.

Além das janelas de recepção iniciais da classe A, os dispositivos de classe B são sincronizados com a rede usando "balizas" periódicas e abrem "*slots* para verificação" do *downstream* em uma programação. Isso fornece à rede a capacidade de enviar um *downlink* com um certo atraso, mas às custas de algum consumo adicional de energia no dispositivo final. O atraso é programável por até 128 segundos para diferentes aplicativos, e o consumo de energia adicional é baixo o suficiente para permanecer válido para aplicativos alimentados por bateria.

Classe C – dispositivos finais bidirecionais com a menor latência:

Esses dispositivos têm uma janela de recepção de dados quase contínua e a fecham somente pela duração da transferência de dados, o que permite que eles sejam usados para resolver problemas que exigem a obtenção de uma grande quantidade de dados.

Além da estrutura de classe A no *uplink*, seguida por duas janelas de *downlink*, a classe C reduz adicionalmente o atraso de *downlink* mantendo constantemente a recepção no terminal quando o dispositivo não transmite (*half duplex*). Com base nisso, o servidor de rede pode iniciar uma transmissão de *downlink* a qualquer momento se o receptor do dispositivo final estiver aberto, portanto, não há atraso. Uma desvantagem é o consumo de energia do receptor (até aproximadamente 50 mW) e, portanto, a classe C é adequada para aplicações onde há energia contínua.

A seguir, a Figura 6 ilustra o envio de mensagens de *uplink* para as diferentes classes dos dispositivos LoRaWAN.

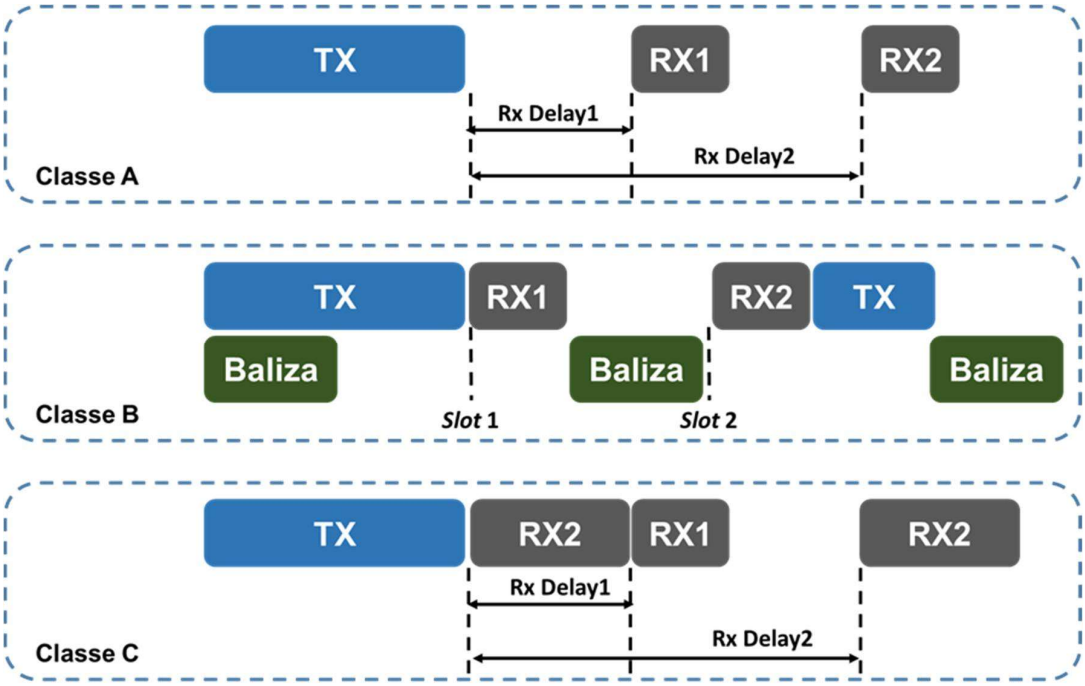

Figura 6 – Classes de dispositivos LoRaWAN.

Fonte: Autor.

3.1.1.2 *Gateways (Hubs)*

Gateway LoRa (ou *Hub*) é um dispositivo que recebe dados de dispositivos finais usando um canal de rádio e os envia para a rede de trânsito Ethernet, Wi-Fi, redes celulares ou quaisquer outros canais. Os dispositivos finais e o *gateway* formam uma topologia de rede em estrela. Normalmente, este dispositivo contém transceptores multicanais para processar sinais em vários canais ao mesmo tempo ou até mesmo vários sinais em um canal. Assim, vários desses dispositivos fornecem cobertura de rede e transferência de dados bidirecional transparente entre nós finais e o servidor.

A comunicação entre os *hubs* e o servidor central da rede LoRaWAN (rede de transporte *backhaul*) é realizada usando tecnologias tradicionais (Ethernet, Wi-Fi, GSM) via TCP/IP.

Se os *gateways* se conectarem ao servidor de rede por meio de conexões IP padrão, os nós finais usarão uma conexão sem fio com um ou mais *gateways*. Todos os nós finais, como regra, são bidirecionais, mas também suportam a operação em um modo que possibilita realizar atualizações de *software* em grupo pelo ar (FOTA – *Firmware Over The Air*) ou transmitir outras mensagens em massa (*Broadcast*), o que reduz o tempo para enviá-las. Dependendo da capacidade de canal desejada e dos locais de instalação, diferentes versões de *gateways* estão disponíveis, elas podem ser instaladas tanto em ambientes internos quanto externas.

Os *end nodes* da rede LoRaWAN podem estar na área de cobertura de um ou vários *gateways*. O *gateway* em redes com alta densidade de dispositivos são *hubs* especiais multicanais que têm a capacidade de receber dados de vários nós simultaneamente. É esse recurso do *gateway* que afeta diretamente a densidade máxima de dispositivos (*end nodes*) na área atendida por um *hub*.

3.1.1.3 *Network Server* (Servidor de Rede)

O servidor de rede (*Network Server*) é projetado para gerenciar a rede: configurando a programação, adaptando a velocidade, armazenando e processando os dados recebidos.

O problema de possíveis colisões durante a transmissão simultânea de dados por vários pontos é resolvido pelo servidor de rede LoRaWAN, que endereça os nós da rede via *gateways*, alocando intervalos de tempo para envio e recebimento individualmente. O endereçamento ocorre em um DevAddr (*Device Address Assigment*) de 32 bits, exclusivo para cada nó.

O servidor central da rede LoRaWAN toma decisões sobre a necessidade de alterar a taxa de transferência de dados por nó, potência do transmissor, escolha do canal de transmissão, seu início e duração ao longo do tempo, controla a carga das baterias do nó final, ou seja, controla completamente toda a rede e controla cada dispositivo separadamente.

Cada pacote de dados enviado do nó final LoRaWAN contém um identificador de aplicativo AppEUI (*Application ID*) exclusivo pertencente à aplicação no servidor do provedor de serviços ao qual se destina e esse identificador é usado pelo servidor de rede LoRaWAN para rotear e processar o pacote no servidor de aplicação (*App Server*).

Na prática, como regra, os serviços do provedor de serviços são fornecidos pelo fabricante do nó final, que suporta o serviço de processamento de dados, no qual os pacotes do servidor de rede LoRaWAN são roteados para trabalhar com esses dados para os usuários finais.

3.1.1.4 *Application Server* (Servidor de Aplicação)

O servidor de aplicação (*Application Server*) é uma plataforma que executa o primeiro nível de criptografia e processa dados recebidos de terminais e enviados para terminais. Além de trabalhar com dados, o servidor de aplicações pode gerenciar terminais a partir do nível da aplicação (por exemplo, transferi-los para outro modo de operação de classe, controlar a transferência de dados adaptativa, *multicast*, etc.) e pode monitorar remotamente a operação dos nós finais e coletar os dados necessários a partir deles.

Durante a fabricação, as seguintes constantes são inseridas nos dispositivos finais:

- DevEUI (*Device Identifier* – um identificador de dispositivo único de 64 bits);
- AppEUI (*Application Identifier* – identificador de aplicação exclusivo de 64 bits);
- AppKey (Chave da Aplicação – uma chave de criptografia exclusiva de 128 bits). Usado no processo de cálculo das chaves de criptografia de sessão AppSKey e NwkSKey.

A ativação dos dispositivos (Figura 7) pode ser realizada através de RF (Rádio Frequência) ou pelo operador. Durante o processo de ativação, os seguintes dados são gerados:

- DevAddr (Endereço do Dispositivo Final – o endereço local do dispositivo em uma rede particular de 32 bits). Consiste em dois campos: NetID e NwkAddr. Quanto menor for o NetID (identificador de rede da operadora atribuído pela LoRa Alliance, o tamanho mínimo é de 6 bits), maior será o campo NwkAddr e mais dispositivos diferentes poderão ser registrados na rede (o máximo de um NetID é de 33,5 milhões de terminais de usuário);
- NwkSKey (Chave de sessão de rede – chave de criptografia de sessão de rede de 128 bits). Ele é usado para criptografar dados entre o terminal e o servidor de rede, bem como para calcular o campo *Message Integrity Code* (MIC) para verificar a integridade dos dados quando eles são transmitidos pelo ar;
- AppSKey (Chave de sessão da aplicação – chave de criptografia de sessão da aplicação de 128 bits). Ele é usado para criptografar dados no nível da aplicação (entre o terminal do assinante e o servidor de aplicação).

As chaves de criptografia de sessão são geradas independentemente no terminal do assinante e na parte da rede com base nos identificadores de rede (NetID) e dispositivos (DevEUI), chave de segurança AppKey e também geram números aleatórios exclusivos para cada sessão (Figura 7). Quando o operador ativa o terminal, é impossível alterar as chaves de criptografia da sessão sem desmontar o dispositivo, e é por isso que não é recomendável usar essa opção de ativação.

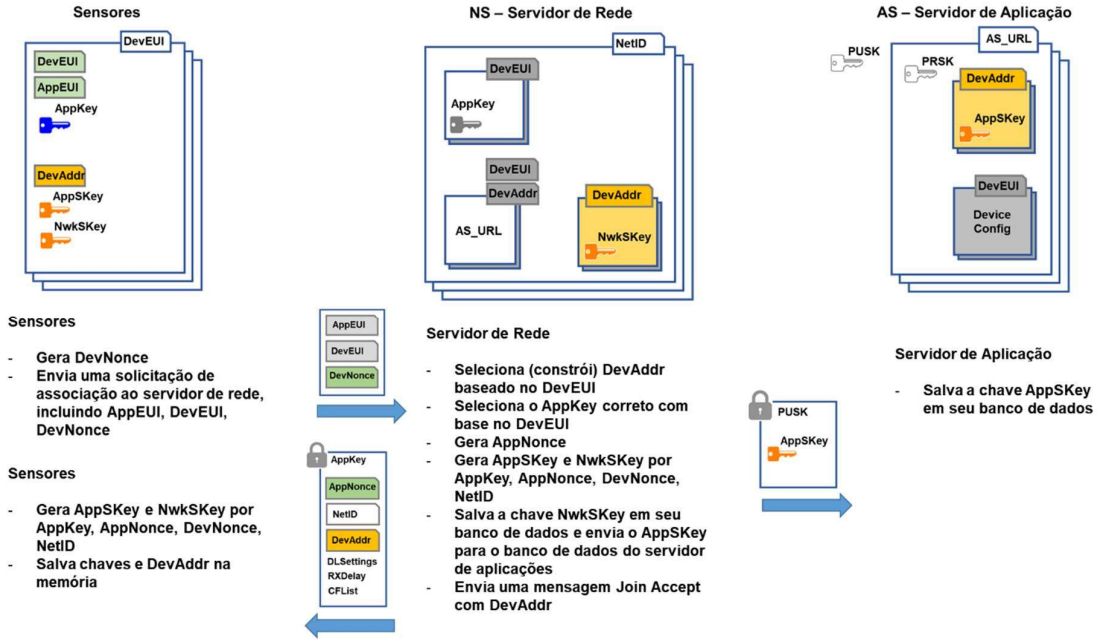

Figura 7 – Procedimento de ativação do terminal do "assinante" (*end node*) via rádio.

Fonte: Autor.

DevAddr, NwkSKey e AppSKey são armazenados na memória do dispositivo, DevAddr e NwkSKey no servidor de rede e AppSKey no servidor de aplicações.

3.1.2 Estrutura dos quadros da camada MAC

Todas as mensagens de *uplink* e *downlink* de LoRa carregam um *payload* da camada física (PHY) começando com um cabeçalho da camada MAC (MHDR – MAC *Header*) de apenas um byte, seguido por um *payload* da camada MAC e terminando com um código de integridade da mensagem (MIC – *Message Integrity Code*) de quatro bytes.

O cabeçalho MAC (MHDR) define a versão do protocolo e o tipo de mensagem, isto é, se é um dado ou um quadro de gerenciamento, se é de *uplink* ou *dowlink*, se deve ser reconhecido, etc. O cabeçalho MAC também pode notificar que esta é uma mensagem específica do fornecedor do dispositivo (*end node*). Em um procedimento de *join* para ativação do nó final, o *payload* da camada MAC pode ser substituído pela solicitação de *join* (*join request*) ou pelas mensagens de aceitação de *join* (*join accept*). A porção inteira do cabeçalho e do *payload* MAC é usada para calcular o valor de MIC com uma chave de sessão de rede (NwkSKey). O valor MIC é usado para impedir a falsificação de mensagens e autenticar o nó final. Por outro lado, as mensagens de dados podem transportar comandos MAC no *payload* do

quadro (FRM *Payload*), que também podem ser transportados no cabeçalho do quadro (FHDR – *Frame Header*), dependendo do valor do FPort (Figura 8). Os comandos MAC destinam-se a configurar o rádio e parâmetros da camada MAC. Um subcampo importante no FHDR é um bit que permite reconhecer a última mensagem de dados confirmados recebida.

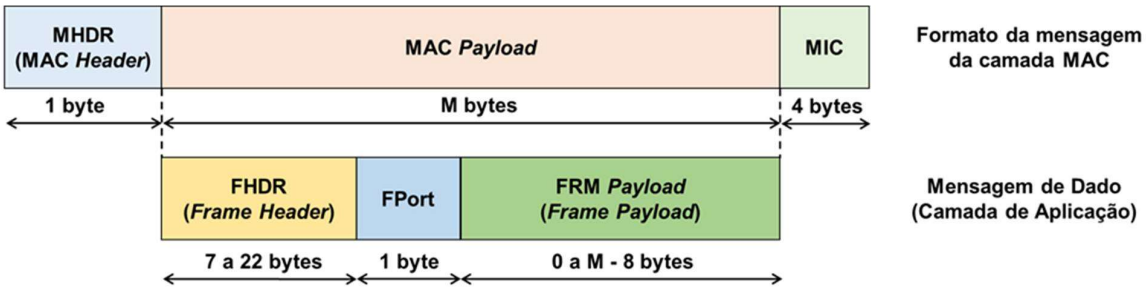

Figura 8 – Formato da mensagem da camada MAC LoRaWAN.

Fonte: Adaptado de LoRaWAN 1.0.3 *Specification*, c2018 e CASALS et al., 2017.

O campo FPort está presente quando o campo de *payload* do quadro (FRM *Payload*) contém dados (ou seja, tem um comprimento diferente de zero) (CASALS et al., 2017). Se o campo de *payload* do quadro (FRM *Payload*) não estiver vazio, o FPort deve estar presente. Se presente, um valor de FPort 0 indica que o FRM *Payload* contém apenas comandos MAC (LORAWAN 1.0.3 SPECIFICATIONS, c2018).

"M" denota o tamanho máximo do campo de *payload* do MAC. O campo do cabeçalho do quadro (FHDR) possui um tamanho de 7 bytes se não contém opções e até 22 bytes quando as opções são usadas (CASALS et al., 2017).

Ao contrário do TCP, o reconhecimento dos quadros de dados LoRaWAN é opcional. Somente no caso de uma confirmação ser necessária, seria utilizado o tipo de mensagem de dados confirmada. A parte receptora confirma esse quadro respondendo com um quadro de dados com o bit ACK definido como 1.

Esse reconhecimento de quadro opcional é ideal para LoRaWAN, já que o tempo de antena dos dispositivos é limitado e uma certa quantidade de perda de pacotes pode não ser um grande problema.

Para validar cada quadro de dados, um MIC (código de integridade da mensagem) é adicionado a cada quadro. É basicamente uma assinatura calculada sobre o quadro, usando a chamada chave de sessão de rede como segredo. Isso significa que mesmo se a mesma carga útil é transmitida várias vezes, cada quadro possui uma assinatura exclusiva (devido ao contador de quadros que é incrementado para cada transmissão).

A seguir é apresentada a estrutura e encapsulamento dos quadros, seus campos e respectivos comprimentos em bytes, desde a camada física (PHY) até a camada de acesso ao meio (MAC) (Figura 9).

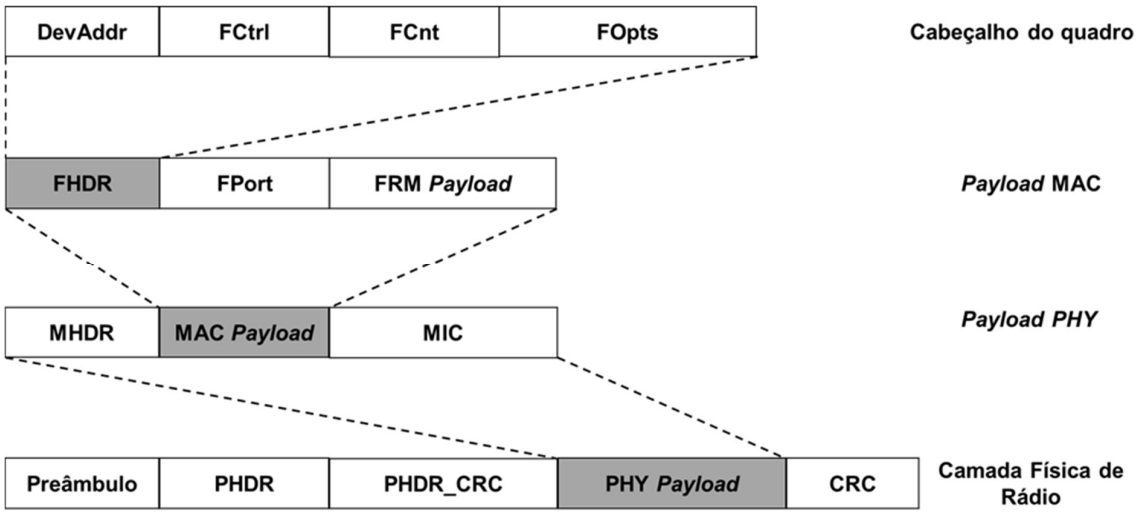

Figura 9 – Encapsulamento da mensagem da camada MAC LoRaWAN.

