

UNIVERSIDADE PAULISTA

AGNALDO DO NASCIMENTO PEREIRA

PROTOCOLOS DE COMUNICAÇÃO PARA INTERNET DAS COISAS

LIMEIRA- SP

2018

Agnaldo do Nascimento Pereira

PROCOLOS DE COMUNICAÇÃO PARA INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharel em Ciências da Computação da Universidade Paulista como requisito parcial para a obtenção do título de Cientista da Computação.

Orientador: Profº Marcos V. Gialdi

Co-Orientador: Profº Antônio Matheus

LIMEIRA - SP

2018

Agnaldo do Nascimento Pereira

PROTOCOLOS DE COMUNICAÇÃO PARA INTERNET DAS COISAS

Relatório final, apresentado à Universidade Paulista, como parte das exigências para a obtenção do título de Cientista da Computação.

Limeira, São Paulo, ___ de _____ de ___

BANCA EXAMINADORA

Profº-----

Profº -----

Aos meus amigos, pelas alegrias, tristezas e dores compartilhadas. Com vocês, as pausas entre um parágrafo e outro de produção melhora tudo o que tenho produzido na vida.

AGRADECIMENTOS

Meus agradecimentos vão em especial para os professores Antônio Matheus, Amaury André e Marcos Gialdi por proporcionar uma nova oportunidade de estar apresentando este Trabalho de Conclusão de Curso após três anos e meio distante do meio acadêmico.

Agradeço também aos novos colegas de classe por compartilharem ideias e críticas construtivas à construção e apresentação deste, dando uma noção e preparação para a banca efetivamente.

*“Se fosse fácil achar o caminho das pedras,
tantas pedras no caminho não seriam ruins.”*

Engenheiros do Hawaii - Outras Frequências

RESUMO

Internet das coisas vem se despontando como uma área em grande ascensão. A conexão de dispositivos à internet é um tema muito procurado em sites de pesquisa por profissionais e aspirantes a desenvolvedores de novas ferramentas e tecnologias, no entanto a maior parte da busca se foca em tecnologias que fazem uso de protocolos que se focam na parte final da comunicação, o envio das informações aos servidores. Fazendo uma busca mais aprofundada no tema descobre-se que existem protocolos com focos distintos desde a comunicação em seu mais baixo nível, 0 e 1, em rede cabeada ou sem fio, protocolos focados em estratégias de roteamento e endereçamento, até o nível onde a informação já possui um formato legível ao ser humano e é mais fácil a implementação de customizações. Não existe um protocolo que trabalhe sozinho nesse processo, eles se comunicam dentro de uma hierarquia de camadas. As redes para a conexão de dispositivos à internet também não precisam ser únicas, um projeto pode se fazer valer das melhores características de cada protocolo e topologia de rede nas quais são integrados para melhor aproveitamento de recursos.

ABSTRACT

The Internet of Things is an area in fast rise. Connecting devices to the Internet is a highly researched topic by professionals and aspiring developers of new tools and technologies, but most of the research focuses on technologies that make use of protocols focused on the final part of the communication, sending the information to the servers. Further research on the subject reveals that there are protocols with different focuses of communication, from the lowest level, 0 and 1, in wired or wireless networks, protocols focused on routing and addressing strategies, to the level at which the information already has a readable format and it is easier to implement customizations. There is no protocol that works alone in this process, they communicate within a hierarchy of layers. Networks for connecting devices to the Internet also do not have to be unique, a project can make use of the best features of each protocol and network topology in which they are integrated for a better use of the resources.

LISTA DE SIGLAS

6LoWPAN - IPv6 over Low power Wireless Personal Area Networks
AMQP - Advanced Message Queuing Protocol
BLE - Bluetooth Low Energy
CARP - Routing Protocol for Low Power and Lossy Networks
CoAP - Constrained Application Protocol
CORPL - Cognitive Routing Protocol for Low Power and Lossy Networks
DAG - Directed Acyclic Graph
DECT/ULE - Digital Enhanced Cordless Telecommunications Ultra Low Energy
DODAG - Destination Oriented Directed Acyclic Graph
G.9959 - Short range narrow-band digital radiocommunication transceivers
IEEE - Institute of Electrical and Electronics Engineers
IOT - Internet of Things
IP - Internet Protocol
IPv6 - Internet Protocol Version 6
LoRa - Long Range
LoRaWAN - Long Range Wide Area Network
LTE-A - Long Term Evolution Advanced
MAC - Media Access Control Layer
MQTT - Message Queuing Telemetry Transport
OSI - Open System Interconnection
RPL - Routing Protocol for Low Power and Lossy Networks
SMQTT - Secure Message Queuing Telemetry Transport
ULE - Ultra Low Energy
XMPP - Extensible Messaging and Presence Protocol

Sumário

1. INTRODUÇÃO	12
2. OBJETIVO	13
2.1. Objetivo Geral	13
2.1. Objetivo Específicos	13
3. METODOLOGIA	14
4. INTERNET DAS COISAS	15
4.1. Aplicações	15
4.2. Expansão	17
4.3 Segurança	17
5. PROTOCOLO DE COMUNICAÇÃO	18
6. MODELO OSI	19
6.1. Camada de Física	20
6.2. Camada de Dados ou Enlace	20
6.3. Camada de Rede	20
6.4. Camada de Transporte	21
6.5. Camada de Sessão	21
6.6. Camada de Apresentação	21
6.7. Camada de Aplicação	22
7. PROTOCOLOS PARA IOT	22
7.1. Protocolos da Camada Física	23
7.1.1. LoRaWAN	23
7.1.2. Sigfox	24
7.2. Protocolos da Camada de Enlace	26
7.2.1. IEEE 802.15.4e	26
7.2.1.1. Bandas de Frequência	26
7.2.1.2. Topologias de Rede	27
7.2.2. IEEE 802.11 AH	29
7.2.2.1. Camada Física e MAC	30
7.2.3. Bluetooth Low Energy	31
7.2.3.1 Topologias de Rede	31
7.2.3.2. Aplicações e Vantagens sobre o Bluetooth Clássico	32
7.2.4. Zigbee Smart Energy	32
7.2.4.2 A especificação Zigbee IP	33
7.2.4.3 Aplicações	33
7.2.5. G.9959	34

7.2.5.1. Características	34
7.2.5.2. Modos de Operação	34
7.2.6. LTE-A	35
7.2.6.1 Arquitetura	35
7.2.7. DECT/ULE	36
7.2.7.1. Características, Topologia e Aplicações	37
7.3. Protocolos da Camada de Rede	38
7.3.1. RPL	38
7.3.1.1. Funcionamento	38
7.3.2. CORPL	39
7.3.3. CARP	40
7.3.3.1. Princípios de Funcionamento	40
7.3.3.2. Contraponto	41
7.4. Protocolos da Camada de Encapsulamento e Transporte	41
7.4.1. 6Lo	41
7.4.2. 6LoWPAN	42
7.4.2.1. Segurança	43
7.4.3. IPv6 over G.9959	43
7.4.4. IPv6 over Bluetooth Low Energy	43
7.5. Protocolos de Sessão	44
7.5.1. MQTT	44
7.5.1.1. O Modelo Publish/Subscribe e o Broker	45
7.5.1.2. Vantagem	46
7.5.1.3. Contraponto	46
7.5.2. SMQTT	47
7.5.3. AMQP	48
7.5.3.1. Segurança e Interoperabilidade	49
7.5.4. CoAP	50
7.5.4.1. Arquitetura	50
7.5.5. XMPP	51
7.5.5.1. Contraponto	52
7.5.5.2. Segurança	52
8. CONCLUSÃO	53
9. BIBLIOGRAFIA	55

1. INTRODUÇÃO

O desenvolvimento tecnológico avançou muito nas últimas duas décadas. A disponibilização de conhecimento por meio da internet deu início a criação e a popularização de meios aquisitivos informação, como, por exemplo, de sensores desde os mais simples como umidade e temperatura até os mais complexos como pressão e posicionamento, e envio destas à grandes bases de dados, compartilhadas ou não, para fins de acompanhamento e/ou predição de padrões. Dispositivos de tamanhos reduzidos, chegando ao tamanho de moedas, já são capazes de transmitir informação por meios sem fio.

Projetos que incorporam aquisição de informação de forma distribuída e independente e, então, as centralizam em uma base de dados, quando fazem uso da internet são comumente classificados como Internet das Coisas. O conceito de Internet das coisas pode ser visto em ação em projetos como a geladeira que identifica e avisa ao usuário quando algo está faltando ou próximo do vencimento, acompanhamento de clima e qualidade do solo - no auxílio de planejamento e manejo de propriedades rurais - e em relógios que monitoram batimentos cardíacos e pressão arterial enviando diretamente ao médico do paciente para acompanhamento da saúde dentre outras incontáveis situações possíveis.

Pontos importantes a serem considerados na elaboração de projetos em Internet das Coisas são velocidade e alcance para o tráfego de dados, pois podem interferir diretamente na vida útil das baterias, quando estes a utilizarem.