Fonte: Adaptado de LoRaWAN 1.0.3 Specification, c2018 e ARAS et al., 2017.

A tabela a seguir descreve os campos das camadas MAC e aplicação, conforme ilustrado na Figura 9 anterior.

Tabela 1 - Acrônimos, descrição e comprimento dos campos das mensagens da camada MAC LoRaWAN.

Campo da mensagem MAC	Descrição	Comprimento
MHDR	Cabeçalho MAC	1 byte
MAC Payload	Dado da camada superior (camada de Aplicação)	M bytes
MIC	Código de Integridade da Mensagem	4 bytes
FHDR	Cabeçalho do quadro	até 22 bytes
Fport	Campo de porta (opcional)	1 byte
FRM Payload	Payload do quadro (opcional)	M - 8 bytes
DevAddr	Endereço do dispositivo	4 bytes
FCtrl	Byte de controle do quadro	1 byte
FCnt	Contador do quadro	2 bytes
FOpts	Opções do quadro. Usadas para comandos da camada MAC	até 15 bytes

Fonte: Autor.

3.1.3 *Throughput*

Além do salto de frequência, todos os pacotes de comunicação entre dispositivos finais e *gateways* também incluem um parâmetro *Data Rate*. A seleção DR permite estabelecer um *trade-off* dinâmico entre o intervalo de comunicação e a duração da mensagem. Além disso, graças à tecnologia de espalhamento espectral, a comunicação com diferentes DR não interfere entre si e cria um conjunto de canais virtuais de "código" que aumentam a capacidade do *gateway*. Para maximizar a autonomia dos dispositivos finais e da largura de banda geral da rede, o servidor de rede LoRaWAN controla a configuração de DR e a potência de saída de RF para cada dispositivo final individualmente usando um esquema de taxa de dados adaptável (ADR – *Adaptable Data Rate*).

A taxa de transferência de dados no modo LoRaWAN varia de 0,3 kbit/s a 50 kbit/s (no modo FSK – *Frequency-Shift Keying*).

3.1.4 Segurança

A segurança é uma preocupação principal para qualquer implantação em massa de IoT e a especificação LoRaWAN define duas camadas de criptografia:

- Uma chave de sessão de rede exclusiva de 128 bits (NwkSKey) compartilhada entre o dispositivo final e o servidor de rede;
- Uma chave de sessão de aplicativo de 128 bits (AppSKey) exclusiva compartilhada de ponta a ponta no nível da aplicação.

Os algoritmos AES (*Advanced Encryption Standard*) são usados para fornecer autenticação e integridade de pacotes ao servidor de rede e criptografia de ponta a ponta ao servidor de aplicativos. Ao fornecer esses dois níveis, torna-se possível implementar redes compartilhadas sem que o operador de rede tenha visibilidade dos dados de carga útil dos usuários.

As chaves podem ser ativadas por personalização (ABP – *Activated By Personalisation*) na linha de produção ou durante o comissionamento ou podem ser ativadas pelo ar (OTAA – *Over The Air Activation*) no campo.

A segurança LoRaWAN foi projetada para atender aos critérios gerais de projeto: baixo consumo de energia, baixa complexidade, baixo custo e alta escalabilidade.

A autenticação mútua é estabelecida entre um dispositivo final LoRaWAN e a rede LoRaWAN como parte do procedimento de entrada na rede.

A segurança LoRaWAN implementa ainda mais criptografia de ponta a ponta para mensagens trocadas entre os dispositivos finais e servidores de aplicativos. LoRaWAN é uma das poucas redes IoT com implementação de criptografia de ponta a ponta. Em algumas redes celulares tradicionais, o tráfego é criptografado pela interface aérea, mas é transportado como texto simples na rede principal do operador. Consequentemente, os usuários finais ficam sobrecarregados ao selecionar, implantar e gerenciar uma camada adicional de segurança (geralmente implementada por algum tipo de VPN ou de criptografia, como TLS). Essa abordagem não é adequada em LPWANs onde camadas de segurança exageradas adicionam considerável *overhead*, consumo de energia, complexidade e custo (LORA-ALLIANCE, 2019).

3.2 Sigfox

Sigfox é uma tecnologia de comunicação sem fio de baixa velocidade para dispositivos com baixo consumo de energia, e geram uma pequena quantidade de tráfego por dia, por exemplo, medidores inteligentes, sensores de luz, sistemas de alarme contra incêndio e roubo, sensores de estacionamento inteligentes, etc. Foi inventada e patenteada em 2009 por uma empresa francesa com o mesmo nome. A primeira rede SigFox foi implantada na França em 2012 e, até 2014, já havia cobertura em todo o território francês.

Em 2015, o SigFox planejava entrar no mercado dos EUA, mas enfrentou problemas na faixa de frequência permitida, uma vez que a faixa de frequência usada nos EUA é mais suscetível a interferências do que a faixa europeia. Neste mesmo período, a tecnologia SigFox se espalhou em países da região do leste da Ásia.

A política do SigFox implica o fornecimento de informações abertas sobre o *hardware* necessário para a construção de uma rede (estações base e módulos), enquanto o *software* é privado e vendido para os operadores como um serviço. Atualmente, o SigFox está presente em mais de 60 países.

Sigfox é uma abordagem de sistema celular que permite que dispositivos finais se conectem a estações base equipadas com rádios cognitivos definidos por *software* (AKPAKWU G. A. et al., 2018). Utiliza uma banda de frequências de 868MHz, dividindo o espectro em 400 canais de 100Hz. Sua cobertura é de 30-50 km em áreas rurais e cerca de 3-10 km em ambientes urbanos.

Para transmissão de dados, o SigFox usa uma banda de frequência ultra estreita (UNB) com chaveamento de fase binária (BPSK), e para codificação de dados muda a fase da onda de rádio. Isso permite reduzir o nível de ruído no lado de recepção, portanto, para tornar o dispositivo de recepção mais barato.

- Alcance: 30-50 km (3-10 km em áreas com ruídos e inacessíveis);
- Vida útil dos dispositivos sem substituir a bateria: 20 anos a partir de 2 pilhas AA;
- Frequências utilizadas: 868 MHz (Europa) e 915 MHz (EUA);
- Topologia de rede: estrela (estação base à qual os terminais se conectam).

Um ponto de acesso pode gerenciar cerca de um milhão de dispositivos finais e cada dispositivo final pode enviar cerca de 140 mensagens por dia com uma taxa de dados de 100bps. Cada mensagem deve ter no máximo 12 bytes de tamanho (excluindo o cabeçalho da mensagem e as informações de transmissão).

O número máximo de mensagens originadas nos dispositivos finais (*end points*) também é definido: 4 mensagens por dia com uma carga útil de 8 bytes.

3.2.1 Arquitetura de redes Sigfox

A rede Sigfox possui uma arquitetura horizontal e estreita, composta por duas camadas principais (Figura 10):

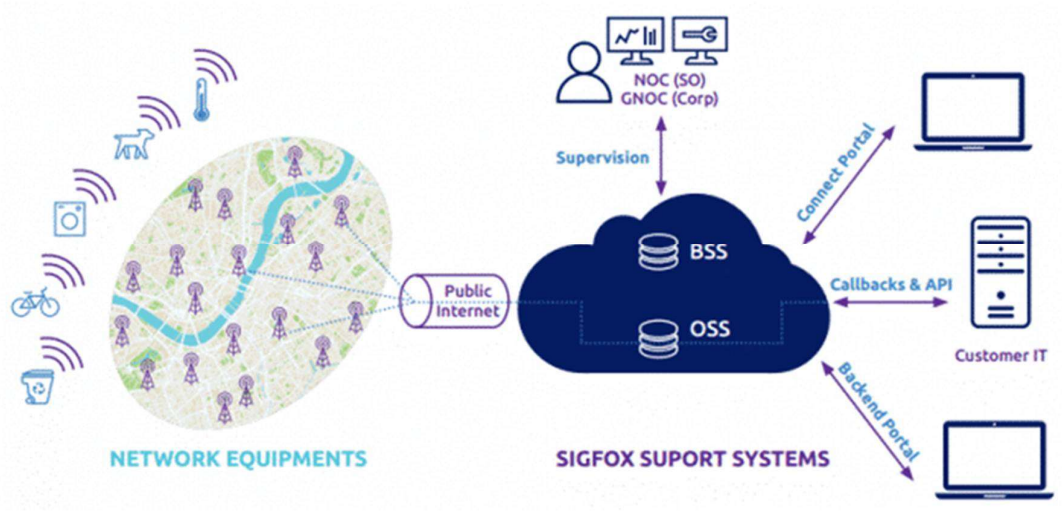

Figura 10 – Arquitetura da rede Sigfox.
Fonte: Sigfox Technical Overview, 2017.

A camada *Network Equipment* consiste essencialmente em estações base responsáveis pelo recebimento das mensagens enviadas pelos dispositivos e envio das mesmas para a camada Sigfox *Support Systems* (SIGFOX TECHNICAL OVERVIEW, 2017).

A camada Sigfox *Support System* constitui a rede principal sendo encarregada de processar as mensagens e enviá-las através de *callbacks* para o sistema do cliente. Essa camada fornece também o ponto de entrada para os diferentes atores do ecossistema (operadores Sigfox, canais Sigfox e clientes finais) para interagir com o sistema através de interfaces de atendimento na *web* ou APIs. Ela também inclui módulos e recursos que são essenciais para garantir a implantação, operação e o monitoramento da rede, como o sistema de suporte empresarial para pedidos e cobranças, e suporte de rádio para garantir o bom funcionamento da rede.

A arquitetura plana da rede Sigfox (Figura 11) é a chave para reduzir os custos de investimentos e operacionais. O *Software Defined Radio* (SDR) Sigfox ajuda a reduzir os custos das estações base e a aumentar sua flexibilidade. Esta flexibilidade de um rádio definido por *software* reduz substancialmente o custo total de operação, garantindo que um único *hardware* seja capaz de operar no mundo inteiro.

Nessa arquitetura a operadora Sigfox (no Brasil, a WND) entrega aos seus parceiros as camadas de rede intermediárias prontas para uso. Cabe ao desenvolvedor a criação da aplicação na nuvem e a escolha ou criação dos dispositivos que pretende usar.

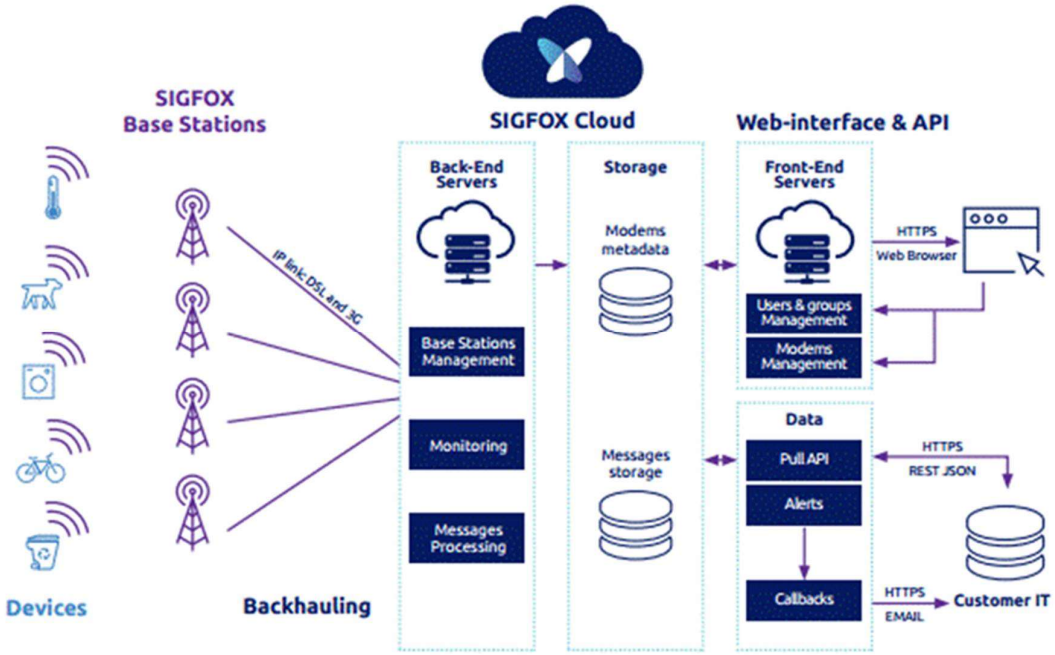

Figura 11 – Arquitetura plana da rede Sigfox.

Fonte: Sigfox Technical Overview, 2017.

3.2.2 Estrutura dos quadros da camada MAC

Para atender as restrições de autonomia de bateria e custo dos objetos conectados, o protocolo Sigfox é otimizado para mensagens pequenas. O tamanho da mensagem vai de 0 a 12 bytes. Embora a princípio isto pareça pouco, com uma mensagem de até 12 bytes é o suficiente para a maioria das aplicações de IoT para objetos simples. Com 132 bytes é possível enviar informações de sensores, eventos, coordenadas de GPS e dados da aplicação.

A tabela a seguir exibe alguns exemplos de mensagens:

Tabela 2 – Exemplos de mensagens Sigfox

Mensagem	Tamanho da Mensagem
Coordenada de GPS	6 bytes
Temperatura	10 bits (de -40°C a +105°C, com 0,1°C de precisão)
Velocidade	1 byte (0 a 255 Km/h)
Status do Objeto	1 bit
Keep Alive	0 bytes

Fonte: Autor.

A tecnologia Sigfox usa modulação de banda estreita (UNB) para enviar e receber mensagens. Para ser mais específico, o Sigfox envia três mensagens usando vários canais e a duração do pacote é 2 ms. A camada física também lida com o processo do mecanismo de enquadramento durante transmissão e recepção. Cada quadro de mensagem inclui bits de preâmbulo, bits de sincronização de quadro, identificador de dispositivo, carga útil (*payload*), códigos de autenticação e também a sequência de verificação de quadros (FCS). A estrutura genérica dos quadros de *uplink* e *dowlink* é apresentada na Figura 12.

Em primeiro lugar, um preâmbulo é usado para fins de sincronização e certas palavras de bit são usadas pelo receptor para decifrar os bits. Essa técnica elimina a necessidade para sinalizadores adicionais e, além disso, leva à redução do tamanho do pacote. Os quadros Sigfox não são criptografados pelo próprio protocolo Sigfox. A criptografia é feita pelo próprio cliente na camada de aplicação. A camada de aplicação também fornece outras funcionalidades necessárias exigidas pelos clientes e as mais importantes são mensagens, serviços da *web* e a função de retorno de chamada.

A seguir são apresentadas as estruturas dos quadros de *uplink* e *downlink* da camada MAC das redes Sigfox (Figura 12), seus respectivos campos e comprimentos em bytes.

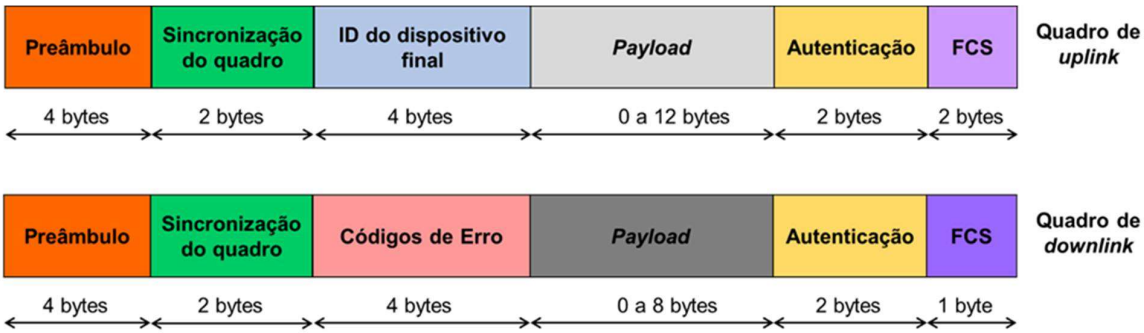

Figura 12 – Estrutura dos quadros de *uplink* e *downlink* da camada MAC Sigfox.

Fonte: Autor.

O campo FCS (*Frame Check Sequence*) é muito semelhante ao campo MIC (*Message Integrity Code*) dos quadros da camada MAC das redes LoRaWAN, ambos utilizados para a detecção de erros no envio de pacotes.

3.2.3 *Throughput*

O protocolo Sigfox é baseado principalmente no protocolo LTN (*Low Throughput Network*). A mensagem tem 12 bytes e inclui um número de sequência para fins de segurança.

Ao empregar a banda ultra-estreita, a Sigfox utiliza a largura de banda de frequência de maneira eficiente e apresenta níveis de ruído muito baixos, levando a um consumo de energia muito baixo, alta sensibilidade ao receptor e *design* de antena de baixo custo à custa da taxa de transferência máxima de apenas 100 bps. Inicialmente, a Sigfox suportava apenas a comunicação de *uplink*, mas posteriormente desenvolveu a tecnologia bidirecional com uma assimetria de *link* significativa. A comunicação de *link* direto, ou seja, os dados das estações base para os dispositivos finais só podem ocorrer após uma comunicação de *uplink*.

O número de mensagens através de *uplink* é limitado a 140 mensagens por dia. O comprimento máximo da carga útil (*payload*) para cada mensagem de *uplink* é 12 bytes. No entanto, o número de mensagens no *link* direto é limitado a quatro mensagens por dia, o que significa que o reconhecimento de todas as mensagens de *uplink* não é suportado. O comprimento máximo da carga útil para cada mensagem de *downlink* é de oito bytes (MEKKI K. et al., 2019).

3.2.4 Segurança

A segurança é a maior preocupação para os dispositivos IoT baseados em Sigfox. Os dispositivos de IoT industriais precisam ser seguros, caso contrário, *hackers* podem invadir bancos de dados e arquivos sigilosos para uso ilegal. Portanto, os dispositivos IoT precisam estar atualizados em questões de segurança. Um sistema IoT seguro deve ter quatro elementos principais: segurança, privacidade, confiabilidade e confiança.

Em (CENTENARO M. et al., 2016 e POURSAFAR N. et al., 2017), autores apontam o fato de que os dispositivos Sigfox têm um baixo nível de segurança e apresentam maiores riscos de segurança em potencial. Atualmente, no entanto, os dispositivos Sigfox são mais seguros com a criptografia de ponta a ponta do dispositivo. Além disso, os dispositivos Sigfox não são operados usando o protocolo da Internet (TCP / IP) e cada dispositivo é equipado com o ID do dispositivo exclusivo. Além disso, ele não está conectado a nenhuma rede específica ou estação base. A rede Sigfox é construída de forma que possa se proteger de ameaças de ataques de negação de serviço (DDoS – *Distributed Denial of Service*) ou clonagem massiva de dispositivos. Os dispositivos Sigfox transmitem ou recebem dados da Internet. Primeiro, um dispositivo IoT transmite uma mensagem no ar, essas mensagens são recebidas por várias

estações base. Essas mensagens são entregues na rede principal. Por padrão, os dispositivos Sigfox são projetados com um *firewall* muito rigoroso. Portanto, ele nunca tem a capacidade de enviar dados para pessoas não autorizadas via Internet, como mostra a Figura 13.

Figura 13 – Esquemas de segurança dos dispositivos Sigfox.
Fonte: Sigfox Technical Overview, 2017.

A Sigfox construiu a segurança de seus dispositivos das seguintes maneiras (FUJDIAK R. et al., 2018):

- Cada dispositivo Sigfox é equipado com chave de autenticação exclusiva. A autenticação de dispositivo é feita com o ID do dispositivo e criptografia AES (*Advanced Encryption Standard*) método sem transmissão OTA (*key over the air*);
- Chave estática do fabricante, exclusiva para todos os dispositivos e usada durante o registro do dispositivo;
- Um ID exclusivo usado para a autenticação de cada dispositivo;
- Um código de integridade da mensagem (MIC) que garante a sequência da mensagem, normalmente tem de 2 a 5 bytes;
- Finalmente, a criptografia AES-128 na camada de aplicação.

A criptografia, realizada na camada de aplicação, é de responsabilidade do cliente projetar um modelo de criptografia para sua carga útil.

Além disso, as estações base também armazenam credenciais para se comunicar com a rede principal da Sigfox.

O *back-end* da Sigfox também armazena chaves de autenticação de dispositivos finais para trocar dados com segurança. As mensagens Sigfox contêm um número de sequência que é sincronizado com a Nuvem Sigfox com o objetivo de resistência contra falsificação (HEMJAL A., 2019).

3.3 ZigBee

O padrão IEEE 802.15.4 é o mais novo da série sem fio (adotado em outubro de 2003). Em sua base, a ZigBee Alliance (www.zigbee.org) desenvolveu uma especificação de protocolos de rede e camada de aplicação, que foi anunciada em dezembro de 2004 sob o nome "ZigBee". A ZigBee Alliance inclui mais de 180 empresas trabalhando juntas para promover padrões, uma pilha de protocolos e perfis de aplicações para os setores de consumo e industrial da economia. As aplicações concentram-se, em especial, na automação predial, no monitoramento industrial e sensores.

A principal área de aplicação do ZigBee / IEEE 802.15.4 é a transferência de informações de partes móveis e rotativas de mecanismos (transportadores, robôs, etc.), controle industrial e sistemas de monitoramento, redes de sensores sem fio, rastreamento de rotas de movimento e localização de ativos e equipamentos e agricultura "inteligente".

Ao contrário de outras tecnologias sem fio, onde a tarefa é fornecer transmissão de alta velocidade, maior alcance ou alta qualidade de serviço, ZigBee / IEEE 802.15.4 foi originalmente criado de acordo com os critérios de curto alcance, baixo preço, baixo consumo de energia, baixa velocidade de transmissão e tamanho pequeno. Essas propriedades se encaixam perfeitamente nos requisitos da maioria dos sensores industriais. Portanto, ZigBee é frequentemente identificado com a rede sem fio industrial WSN (Rede de Sensores Sem Fio). Os dispositivos ZigBee são usados em aplicações nos quais o Bluetooth é muito caro e não requer uma alta taxa de transferência.

O ZigBee, como o Bluetooth, usa a banda 2.4 GHz (amplamente utilizada no Brasil), dividida em 16 canais. A norma também prevê o uso de frequências de 868 MHz na Europa e 915 MHz nos Estados Unidos. A taxa de transferência máxima é de 250 Kbps na banda de 2,4 GHz.

Apesar do fato de que a estrutura básica do padrão IEEE 802.15.4 é construída na suposição de que a comunicação típica será realizada a uma distância de cerca de 10 m, o padrão não estabelece os requisitos para a potência do transmissor. Esse parâmetro é regido por regulamentações de rádio específicas de cada país. O mais amplamente utilizado no mercado

são os transmissores com uma potência de 1 mW, que fornecem conectividade em distâncias de até 10 metros, bem como transmissores com uma potência de 10 mW, que aumentam a distância para 80 metros e até 1 km em linha de visão. A faixa de comunicação pode ser aumentada usando um *design* de antena especial.

O modelo OSI da rede ZigBee é apresentado na Tabela 3. Ele inclui uma camada física (PHY), uma camada de ligação consistindo de acesso ao meio, subcamada de transmissão, MAC e LLC (*Logic Link Control*), que são definidos na norma IEEE 802.15.4, uma camada de rede (NWK), uma camada de aplicação (APL), consistindo de uma subcamada de suporte de aplicativo (APS), uma camada de objeto de dispositivo ZigBee (ZDO) e objetos de aplicativo definidos pelo fabricante do dispositivo ZigBee.

Tabela 3 – Níveis do modelo OSI da rede ZigBee / IEEE 802.15.4

Nível	Modelo OSI	ZigBee	Funções
7	Aplicação	APL (APS, ZDO e objetos de aplicação) ZigBee	Mensagens, descoberta de dispositivos, determinação de função de dispositivo
6	Apresentação	-	-
5	Sessão	-	-
4	Transporte	-	-
3	Rede	NWK ZigBee	Roteamento de segurança
2	Enlace (transferência de dados)	LLC IEEE 802.15.4	CSMA / CA, transferência de baliza, sincronização
		SSCS IEEE 802.15.4	
		IEEE 802.15.4 MAC	
1	Físico	PHY IEEE 802.15.4	Canal de rádio de 2,4 GHz

Fonte: Autor.

A subcamada MAC gerencia o acesso ao canal de rádio usando o método CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Também é responsável pela transmissão de quadros de sinalização (*overhead*), sincronizando e fornecendo métodos confiáveis para transmissão de informações. A subcamada SSCS (*Service Specific Convergence Sublayer*) desempenha o papel de uma interface entre os sub níveis LLC e MAC. A subcamada LLC comunica a camada de rede com a camada MAC.

A camada NWK usa métodos que fornecem:

- Registro/exclusão na rede de um novo dispositivo;
- Segurança de transmissão de quadros;

- Indicação da rota do quadro para o destino;
- Estabelecimento de rotas entre dispositivos na rede;
- Detecção de vizinhos mais próximos na rede;
- Memorização das informações necessárias sobre os nós vizinhos.

3.3.1 Arquitetura de redes ZigBee

Como é possível observar na Figura 14, as redes ZigBee possuem basicamente três tipos de dispositivos:

- Coordenador – forma a topologia de rede e pode estabelecer pontes com outras redes. Cada rede ZigBee possui apenas um coordenador;
- Roteador – funciona como um *link* intermediário, transmitindo dados de outros dispositivos na direção certa;
- Dispositivo final – transmite dados para o coordenador ou roteador e não pode se comunicar com dispositivos semelhantes a ele.

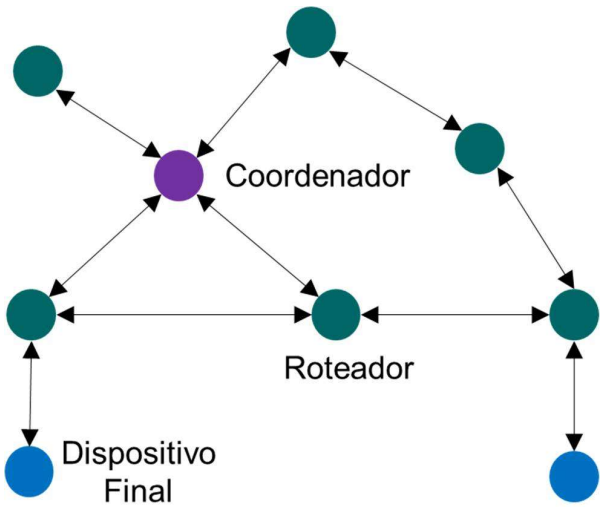

Figura 14 – Tipos de dispositivos de redes ZigBee.

Fonte: Autor.

A definição dos papéis de cada dispositivo nas redes ZigBee é feita no subnível ZDO (*ZigBee Device Object*). Além disso, este subnível também é responsável por iniciar ou responder uma solicitação de conexão e pela descoberta de dispositivos na rede e quais serviços eles fornecem.

A topologia de rede Zigbee é suportada pelo nível NWK e pode estar na forma de uma estrela, uma árvore ou uma rede *mesh*.

Na topologia em estrela, a rede é controlada pelo coordenador. O coordenador é responsável por inicializar e manter os dispositivos de rede e todos os dispositivos finais que interagem diretamente com ele.

Na estrutura da rede celular e em árvore, o coordenador é responsável pela organização da rede e pela seleção de alguns parâmetros-chave, mas a rede pode ser expandida usando roteadores ZigBee.

Em uma rede com uma topologia em árvore, os roteadores movem dados e controlam mensagens usando uma estratégia de roteamento hierárquico. As redes de árvores podem usar estratégias de roteamento utilizando "balizas" (*beacons*) (Figura 17).

A rede celular deve fornecer comunicação ponto a ponto completa de dispositivos, ou seja, não há dispositivos de diferentes níveis na rede (coordenadores, roteadores, etc. – todos os dispositivos são iguais).

Outra característica das redes ZigBee é a capacidade de retransmitir dados transmitidos através de muitos nós intermediários na rede, e quando um dos nós falha ou desliga, a rede encontra automaticamente outra maneira de transferir informações. Quando o dispositivo é ligado, a rede o reincorpora.

O padrão distingue entre dois tipos de dispositivos: dispositivos de função completa (FFD – *Full Function Devices*) e dispositivos com um conjunto reduzido de funções (RFD – *Reduced Function Devices*). Os FFD podem operar em uma rede com topologia de árvore como um coordenador de rede ou como um dispositivo final. Os FFD podem trocar informações com outros FFD ou RFD, mas os RFD só podem se comunicar com os FFD. RFD é muito mais simples e mais barato que o FFD. Qualquer rede deve conter pelo menos um dispositivo FFD com todos os recursos.

Dependendo dos requisitos de uma aplicação específica, uma rede baseada no padrão IEEE 802.15.4 pode ter uma das duas topologias: estrela (Figura 15a) ou malha (*peer-to-peer*) (Figura 15b).

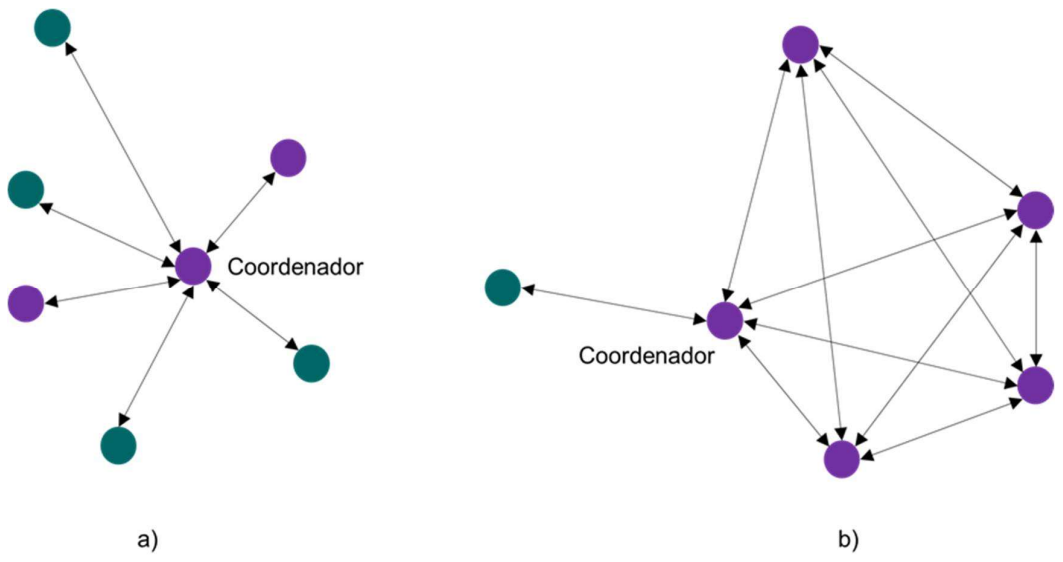

Figura 15 – (a) topologia em estrela; (b) topologia *peer-to-peer*. Círculo roxo – dispositivo com funcionalidade completa (FFD); Círculo verde – dispositivo com funcionalidade reduzida (RFD).

Fonte: Autor.

Todos os dispositivos na rede, independentemente da topologia, devem ter um endereço estendido exclusivo de 64 bits. Esse endereço é usado para comunicação dentro da rede ou pode ser alterado para um endereço curto de 16 bits alocado pelo coordenador no processo de conexão de dispositivos à rede. O coordenador pode ser conectado à rede elétrica e os outros dispositivos de rede podem ser alimentados por bateria.

A rede em malha (*peer-to-peer*) também tem um coordenador, mas é diferente, pois qualquer dispositivo pode trocar dados com qualquer outro se estiver ao alcance do rádio, enquanto que em uma topologia em estrela, qualquer dispositivo só pode interagir com o coordenador. É importante observar que a rede *peer-to-peer* é sempre mais cara, pois contém apenas dispositivos com recursos completos, mas, por isso, permite organizar redes de uma topologia mais complexa, incluindo as "celulares". A maioria das aplicações industriais requer redes *peer-to-peer*. Estes incluem gerenciamento e monitoramento, redes de sensores, rastreamento da localização de ativos, agricultura inteligente, sistemas de segurança e etc. Redes *peer-to-peer* podem ser especializadas, auto organizadas e auto recuperáveis. Elas permitem que sejam transferidas informações entre os nós da rede, independentemente da distância entre eles, usando nós intermediários como repetidores. Essas funções são executadas pela camada de aplicação do modelo OSI.

Várias redes podem interagir umas com as outras. Para fazer isso, cada rede deve ter um identificador de rede exclusivo. Graças a ele, endereços abreviados podem ser usados dentro da

rede. Portanto, o endereço completo do dispositivo para acesso a partir do exterior (de outra rede) consiste no endereço de rede e no endereço curto do dispositivo.

A estrutura básica da rede de topologia em estrela é mostrada na Figura 15a. Depois de habilitar primeiro um dispositivo de rede completo, ele pode organizar sua própria rede e se tornar um coordenador de rede. Todas as redes de topologia em estrela operam independentemente umas das outras. Isso é obtido selecionando-se um identificador de rede que não seja usado por outras redes que estejam dentro do alcance dessa rede. Depois de selecionar um identificador de rede, o coordenador pode aceitar outros dispositivos na rede, tanto FFD quanto RFD.

Em uma rede *peer-to-peer* (Figura 15b), cada dispositivo pode interagir com qualquer outro dispositivo que esteja dentro do seu alcance. Um dos dispositivos é atribuído ao coordenador, por exemplo, aquele que é conectado pela primeira vez à rede. Com a expansão adicional da rede, é possível alterar a topologia ponto a ponto e criar uma topologia híbrida, que também conterá dispositivos com funcionalidade reduzida.

Um exemplo do uso de comunicação *peer-to-peer* entre dispositivos pode ser uma árvore de *clusters* (Figura 16). Uma árvore de *cluster* é um caso especial de uma rede *peer-to-peer* na qual a maioria dos dispositivos é totalmente funcional. Dispositivos com funcionalidade reduzida só podem ser conectados a uma árvore de *cluster* como nós finais nas extremidades das ramificações, já que podem ser conectados a apenas um dispositivo completo. Um dos dispositivos com recursos completos na rede deve desempenhar o papel de coordenador de rede e garantir a sincronização com outros dispositivos. O coordenador da rede deve ter recursos computacionais aumentados.

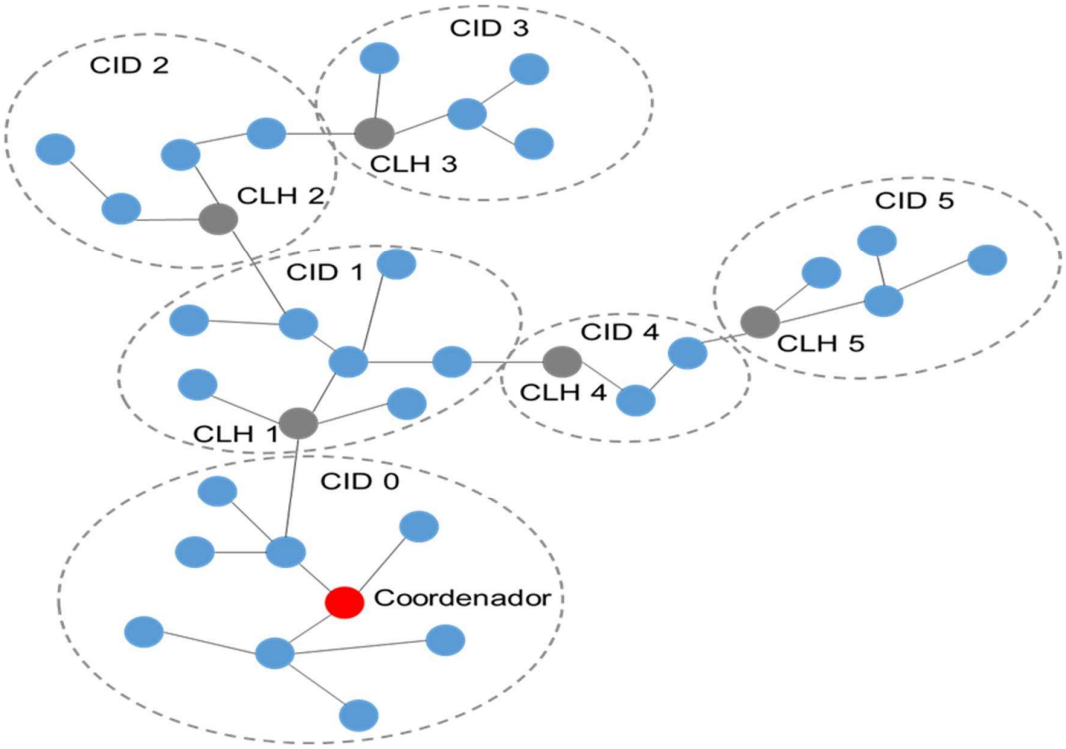

Figura 16 – Exemplo de rede com topologia em árvore de *cluster*. (CID = *Cluster* ID; CLH = *Cluster Head*).

Fonte: Autor.