Protocolos de comunicação são um conjunto de regras para que haja comunicação entre duas partes. No contexto de Internet das Coisas existem protocolos para níveis e finalidades diferentes, saber fazer uma boa escolha pode ser determinante na viabilização de um projeto.

2. OBJETIVO

2.1. Objetivo Geral

Apresentar e analisar as características dos protocolos de comunicação utilizado em Internet das Coisas.

2.1. Objetivo Específicos

- Apresentar o conceito de Internet das Coisas.
- Definir o que é um protocolo de comunicação.
- Fazer um paralelo com as camadas do modelo OSI.
- Demonstrar que o processo de comunicação envolve passa por diversa etapas e que cada uma tem um papel bem definido.
- Em conjunto com os requisitos de um projeto, auxiliar no processo de escolha dos protocolos a serem utilizados.

3. METODOLOGIA

Este trabalho será desenvolvido na forma de tópicos com uma apresentação básica sobre os conceitos principais de cada protocolo de comunicação mostrado.

No início, capítulos 4, 5 e 6, serão abordados três princípios: Internet das coisas, conceitos básicos, possibilidades de aplicação e segurança; Protocolo de comunicação, definição básica; Modelo OSI junto com a apresentação das principais funções da estruturação de suas camadas.

No capítulo 7 serão apresentados protocolos de comunicação fazendo um paralelo com as camadas do modelo OSI.

Ao final, capítulo 8, serão feitas considerações sobre os protocolos com base em suas principais características visando auxiliar na escolha desses de acordo com os requisitos de um projeto.

4. INTERNET DAS COISAS

Internet das Coisas é uma tradução literal da expressão em inglês Internet of Things, representada pela sigla IoT [38]. A Internet das Coisas é um conceito que dispõe que a maioria dos dispositivos que utilizamos diariamente está conectada entre si e pela Internet [40]. A ideia é que, cada vez mais, o mundo físico e o digital se tornem um só, através dispositivos que se comuniquem uns com os outros, os data centers e suas nuvens [39].

Uma definição mais completa seria uma infraestrutura de rede global, conectando objetos reais e virtuais através da exploração da captura de dados e capacidades de comunicação. Esta infraestrutura inclui a Internet atual e sua evolução, e o desenvolvimento das redes. Isto oferecerá identificação específica ao objeto, capacidades de conexão e sensoriamento como as bases para o desenvolvimento de serviços e aplicações cooperativas independentes. Essa infraestrutura será caracterizada por um alto grau de captura autônoma de dados, transferência de eventos, conectividade de rede e interoperabilidade [43].

A ideia de conectar objetos é discutida desde 1991, quando a conexão TCP/IP e a internet que conhecemos hoje começou a se popularizar [39]. A ideia real de dispositivos conectados remonta aos anos 70. Naquela época, a ideia costumava ser chamada de “internet embutida” ou “computação generalizada”. Mas o atual termo “Internet das Coisas” foi cunhado por Kevin Ashton, em 1999, durante seu trabalho na Procter & Gamble [40].

A IoT vai impactar diretamente na vida das pessoas e nos negócios, modificando perfis de compra e hábitos de consumo. Tanto que o Instituto Global McKinsey estimou que a Internet das Coisas vai gerar entre US\$ 3,9 e 11,1 trilhões anuais em novos negócios [42].

4.1. Aplicações

A Internet das Coisas, também conhecida como IoT, é mais do que apenas uma conveniência para os consumidores. Ela oferece novas fontes de dados e

modelos de operação de negócios que podem aumentar a produtividade de diversas indústrias [41].

Já nos dias de hoje, são muitos os objetos conectados, desde geladeiras a óculos, elevadores e carros. A rede pode intervir em pequenos gadgets ou em infraestruturas complexas. Pensando em toda essa usabilidade, vêm surgindo iniciativas que envolvem empresas grandes para unificar a Internet das Coisas [39].

Na área da saúde podemos citar com pulseiras capazes de monitorar desde a atividade física de uma pessoa até a frequência de batimentos cardíacos e marca-passos capazes de disparar um alerta ao identificar um comportamento anormal com o coração do paciente.

Muitas pessoas já estão usando dispositivos *wearables* para ajudar no monitoramento de atividades físicas, sono e outros hábitos – entretanto esses itens estão apenas arranhando a superfície do impacto que pode ser gerado na área da saúde por essa ferramenta; aparelhos de monitoramento de pacientes, registros eletrônicos e outros acessórios inteligentes podem ajudar a salvar vidas [41].

Aplicado ao varejo a IoT pode auxiliar em controle de inventário e na segurança, como também fornecer experiências personalizadas para os clientes. Sistemas de rastreamento utilizando a tecnologia de beacons pode identificar a posição de um cliente dentro da loja através de seu smartphone e, ao se aproximar de algum produto ou sessão ser notificado de uma promoção ou afins.

No mundo automotivo mesmo os carros ainda não tendo chegado ao ponto de se dirigirem sozinhos, eles estão, sem dúvida, mais avançados tecnologicamente do que nunca. A IoT também impacta meios de transporte numa escala maior: empresas de entrega podem rastrear sua frota utilizando soluções de GPS. Estradas podem ser monitoradas através de sensores, para mantê-las o mais seguras possível [41].

Estes são apenas exemplo muito simples e superficiais do potencial da Internet das Coisas, outros campos de atuação que podemos citar aqui é agropecuário, manufatura, serviços públicos, logística, fábricas, transporte público, hospitais e clínicas, etc.

4.2. Expansão

A limitação de tempo e da rotina fará com que as pessoas se conectem à Internet de outras maneiras. Segundo Ashton, assim, será possível acumular dados do movimento de nossos corpos com uma precisão muito maior do que as informações de hoje. Com esses registros, se conseguirá reduzir, otimizar e economizar recursos naturais e energéticos, por exemplo. Para o especialista, essa revolução será maior do que o próprio desenvolvimento do mundo online que conhecemos hoje [39].

4.3 Segurança

O impacto da IoT no mundo tem sido significativo – e está apenas começando [41].

Se a Internet das Coisas descreve um cenário em que quase tudo está conectado, é claro que há riscos associados. Os riscos não são apenas individuais, pode haver problemas de ordem coletiva. Por exemplo, em uma cidade que tem todos os semáforos conectados onde o sistema de gerenciamento de trânsito controla cada um deles de modo inteligente para diminuir congestionamentos, oferecer desvios em vias bloqueadas por acidentes e criar rotas alternativas quando há grandes eventos. Se esse sistema for atacado ou falhar, o trânsito da cidade se tornará um caos em questão de minutos [38].

A interconexão dos sistemas permite um mundo mais responsivo, inteligente e eficiente. O que significa dizer que a partir da interpretação de dados, captados e armazenados previamente, os objetos serão capazes de dialogar com os usuários, promovendo melhorias na qualidade de vida, maior produtividade e agilidade nos processos. Além de otimizar recursos, essa nova onda de produtividade permitirá que as pessoas foquem naquilo que não pode ser automatizado [42].

Nós deveríamos pensar menos na Internet das Coisas e mais na Inteligência das Coisas [41].

5. PROTOCOLO DE COMUNICAÇÃO

Para que haja uma comunicação entre dois pontos, um emissor e um receptor, é necessário que se tenha previamente acordado um padrão de regras de organização da informação bem como o meio pelo qual ela é transmitida para que a informação seja transmitida de forma clara.

Em uma conversa clara entre duas pessoas, onde toda a informação é passada com clareza, é necessário que ambas as partes falem o mesmo idioma e que seja sinalizado de forma de que a informação seja transferida e recebida corretamente.

Um protocolo de comunicações é um conjunto de normas que estão obrigadas a cumprir todas as máquinas e programas que intervêm em uma comunicação de dados entre computadores sem os quais, a comunicação seria caótica e, portanto impossível [2].

No domínio das redes de computação, um protocolo é um conjunto de especificações objetivas utilizadas para se implementar a transferência de dados entre dois ou mais sistemas computacionais. É um conjunto de regras-padrão que caracterizam o formato, a sincronização, a sequência e, ainda, a detecção de erros e falhas na comutação de pacotes, isto é, na transmissão de informação entre computadores. Os protocolos podem ser implementados pelo hardware, software ou por uma combinação dos dois[1].