Ao formar uma rede de tipo árvore de *cluster*, o coordenador de rede se atribui como o chefe do primeiro *cluster* (*Cluster Head* – CLH) e atribui seu ID de *cluster* a 0 (*Cluster IDentifier* CID = 0) e seleciona o identificador de toda a árvore de *cluster* sendo formada. Depois disso, o coordenador envia um comando de transmissão com um quadro de localização para todos os dispositivos vizinhos. Os dispositivos que recebem uma "baliza" podem solicitar permissão para ingressar no cluster sendo formado. Se o coordenador da rede permitir a adesão, ele adicionará um novo dispositivo à sua lista de dispositivos vizinhos. Em seguida, o dispositivo recém adicionado adicionará o CLH como um dispositivo pai à sua lista vizinha e enviará periodicamente um sinalizador. Agora outros dispositivos podem se conectar a ele. Se o dispositivo que deseja se conectar à rede não puder encontrar o CLH, ele poderá se conectar a qualquer outro dispositivo que possa ser o pai.

O caso especial mais simples de uma árvore de *cluster* é um único *cluster*, no entanto vários clusters podem ser combinados para formar uma árvore de clusters (Figura 16). Para fazer isso, o coordenador de rede atribui um dos dispositivos com recursos completos à "cabeça" do *cluster* vizinho e atribui a ele um número de cluster CID = 1.

3.3.2 Estrutura dos quadros da camada MAC

A subdivisão MAC controla o sinalizador (baliza), o acesso ao canal, atribui intervalos de tempo garantidos, verifica a precisão da transmissão de quadros, transmite um quadro de confirmação de recebimento e executa parte do trabalho para garantir a segurança das informações.

O padrão IEEE 802.15.4 permite o uso opcional da estrutura da mensagem de *superframe* (Figura 16). O formato do *superframe* é determinado pelo coordenador da rede. O *superframe* é delimitado em ambos os lados por "balizas", dividido em 16 *slots* de igual comprimento e enviado pelo coordenador da rede. A "baliza" é colocada no lugar do primeiro *slot* de cada *superframe*. O coordenador também pode desativar o modo de mensagem com "balizas". As "balizas" são usadas para sincronizar dispositivos conectados, identificar a rede e descrever a estrutura do *superframe*. Qualquer dispositivo que deseje iniciar o processo de comunicação entre as duas "balizas" deve usar o mecanismo de acesso ao *slot* CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance* – Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão). O envio de mensagens deve ser concluído antes da chegada da próxima "baliza".

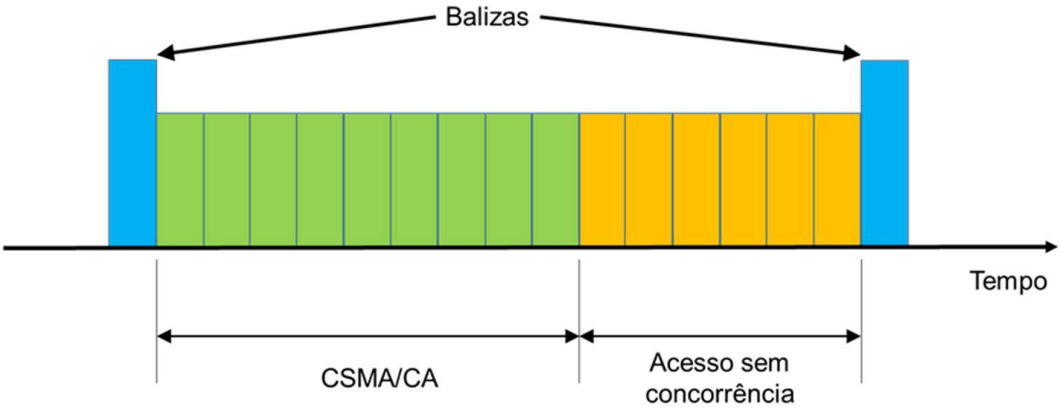

Figura 17 – Estrutura de *superframe* com intervalos de tempo definidos.

Fonte: Autor.

Numa rede com "balizas", é utilizado um mecanismo de acesso CSMA/CA com intervalos, em que o início do intervalo de tempo deve coincidir com o limite do *superframe* do coordenador de rede, ou seja, o início do *slot* para cada dispositivo deve ser sincronizado com o início da transferência do sinal pelo coordenador da rede. Como o dispositivo não pode iniciar

a transmissão até que o sinalizador (baliza) seja encontrado e os sinalizadores sejam enviados apenas pelo coordenador da rede, este, com a ajuda dos sinalizadores (balizas), realiza a programação das trocas de dados em toda a rede. Nesse caso, o nível PHY deve garantir que todas as transmissões na rede comecem simultaneamente com o início dos *slots*. A introdução da sincronização descrita reduz a probabilidade de transmissão simultânea de mensagens por vários nós na rede.

Para dispositivos que requerem entrega urgente ou grande largura de banda, o coordenador da rede pode reservar uma parte do *superframe* em que não haverá concorrência para o canal (Figura 17), pois neste momento o coordenador da rede proíbe qualquer transmissão para todos os outros dispositivos. Essa parte dos *slots* do *superframe* é chamada de GTS (*Guaranteed Time Slots* – Intervalos de tempo garantidos).

A estrutura do quadro foi projetada de forma simples, garantindo transmissão de dados confiável em um canal com ruído. De acordo com o modelo OSI, cada camada subjacente adiciona seu próprio cabeçalho (*overhead*) ao protocolo. O padrão fornece quatro tipos de quadros:

- Quadro de Baliza;
- Quadro de dados (*payload*);
- Quadro de notificação de recebimento;
- Subcamada MAC.

O quadro de dados (Figura 18) começa com o “Preâmbulo”, que, juntamente com o campo “Iniciar”, serve para sincronizar dados no receptor, o campo “Comprimento” contém o comprimento do campo da subcamada MAC em bytes. O campo "Controle" contém informações de serviço no gerenciamento de quadros, o campo "Número" contém o número de série de dados, o campo "Endereço" contém informações de endereço, incluindo um endereço curto (16 bits) ou estendido (64 bits). O quadro termina com um campo de soma de controle (CS – *CheckSum*).

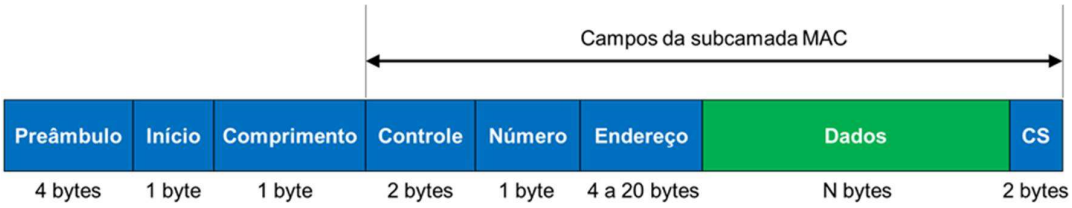

Figura 18 – O formato do quadro de dados de acordo com o IEEE 802.15.4.
Fonte: Autor.

3.3.3 *Throughput*

As transmissões por tecnologias sem fio de baixa potência compreendem duas partes: os bits que implementam o protocolo (por exemplo, ID do pacote e comprimento, canal e *check sum*, coletivamente conhecidos como *overhead*) e as informações que estão sendo comunicadas (conhecidas como *payload*). A proporção carga útil / sobrecarga + carga útil determina a eficiência do protocolo.

A taxa de dados "brutos" (*overhead* mais *payload*) é uma medida do número de bits transferidos por segundo e geralmente é o valor citado na especificação da tecnologia. As tecnologias sem fio de baixa potência geralmente exigem a transferência periódica de pequenas quantidades de informações do sensor entre os nós e um dispositivo central, minimizando o consumo de energia, de modo que as larguras de banda são geralmente modestas.

Em algum momento, o limite de taxa de transferência do ZigBee pode se tornar uma barreira séria para o desenvolvimento adicional de seu ecossistema. O padrão 802.15.4 do IEEE, que define a camada física da pilha de protocolos ZigBee, restringe a taxa de dados a 250 kbps, e somente o IEEE pode introduzir ajustes a esse respeito. Este é o valor teórico máximo, entretanto a taxa de transferência real depende das condições de configuração e operação. Existem vários trabalhos que, através de experimentos, obtiveram valores de *throughput* para diferentes configurações.

Por exemplo, ALENA R. et al., 2010 afirmaram que o ZigBee fornece capacidade de largura de banda de médio alcance em uma taxa de transferência sustentável de aproximadamente 100 Kbps suportando redes de sensores de alta performance para redes de sensores mais escalonáveis, enquanto SOIJOYO S. e ASHARI A., 2017, através de seus experimentos, obtiveram uma taxa de transferência entre 5 Kbps a 35 Kbps baseado nos módulos ZigBee RF da Digi *International.*

3.3.4 Segurança

O padrão ZigBee inclui medidas de segurança complexas para garantir o estabelecimento de chaves segurança, redes seguras e segurança de quadros. (ZIGBEE

ALLIANCE, 2008). Esses serviços são implementados na rede e no *Application Support Sublayer* (APS), uma subcamada da camada de aplicação. O protocolo ZigBee é baseado em um modelo de "confiança aberta". Isso significa que todas as camadas da pilha de protocolos confiam umas nas outras. Portanto, a proteção criptográfica ocorre apenas entre dispositivos. Cada camada é responsável pela segurança de seus respectivos quadros. A segurança das redes ZigBee é baseada em chaves de criptografia. É possível distinguir entre dois tipos de chaves de segurança. (ZIGBEE ALLIANCE, 2008).

A chave de rede é usada para proteger a comunicação do tipo *broadcast*. Essa chave de 128 bits é compartilhada entre todos os dispositivos na rede. Geralmente várias chaves de rede são armazenadas pelo *Trust Center*, mas apenas uma chave de rede é a chave de rede ativa. A chave de rede ativa é identificada por um número sequencial e pode ser usado pelas camadas de rede e aplicação de um dispositivo.

Um dispositivo deve adquirir uma chave de rede via transporte de chaves ou pré-instalação. A chave de *link* é usada para proteger comunicações do tipo *unicast* na camada de aplicação. Esta chave de 128 bits é compartilhada apenas entre dois dispositivos. As chaves de *link* são adquiridas via transporte de chaves, estabelecimento de chaves ou pré-instalação e pode ser usada apenas pela subcamada APS (*Application Support Sublayer*) (ZILLNER T., 2015).

3.4 6LoWPAN

O 6LoWPAN é um padrão aberto definido no RFC 6282 pela *Internet Engineering Task Force* (IETF), uma organização de padronização que define muitos dos padrões abertos usados na Internet, como UDP, TCP e HTTP. Um recurso notável do 6LoWPAN é que ele foi originalmente projetado para suportar redes sem fio de baixa potência de 2,4 GHz construídas no IEEE 802.15.4, mas agora esse padrão foi adaptado e usado em muitas outras mídias de transmissão de rede, incluindo redes sem fio no mercado.

Os principais recursos das redes 6LoWPAN são:

- Disponibilidade de qualquer nó da rede pelo seu endereço;
- Não há necessidade de um *gateway* de nível de aplicação para trabalhar com nós de rede.

O 6LoWPAN é um protocolo de camada de rede, portanto ele pode ser usado com qualquer camada de enlace físico e de dados. Uma situação semelhante é com a pilha TCP/IP.

Além disso, não é necessário usar um meio de transmissão sem fio. Para suportar grandes redes, os nós 6LoWPAN podem atuar como roteadores. Existe ainda a possibilidade de roteamento com uma orientação de nível de sinal, que permite que os dados sejam transmitidos em baixa potência, economizando recursos energéticos da fonte de energia.

A implementação atualmente proposta da pilha de protocolos 6LoWPAN é projetada para o intervalo sub-gigahertz, e isto não é por acaso (OLSSON, 2014). Em primeiro lugar, essa banda não requer licenciamento em quase todos os países do mundo (de uma forma ou de outra, várias bandas de frequência nesta banda estão disponíveis para uso livre). Em segundo lugar, com custos de energia iguais para recepção e transmissão, em comparação com a banda de 2,4 GHz, devido aos comprimentos de onda mais longos, é possível garantir uma comunicação estável a uma distância maior. Também visivelmente menos influência de obstáculos, o que é importante para os sistemas que operam em ambientes urbanos. Isso permite o uso de transceptores sub-gigahertz para redes tanto em escala pessoal (até 10 metros) quanto local. O limite superior do alcance de comunicação é de cerca de 800 metros. As taxas de dados também são suficientes para aplicações típicas de redes de sensores (de 50 a 200 kbps).

Os aplicativos de destino da pilha 6LoWPAN incluem redes dimensionáveis razoavelmente grandes com conectividade IP (Internet, intranet ou extranet). Apesar da boa escalabilidade, gerenciamento potencialmente transparente e fácil acesso aos nós, eles não são adequados para todas as aplicações. Em particular, a versão atual da pilha de protocolos padrão requer a atividade constante dos roteadores para a correta transferência de dados. No entanto, esse recurso permite minimizar a quantidade de memória *flash* ocupada pela pilha 6LoWPAN no dispositivo final (nó de rede) e, portanto, minimizar o custo do processador de rede.

Há muitas características e aplicações em comum entre ZigBee e 6LoWPAN, como mostrado na Figura 19. Entretanto, ambos os padrões “competem” em algumas aplicações, mas, em outras, se “complementam”, aumentando a integração de serviços e ampliando a cobertura da rede.

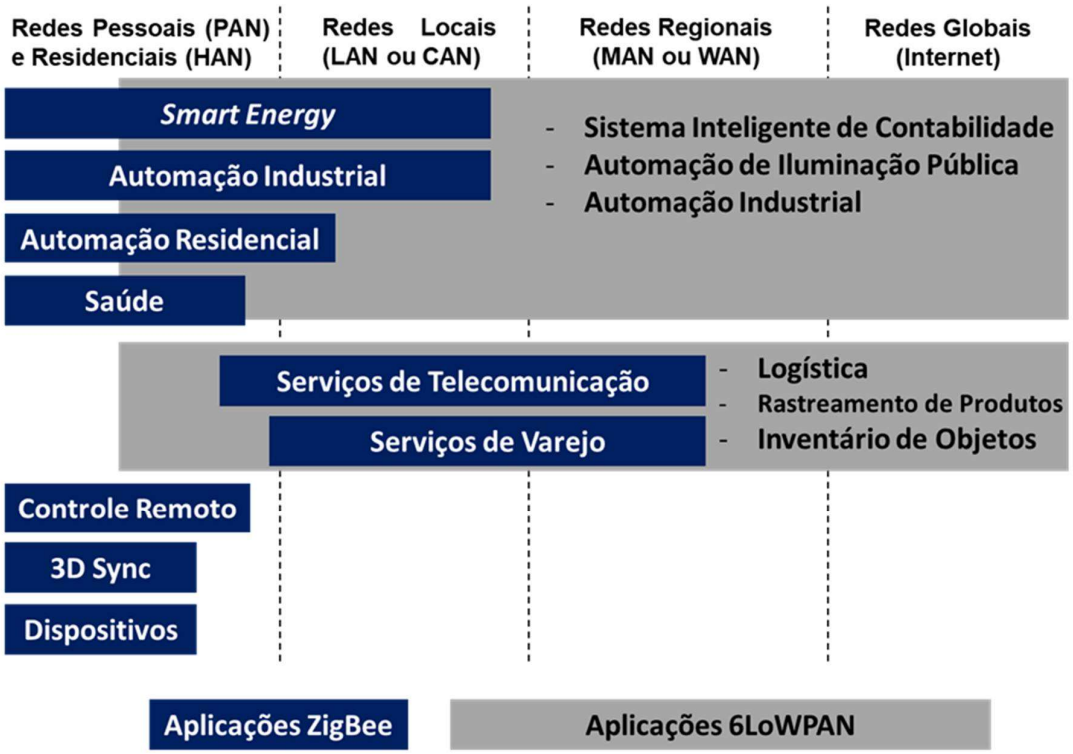

Figura 19 – Comparativo de áreas de aplicação e possibilidade de cobertura dos serviços ZigBee e 6LoWPAN.

Fonte: Autor.

Principais aplicações:

- Controle de iluminação pública;
- Automação industrial;
- Sistemas de logística, rastreamento de mercadorias ou itens de estoque;
- Sistemas de segurança comercial, sistemas de controle de acesso;
- Algumas aplicações militares.

O poder da rede é determinado pelo número de nós envolvidos e pela capacidade dos protocolos de usar efetivamente os recursos inerentes. As capacidades de rede são usadas em muitas áreas de atividade: monitoramento e gerenciamento de instalações, coleta, transferência e processamento primário de dados e muito mais. Nesse caso, os nós de rede podem ter diferenças significativas em computação, recursos de comunicação e recursos de memória.

O padrão 6LoWPAN conecta muitos dispositivos à nuvem. Baixo consumo de energia, nós endereçáveis por IP e suporte para redes *mesh* grandes tornam essa tecnologia sem fio uma boa opção para aplicações de Internet das Coisas (IoT).

Uma qualidade particularmente valiosa da rede é sua capacidade de integrar vários dispositivos com diferentes funções e recursos fornecidos. O papel determinante é desempenhado pelos protocolos de rede (pilha de protocolos).

Um exemplo notável disso é a pilha de protocolos TCP/IP, subjacente à grande maioria das redes modernas de vários níveis. O maior e mais usado deles é a Internet, que fornece comunicações, serviços e serviços globais. Mais importante, os padrões de processamento de informações e desenvolvimento de aplicativos foram desenvolvidos para redes TCP/IP. A rede da Internet já inclui vários bilhões de nós e está rapidamente migrando para a nova versão do protocolo IP (IPv6), que oferece um esquema de endereçamento mais flexível e um fornecimento melhor de espaço de endereçamento.

A disseminação de sistemas automatizados, sejam na indústria, saúde ou agricultura está originando extensas redes de sensores, unidades e mecanismos controlados. Mesmo para um pequeno objeto automatizado, seu número pode exceder várias centenas. Além disso, as tarefas modernas de automação exigem interação máquina a máquina transparente (interação M2M), serviços avançados, interação com bancos de dados e até mesmo uma interface de usuário. Nesse sentido, usar a infraestrutura da Internet para construir um sistema escalonável distribuído parece muito tentador.

O suporte direto a protocolos da Internet para a grande maioria dos nós da rede de sensores não é possível. Existem várias razões para isso:

- Recursos limitados de fornecimento de energia (dispositivos independentes);
- Capacidades computacionais insuficientes;
- Pequena quantidade de memória.

Para superar essa situação, o IETF (*Internet Engineering Task Force*) desenvolveu a pilha de protocolos 6LoWPAN ("IPv6 sobre Redes Pessoais Sem Fio de Baixa Potência" – padrão pessoal de interconexão IPv6 sobre redes pessoais sem fio IEEE 802.15.4 de baixa potência) (SHELBY e BORMANN, 2009) é a versão IPv6 de redes de sensores sem fio baixo consumo de energia.

O nome completo "IPv6 sobre redes de área pessoal sem fio de baixo consumo" significa "transferência de pacotes IPv6 através de redes pessoais sem fio de baixo consumo", portanto, 6LoWPAN é uma tecnologia de rede ou nível de adaptação que permite transmitir pacotes IPv6 eficientemente utilizando o padrão IEEE 802.15.4.

3.4.1 Arquitetura de redes 6LoWPAN

A arquitetura de rede 6LoWPAN é um pouco diferente das arquiteturas de rede IP tradicionais (a presença de equipamentos especializados de comutação, roteadores, conversores de mídia) e das arquiteturas de rede de aquisição de dados sem fio existentes. O mais próximo disso é a arquitetura das redes WiFi, embora haja várias diferenças em relação a isso.

A Figura 20 mostra um exemplo de uma rede de malha 6LoWPAN, muito parecida com uma rede IPv6. A conexão com a Internet é fornecida por um ponto de acesso (AP – *Access Point*) agindo como um roteador IPv6. Em uma configuração típica, vários dispositivos diferentes são conectados ao ponto de acesso, como PCs, servidores e assim por diante. A rede 6LoWPAN está conectada a uma rede IPv6 através do uso de um roteador de borda. O roteador de borda executa três ações: troca de dados entre dispositivos 6LoWPAN e a Internet (ou outra rede IPv6), troca local de dados entre dispositivos na rede 6LoWPAN e formação e manutenção de uma sub rede de rádio (rede 6LoWPAN).

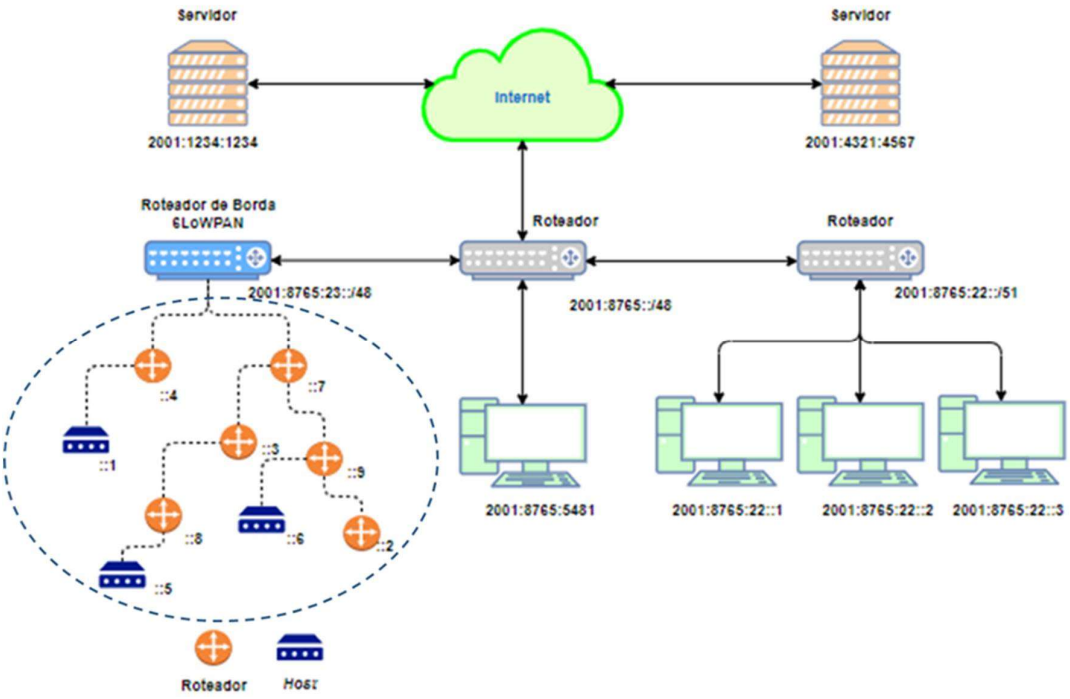

Figura 20 – Exemplo de rede IPv6 com uma rede de malha 6LoWPAN.

Fonte: Modificado de Olsson, 2014

Ao interagir de maneira natural com o IP no formato nativo, as redes 6LoWPAN se comunicam com outras redes por meio de roteadores IP padrão. Conforme mostrado na Figura 20, as redes 6LoWPAN normalmente operam como terminais na borda da rede global. Isso

significa que os dados de entrada são destinados a um dos dispositivos no 6LoWPAN. Uma rede 6LoWPAN pode ser conectada a outras redes IP através de um ou mais roteadores de borda que enviam datagramas IP entre diferentes meios de transmissão. A conectividade com outras redes IP pode ser fornecida por meio de qualquer canal arbitrário, como Ethernet, Wi-Fi ou 3G/4G. Como o 6LoWPAN especifica apenas operações IPv6 sobre o padrão IEEE 802.15.4, os roteadores de borda também podem suportar mecanismos de transição IPv6 para conectar redes 6LoWPAN a redes IPv4.

Como os roteadores de borda enviam datagramas na camada de rede, eles não suportam estados no nível da aplicação. Redes com uma arquitetura diferente, como ZigBee ou redes proprietárias, exigem *gateways* para executar aplicações complexas que permitem converter tráfego de rede sem fio específico antes de enviar dados para um canal IP padrão. Esses *gateways* de aplicação devem entender qualquer perfil de aplicação que possa ser usado na rede e quaisquer alterações nos protocolos de aplicação nos nós sem fio também devem ser acompanhadas por alterações no *gateway*. Em contraste, os roteadores baseados em IP nos limites da rede, como um roteador de borda, são independentes dos protocolos de aplicação usados no 6LoWPAN. Isso reduz a carga no roteador de borda, por exemplo, permitindo assim o uso de dispositivos embarcados com baixo custo, *software* mais simples e *hardware* menos sofisticado. Ao mesmo tempo, a arquitetura IP não impede o uso de *proxies* e memória cache, que são amplamente utilizados na Internet moderna, para otimizar a rede.

Dois outros dispositivos estão incluídos na típica rede 6LoWPAN: roteadores e *hosts*. Os roteadores, conforme definidos pelo nome, podem retransmitir dados destinados a outros nós na rede 6LoWPAN. Os *hosts*, também chamados de terminais, não podem enviar dados para outros dispositivos na rede. O *host* também pode ser um dispositivo "adormecido" que "acorda" periodicamente para verificar os dados de seu "pai" (roteador), o que permite um consumo de energia muito baixo.

As redes 6LoWPAN são sub redes de redes IPv6, ou seja, eles podem se comunicar com outras redes e nós da rede IP, mas não estão transitando pelo tráfego da rede. As redes 6LoWPAN consistem em nós que também podem desempenhar o papel de roteadores (*host* e roteador), além de um ou mais roteadores de borda podem estar presentes na rede. A participação no roteamento não é um requisito para um nó de rede e pode desempenhar um papel semelhante ao de um dispositivo final nas redes ZigBee ou um dispositivo com funcionalidade limitada para redes 802.15.4, na terminologia de 6LoWPAN ("*host-node*" – *host*).

Um nó capaz de realizar roteamento dentro da rede 6LoWPAN é chamado de roteador ou roteador de borda. O roteador de borda é responsável pela interação da sub rede 6LoWPAN com a rede IPv6, participa do procedimento de inicialização e roteamento na sub rede 6LoWPAN, realiza compressão/descompactação de cabeçalhos IPv6 ao trocar com uma rede externa, no caso de conexão a uma rede IPv4, pode desempenhar o papel de um *gateway* entre IPv6 e IPv4. Os nós de sub rede compartilham o prefixo IPv6 de 64 bits, que também faz parte do endereço de rede do roteador de borda. Para endereçamento dentro da rede, é possível usar os restantes sessenta e quatro bits (o endereço MAC da interface de rede) ou usar a compactação de endereço e um esquema de endereçamento de 16 bits encurtado (os dois bytes inferiores do endereço MAC). Supõe-se que o endereço de rede inclua diretamente o endereço da interface de rede, o que elimina a necessidade de usar o ARP (*Address Resolution Protocol* – protocolo de resolução de endereço de rede).

Existem três tipos de redes 6LoWPAN: 1) *ad hoc*, 2) rede 6LoWPAN simples, 3) rede 6LoWPAN estendida (Figura 21).

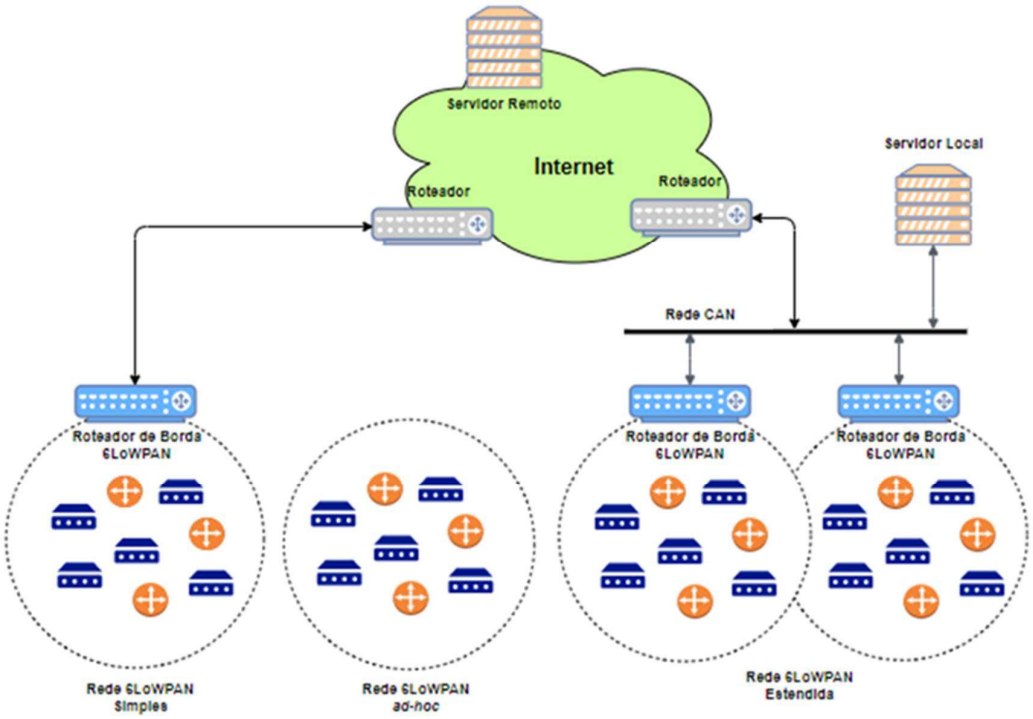

Figura 21 – Arquitetura de redes 6LoWPAN.

Fonte: Autor.

A rede *ad hoc* não tem conexão com uma rede IP externa e não possui um roteador de borda. É uma rede auto organizada que usa a pilha de protocolos 6LoWPAN para organizar o trabalho e transferir dados entre nós.

A rede 6LoWPAN simples é conectada a uma rede IP diferente usando um roteador de borda. O roteador de borda pode ser conectado diretamente a uma rede IP externa (uma conexão ponto-a-ponto, por exemplo, um modem GPRS/3G).

A rede 6LoWPAN estendida consiste em uma ou várias sub redes conectadas a uma rede IP externa através de vários roteadores de borda conectados a uma rede (por exemplo, a rede local de uma organização). Ao mesmo tempo, os roteadores de borda na rede estendida compartilham o mesmo prefixo de rede. Os nós de rede estendidos podem se mover livremente dentro da rede e trocar com a rede externa através de qualquer roteador de limite (geralmente uma rota é escolhida com os melhores indicadores de qualidade de sinal - nível de erro, nível de sinal).

A interação entre os nós da rede 6LoWPAN, bem como a interação com nós externos, é realizada da mesma forma que em uma rede IP convencional. Cada nó tem seu próprio endereço IPv6 exclusivo e pode receber e transmitir pacotes IPv6.

3.4.2 Estrutura dos quadros da camada MAC

O 6LoWPAN usa uma pilha de cabeçalhos e, similarmente ao IPv6, cabeçalhos estendidos. Os cabeçalhos 6LoWPAN (Figura 22) regulam as funções de cada um dos três sub cabeçalhos (endereçamento de célula, fragmentação e compressão de cabeçalho). O formato do cabeçalho é determinado usando o campo de tipo de cabeçalho colocado no início de cada cabeçalho. A pilha de cabeçalhos é fácil de analisar e leva em conta as legendas que serão removidas se não forem necessárias. O cabeçalho de fragmentação é ignorado para pacotes que estão aninhados em um quadro IEEE 802.15.4. O cabeçalho da célula não é usado se os dados forem enviados apenas entre nós vizinhos.

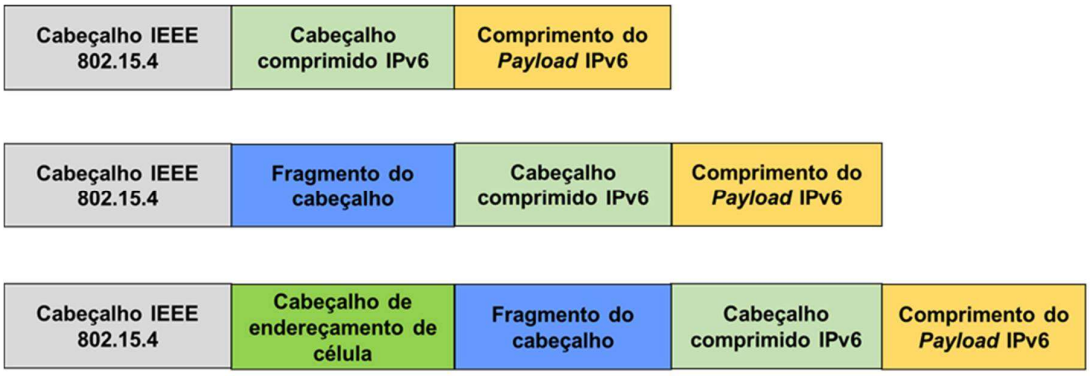

Figura 22 – Pilha de cabeçalhos 6LoWPAN.

Fonte: Autor.

O cabeçalho do fragmento é usado quando a carga útil (*payload*) é muito grande para caber em um quadro IEEE 802.15.4. O cabeçalho do fragmento contém três campos: o tamanho do datagrama, o *tag* do datagrama e seu deslocamento. O tamanho do datagrama descreve a carga útil total (não fragmentada). O *tag* do datagrama identifica um conjunto de fragmentos e é usado para mapear fragmentos da mesma carga útil. O deslocamento do datagrama identifica o deslocamento do fragmento dentro da carga útil não fragmentada. O comprimento do cabeçalho do fragmento é de 4 bytes para o primeiro cabeçalho e 5 bytes para todos os subsequentes.

O cabeçalho do endereço da célula é usado para transferir pacotes através de vários saltos em redes 6LoWPAN. O cabeçalho do endereço da célula inclui três campos: o número de saltos, os endereços de origem e de destino. O campo número de saltos é usado para limitar o número de retransmissões dentro da rede ao transferir de um nó para outro, similar ao conceito de *time to live* (TTL). O campo diminui em um com cada salto. Assim que o contador se torna zero, o pacote é descartado. Os campos de endereço de origem e endereço de destino indicam os pontos de extremidade IP. Ambos os campos contêm endereços IEEE 802.15.4 e podem ser encurtados ou estendidos, conforme definido no padrão IEEE 802.15.4. O comprimento do cabeçalho do endereço da célula é de 5 a 17 bytes, dependendo do método de endereçamento usado.

3.4.3 *Throughput*

Com o objetivo de aumentar a largura de banda, o IPv6 aumenta a unidade de transmissão máxima (MTU) de 576 a 1280 bytes. IPv6 também reflete mudanças e avanços nas

tecnologias da camada de *link* que a Internet usa. Ethernet é a tecnologia de *link* dominante e seu rendimento aumentou ao longo dos anos. O Wi-Fi reflete os recursos da Ethernet suportando o tamanho de MTU semelhante e *links* com taxas muito altas. Tanto a Ethernet como o Wi-Fi operam no contexto de dispositivos de alta potência e capacidade.

Por outro lado, o IEEE 802.15.4 foi projetado para servir um mercado diferente; aplicações de longa duração que exigem um grande número de dispositivos de baixo custo e potência ultrabaixa. A taxa de transferência sob este padrão é limitada a 250 kbps e o comprimento do quadro é limitado a 127 bytes para garantir baixas taxas de erro de bit e pacote em um ambiente de rádio frequência com perdas.

Além disso, O IEEE 802.15.4 usa dois endereços: um endereço curto de 16 bits e um endereço estendido de 64 bits. Estes endereços reduzem o *overhead* do cabeçalho e minimizam requisitos de memória. Além disso, o 6LoWPAN opera mais comumente em vários saltos formando uma rede *mesh* de baixa potência, uma diferença das redes baseadas em Ethernet ou Wi-Fi.

Finalmente, os dispositivos usados para implementar o 6LoWPAN são normalmente restritos em termos de recursos, tendo cerca de 16 kB de RAM e 128 kB de ROM (OLSSON, 2014).

3.4.4 Segurança

A segurança ainda é uma questão necessária para sistemas de IoT e esse problema precisa ser resolvido. Devido à natureza da IoT, cujo conjunto de nós tem, em muitos casos, funções muito limitadas, há muitos pontos para atacar de fora.

Outro aspecto crítico é que os dados que circulam em um sistema típico de IoT não são apenas “dados”. O interesse de um invasor por eles é muito maior, pois os dados do sistema sem fio podem ser usados, por exemplo, para abrir a porta da sua casa ou ativar/desativar remotamente o alarme.

Para aumentar a segurança dos dados, o 6LoWPAN utiliza o sistema de transmissão segura de dados AES-128, definido no IEEE 802.15.4. A segurança de *link* de dados é fornecida pela autenticação e criptografia. Além da segurança da camada de enlace nos sistemas 6LoWPAN, o mecanismo de segurança da camada de transporte (TLS) demonstra excelente desempenho. O TLS, conforme definido no RFC 5246, é executado por meio do TCP. No caso de recursos limitados, onde o UDP é selecionado como o protocolo da camada de transporte, o RFC 6347 (segurança de datagrama da camada de transporte) pode ser usado para fornecer

segurança na camada de transporte. No entanto, deve-se notar que a implementação do TLS/DTLS requer que os dispositivos tenham os recursos necessários, como um mecanismo de codificação de *hardware* para garantir o uso de um conjunto de criptografia estendido.

4. Trabalhos Relacionados

Existem vários trabalhos que apresentam análises qualitativas ou quantitativas dos principais protocolos de comunicação de redes de sensores sem fio atualmente utilizados em soluções de IoT. No entanto, não foram encontrados trabalhos relacionados uma comparação qualitativa dos protocolos de IoT LoRaWAN, Sigfox, ZigBee e 6LoWPAN para aplicações industriais de monitoramento de ativos e manutenção preditiva.