6. MODELO OSI

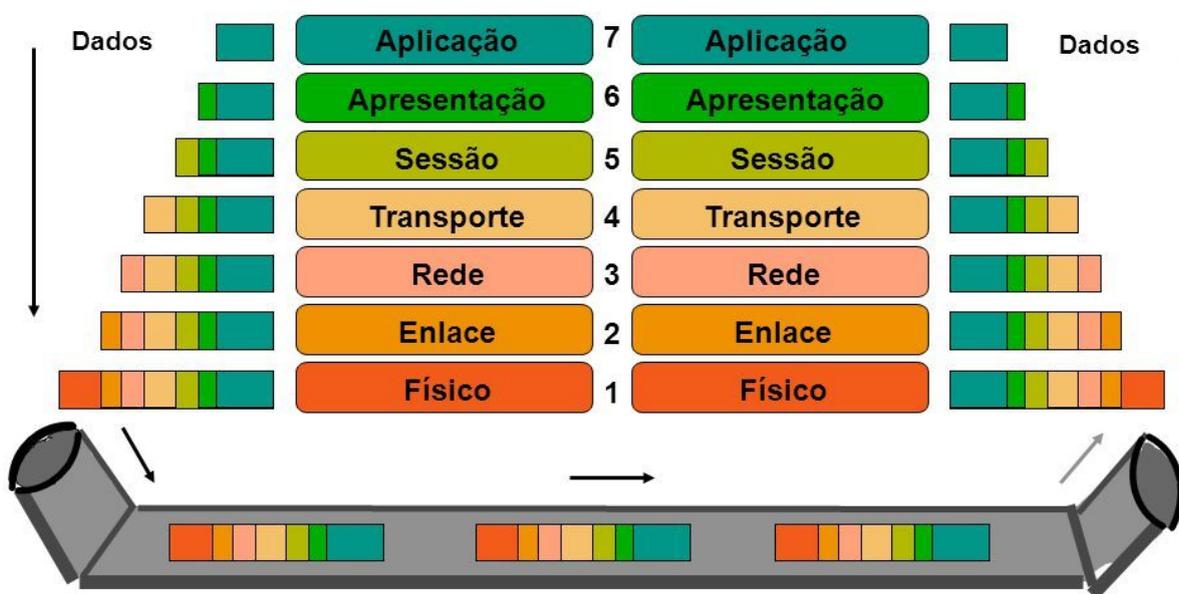
Para dar continuidade ao tema deste trabalho será apresentado neste tópico o Modelo OSI e o conceito introdutório de cada uma de suas camadas para uma melhor compreensão dos protocolos que serão apresentados adiante.

O modelo OSI (Open System Interconnection) foi criado em 1984 pela ISO (International Organization for Standardization) e define como a troca de informação irá ocorrer entre os dispositivos na rede. Tem como principal objetivo ser um modelo padrão para protocolos de comunicação entre diversos tipos de sistema, ou seja, ele possibilita a comunicação entre hardware, software e tecnologias de redes distintas. As 7 camadas do modelo dividem a comunicação em partes menores, facilitando a compreensão e o gerenciamento de incidentes/problemas.

Este modelo exige o cumprimento de etapas para atingir a compatibilidade, portabilidade, interoperabilidade e escalabilidade. São elas: a definição do modelo, definição dos protocolos de camada e a seleção de perfis funcionais.

O Modelo OSI é composto por 7 camadas, sendo que cada uma delas realizam determinadas funções.

O Modelo OSI – Transmissão de dados



Fonte: <https://slideplayer.com.br/slide/1733041/>

6.1. Camada de Física

A camada física define as características mecânicas, elétricas, funcionais e os procedimentos para ativar, manter e desativar conexões físicas para a transmissão de bits.

Os protocolos da Camada Física devem ser independentes do meio de transmissão de modo que um dado terminal possa ser utilizado em diversos meios, como pares metálicos, fibra óptica ou rádio, por exemplo [9].

6.2. Camada de Dados ou Enlace

A camada de dados, ou também conhecida como Enlace de Dados, tem por objetivo assegurar a transferência confiável de dados entre sistemas conectados diretamente por um meio físico [10].

A Camada de Enlace de Dados envolve tipicamente as seguintes funções:

- Ativação e desativação do Enlace de Dados;
- Supervisão e Recuperação em caso de anormalidades;
- Sincronização;
- Segmentação e delimitação das unidades de dados;
- Controle de erros e seqüenciamento das unidades de dados;
- Controle de Fluxo.

6.3. Camada de Rede

A camada de rede tem por objetivo fornecer um suporte de comunicação fim a fim para as camadas superiores. Isto inclui a escolha do modo de transferência e da qualidade de serviço (por exemplo no que se refere aos requisitos de retardo na transferência), o endereçamento da unidade de dados ao seu destino final na rede ou na sub-rede (segmento de rede) externa, o interfuncionamento com elementos de rede externos se necessário, a notificação de eventuais deficiências de segmentos externos, controle de fluxo fim a fim e outras funções [10].

6.4. Camada de Transporte

A camada de transporte é a camada responsável pelo controle da transferência de dados, incluindo a qualidade do serviço e a correção de erros fim a fim. A Camada de Transporte deve considerar os requisitos da aplicação, através dos parâmetros que descrevem as Classes de Serviço e as limitações da rede. São parâmetros de definição da Classe de Serviço [10]:

- Vazão ou *throughput* (bit/s);
- Atraso ou latência de propagação (ms);
- *Jitter* ou Variação no atraso de propagação (ms) ;
- Probabilidade de falha no estabelecimento da conexão;
- Taxa de erro residual.

6.5. Camada de Sessão

A camada de sessão tem por objetivo o controle dos procedimentos de diálogo através da abertura e fechamento de sessões [10].

A camada de Sessão inclui as seguintes funções, entre outras:

- Transferência de dados em ambas direções, normal ou expressa;
- Gerência de Token;
- Controle de Diálogo;
- Sincronização e gerência de atividades;

6.6. Camada de Apresentação

A camada de apresentação é responsável pela sintaxe de dados. Significa que a forma como os conteúdos serão manipulados pela Camada de Aplicação é montada e desmontada pela Camada de Apresentação. Os aspectos de criptografia, se necessários por questões de segurança da comunicação, são também de responsabilidade desta Camada [10].

6.7. Camada de Aplicação

A camada de aplicação é responsável pela semântica da comunicação. É o nível que possui o maior número de protocolos existentes, devido ao fato de estar mais perto do usuário e os usuários possuem necessidades diferentes.

Esta camada fornece ao usuário uma interface que permite acesso a diversos serviços de aplicação, convertendo as diferenças entre diferentes fabricantes para um denominador comum [10].

7. PROTOCOLOS PARA IOT

O desenvolvimento de um projeto em IoT, mesmo que ignorado, faz uso das abstrações das camadas do modelo OSI em diferentes níveis de sua implementação. Redes de sensores que possam estar fisicamente distantes utilizam de módulos capazes de enviar os dados obtidos à longas distâncias em meios sem fio para então serem recebidas e processadas de acordo com as necessidades e posteriormente enviados à uma base de dados na internet. Ou mesmo pequenos dispositivos são capazes de se comunicar com aparelhos celulares e estes por sua vez fazem um processo de sincronização com uma base de dados localizada na internet. Esse nível de encapsulamento utiliza dos conceitos e abstrações das camadas OSI.

Abaixo seguem protocolos para IoT com base nas camadas do modelo OSI.

7.1. Protocolos da Camada Física

7.1.1. LoRaWAN

LoRa é uma tecnologia de radiofrequência que permite comunicação a longas distâncias, de poucos quilômetros em meio urbano até dezenas de quilômetros em meio rural, com consumo mínimo de energia. Suas principais aplicações são sistema de IoT (internet das coisas) como sensores e monitores remotos (pressão, luz, on-off, temperatura, etc.), sobretudo aqueles operados a bateria, de mensagens curtas e em alguns casos em locais de difícil acesso [67].



<https://starbeamrainbowlabs.com/blog/article.php?article=posts%2F279-LoRaWAN.html>

LoRaWAN (*Long Range Wide Area Network*) é uma especificação LPWAN (*Low Power Wide Area Network*) [45] que define a arquitetura do sistema bem como os parâmetros de comunicação usando a tecnologia LoRa [67], foi projetada para criar redes de longa distância, numa escala regional, nacional ou global, formada por dispositivos operados por bateria e com capacidade de comunicação sem fio [45].

Focado em aplicações para redes WAN (*Wide Area Network*), o LoRa foi desenhado para prover comunicação de baixo consumo energético e oferecer *features* específicos para segurança em comunicação M2M [4]. Trata-se de um protocolo otimizado de baixo consumo de energia, projetado para redes sem fio escaláveis com milhões de dispositivos. Suporta operação redundante, tecnologias de economia de energia, baixo custo e livre de localização para suportar as necessidades futuras da IoT, ao mesmo tempo em que permite recursos de mobilidade e facilidade de uso [25]. Mantido pela LoRa Alliance, esse protocolo

possui velocidade entre 0.3 kbps até 50 kbps. É um dos protocolos IoT mais populares [4].

A especificação LoRaWAN trata de requisitos presentes na IoT como comunicação segura e bidirecional, mobilidade e tratamento de serviços de localização. Além disso, o padrão oferece suporte a IPv6, adaptação ao 6LoWPAN e funciona sobre a topologia estrela. O fator atrativo do LoRaWAN é o seu baixo custo e a quantidade de empresas de *hardware* que estão o adotando. O consumo de energia na LoRaWan é considerado pequena, o que permite aos dispositivos se manterem ativos por longos períodos. A LoRaWANs utiliza a frequência ISM sub-GHz fazendo com que as ondas eletromagnéticas penetrem grandes estruturas e superfícies, a distâncias de 2 km a 5 km em meio urbano e 45 km no meio rural. Os valores de frequência mais usadas pelo LoRaWan são: 109 MHz, 433 MHz, 866 MHz e 915 MHz [45].

7.1.2. Sigfox

A Sigfox é uma tecnologia baseada em UNB, do inglês *Ultra Narrow Band* ou Banda Ultra Limitada, foco na construção de redes sem fio para conectar objetos de baixo consumo de energia. Foi criada pela empresa de mesmo nome em 2009 [71] e atua como uma operadora para IoT, com suporte a uma série de dispositivos. A principal função é abstrair dificuldades de conexão e prover uma API para que os usuários implementem sistemas IoT com maior facilidade [45]. A rede Sigfox foi lançada, oficialmente, no Brasil em setembro de 2017 através da empresa WND Brasil [71].



<http://www.tst-sistemas.es/en/sigfox-technologie/>

Sigfox é uma alternativa intermediária entre WiFi que possuem alcance muito curto e redes de longo alcance, como as redes de celular (3G,4G, etc) [4]. A

tecnologia de transmissão usa a banda de rádio ISM , do inglês *Industrial, Scientific and Medical* ou Industrial, Científica e Médica, de 868MHz na Europa e 902MHz nos Estados Unidos e América Latina, denominada “rede de área ampla de baixa potência (LPWAN – *Low Power Wide Area*) [4]. Os sinais de rádio ultrapassam objetos sólidos, e requer pouca energia. Usando topologia em estrela, transmite os pacotes para mais de um ponto. Uma característica importante é sua facilidade de cobrir grandes áreas e alcançar objetos subterrâneos [71]. Seu alcance fica por volta de 3 e 10 quilômetros em zonas urbanas e em zonas rurais entre 30 e 50 quilômetros [4].

O custo para esse ganho em alcance na comunicação é a baixa velocidade de transmissão. Ao utilizar baixas frequências a taxa de transferência também cai consideravelmente, sendo assim ao utilizar a banda ISN o Sigfox trabalha com uma faixa de transmissão entre 10 bit/s e 1 kbit/s e MTU 96 bytes. O SigFox possui baixo consumo de energia e opera na faixa de 900MHz [45].

A tecnologia Sigfox oferece uma solução de comunicação baseada em software, onde toda a complexidade da rede e da computação é gerenciada em nuvem e não nos dispositivos [70]. É uma solução de baixo custo, confiável, de baixa potência de transmissão para conectar sensores e dispositivos, principalmente visando o mundo de IoT e a nova Indústria 4.0. O protocolo Sigfox concentra-se em grande autonomia com baixo consumo de energia, permitindo anos de vida útil da bateria, simplicidade na configuração, solicitação de conexão ou sinalização, baixo custo de hardware utilizado nos dispositivos para uma rede e, graças ao seu baixo custo e facilidade de configuração, pode-se também usar o Sigfox como uma solução secundária para qualquer outro tipo de rede, como por exemplo Wi-Fi, Bluetooth, GPRS etc [69].

7.2. Protocolos da Camada de Enlace

7.2.1. IEEE 802.15.4e

O IEEE é uma associação sem fins lucrativos criada nos Estados Unidos em 1963. Um de seus objetivos é gerar conhecimento nos campos de engenharia elétrica, eletrônica e computação. O IEEE, ao longo dos anos, vem padronizando diversos protocolos de comunicação sem fio, tendo em vista o crescimento e a interoperabilidade de tecnologias já existentes no mercado e aquelas que serão desenvolvidas.

A norma IEEE 802.15.4 define todas as especificações de comunicação da camada física e da camada de acesso ao meio para redes de comunicação sem fio que operam com baixa taxa de transmissão de dados, definidas também pela sigla LR-WPAN (*Lower Rate Wireless Personal Area Network*) [11].

Baixa transmissão de dados implica em uma economia de energia considerável, uma vez que a transmissão via redes sem fio possui um alto consumo relativo de energia, impactando diretamente sistemas que não sejam alimentados com uma fonte externa e dependem de baterias.

7.2.1.1. Bandas de Frequência

O padrão IEEE 802.15.4 trabalha com algumas bandas de frequências bem definidas. São elas:

- 868 MHz

Possui apenas um canal de transmissão e é utilizado nos países da Europa.

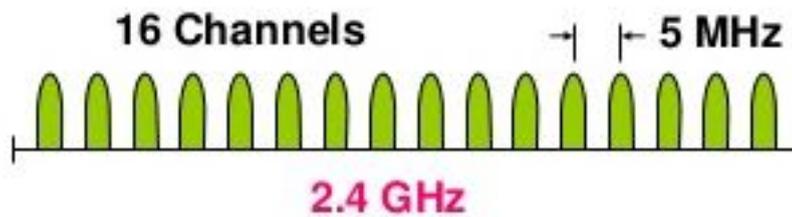
- 915 MHz

Possui 10 canais de transmissão e é utilizada nos Estados Unidos e alguns outros países das Américas.

- 2,4 GHz

Usualmente utilizada no restante do mundo, esta por sua vez possui 16 canais de transmissão que podem ser utilizados da mesma banda de transmissão.

A figura abaixo ilustra os canais da banda de transmissão de 2,4 GHz.



Como se pode observar na imagem dentro de um intervalo de 2,4 GHz, a representação de cada canal de transmissão é feita por uma pausa na transmissão por 5 MHz.

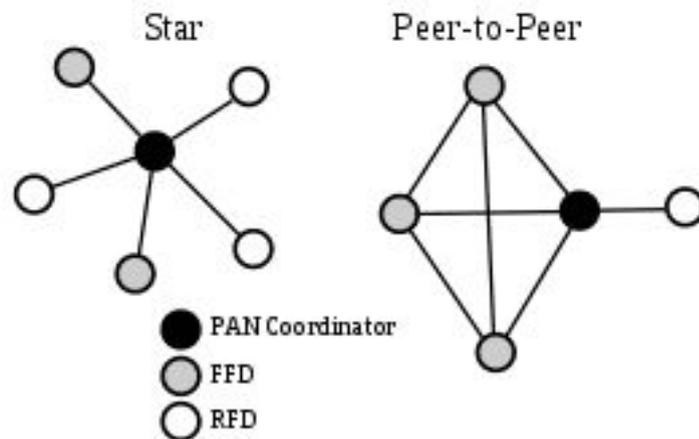
Um ponto interessante a se observar é a disponibilidade da utilização da banda de frequência de 2,4 GHz. Esta é amplamente empregada, devido à disponibilidade em todo mundo para uso sem licença, baixa latência, alta taxa de dados e fornecimento de mais canais. Porém as outras duas bandas fornecem menor índice de interferência e menor quantidade de usuários possuindo uma maior cobertura.

7.2.1.2. Topologias de Rede

Dentro do padrão IEEE 802.15.4 são definidos dois tipos de dispositivos, que são o FFD (*Full Feature Device*) e RFD (*Reduce Feature Device*).

Os FFD são classificados como sendo dispositivos mais completos, pois podem desempenhar a função de coordenador ou roteador, o que resulta no acesso a todos os dispositivos dentro do seu alcance de transmissão. Já os RFD por suas vezes são dispositivos mais limitados, pois possuem uma pilha de tarefas reduzidas, como por exemplo, não rotear dados.

As topologias presentes dentro do IEEE 802.15.4 podem ser nas configurações estrela e peer-to-peer. A topologia estrela possui um nó central que conecta-se com todos os dispositivos. Em alternativa, a configuração *peer-to-peer* permite que os dispositivos comuniquem-se entre si, respeitando a função dos dispositivos em questão.



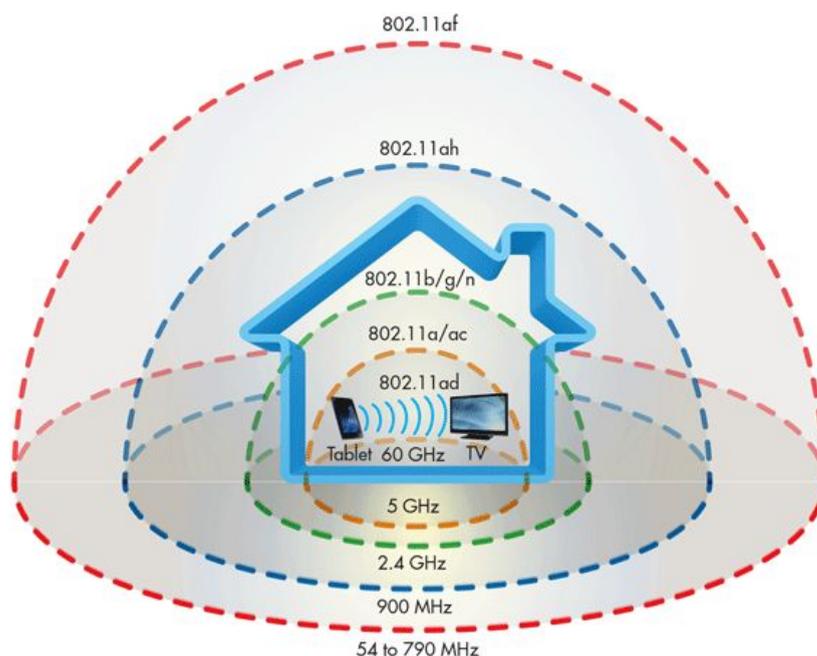
Para configuração da topologia de rede da norma IEEE 802.15.4 são necessários o PAN coordenador, coordenador e *end device*. O PAN coordenador tem como função a criação da rede sem fio, enquanto o coordenador roteia as informações e os end devices possuem suas tarefas reduzidas.