C. Buratti et al. (BURATTI C. et al., 2016) compararam o desempenho de ZigBee, 6LoWPAN e SDWN (*Software Defined Wireless Network*) através de experimentos realizados no EuWIn (*European Laboratory of Wireless Communications*), utilizando a plataforma NEWCOM#, nos quais foram avaliadas várias métricas de performance, incluindo *round-trip-time* e *overhead*. No entanto, LoRaWAN e Sigfox não foram considerados nessa pesquisa nem a aplicação desses protocolos na indústria.

J. Kaur et al. (KAUR J. AND KAUR K., 2016) apresentaram um *framework* para a tomada de decisão em vários setores da indústria (mineração, alimentos, transporte e abastecimento de água), utilizando tecnologias de IoT. No entanto, foram explorados apenas os protocolos da camada de aplicação CoAP, MQTT, XMPP, AMQP e DDS. Os protocolos de acesso LoRaWAN, Sigfox, 6LoWPAN e ZigBee não foram considerados nessa pesquisa.

F. Bonavolontà et al. (BONAVOLONTÀ F. et al., 2017) descreveram o que eles consideram como o estado da arte para a aplicação de tecnologias sem fio na indústria 4.0. Foram descritas as vantagens e desvantagens das tecnologias de redes pessoais (PAN) ou de curta distância e das tecnologias de área ampla de baixa potência (LPWAN). Esse trabalho apresentou as vantagens do protocolo 6LoWPAN, como a utilização de cabeçalhos comprimidos para comunicação com o protocolo de internet (IP), entretanto concluiu que a sua adoção não pode ser considerada uma solução válida para todas as situações, principalmente para aquelas que requerem maior alcance e menor consumo de energia. O estudo também apresentou as tecnologias LoRaWAN e Sigfox como sendo as mais bem-sucedidas dentre os fabricantes de soluções de LPWAN disponíveis na atualidade, para solucionar as limitações das tecnologias de rede pessoal (6LoWPAN e ZigBee). No entanto, os autores não apresentaram um comparativo das tecnologias citadas para aplicações industriais e concluíram que não existe um protocolo que possa ser mais bem definido do que outros, mas a escolha da solução ideal depende de muitos fatores e dos níveis específicos de informação que tem de ser implementados.

M. Iglesias-Urkia et al. (IGLESIAS-URKIA M. et al., 2017) analisaram a performance, em termos de latência, escalabilidade e *overhead*, dos protocolos de IoT CoAP e MQTT, com o intuito de definir um *benchmark* em aplicações de controle e monitoramento industriais. Os autores realizaram experimentos práticos através de uma montagem utilizando sensores e atuadores conectados a um *switch* FastEthernet. Entretanto, o estudo não abordou as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN.

S. Al-Sarawi et al. (AL-SARAWI S. et al., 2017) apresentaram um comparativo qualitativo entre as principais tecnologia sem fio de IoT (6LoWPAN, Bluetooth, ZigBee, RFID, NFC, Z Wave, Sigfox e Cellular), para diversas aplicações: monitoramento e controle industrial, aparelhos de áudio sem fio, rastreamento, inventário, acesso, pagamento, iluminação pública, medidores de energia, comunicação M2M e monitoramento e controle residenciais. Para a elaboração desse comparativo, o trabalho utilizou os critérios: frequência/banda, tipo de rede, topologia, consumo, taxa de dados, alcance, segurança, tipo de modulação, recursos e aplicações comuns. No entanto, não foi abordada a tecnologia LoRaWAN nem aprofundada a aplicação no monitoramento industrial e seus principais requisitos.

A. Glória et al. (GLORIA A. et al., 2017) compararam o desempenho dos protocolos de comunicação sem fio LoRaWAN e ZigBee com padrões de redes cabeadas I^2C e RS232, tomando como parâmetros *throughput*, atraso da mensagem e eficiência. O trabalho apresentou os resultados de testes realizados nas tecnologias já mencionadas, utilizando *hardware* Raspberry Pi, Arduino e ESP-12.

No primeiro teste, com o objetivo de obter o *throughput* do sistema, foi utilizada uma montagem onde o mestre envia uma quantidade contínua de pacotes de dados, sem intervalo entre eles, e o escravo apenas os recebe, registrando o *timestamp* e aumenta o número de pacotes recebidos. Dessa forma, é possível obter a quantidade de pacotes que o escravo processa por segundo.

No segundo, similarmente, são enviados apenas 100 pacotes no intervalo de um segundo. O escravo recebe os pacotes e registra o tempo entre os pacotes. Com isso, o tempo médio é calculado, a fim de obter a demora (atraso) para receber os pacotes.

No terceiro, 1000 pacotes são enviados para o escravo e este só aumenta o número de pacotes recebidos se os dados são iguais aos enviados. Dessa forma, é possível identificar os pacotes perdidos ou com erros.

No entanto, não foram mencionados nesse trabalho os protocolos Sigfox nem 6LoWPAN e também não foram utilizadas as métricas de latência e *overhead*.

Os resultados e as conclusões dessas pesquisas serviram de base, mesmo que parcialmente, para a elaboração deste trabalho, principalmente na obtenção dos parâmetros quantitativos de latência, topologia, *throughput* e *overhead* obtidos a partir de testes e simulações.

Até onde sabemos, este estudo é a única comparação qualitativa entre os protocolos de rede de acesso de IoT LoRaWAN, Sigfox, ZigBee e 6LoWPAN para aplicações em monitoramento de ativos industriais.

A Tabela 4 a seguir apresenta resumidamente os trabalhos que serviram de base para o desenvolvimento deste estudo, identificando os aspectos em comum e destacando os *gaps* em relação ao proposto nos objetivos.

Tabela 4 – Quadro resumo da bibliografia estudada

Autor(es)	Título do Trabalho	Ano	Aspectos que coincidem com a Proposta deste trabalho	GAPs em relação a este trabalho
C. Buratti et al.	Testing Protocols for the Internet of Things on the EuWin Platform	2016	- Compara ZigBee e 6LoWPAN - Usa as métricas de Perda de Pacotes e *Overhead*	- Não menciona LoRaWAN nem Sigfox - Não utiliza as métricas de *Throughput* nem Latência
J. Kaur et al.	Availing Internet of Things in Industrial Decision Making -A Survey	2016	- Apresenta um *framework* para a tomada de decisão em vários setores da indústria	- Não menciona a aplicação em monitoramento de ativos industriais - Não menciona LoRaWAN, Sigfox, 6LoWPAN nem ZigBee
F. Bonavolontà et al.	Enabling wireless technologies for Industry 4.0: State of the Art	2017	- Apresenta as vantagens do protocolo 6LoWPAN - Apresenta as tecnologias LoRaWAN e Sigfox	- Não apresenta as características da tecnilogia ZigBee - Não apresenta um comparativo das tecnologias citadas para aplicações industriais
M. Iglesias-Urkia et al.	Towards a lightweight protocol for Industry 4.0: An implementation based benchmark	2017	- Utiliza as métricas de Latência e *Overhead* para a análise de performance - Define *benchmarks* em aplicações de controle e monitoramento industriais	- Não abordou as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN
S. Al-Sarawi et al.	Internet of Things (IoT) Communication Protocols : Review	2017	- Apresenta comparativo qualitativo entre as principais tecnologia sem fio de IoT (6LoWPAN, Bluetooth, ZigBee, RFID, NFC, Z Wave, Sigfox e Cellular), para diversas aplicações, incluindo monitoramento e controle industriais	- Não foi abordada a tecnologia LoRaWAN - Não foi aprofundada a aplicação no monitoramento industrial e seus principais requisitos
A. Glória et al.	Comparison of Communication Protocols for Low Cost Internet of Things Devices	2017	- Compara o desempenho dos protocolos de comunicação sem fio LoRaWAN e ZigBee - Utiliza o critério de *throughput*	- Não foram mencionados neste trabalho os protocolos Sigfox nem 6LoWPAN - Não foram utilizadas as métricas de latência, perda de pacotes e *overhead*

Fonte: Autor.

5. Desenvolvimento da Proposta

Com o objetivo de avaliar qualitativamente quais das tecnologias mais se adequam para aplicações de monitoramento de ativos industriais, são considerados neste trabalho os parâmetros *throughput*, latência, topologia, *overhead,* segurança e consumo de energia.

Ao elencar e analisar estes seis critérios para a comparação dos protocolos LoRaWAN, Sigfox, ZigBee e 6LoWPAN, será possível obter uma base comparativa que permitirá auxiliar a escolha de um destes em aplicações industriais de IoT.

5.1 *Throughput*

A largura de banda e a taxa de dados são usadas para determinar a quantidade de dados sendo transferidos (taxa de bits) em uma determinada unidade de tempo, normalmente, segundos. Largura de banda significa a faixa de espectro em Hertz que um sistema pode usar para comunicação digital. A taxa de dados depende da largura de banda da conexão de internet. Se a largura de banda for alta, a taxa de bits tende a ser alta.

A largura de banda em bits/s também pode se referir à largura de banda consumida, correspondendo ao *throughput*, ou seja, a taxa média de transferência de dados bem-sucedida através de um caminho de comunicação. Este sentido se aplica a conceitos e tecnologias como modelagem de largura de banda, gerenciamento de largura de banda, limite de largura de banda, alocação de largura de banda (por exemplo, protocolo de alocação de largura de banda e alocação de largura de banda dinâmica).

A largura de banda de um fluxo de bits é proporcional à largura de banda média consumida de um sinal em hertz (a largura de banda espectral média do sinal analógico que representa o fluxo de bits) durante um intervalo de tempo estudado.

A largura de banda do canal pode ser confundida com uma taxa de transferência de dados útil (ou *goodput*). Por exemplo, um canal com R bps (*bits per second*) pode não necessariamente transmitir dados com taxa R, pois protocolos, criptografia e outros fatores podem adicionar uma sobrecarga considerável (*overhead*).

Além disso, os pacotes de dados podem ser perdidos, o que reduz ainda mais a taxa de transferência de dados útil. Em geral, para qualquer comunicação digital efetiva, é necessário um protocolo de enquadramento; o *overhead* e o *throughput* efetivo dependem da implementação. O rendimento útil é menor ou igual à capacidade real do canal, mais a sobrecarga de implementação.

5.2 Latência

Em uma rede, latência é sinônimo de atraso, uma expressão de quanto tempo leva para um pacote de dados ir de um ponto designado para o outro (do dispositivo de monitoramento ou sensor até os *gateways* ou, até mesmo, aos servidores de rede de IoT), medida através do tempo de ida e volta para o envio de um pacote que é devolvido para o remetente.

A latência da rede pode ser entendida como o somatório dos atrasos impostos pela rede e pelos equipamentos utilizados na comunicação.

Resumidamente, os fatores contribuintes (atrasos) para a latência de rede são:

Atraso na Propagação: Tempo necessário para a propagação do sinal elétrico, óptico ou de rádio frequência no meio sendo utilizado (fibra óptica, satélite, coaxial) e é um parâmetro imutável onde o gerente de rede não tem nenhuma influência.

Uma vez que o pacote foi empurrado para dentro do enlace, o atraso de propagação é o tempo de viagem até o próximo nó. Este tempo é função da distância entre os nós e da velocidade de propagação do sinal no meio físico. A velocidade de propagação depende do meio físico (par trançado, fibra óptica, espectro eletromagnético, etc.) e é um pouco menor ou igual a velocidade da luz. Para distâncias pequenas, como num enlace entre dois sensores em uma rede sem fio, este atraso pode ser desprezível, ficando na ordem de poucos microssegundos. Para grandes distâncias, como num enlace de satélite, pode levar um tempo importante, da ordem de centenas de milissegundos.

Atraso na Transmissão: É o tempo necessário para que cada bit do pacote seja empurrado para dentro do enlace. Se o tamanho do pacote for S bits e a taxa de transmissão do enlace for T bits/seg, então o atraso de transmissão será S/T segundos. O tamanho do pacote introduz atraso, portanto, em uma transmissão, um pacote maior levará mais tempo para ser recebido do que um pacote menor.

Atraso devido ao Processamento nos Equipamentos (roteadores, *switches*, servidores de acesso remoto (RAS), *firewalls*, etc.): É o tempo necessário para examinar o cabeçalho do pacote, checar a integridade dos dados recebidos e determinar para onde o mesmo deverá ser encaminhado. Estes atrasos geralmente estão na ordem de microssegundos.

Cada nó leva tempo para examinar e possivelmente alterar o cabeçalho de um pacote (por exemplo, alterar a contagem de saltos no campo *time to live*).

Atraso de Fila: É o tempo que cada pacote espera em fila nos roteadores antes de ser encaminhado ao próximo enlace. Este atraso é variável e depende do tráfego na rede. Se a fila

estiver vazia e não houver outro pacote sendo transmitido o atraso é zero. Se há pacotes na fila o tempo de espera pode ser longo e pode chegar a ordem de milissegundos. Portanto, pela característica aleatória, esta parcela de atraso pode ser a mais relevante de todas.

Desta forma, o atraso total ou latência pode ser definido pela seguinte expressão matemática:

$$Atotal = Aproc + Afila + Atrans + Aprop$$

Onde:

- Atotal – Atraso total;
- Aproc – Atraso por processamento;
- Atrans – Atraso de transmissão;
- Aprop – Atraso na propagação.

5.3 Topologia

Nem todos os dispositivos no presente e no futuro próximo receberão acesso direto à Internet. Como sempre, todos os dispositivos estão conectados a uma rede, mas essa rede é diferente da compreensão tradicional da Internet. Muitos dispositivos (especialmente a Internet das coisas) não precisam de acesso constante à Internet, mas há aspectos importantes, como conexões confiáveis e consumo de energia que precisam ser observados.

Além disso, deve-se notar que a Internet das Coisas invariavelmente utiliza a Internet tradicional para transmissão e comunicação de dados. Independentemente da tecnologia e topologia utilizadas, esta conexão com a internet é feita através de *gateways*. Os *gateways* desempenham um papel fundamental em qualquer topologia de redes de IoT.

De forma resumida, estão descritas a seguir as topologias de rede mais tradicionais e as suas respectivas características.

Anel: Todos os nós são conectados um após o outro, todas as informações também passam um após o outro de um nó para o próximo, passando para o nó desejado. As informações são recebidas por todos os nós encontrados durante a transmissão de dados. Os dados podem se mover em diferentes direções do anel.

Linha: Parece um anel do qual um nó comum foi removido. Todas as informações vão para os nós um após o outro entre os nós.

Barramento: Cada nó é conectado a um único canal de troca de informações e transmitido, um após o outro, porque os dispositivos conectados levam os dados ao barramento. Por isso, é mais fácil conectar dispositivos a essa topologia, mas a velocidade permanece muito baixa. Essa topologia é adequada para sensores e para aplicações que não requerem alto *throughput*.

Estrela: Uma estrela, resumidamente, é uma conexão ponto-a-ponto em que todos os dispositivos estão conectados a um nó comum (*hub*). Muitas tecnologias utilizam esta topologia e, portanto, como resultado, isso se tornou um tipo de padrão para a maioria das redes de dispositivos. Um exemplo disso é o Wi-Fi.

Uma árvore é um caso especial de uma estrela, em que os nós de uma árvore podem ser um hub, um nó final ou um roteador.

Malha (*mesh*): Essa topologia não possui uma estrutura clara, porque vários nós podem interagir entre si. É a topologia típica para dispositivos sem fio sem fio. Um requisito importante para este tipo de topologia é a propriedade de auto-organização da rede (a capacidade de determinar automaticamente a topologia da rede e o caminho da transferência de dados).

As redes mais comuns para a Internet das Coisas são:

- Estrela (LoRaWAN, Sigfox, Wi-Fi);
- Celular ou Malha (ZigBee, 6LoWPAN).

Diferentes aplicações podem requerer topologias específicas, dadas as características técnicas, arquitetura e até mesmo distribuição geográfica dos dispositivos. É importante avaliar os impactos que cada topologia irá impor aos requisitos de qualidade do serviço e desempenho das redes.

5.4 *Overhead*

O envio confiável de uma carga útil de dados através de uma rede de comunicações requer o envio de mais do que apenas a própria carga útil. Envolve também o envio de vários dados de controle e sinalização necessários para alcançar o destino. Isso cria um *overhead* de

protocolo, uma vez que os dados adicionais não contribuem para o significado intrínseco da mensagem (dados da aplicação).

O *overhead* de protocolo pode ser expresso como uma porcentagem de bytes de não aplicação (protocolo e sincronização de quadros) dividida pelo número total de bytes na mensagem.

5.5 Segurança

As aplicações de IoT e as áreas inteligentes lidam com muitos dados diariamente e esses dados são compartilhados entre os dispositivos. Informações sobre casas, prédios e carros são compartilhadas entre dispositivos o tempo todo. Toda essa informação exige um melhor sistema de gerenciamento. Os sistemas de segurança existentes não são adequados de várias maneiras e podem causar sérios problemas ao usuário. Um erro pode tornar a segurança doméstica, carros, prédios e dados salvos vulneráveis. Os crimes cibernéticos são possíveis devido a essas áreas de vulnerabilidade. (3. Comparative overview...)

Atualmente, a segurança é a maior preocupação para serviços baseados na Internet. Para tornar a IoT mais bem-sucedida no mercado de tecnologia, ela precisa estar em conformidade com um certo nível de padrão de segurança. Por exemplo, em uma casa inteligente, um detector de fumaça inteligente é instalado com *software* malicioso. Além disso, o detector de fumaça está conectado aos outros dispositivos eletrônicos domésticos. Se um *hacker* puder obter acesso não autorizado ao detector de fumaça inteligente, o invasor também poderá ter acesso a outros dispositivos. Portanto, todos os dispositivos IoT precisam atender a um determinado nível de padrões de segurança. O dispositivo IoT deve estar em conformidade com os seguintes requisitos de segurança:

- Controle de acesso e autenticação de dispositivo
- Privacidade dos usuários
- Segurança de dados
- Resiliência a ataques maliciosos
- Segurança da conexão
- Tolerância a falhas

Para obter acesso não autorizado aos dispositivos IoT, o invasor ou *hacker* pode atacar o sistema de rede de dentro ou de fora da rede. Os dispositivos IoT são dispositivos de baixo

custo; portanto, os operadores ou usuários da IoT precisam ter mais consideração sobre como implementarão a segurança nos dispositivos da IoT. (ae. Sigfox (Frame))

5.6 Consumo de energia

A Internet das Coisas (IoT) visa conectar pequenos dispositivos restritos à Internet através do protocolo IP, o que permite novos aplicativos de comunicação. O consumo de energia extremamente baixo é fundamental para os dispositivos de IoT, pois eles operam principalmente com baterias e precisam atingir uma vida útil da ordem de vários anos sem a substituição da bateria (MORIN E. et al., 2017).