Traçando um paralelo com Internet das Coisas e os componentes comumente utilizados, o PAN coordenador pode ser representado pelo módulo responsável diretamente pela comunicação sem fio dos dados trafegados na rede para um serviço web para armazenamento desses dados ou para um centralizador de dados também conhecido como *broker*, o *ESP8266* seria um exemplo. O coordenador pode ser representado por um nó que interpreta dados de um sensor e aplica alguma ação sobre um atuador com base no valor obtido pelo sensor, o Arduino é muito utilizado com esse propósito durante a etapa de protótipo de um projeto. O *end device* é representado pelo dispositivo que efetivamente fornece os dados desejados, tipicamente sensores como por exemplo sensor de temperatura, umidade, pressão, luminosidade, etc.

7.2.2. IEEE 802.11 AH

Com o rápido crescimento da demanda por banda ISM (*Industrial Scientific and Medical*, bandas de transmissão sem fio reservadas internacionalmente para o desenvolvimento Industrial, científico e médico), surgiram então as redes sem fio operando em frequências próximas de 900MHz.

Atualmente existem dispositivos que já funcionam em redes proprietárias nessa faixa de frequência, alguns sendo adaptações de dispositivos fabricados para trabalhar com outros padrões IEEE (como o IEEE 802.11a), apenas mudando a frequência de operação. Tais produtos ganham vantagem nas aplicações de redes de sensores, mas têm a desvantagem de não serem padronizados de acordo com uma norma.



Nesse cenário, surge o projeto IEEE 802.11ah, desenvolvido pelo grupo IEEE 802.11, com o objetivo de criar uma norma para redes sem fio operando em frequências abaixo de 1GHz. O motivo principal para a utilização de uma nova banda isenta de licença abaixo de 1GHz é, além do alívio de tráfego nas bandas já existentes, explorar as características das ondas de menores frequências, comparando com as utilizadas atualmente.

Por ser baseado em ondas de baixa frequência, o padrão IEEE 802.11ah torna possível obter redes sem fio com maior alcance. Pontos de atenção importantes abordados nesta norma são problemas de interferência entre pontos de acesso de redes distintas, por causa do maior alcance dos sinais.

As bandas ISM abaixo de 1GHz são diferentes ao redor do mundo. Portanto, a distribuição de canais no espectro foi feita de maneira diferente para cada país.

Para uma rede de dispositivos desenvolvida com o conceito de Internet das Coisas, uma característica de suma importância nesse modelo é a possibilidade de um grande número de dispositivos se comunicando graças a um menor índice de interferências na mesma faixa de frequência e menor potência necessária para se trabalhar com frequências abaixo de 1 GHz. Diminuir a potência utilizada para a transmissão dados em baixa frequência também impacta em outro requisito importante para diversos projetos, aumenta a vida útil das baterias.

7.2.2.1. Camada Física e MAC

O padrão 11ah tem em sua camada física suporte para canais de 2MHz, 4MHz, 8MHz e 16MHz. Adicionalmente, canais de 1 MHz são adotados como unidades de canal base. Dessa forma, assim como nos padrões IEEE 802.11n e IEEE 802.11ac, canais de maior largura serão obtidos pela união de canais mais estreitos.

Com relação a camada MAC (*Media Access Control*), o padrão IEEE 802.11ah prevê algumas mudanças que podem trazer melhorias se comparadas com as camadas já presentes nos outros padrões 802.11, principalmente no que tange maior número de estações, economia de energia e mecanismos para maior taxa de transmissão.

O que pode ser uma das maiores deficiências do 802.11ah é a baixa taxa de transmissão. Com o intuito de compensar de alguma forma essa característica, foi proposto um novo formato de pacote na camada MAC. O novo formato traz um novo cabeçalho MAC mais compacto para diminuir o *overhead*. Além disso, alguns campos são retirados e passados para o cabeçalho da camada física. Com essas modificações pode-se obter um cabeçalho no mínimo 12 bytes menor.

7.2.3. Bluetooth Low Energy

O *Bluetooth Low Energy* (BLE), também conhecido como *Bluetooth Smart*, é uma tecnologia de rede de área pessoal sem fios concebida e comercializada pela *Bluetooth Special Interest Group*. Em comparação com Bluetooth Clássico, o *Bluetooth Smart* destina-se a fornecer consumo de energia e custos consideravelmente reduzidos, procurando manter um alcance de comunicação similar.

Assim como o nome sugere, o principal foco do BLE é a economia de energia. Um dispositivo se comunica com outros esporadicamente para um envio de pacotes extremamente reduzidos, ficando em modo IDLE, em espera, no restante do tempo. As conexões duram apenas milissegundos com um consumo de pico por volta de 6 mA, e consumo médio de 1uA durante o tempo em espera. Tais características elevam a vida útil das baterias de meses até anos de funcionamento com a mesma carga.

7.2.3.1 Topologias de Rede

Bluetooth Low Energy não suporta atualmente a formação de redes multi-hop na camada de enlace. Em vez disso, um nó central atua como um roteador entre nós periféricos de baixa potência [25].

As três principais topologias de redes utilizadas em redes utilizando BLE são a *peer-to-peer* (P2P), estrela e rede mesh.

A topologia de rede P2P, cria uma conexão ponto a ponto entre dois dispositivos. Essa comunicação permite uma comunicação bidirecional entre os pontos e não limitada a apenas dois dispositivos, um dispositivo pode se comunicar com diversos outros desde de seja implementada uma conexão P2P com cada dispositivo que se deseja habilitar comunicação.

A topologia de rede em estrela define um dispositivo como sendo um nó *master*, responsável por receber dados de outros dispositivos que normalmente possuem um papel bem definido, e nós *slave* que se comunica exclusivamente com o nó master da sua rede.

A topologia de rede mesh, é a união de várias redes em estrela. Porém, agora um dispositivo master pode ter bilhões de *slaves*, devido a um aumento de 3 bits para 48 bits no espaço destinado aos endereços.

7.2.3.2. Aplicações e Vantagens sobre o Bluetooth Clássico

As características do BLE possibilitam a criação de componentes de pequeno porte capazes de se comunicar por meios sem fios e com um consumo extremamente baixo de energia aumentando a vida útil da bateria.

Com milhares de possibilidades, o BLE pode auxiliar em aplicações que vão desde a monitoração de nossa saúde, com sensores para informar pressão sanguínea ou o pulso de um indivíduo, até automatização em espaço civil e empresarial em que vivemos.

Essencialmente, os propósitos do BLE e do *Bluetooth* clássico são diferentes. Enquanto o BLE é vital para aplicações com um mínimo tráfego de dados associados ao baixo consumo de energia, o *Bluetooth* clássico pode alcançar altas taxas e transferir uma grande quantidade de dados, porém consome a vida útil da bateria rapidamente, além de seu preço ser bem maior.

7.2.4. Zigbee Smart Energy

As redes ZigBee são conhecidas por usufruírem de uma eletrônica simples, de baixo custo e baixo consumo (uma bateria pode durar até 1000 dias) e permite grande escalabilidade e expansão, o que torna esta tecnologia a ideal para sensores, controladores, monitorização remota e dispositivos eletrônicos portáteis [18].

O ZigBee é um padrão que utiliza a definição do IEEE 802.15.4, operando em faixas de frequências livres (ISM), 868 MHz na Europa, 915 MHz nos EUA e Austrália, e de 2,4 GHz na maioria das jurisdições em todo o mundo [24] com baixo custo, além de conter funcionalidade de rede, homologado em Maio de 2003 e foi desenvolvido para redes de comunicação que precisassem de uma baixa taxa de transmissão de dados e uma alta robustez e curta distância [17]. As taxas de transmissão de dados variam de 20 a 900 kbps.

7.2.4.2 A especificação Zigbee IP

Este padrão é baseado em IP e oferece recursos de gerenciamento e eficiência de energia. O Zigbee IP é a primeira especificação IPv6 baseada em padrões abertos para redes de sensores sem fio. O IP Zigbee foi projetado para fornecer uma pilha de protocolo IPv6 que pode operar em dispositivos de baixo custo e de baixa potência, e também suporta os requisitos do Zigbee Smart Energy. Esta combinação permite a criação de dispositivos sem fio com longa duração da bateria [16].

O Zigbee IP permite que dispositivos de baixa potência participem ativamente com outros dispositivos Ethernet, Wi-Fi e HomePlug habilitados para IPv6 sem a necessidade de gateways intermediários [16].

7.2.4.3 Aplicações

Nos dias de hoje organizações utilizam os protocolos IEEE802.15.4 associados ao Zigbee para entrega de soluções eficientes em uma variedade de áreas incluindo controle de dispositivos eletrônicos e gerenciamento e eficiência de consumo em prédios comerciais e industriais [23].

Alguns exemplos de aplicação de redes ZigBee Smart Energy são o projeto Inovcity Aparecida na cidade de Aparecida em SP, a Ecil Energia instalou mais de 15,4 mil medidores eletrônicos para leitura de dados de consumo bem como operações remotas [20] e utilizado como o padrão de comunicação mais adequado para o domínio de rede de um Smart Grid residencial pelo U.S. National Institute for Standards and Technology (NIST) [17].

7.2.5. G.9959

Padronizado pela ITU [7], do inglês, *International Telecommunication Union*, agência da ONU especializada em tecnologias de informação e comunicação destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais [28], o protocolo G.9959 tem como foco áreas de redes pessoais (PAN, do inglês *Personal Area Networks*) de baixa potência [27].

Foi desenvolvido para atuar em redes com baixa largura e custo de banda, oferecendo uma comunicação sem fio half-duplex confiável. Desenvolvido com foco em aplicações de tempo real onde o tempo é um fator crítico, a confiabilidade da comunicação aliado a um baixo consumo de bateria são requisitos primordiais [25].

7.2.5.1. Características

Algumas das características de camada de enlace incluem: endereçador único de rede que permite 232 dispositivos conectados à rede, mecanismos para evitar colisões no tráfego das informações, retransmissão automática para garantir a confiabilidade, padrão de wakeup (“despertar” para iniciar comunicação) dedicado que permite que os nós entrem em modo sleep (modo onde não há tentativa de transmissão de dados) quando estão fora de comunicação e, portanto, economizando energia [25].

As implementações de funções sobre a camada de enlace no protocolo G.9959 inclui canais únicos de acesso, validação de frames, confirmação de recebimento de pacote, referenciado pela sigla ACK em literaturas técnicas, e retransmissão em caso de perda de pacote de dados [25].

7.2.5.2. Modos de Operação

Os modos de operação para o protocolo G.9959 funcionam basicamente de duas formas diferentes: Always Listening (sempre escutando, em tradução direta, representado pela sigla AL) e Frequently Listening (frequentemente escutando, em tradução direta, representado pela sigla FL) ou alternando entre esses dois modos dinamicamente [26].

No modo AL o receptor fica ativo e recebendo informações o tempo todo enquanto estiver ligado [26]. Desta forma obtém-se informações com o mínimo de latência, tempo entre a mensagem ser emitida e recebida, porém eleva o consumo de energia.

No modo FL o receptor é desligado intermitentemente por um período de tempo. Em intervalos regulares, o receptor é ligado por um curto período de tempo. Este modo economiza energia enquanto ainda permite a recepção de quadros. A desvantagem do modo FL é um aumento da latência de transmissão devido ao baixo ciclo de trabalho do receptor [26].

7.2.6. LTE-A

Do inglês, *Long-Term Evolution Advanced*, é um conjunto de padrões desenvolvidos para comunicação de máquina para máquina (M2M) e aplicações sob o conceito de internet das coisas para redes móveis [25].

Para fazer do LTE uma verdadeira tecnologia de 4ª geração (4G), ele foi aprimorado para atender aos requisitos do *IMT-Advanced* publicados pela União Internacional de Telecomunicações (ITU). As melhorias necessárias estão especificadas na versão 10 da 3GPP, também conhecido como *LTE-Advanced* [30].

LTE-A é um protocolo escalável, capaz suportar um aumento súbito de demanda sem a necessidade de se reestruturar ou paradas de rede, e de baixo custo se comparado a outros protocolos de redes de celulares [25].

7.2.6.1 Arquitetura

LTE-A utiliza OFDMA, do inglês *Orthogonal Frequency Division Multiple Access* ou Acesso Múltiplo por Divisão Ortogonal de Frequência, como a tecnologia de acesso à camada de enlace [25]. Isso significa que pelo fato delas serem ortogonais, ou seja, não possuem sobreposição de frequência, elas não interferem entre si [32]. Esta tecnologia divide a frequência em múltiplas bandas que podem ser usadas separadamente [25]. Dessa maneira, os dispositivos que empregam LTE são capazes de trabalhar em meios que apresentam elevados índices de interferência [32].

De acordo com o 3GPP, o maior foco nesse *release* é a capacidade, ou seja, possibilitar maiores taxas aos usuários. O principal diferencial é a sua funcionalidade chamada *Carrier Aggregation*, que possibilita agregação entre portadoras diferentes não contínuas, dando flexibilidade ao espectro, com algoritmos que fazem distribuição de carga e qualidade do sinal entre os usuários. Essa flexibilização pode propiciar uma largura de banda de até 100 Mhz, sendo que a largura entre *downlink* e *uplink* podem ser diferentes, mas a largura no *downlink* deve ser superior [31].

A arquitetura do LTE-A consiste de um core network, núcleo de rede em tradução direta referenciado com a sigla CN, uma rede de acesso ao rádio, referenciado pela sigla RAN, e os nós móveis, tipicamente celulares utilizando a rede LTE-A [25].

O CN é responsável por controlar dispositivos móveis e manter o rastreamento de seus IP's [25].

A RAN é responsável por estabilizar o controle, planos de dados, manuseio da conectividade sem fio e do controle de acesso por rádio [25].

7.2.7. DECT/ULE

Do inglês *Digital Enhanced Cordless Telecommunications* (DECT), Telecomunicações digital sem fio aprimoradas, foi lançado em 1987 e é o padrão para comunicações telefônicas sem fio em todo o mundo. O DECT tem sido uma tecnologia em constante evolução e novas versões da tecnologia. A última versão é DECT *Ultra Low Energy* (ULE) [33].

A tecnologia DECT/ULE é promovida pela *ULE Alliance*, uma organização sem fins lucrativos, que também estabeleceu programas de certificação para redes de automação residencial baseadas na tecnologia DECT ULE [34].

Com a introdução da extensão padrão ULE, DECT se tornou uma tecnologia ideal para automação e segurança industrial. Os dispositivos que implementam esse protocolo são extremamente baratos, com baixo consumo de energia, alta cobertura para o que propõe, livre de interferência, taxa de transferência altamente estáveis e agrega recursos complementares de voz e vídeo [33].

As principais características da tecnologia são o consumo de energia ultra baixo, sendo mais baixo do que protocolos que implementam IEEE 802.11 como o Wi-Fi, e uma cobertura mais ampla, mais ampla que o IEEE 802.15 e Bluetooth Low Energy [34].

7.2.7.1. Características, Topologia e Aplicações

A rede sem fio básica DECT ULE é projetada como topologia de rede em estrela, ou seja, há um dispositivo principal controlador, que controla a rede. Este controlador é conectado sem fio a outros dispositivos chamados de “nós”, que normalmente são dispositivos com funções dedicadas, como sensores, controles remotos, atuadores, medidores inteligentes, etc. Alguns exemplos de dispositivos de nó são travas de porta, detectores de fumaça, detectores de movimento e controles remotos, medidores de gás e eletricidade, monitores de bebês e cuidados com idosos [34].

O DECT ULE fornece dados e comunicação de voz simultâneos, ou seja, os sensores não se limitam a indicar um evento, mas também podem ativar a comunicação por voz. Um bom exemplo é um dispositivo usado no corpo para o cuidado de idosos, que em caso de emergência permite que a pessoa não apenas indique uma situação de emergência, mas também comunique-se com um zelador localizado remotamente com o simples apertar de um botão [34].

Enquanto a DECT é a tecnologia líder em serviços de áudio, ela evoluiu com o ULE (Ultra Low Energy) dedicado para aplicações de automação residencial, segurança e proteção com sua solução de smart house de baixa energia [35].

Com um alcance de 600 m ao ar livre e 70 m no interior, a comunicação é feita ponto a ponto e não em rede de malha, como é feito com Z-wave e ZigBee. Usando a frequência DECT ULE 1.9 GHz, a conectividade sem fio é livre de interferências [35].