Os dispositivos devem poder se comunicar com menos uso da bateria, porque esses dispositivos são implantados longe e precisam funcionar com baterias. Portanto, o consumo de energia deve ser no mínimo para o máximo de dias. Nos próximos anos, isso pode se tornar um grande problema nas IoTs. A eficiência em termos de potência é essencial; portanto, são necessários métodos eficientes de programação. A coleta de energia mecânica é uma parte necessária das IoTs (JAVED F. et al., 2018).

Entretanto, diferentemente das redes de sensores de IoT tradicionais, para aplicações em redes de monitoramento industriais, o consumo de energia tem uma prioridade mais baixa do que outras métricas de desempenho, como latência e *overhead*. Isto é explicado pela grande disponibilidade de fontes fixas de energia próximas aos dispositivos da rede, distribuídas em uma área geográfica reduzida. No entanto, o grau de importância do consumo de energia pode aumentar em aplicações em áreas extensas de cobertura, onde a disponibilidade de fontes fixas de energia é reduzida.

6. Estudo de Caso

Os quatro protocolos de redes de acesso de IIoT (LoRaWAN, Sigfox, 6LoWPAN e ZigBee), objetos de estudo deste trabalho, são amplamente utilizados para diversas aplicações de sensoriamento e monitoramento. Entretanto, essas tecnologias devem ser comparadas, inicialmente, de acordo com as suas características principais. Portanto, primeiramente serão comparadas as tecnologias de longa distância (LPWAN) – LoRaWAN e Sigfox e, posteriormente, as tecnologias de curto alcance, baseadas no padrão IEEE 802.15.4 – 6LoWPAN e ZigBee.

A partir da comparação dois a dois dessas tecnologias, será montada uma base comparativa única, com o resultado das quatro tecnologias juntas.

Entretanto, ao analisarmos não sob o aspecto da tecnologia, mas sim em casos de uso ou aplicações, é possível perceber diferenças que podem tornar uma solução mais adequada do que a outra.

Portanto, conforme definido nos objetivos deste trabalho, a seguir são apresentados os critérios que foram adotados para a análise de performance dessas tecnologias, no monitoramento de ativos industriais e manutenção preditiva.

Neste campo de aplicação, é importante ressaltar algumas premissas importantes:

- Os dispositivos finais são utilizados apenas para monitoramento e não controle;
- A distribuição geográfica dos dispositivos (área de cobertura) normalmente não ultrapassa 1 km²;
- Não há necessidade de monitoramento em tempo real;
- O tráfego de dados é baixo. São transmitidos, de tempos em tempos, apenas dados sobre o estado do equipamento ou componente monitorado.

6.1 Comparativo LoRaWAN *versus* Sigfox

A Tabela 5 exibe uma comparação das principais características entre as tecnologias de rede de longa distância LoRaWAN e Sigfox. Como pode ser visto na tabela, ambas as tecnologias possuem muitas características semelhantes: um alto alcance de comunicação, alta imunidade a ruído, baixa taxa de transferência de dados, baixo consumo de energia e, como resultado, um alto grau de autonomia dos dispositivos terminais.

Tabela 5 – Comparação das características técnicas das redes de longo alcance LPWAN

Parâmetros	LoRaWAN	Sigfox
Alcance	Até 30 Km (campo) 3 – 5 Km (urbano)	30 – 50 Km (campo) 3 – 10 Km (urbano)
Consumo de Energia	200 nA (modo "*sleep*") 40 mA (em operação)	350 nA (modo "*sleep*") 10 mA (em operação)
Throughput	0,3 – 3,75 kbps	100 bps
Latência	500 ms	2 s
Largura de Banda	UWB (até 250 KHz)	UNB (100 Hz)
Frequência	868,8 MHz (Europa) 915 MHz (América) 433 MHz (Asia)	868,8 MHz (Europa) 915 MHz (América)
Imunidade ao ruído	Alta	Alta
Vida da Bateria	~ 10 anos	~ 20 anos
Segurança	AES-64 e 128 bits	AES com HMAC (*Hash-based Message Authentication Code*)
Suporte	LoRa Alliance, IBM e Cisco	Sigfox e Samsung

Fonte: Autor.

6.1.1 *Throughput*

Ambas as tecnologias Sigfox e LoRaWAN possuem uma taxa de dados de apenas alguns bits por segundo, respectivamente 100 bps e 300 – 3.750 bps. Isto é uma característica marcante das tecnologias LPWAN, pois os dispositivos finais passam a maior parte do tempo "dormindo", acordando apenas para o envio de pequenas informações, e privilegia a economia de bateria.

Entretanto, há uma importante diferença entre as duas tecnologias, que coloca as redes Sigfox em grande desvantagem, pois nestas há um limite diário de 140 mensagens de *uplink* partindo dos dispositivos finais. Já nas redes LoRaWAN, o número de mensagens é ilimitado.

6.1.2 Topologia

As hierarquias de ambas as tecnologias são bastante semelhantes. Utilizam *gateways* ou *hubs* para direcionar os dados dos dispositivos finais para servidores de rede, formando assim uma topologia em estrela. O alcance dos dispositivos finais é da ordem de quilômetros e um único *gateway* pode conectar-se a milhares destes dispositivos, fazendo com que a comunicação entre eles seja quase desnecessária.

Entretanto, a grande diferença entre as tecnologias Sigfox e LoRaWAN está na interface entre as camadas de rede e aplicação, pois enquanto na última é possível fazer conexões "transparentes" dos *gateways* com servidores de rede por meio de IP padrão, e então utilizar os dados em qualquer aplicação, em redes Sigfox isto depende de provedor local (no Brasil é a WND) para fornecer este serviço (*Sigfox Support Service*) e disponibilizar os dados para as aplicações. Portanto é necessário identificar se há cobertura deste serviço na localidade onde será implementado o projeto da nova rede. Além disso, o Sigfox controla as próprias estações base, enquanto o LoRA permite que qualquer usuário configure uma rede. Diferentemente da Sigfox, LoRaWAN não é uma tecnologia proprietária e sim aberta. Portanto, podem ser utilizadas soluções para os servidores de rede e de aplicação que mais se adequam às necessidades do projeto.

A camada *Sigfox Support System* constitui a rede principal sendo encarregada de processar as mensagens e enviá-las através de *callbacks* para o sistema do cliente. Esta camada fornece também o ponto de entrada para os diferentes atores do ecossistema (operadores Sigfox, canais Sigfox e clientes finais) para interagir com o sistema através de interfaces de atendimento na *web* ou APIs (*Application Programming Interface* – Interface de Programação de Aplicativos).

A arquitetura de rede LoRaWAN é implantada de forma que os dispositivos finais (*end nodes*) conectam-se aos *gateways* formando uma topologia em estrela. Por padrão, apesar dos dispositivos LoRa suportarem comunicação bidirecional com os *gateways*, normalmente não há comunicação entre dispositivos. Os *gateways* são conectados ao servidor de rede por meio de conexões IP padrão e simplesmente convertem pacotes RF (Rádio Frequência) em pacotes IP e vice-versa. O servidor de rede é encarregado de enviar os pacotes para os respectivos servidores de aplicação que utilizarão estes dados.

Na prática, como regra, os serviços do provedor de serviços são fornecidos pelo fabricante do nó final, que suporta o serviço de processamento de dados, no qual os pacotes do servidor de rede LoRaWAN são roteados para trabalhar com esses dados para os usuários finais.

Uma das grandes diferenças entre Sigfox e LoRaWAN é que o Sigfox controla as próprias estações base, enquanto o LoRaWAN permite que qualquer pessoa configure uma rede.

Com a Sigfox gerenciando sua própria rede, eles têm algum controle sobre aspectos como quantos nós podem se conectar e a localização das estações base.

6.1.3 Latência

Ambas as tecnologias não são indicadas para aplicações que requerem baixa latência, como, por exemplo, envio de áudio e monitoramento em tempo real. No entanto, a aplicação em redes de sensores para o monitoramento (não contínuo) de condição de equipamentos industriais é muito tolerante no que diz respeito à latência.

Entretanto, ao contrário do Sigfox, o LoRa (camada física de redes LoRaWAN) fornece dispositivos classe C para obter baixa latência no envio bidirecional de pacotes. Em contrapartida, isto se dá à custa do aumento do consumo de energia dos dispositivos. Portanto, para aplicações onde a latência não seja um requisito e não haja grande quantidade de dados para enviar, ambas as tecnologias são boas opções.

Outra característica dessas redes é que a operação determinística não pode ser garantida, aumentando assim a latência, se comparada a outras tecnologias comumente encontradas nos ecossistemas industriais (DeviceNet, ControlNet, etc.). Isto se dá, pois, o acesso ALOHA está sujeito a uma contenção que afeta a instabilidade da rede. Apesar disso, pequenas redes LoRaWAN podem fornecer serviços adequados para aplicativos que exigem, por exemplo, amostragem de dados a cada segundo.

6.1.4 *Overhead*

Neste requisito, as tecnologias foram comparadas apenas com relação ao *overhead* gerado entre as camadas física (PHY) e de acesso ao meio (MAC).

O LoRaWAN incorpora ao pacote da camada MAC um *overhead* adicional fornecido pelos dispositivos das classes A, B e C. Essas "despesas" incluem cabeçalhos, comandos e verificações de integridade da mensagem. Ao combinar as "despesas" gerais, o LoRaWAN impõe entre 13 e 27 bytes de *overhead* em cada pacote transmitido por um nó final, sendo o *payload* máximo da camada MAC de 22 bytes.

No LoRa (camada física das redes LoRaWAN), a "Taxa de Código" (*Coding Rate*) refere-se ao código de correção de erro de encaminhamento adicionado a um pacote antes da transmissão. LoRa utiliza o código de Hamming como o código de correção de erro de avanço usado no CR (*Coding Rate*). A configuração CR de 4/5 indica que a cada quatro bits de dados, um bit de código de correção será adicionado e, posteriormente, CR 4/8 refere-se a quatro bits de dados com quatro bits de correção adicionais. O CR induz *overhead* para a transmissão

aumentando o número de bits a serem transmitidos. Esta funcionalidade permite que o receptor verifique a exatidão dos dados recebidos e fornece a possibilidade de corrigir alguns bits errados, entretanto ao custo da elevação do *overhead*.

Em contrapartida, a tecnologia SigFox usa pacotes pequenos. Com um *payload* máximo de 12 bytes (*uplink*), o tamanho total do quadro é de apenas 26 bytes na camada MAC. Portanto o *overhead* do protocolo é significativamente reduzido.

6.1.5 Segurança

Tanto LoRaWAN quanto Sigfox permitem a utilização de chaves de criptografia de 128 bits baseadas no protocolo AES (*Advanced Encryption Standard*).

Entretanto, LoRaWAN utiliza duas camadas de criptografia de 128 bits através das chaves exclusivas de sessão de rede (compartilhada entre o dispositivo final e o servidor de rede) e sessão de aplicação (compartilhada de ponta a ponta no nível de aplicação).

A chave de sessão de aplicação é usada para criptografia e decriptografia de dados. Uma operação XOR é usada para criptografar cada mensagem e também usa um fluxo de chaves gerado pela chave de sessão de rede, chave de sessão de aplicação e contador de mensagens de *uplink* e *downlink* para gerar carga útil criptografada. Mas o tamanho da mensagem antes e depois da criptografia é o mesmo e fornece uma oportunidade para a entidade mal-intencionada recriar o fluxo de chaves da mensagem criptografada. Apesar do mecanismo de segurança, os dispositivos LoRaWAN são suscetíveis a ataques (CHACKO S. e JOB D., 2018).

Em algumas redes celulares tradicionais, o tráfego é criptografado pela interface aérea, mas é transportado como texto simples na rede principal do operador. Redes Sigfox se assemelham muito a redes celulares, sendo inclusive os serviços de rede (incluindo segurança) prestados pelos operadores Sigfox em cada região (WND no Brasil). A segurança em redes Sigfox é realizada através de protocolos proprietários, ao invés de protocolo de internet usual (IP). Isso dificulta, por exemplo, que *hackers* possam endereçar dispositivos finais para obter acesso à rede. Entretanto, a criptografia realizada na camada de aplicação é de responsabilidade do usuário.

Nas redes Sigfox, os dispositivos operam predominantemente *offline*, com um comportamento *built-in*. Quando o Sigfox precisa transmitir ou receber dados da Internet, o dispositivo transmitirá uma mensagem de rádio. Essa mensagem transmitida é recebida pelas estações base e a mensagem é então transmitida à rede principal da Sigfox, que é entregue às

aplicações IoT correspondentes. Essa arquitetura de rede da Sigfox fornece uma lacuna de ar e não é possível acessar um dispositivo final através da Internet de maneira maliciosa.

Em Sigfox, cada dispositivo é fornecido com uma chave de autenticação simétrica exclusiva durante o processo de fabricação. Se um dos dispositivos estiver comprometido, ele poderá causar um impacto limitado na rede. Um *token* criptográfico é calculado usando essa chave de autenticação para cada mensagem de envio ou recebimento. Este *token* é usado para autenticação do remetente e integridade da mensagem. Para detectar as tentativas de reprodução, a rede principal da Sigfox usa um contador de sequência contido em cada mensagem (CHACKO S. e JOB D., 2018). Com isso, comparativamente, Sigfox é umas das tecnologias LPWAN mais seguras.

6.1.6 Consumo de energia

E. Morin et al. (MORIN e. et al., 2017), no seu trabalho, compararam as tecnologias LoRaWAN, Sigfox, *Bluetooth Low Energy* (BLE), IEEE 802.15.4 e IEEE 802.11quanto à vida útil esperada dos dispositivos, utilizando um analisador que computa o consumo de energia nos estados *Sleep*, *Idle*, Tx e Rx. Os resultados mostraram que, comparativamente, LoRaWAN obteve melhores resultados do que Sigfox, para tráfegos de dados ultrabaixos. Sigfox obteve resultados semelhantes aos de LoRaWAN apenas para tamanhos de dados muito pequenos. Portanto, para a aplicação em redes de monitoramento de ativos industriais, onde tanto o tráfego de dados quanto o tamanho dos pacotes são reduzidos, é possível admitir que ambas as tecnologias possuem desempenhos equivalentes.

6.2 Comparativo 6LoWPAN *versus* ZigBee

Tanto ZigBee, quanto 6LoWPAN, foram projetados para aplicações de baixo *throughput* e alimentados por bateria.

O 6LoWPAN resolve vários problemas associados às redes de sensores sem fio, como, por exemplo, a padronização da operação da rede e o acesso aos dados da rede. Ao contrário do padrão ZigBee, o 6LoWPAN estende a padronização quase ao nível de tarefas aplicadas, resolvendo simultaneamente problemas com a integração de pequenos nós sem fio em redes IP.

O 6LoWPAN é relativamente novo no mercado e suas características o tornam ideais para mercados como automação residencial ou industrial com sensores e atuadores,

monitoramento e controle de iluminação pública, medição inteligente de eletricidade e aplicativos IoT típicos com dispositivos conectados à Internet. Como já falado anteriormente, 6LoWPAN utiliza a banda de 2,4 GHz e a banda sub-gigahertz, com base no padrão do IEEE 802.15.4, incluindo suporte para a topologia de grandes redes *mesh*, com transferência de dados confiável e baixo consumo de energia.

A Tabela 6 exibe uma comparação das principais características entre as tecnologias de rede de baixa potência 6LoWPAN e ZigBee.

Tabela 6 – Comparação das características técnicas das redes WPAN.

Parâmetros	6LoWPAN	ZigBee
Alcance	10 – 100 m	10 – 100 m
Consumo de Energia	< 1 µA (modo "sleep") 25 mA (em operação)	< 1 µA (modo "sleep") 30 mA (em operação)
Throughput	250 kbps	250 Kbps
Largura de Banda	WPAN	WPAN
Frequência	868 MHz (EU) 915 MHz (USA) 2,4 GHz	2,4 GHz
Imunidade ao ruído	Alta	Alta
Vida da Bateria	~ 2 anos	~ 20 anos
Segurança	AES-128 bits	AES-128 bits
Suporte	Thread	ZigBee Alliance

Fonte: Autor.

6.2.1 *Throughput*

Ambos são baseados no protocolo IEEE 802.15.4 e possuem *throughput* fixo em 250 kbits/s.

6.2.2 Topologia

No que diz respeito à hierarquia dos dispositivos da rede, existem algumas semelhanças entre as arquiteturas de ambas as tecnologias. No ZigBee, os dispositivos são divididos em "Coordenador", "Roteador" e "Dispositivo Final" (*End Node*). Já no 6LoWPAN, os dispositivos são divididos em "*Hosts*", "Roteadores" e "Roteadores de Borda". Estes últimos

desempenham um papel fundamental na comunicação de redes 6LoWPAN com redes IPv6 (Internet), pois são baseados em IP.

Uma diferença importante estre essas tecnologias é que redes ZigBee (ou outras redes proprietárias) exigem *gateways* para executar aplicações complexas. Esses *gateways* de aplicação devem entender qualquer perfil de aplicação que possa ser usado na rede e quaisquer alterações nos protocolos de aplicação nos nós sem fio também devem ser acompanhadas por alterações no *gateway*. Em contraste, os roteadores baseados em IP nos limites da rede, como os roteadores de borda, são independentes dos protocolos de aplicação usados no 6LoWPAN. Isso reduz o *overhead* nos roteadores de borda, permitindo assim o uso de dispositivos embarcados com baixo custo, *software* mais simples e *hardware* menos sofisticado.

Quanto ao número de dispositivos possíveis, nas redes ZigBee o limite é de 65.000, enquanto em redes 6LoWPAN este número é da ordem de 2^{64}. Isto faz com que a escalabilidade da rede utilizando 6LoWPAN seja muito mais simples.

As topologias em "malha" ou "*clusters* de malhas" são as mais comuns em redes industriais de sensores. Tanto ZigBee quanto 6LoWPAN suportam as topologias em "estrela" e "malha" (*mesh*). Entretanto, somente ZigBee suporta redes com topologia tipo "*cluster* de malhas". A desvantagem para esta topologia é o custo, pois quase todos os dispositivos devem ter funcionalidade completa (FFD).

6.2.3 Latência

Tanto ZigBee quanto 6LoWPAN utilizam CSMA/CA como protocolos de controle de acesso ao meio (MAC), baseado no padrão IEEE 802.15.4. Entretanto, protocolos de comunicação baseados em contenção, como o CSMA, não conseguem fornecer garantia de tempo ao entregar mensagens e são propensos a perda de pacotes. Portanto, ambos ZigBee e 6LoWPAN não são adequados para aplicações que exigem entrega confiável de pacotes. Entretanto, para a aplicação em redes de sensores para o monitoramento de condição de equipamentos industriais, as exigências de latência e confiabilidade na entrega de pacotes são muito tolerantes.