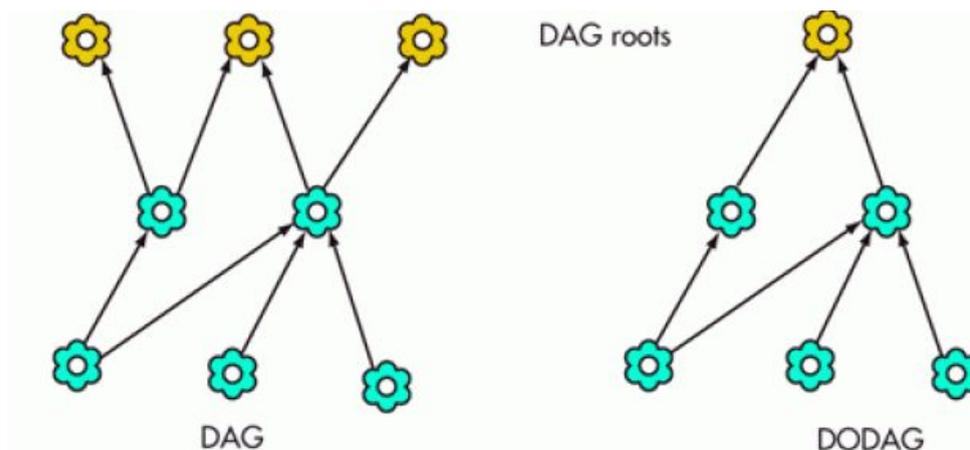
7.3. Protocolos da Camada de Rede

7.3.1. RPL

O RPL é um protocolo de roteamento que utiliza a técnica de vetor de distâncias para definir as rotas. Esse protocolo foi desenvolvido para redes de baixa potência e com perdas, LLNs, baseadas em IPv6[6]. As LLNs se caracterizam por possuir baixas capacidades energéticas e computacionais, e por apresentarem variações da largura de banda [44].

Protocolo para roteamento de redes com baixo consumo de energia e perdas, RPL (*Routing Protocol for Low-power and lossy networks* ou em português Grafo Acíclico Direcionado Orientado ao Destino) tem como objetivo prover um roteamento eficiente de caminhos para três padrões de tráfego: ponto a ponto, multi pontos a multi pontos e ponto a multi pontos (Winter & Thubert, 2010).

Este protocolo define uma árvore de roteamento utilizando o conceito de grafos acíclicos direcionados, DAG. Cada nó pode se associar a mais de um nó, o que difere o RPL dos demais protocolos baseados em árvores [43].



Fonte: <https://www.electronicdesign.com/communications/understanding-wireless-routing-iot-networks>

7.3.1.1. Funcionamento

A organização é orientada ao destino, ou seja, a rede possui um nó raiz que concentra o recebimento dos dados dos demais nós. Essa estrutura recebe o nome

de DODAG (*Destination-Oriented Directed Acyclic Graph*). A rede é formada por um ou mais DODAGs, formando uma instância RPL [43].

A princípio cada nó envia um *DODAG Information Object* (DIO) anunciando-se como a raiz. Esta mensagem é propagada na rede e o DODAG completo é construído gradualmente. Ao se comunicar, o nó envia um objeto de anúncio de destino (DAO) para seus pais, o DAO é propagado para a raiz e a raiz decide onde enviá-lo dependendo do destino. Quando um novo nó deseja ingressar na rede, ele envia uma Solicitação de Informações do DODAG (DIS) para ingressar na rede e a raiz responderá com um DAO-ACK confirmando a associação. Os nós RPL podem ser sem estado, o que é mais comum, ou com estado. Um nó sem estado mantém apenas rastros de seus pais. Apenas root tem o conhecimento completo de todo o DODAG. Assim, todas as comunicações passam pela raiz em todos os casos. Um nó com monitoramento de estado controla seus filhos e pais e, portanto, ao se comunicar dentro de uma subárvore do DODAG, ele não precisa passar pela raiz [25].

Dispositivos de rede executando RPL estão conectados de maneira acíclica. Assim, um DODAG é criado Cada nó mantém a melhor rota para a raiz do DODAG. Para encontrar a melhor rota os nós usam uma função objetivo (OF) que define a métrica de roteamento a ser computada [45].

7.3.2. CORPL

CORPL (*Cognitive Routing Protocol for Low-power*) é uma extensão do protocolo RPL e foi desenhada para redes cognitivas usando a topologia DADOG [50]. O objetivo do CORPL é reter o DAG (grafos acíclicos direcionados) baseado nos princípios do RPL e ao mesmo tempo introduzir modificações que permitem ser aplicadas em ambientes de rádios cognitivos [47] visando encontrar a melhor rota para a transferência dos dados.

Para abordar os desafios acima mencionados, foi desenvolvido uma abordagem de encaminhamento oportunista que consiste em dois passos principais: a seleção de um conjunto de encaminhadores, ou seja, cada nó na rede seleciona múltiplos vizinhos de próximo salto e um esquema de coordenação para garantir que somente melhor receptor de cada pacote para ele (seleção única do remetente).

Tem sido demonstrado que a abordagem de encaminhamento oportunista melhora a capacidade de ponta a ponta e a confiabilidade (explorando as características inerentes ao canal sem fio) da rede, sendo esta última uma preocupação importante para as redes com perdas [49].

O CORPL aproveita a abordagem de encaminhamento oportunista para suportar alarmes sensíveis ao atraso de alta prioridade que precisam chegar ao gateway antes de um dado prazo, bem como selecionar caminhos com interferência mínima para os receptores PU. A proteção PU transmissor é assegurada através do tempo de transmissão ideal para a rede secundária, sujeito a uma restrição de interferências. Isso será discutido em detalhes mais tarde. [49]

7.3.3. CARP

O protocolo CARP (*Channel-Aware Routing Protocol* ou em português Protocolo de roteamento com reconhecimento de canal) é um protocolo de roteamento distribuído projetado para comunicação subaquática. Ele pode ser usado para IoT devido a seus pacotes leves.

CARP faz uso de informações sobre a qualidade do link. Os nós são selecionados como transmissores se eles têm uma história recente positiva de retransmissões ao seu vizinhos [47].

Este protocolo é muito interessante pois permite coletar informações em áreas de difícil acesso à tecnologia que existia anteriormente porque não permitiam uma grande cobertura de área e tendia a ter um alto custo [47].

7.3.3.1. Princípios de Funcionamento

Existem dois cenários: inicialização de rede e encaminhamento de dados. Na inicialização da rede, um pacote *HELLO* é transmitido do coletor para todos os outros nós nas redes. No encaminhamento de dados, o pacote é roteado do sensor para o coletor de forma salto a salto, onde cada próximo salto é determinado independentemente.

O CARP combina a qualidade do link com uma topologia de informações simples baseado em saltos, sendo capaz de criar uma rota em torno de vazios e áreas de sombra, melhorando assim seus benefícios [47].

7.3.3.2. Contraponto

O principal problema com o CARP é que ele não suporta a reutilização de dados previamente coletados. Em outras palavras, se o aplicativo exigir dados do sensor apenas quando ele mudar significativamente, o encaminhamento de dados do CARP não será benéfico para esse aplicativo específico.

Um aprimoramento do CARP foi feito no E-CARP, permitindo que o nó de sincronização salvasse os dados sensoriais recebidos anteriormente. Quando novos dados são necessários, o E-CARP envia um pacote Ping que é respondido com os dados dos nós dos sensores. Assim, o E-CARP reduz drasticamente a sobrecarga de comunicação [25].

7.4. Protocolos da Camada de Encapsulamento e Transporte

7.4.1. 6Lo

O grupo de trabalho IPv6 sobre redes de nós com restrição de recursos (6Lo) na IETF está desenvolvendo um conjunto de padrões para transmissão de quadros IPv6 em vários datalinks. Embora o 6LowPAN e o 6TiSCH, que cobrem o IEEE 802.15.4 e o IEEE 802.15.4e, tenham sido desenvolvidos por diferentes grupos de trabalho, ficou claro que há muito mais datalinks a serem cobertos e, portanto, o 6Lo group foi formado [25].

6Lo se concentra no trabalho que facilita a conectividade IPv6 redes de nó restritas com as características de poder limitado, memória e recursos de processamento, limites superiores rígidos no estado, espaço de código e ciclos de processamento, otimização de energia e uso de largura de banda de rede, falta de alguns serviços como conectividade completa de dispositivos e broadcast / multicast [52].

7.4.2. 6LoWPAN

Encapsula eficientemente os headers grandes do IPv6 em pequenos pacotes IEEE802.15.4 [7].

O 6LoWPan é um protocolo IP (Internet Protocol). O nome é abreviação de *IPv6 Low-power wireless Personal Area Network*. Ao invés de ser uma tecnologia IoT como Bluetooth ou ZigBee, o 6LoWPAN é um protocolo de rede que define o encapsulamento, headers e mecanismos de compressão. O atributo chave é o IPv6 stack, que foi um passo muito importante para viabilizar a Internet das Coisas. Com o IPv6, é possível atribuir a cada objeto ou equipamento do mundo o seu IP único e conectá-lo à internet [4].

O IPv6 in Low-Power Wireless Personal Area Networks Working Group ficou responsável por padronizar o Internet Protocol version 6 (IPv6) para redes que fazem uso de rádios sobre o padrão IEEE 802.15.4 que, por sua vez, especifica as regras das camadas mais baixas (enlace e física) para redes sem fio pessoais de baixa potência de transmissão [6].

O protocolo 6LoWPAN possibilita que pacotes IPv6 sejam transportados sobre redes sem fio de baixo consumo de energia. Mulligan (2007) afirma que 6LoWPAN é a chave para o uso da internet em objetos inteligentes, uma vez que ele permite o uso do IPv6 em dispositivos com baixo consumo de energia, processamento limitado e baixo consumo de banda em redes sem fio [46].