Para reduzir a latência na entrega de pacotes, principalmente em situações de alto tráfego, o ZigBee pode variar o comprimento dos *superframes* utilizando balizas. Um *superframe* de período mais curto resulta em menor latência na entrega de pacotes e maior utilização da largura de banda, mas resulta em maior consumo de energia, enquanto um *superframe* de período mais longo tem o efeito oposto. Outro fator importante é o tipo de

roteamento utilizado na camada de rede, que pode aumentar consideravelmente a latência na entrega de pacotes. Isso se dá devido ao algoritmo *ad hoc on-demand distance vector* (AODV), no qual os próprios dispositivos são responsáveis pela descoberta de rotas. A latência em redes ZigBee pode facilmente atingir dezenas de milissegundos (ZAND P. et al., 2012 e LI X. et al., 2008).

Já o 6LoWPAN, utiliza uma subcamada de adaptação entre as camadas MAC/PHY e NWK, o que permite o roteamento utilizando endereços IPv6. O roteamento no modo *unreliable* pode atingir latências entre 2 e 6 ms (para endereços MAC de 16 bits e frequência de 2,4 GHz) (MULLIGAN G. e BORMANN C., 2008). Portanto, comparativamente, 6LoWPAN fornece menores valores de latência na entrega de pacotes em relação ao ZigBee.

6.2.4 *Overhead*

Bem como a latência, o *overhead* de roteamento pode ser considerado um requisito para o roteamento em redes de sensores e, portanto, base de comparação entre diferentes tecnologias.

Na Tabela 7, é comparado o *overhead* gerado pelos protocolos ZigBee e 6LoWPAN, considerando uma carga útil de 20 bytes, ambiente estático e tráfego *unicast*. O *overhead* é maior na rede 6LoWPAN do que na rede ZigBee (BURATTI C. et al., 2016).

Tabela 7 – *Overhead:* Comparação entre protocolos.

Protocolo	Pacotes: 1 salto	Pacotes: 2 saltos	Bytes: 1 salto	Bytes: 2 saltos
ZigBee	4,7	8,7	6,5	11,4
6LoWPAN	6,2	9,5	10,9	16,8

Fonte: BURATTI C. et al., 2016.

Referindo-se ao *overhead* em número de bytes, a diferença também é percebida, já que cabeçalhos ZigBee são mais curtos do que 6LoWPAN (BURATTI C. et al., 2016).

6.2.5 Segurança

Ambas as tecnologias utilizam chaves de criptografia de 128 bits (AES-128) para a comunicação na camada de enlace.

Entretanto, por ser baseado em IP, 6LoWPAN utiliza TCP/IP como protocolo da camada de transporte. Portanto, além da segurança da camada de enlace, 6LoWPAN também utiliza o mecanismo de segurança da camada de transporte (TLS – *Transport Layer Security*). O TLS, conforme definido no RFC 5246, é executado por meio do TCP, aumentando assim ainda mais a segurança na troca de mensagens, se comparado ao ZigBee e outras tecnologias de IoT.

6.2.6 Consumo de energia

O padrão IEEE 802.15.4 foi desenvolvido especialmente para aplicações de baixo consumo de energia. Entretanto, 6LoWPAN (*IPv6 Over Low Power Wireless Personal Area Networks*), que utiliza o protocolo de internet sobre o padrão 802.15.4, apresenta um desempenho no consumo de energia inferior, se comparado com outras tecnologias baseadas no mesmo padrão (ZigBee, por exemplo).

Como esperado, o *overhead* causado pelo cabeçalho IPv6 nas redes 6LoWPAN, comparativamente, requerem mais processamento e provocam maior "esforço" de roteamento dos dispositivos, principalmente quando o protocolo de transporte utilizado é o TCP/IP.

Portanto, ZigBee possui melhor eficiência no consumo de energia se comparada à 6LoWPAN.

O trabalho de E. Morin et al. (MORIN e. et al., 2017) também menciona o melhor desempenho das tecnologias baseadas no padrão IEEE 802.15.4, se comparadas às tecnologias de longo alcance (LoRaWAN e Sigfox). Portanto, é possível concluir que, dentre as quatro tecnologias estudadas neste trabalho, ZigBee é que apresenta o melhor desempenho no consumo de energia na aplicação em redes de monitoramento de ativos industriais.

6.3 Resumo da análise comparativa

Para realizar a comparação qualitativa dos critérios entre as quatro tecnologias, foi adotada uma escala numérica de 1 a 5, em que 1 é a pior nota e 5 é a melhor nota. Portanto, por exemplo, um *Throughput* que obteve nota 4 é melhor, comparativamente, do que outro que obteve nota 3.

Semelhantemente, para que fosse possível obter a mesma base de comparação entre os seis critérios (*throughput*, latência, topologia, *overhead*, segurança e consumo de energia), os

critérios de latência, *overhead* e consumo de energia foram substituídos, respectivamente por "baixa latência", "baixo *overhead*" e "baixo consumo de energia". Dessa forma, uma "baixa latência" que obteve nota 3 é melhor, comparativamente, do que outro que obteve nota 2.

Portanto, a seguir, são apresentados os gráficos de barras que resumem a pontuação de cada tecnologia nos seis critérios selecionados (Figura 23).

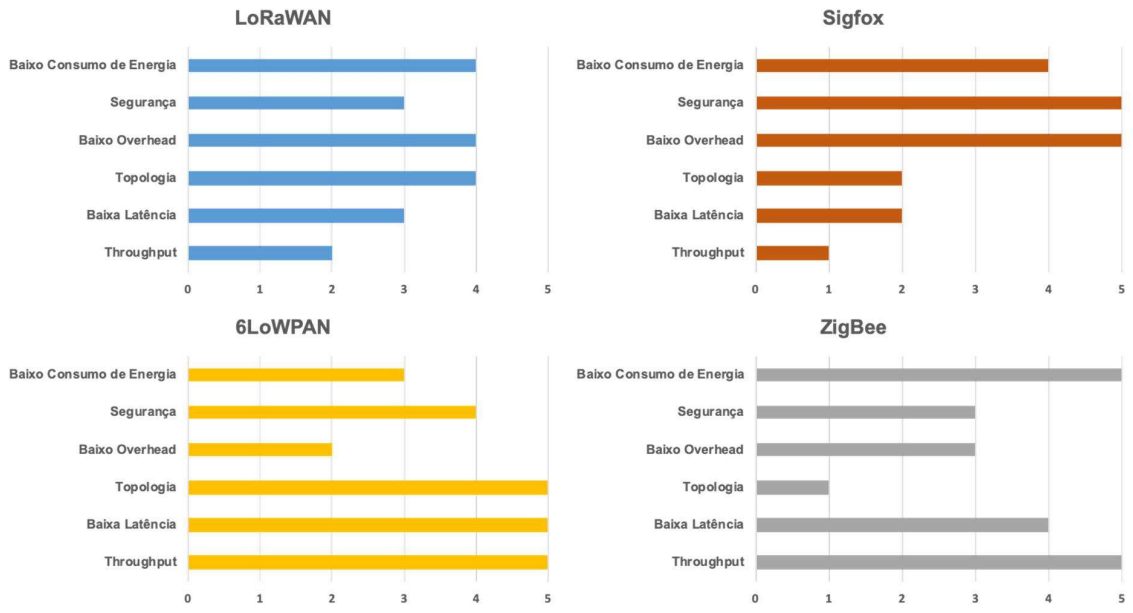

Figura 23 – Gráficos resumo da análise comparativa entre as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN.

Fonte: Autor.

Obtendo a melhor pontuação em três dos seis critérios (3/6), a partir da bibliografia estudada, 6LoWPAN demonstrou ser a melhor escolha para aplicações em monitoramento de ativos e equipamentos industriais.

A Figura 24 a seguir resume graficamente o desempenho das tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN nos critérios de *throughput*, latência, topologia, *overhead*, segurança e consumo de energia.

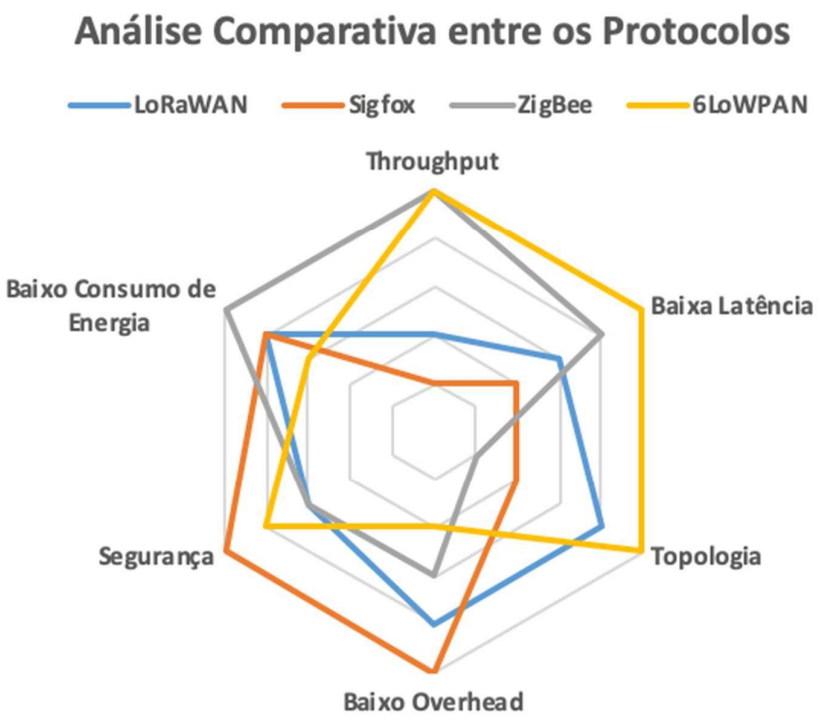

Figura 24 – Gráfico de radar da análise comparativa entre as tecnologias LoRaWAN, Sigfox, ZigBee e 6LoWPAN.

Fonte: Autor.

7. Conclusão

A análise revelou que cada tecnologia tem muitas vantagens e características que a destacam individualmente, portanto nenhuma das opções estudadas pode ser descartada e tem um lugar no mundo moderno da tecnologia.

Na implementação de soluções de IIoT, as aplicações serão muito mais relevantes do que o tipo de rede, pois essa ainda permanecerá sem padronização por muito tempo. As tecnologias são apenas ferramentas. Portanto, devem ser escolhidas aquelas tecnologias que resolvem os problemas propostos, levando em consideração as características específicas de cada aplicação.

Neste trabalho, o campo de aplicação é o monitoramento de ativos industriais para a implementação de manutenção preditiva e gestão de ativos. Portanto, a partir da análise comparativa das tecnologias LoRaWAN, Sigfox, 6LoWPAN e ZigBee, descritas na bibliografia estudada, aquela que se mostrou mais adequada e reúne mais características favoráveis para esta aplicação foi 6LoWPAN, obtendo a melhor pontuação em três dos seis critérios primordiais para o monitoramento de ativos e que foram selecionados para a comparação.

Além das características abordadas neste trabalho, outra grande vantagem da tecnologia 6LoWPAN, se comparada às demais, é a conexão praticamente direta de dispositivos à internet, por meio de endereços IPv6. Isto facilita muito a utilização dos dados coletados por aplicações nas camadas mais superiores da rede, por exemplo, por softwares APMs (*Asset Performance Management*) ou ERPs (*Enterprise Resource Planning*).

Ainda vale ressaltar que, para muitos casos de aplicação, também há a possibilidade de soluções mistas, que combinam mais de uma tecnologia. Por exemplo, por possuir uma infraestrutura mais flexível do que as demais, LoRaWAN pode ser combinada a outras tecnologias na camada de rede.

Trabalhos futuros podem utilizar critérios diferentes para comparar estes protocolos de comunicação. Tais critérios incluem perda de pacotes, alcance, tipo de criptografia, tipo de modulação e coexistência com outros protocolos e dispositivos. Outra oportunidade a ser estudada é a interferência de alguns destes protocolos de IoT com outras tecnologias comumente encontradas nos ambientes industriais, tais como redes celulares, Wi-Fi e rádios de comunicação.

Referências Bibliográficas

ALENA R., GILSTRAP R., BALDWIN J., STONE T. AND WILSON P. Fault Tolerance in ZigBee Wireless Sensor Networks. IEEEAC Paper #1480, Version I, Updated December 9, 2010.

AL-SARAWI S., ANBAR M., ALIEYAN K. AND ALZUBAIDI M. Internet of Things (IoT) Communication Protocols: Review. 8th International Conference on Information Technology (ICIT) 2017.

ARAS E., RAMACHANDRAN G. S., LAWRENCE P. AND HUGHES D. Exploring The Security Vulnerabilities of LoRa. 2017. iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium.

BARSKOV A. “IIoT: da visão aos projetos". Network Solutions Journal/LAN (Editora "Sistemas abertos"), N° 12, 2016.

BONAVOLONTÀ F., TEDESCO. A, MORIELLO R. S. L. AND TUFANO A., Enabling wireless technologies for Industry 4.0: State of the Art. IEEE, 2017.

BURATTI C., STAJKIC A., GARDASEVIC G., MILARDO S., ABRIGNANI M. D., MIJOVIC S., MORABITO G. AND VERDONE R., “Testing Protocols for the Internet of Things on the EuWIn Platform”. IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 1, FEBRUARY 2016.

CASALS L., MIR B., VIDAL R. AND GOMEZ C. Modeling the Energy Performance of LoRaWAN. 2017. Sensors 2017, 17, 2364.

CENTENARO M., VANGELISTA L., ZANELLA A., AND ZORZI M., “Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios”. IEEE Wireless Communications, vol. 23, pp. 60–67, October 2016.

CHACKO S. AND JOB D., “Security mechanisms and vulnerabilities in LPWAN”, IOP Conference Series: Materials Science and Engineering 396, 2018.

FUJDIAK R., BLAZEK P., MIKHAYLOV K., MALINA L., MLYNEK P., MISUREC J., AND BLAZEK V., “On track of sigfox confidentiality with end-to-end encryption,” in Proceedings of the 13th International Conference on Availability, Reliability and Security, p. 19, ACM, 2018.

G. A. AKPAKWU et al.: Survey on 5G Networks for the IoT: Communication Technologies and Challenges, 2018.

GENERAL ELECTRICS DIGITAL. See How SSE Achieved Greater Plant Reliability. 13 de Janeiro de 2016. Disponível em: < https://www.ge.com/power/case-studies/sse>. Acesso em: 20 de outubro de 2018.

GLÓRIA A., CERCAS F., SOUTO N., South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2017.

HEMJAL A.: Sigfox based Internet of Things: Technology, Measurements and Development Master of Science thesis Tampere University Master’s Degree Programme in Electrical Engineering May, 2019.

HONG ZH., BINGWU L. E PINGPING D. The Technology System Framework of the Internet of Things and Its Application Research in Agriculture. Daoliang Li; Yingyi Chen. 5th Computer and Computing Technologies in Agriculture (CCTA), October 2011, Beijing, China. Springer, IFIP Advances in Information and Communication Technology, AICT-368 (Part I), pp.293-300, 2012.

IGLESIAS-URKIA M., ORIVE A., BARCELO M., MORAN A., BILBAO J. AND URBIETA A. Towards a lightweight protocol for Industry 4.0: An implementation-based benchmark. Ikerlan Technology Research Centre, Information and Communication Technologies Area, 2017.

JAVED F., AFZAL M. K., SHARIF M. AND KIM B., “Internet of Things (IoT) operating systems support, networking technologies, applications and challenges: A comparative review”. IEEE Communications Surveys & Tutorials, vol. 20, No. 3, Third quarter 2018.

KAUR J. AND KAUR K. Availing Internet of Things in Industrial decision making — A survey. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) 2016.

LI X., FANG K., GU J. AND ZHANG L. An Improved ZigBee Routing Strategy for Monitoring System. First International Conference on Intelligent Networks and Intelligent Systems, 2008.

LORA-ALLIANCE. Disponível em: < https://lora-alliance.org/about-lorawan >. Acesso em: 15 de junho de 2019.

LORAWAN SPECIFICATION, LoRa Alliance, c2018, ver. 1.0.3.

MEKKI K., BAJIC E., CHAXEL F. AND MEYER F. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express 5, 2019.

MORIN E., MAMAN, M., GUIZZETTI R. AND DUDA A., "Comparison of the Device Lifetime in Wireless Networks for the Internet of Things". IEEE Access, vol. 5, 2017.

MULLIGAN G. AND BORMANN C. IPv6 over Low power WPAN WG (6lowpan). 73rd IETF, 2008.

N. POURSAFAR, M. E. E. ALAHI, AND S. MUKHOPADHYAY, "Long-range wireless technologies for iot applications: a review," in 2017 Eleventh International Conference on Sensing Technology (ICST), pp. 1–6, IEEE, 2017.

OLSSON J., "6LoWPAN demystified", 2014, Texas Instruments.

PONTE F. e LIM G. F., "Critérios para comparação entre redes industriais – Ethernet, Controlnet e Devicenet". XIV edição da Conferência Brasileira de Dinâmica, Controle e Aplicações (DINCON), 2019.

QU B., JING X., WANG X., LI Y. AND LIANG Y. Design on Cucumber Traceability System Based on the Internet of Things. In: Li D., Chen Y. (eds) Computer and Computing Technologies in Agriculture V. CCTA 2011. IFIP Advances in Information and Communication Technology, vol 368. Springer, Berlin, Heidelberg.

SHELBY Z. e BORMANN C. 6LoWPAN: A Internet sem fio embutida. John Wiley & Sons Ltd. 2009. 245 s.

SIGFOX, “Make things come alive in a secure way,” tech. rep., Sigfox, 2 2017.

SIGFOX TECHNICAL OVERVIEW, 2017

SOIJOYO S. AND ASHARI A. Analysis of Zigbee Data Transmission on Wireless Sensor Network Topology. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 9, 2017.

ZAND P., CHATTERJEA S., DAS K. AND HAVINGA P. Wireless Industrial Monitoring and Control Networks: The Journey So Far and the Road Ahead. Journal of Sensor and Actuator Networks, 2012.

ZHOU L., SONG L. XIE C. ZHANG J. Applications of Internet of Things in the Facility Agriculture. In: Li D., Chen Y. (eds) Computer and Computing Technologies in Agriculture VI. CCTA 2012. IFIP Advances in Information and Communication Technology, vol 392. Springer, Berlin, Heidelberg.