Por ser baseado em tecnologia IP que já é amplamente difundida pode aproveitar das ferramentas de diagnóstico e gerenciamento de redes IP já existente. São facilmente conectados a outras redes IP sem a necessidade de tradutores e *proxies*, aproveitando assim toda a infraestrutura já existente das redes IP [46].

A implementação deste protocolo já pode ser considerado uma Internet das Coisas. De acordo com Ko et al. (2011) é importante manter uma pilha IPv6 eficiente que funcione em redes remotas de recursos limitados. Assim o uso de uma camada 6LoWPAN é um requisito para redes de sensores [46].

7.4.2.1. Segurança

O 6LoWPAN por si só não oferece nenhum mecanismo de segurança. No entanto, documentos relevantes incluem a discussão de ameaças de segurança, requisitos e abordagem a serem considerados na camada de rede IoT. Por exemplo, a RFC 4944 discute a possibilidade de endereços duplicados da interface EUI-64, que devem ser únicos [RFC4944]. RFC 6282 discute as questões de segurança que são levantadas devido aos problemas introduzidos no RFC 4944 [RFC6282]. O RFC 6568 aborda possíveis mecanismos para adotar a segurança em dispositivos com sensores sem fio restritos [RFC6568]. Além disso, alguns rascunhos recentes no [6Lo] discutem mecanismos para obter segurança no 6LoWPAN. [25].

7.4.3. IPv6 over G.9959

O RFC 7428 define o formato de quadro para transmissão de pacote IPv6 em redes ITU-T G.9959. G.9959 define um identificador de rede doméstica de 32 bits exclusivo atribuído pelo controlador e pelo identificador de host de 8 bits alocado para cada nó. Um endereço local de link IPv6 deve ser construído pelo identificador de host de 8 bits derivado da camada de link para que ele possa ser compactado no quadro G.9959. Além disso, a mesma compactação de cabeçalho como em 6lowPAN é usada aqui para ajustar um pacote IPv6 em quadros G.9959. O RFC 7428 também fornece um nível de segurança por uma chave de rede compartilhada que é usada para criptografia. No entanto, aplicativos com um nível mais alto de requisitos de segurança precisam lidar com a criptografia e autenticação de ponta a ponta usando seus próprios mecanismos de segurança de camada superior [6Lo] [25].

7.4.4. IPv6 over Bluetooth Low Energy

O Bluetooth Low Energy, também conhecido como Bluetooth Smart ou BLE, foi introduzido no Bluetooth V4.0 e melhorado no V4.1 [25].

O uso do IPv6 sobre o *Bluetooth Low Energy* permite que cada dispositivo tenha seu próprio endereço IP para poder se conectar diretamente à Internet. Isso eliminará a dependência dos smartphones e permitirá que bilhões de dispositivos se conectem e troquem informações de maneira padronizada pela Internet [53].

RFC7668, que especifica o IPv6 através do Bluetooth LE, reutiliza a maioria das técnicas de compressão 6LoWPAN [25]. Como o Bluetooth Low Energy não se comunica de forma nativa com o IP, a melhor maneira de conseguir isso é usar o 6LoWPAN. Isso simplifica os cabeçalhos IP, compacta os dados e encapsula os pacotes IP para permitir que eles sejam enviados via Bluetooth de maneira eficiente, economizando largura de banda e energia [53].

A combinação de baixa energia Bluetooth e IPv6 nos aproxima muito da meta de ter dispositivos pequenos e de baixo consumo de energia que possam se comunicar diretamente entre si e com a Internet, sem ter que ter hubs diferentes de cada fabricante no meio [53].

7.5. Protocolos de Sessão

7.5.1. MQTT

O MQTT foi inventado e desenvolvido inicialmente pela IBM no final dos anos 90. Sua aplicação original era vincular sensores em pipelines de petróleo a satélites. Como seu nome sugere, ele é um protocolo de mensagem com suporte para a comunicação assíncrona entre as partes. Um protocolo de sistema de mensagens assíncrono desacopla o emissor e o receptor da mensagem tanto no espaço quanto no tempo e, portanto, é escalável em ambientes de rede que não são confiáveis [55].

O principal objetivo do MQTT é minimizar o uso de largura de banda da rede e recursos dos dispositivos. Além disso, o MQTT provê mecanismos para a garantia de entrega de mensagens. Utiliza os protocolos das camadas de transporte e rede da arquitetura TCP/IP [45].

Segue uma arquitetura de transporte de mensagens utilizando o modelo de publicação e assinatura (publish and subscribe ou simplesmente pub/sub)

extremamente leve [54] e é projetado para fornecer conectividade embutida entre aplicativos e middleware em um lado e redes e comunicações no outro lado [25].

Uma das grandes vantagens do MQTT é a eficiência energética do modelo pub/sub, que também pode ser escalado com facilidade [6].

7.5.1.1. O Modelo Publish/Subscribe e o Broker

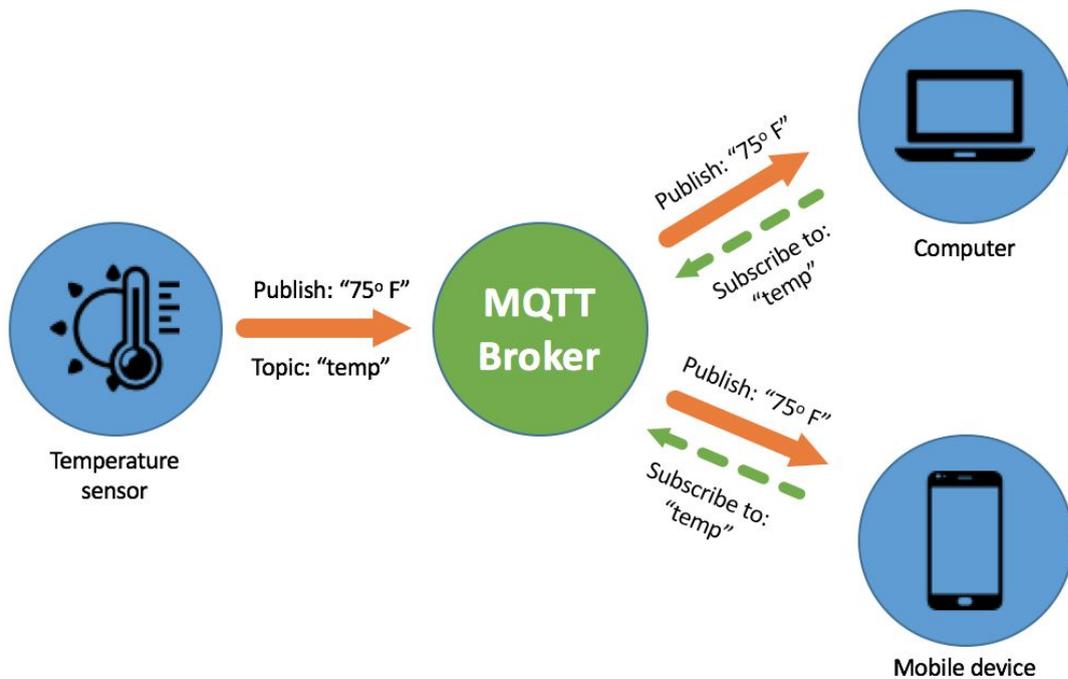
O MQTT é um protocolo de aplicação leve, baseado na topologia publish/subscribe para envio de mensagens. Muito aplicado em cenários de comunicação remota entre dispositivos onde a quantidade de dados comunicados é reduzida e a largura de banda para comunicação é limitada [56].

O princípio de funcionamento do protocolo parte da utilização de um Servidor MQTT, também conhecido como Broker MQTT. Tal Servidor implementa estruturas de armazenamento de dados, referenciadas como tópicos. Cada tópico refere-se a uma estrutura de publicação (publisher) de dados, mas também possibilita a leitura (subscriber) dos dados [56].

Os publicadores (ou publishers) são responsáveis por se conectar ao broker e publicar mensagens [58]. São basicamente os sensores leves que se conectam ao broker para enviar seus dados e voltar a dormir sempre que possível [25]. Esta estratégia visa conservar e aumentar a vida útil das baterias que normalmente são utilizadas nos dispositivos provedores de dados.

Os assinantes (ou subscribers) são responsáveis por se conectar ao broker e receber as mensagens que lhes forem de interesse [58]. São aplicativos que estão interessados em um determinado tópico, ou dados sensoriais [25].

O broker é responsável por receber, enfileirar e disparar as mensagens recebidas dos publishers para os subscribers [58]. Os brokers classificam os dados sensoriais em tópicos e os enviam para os assinantes (subscribers) interessados nos tópicos [25].



Fonte: <https://www.appcelerator.com/blog/2018/03/api-builder-and-mqtt-for-iot-part-1/>

7.5.1.2. Vantagem

Um dos pontos fortes desse protocolo é o desacoplamento entre o publisher e o subscriber. Os dois elementos têm conhecimento zero um do outro, permitindo uma independência muito grande entre os elementos que populam as mensagens no broker e os elementos que irão consumir essa informação [57].

E essa independência favorece, e muito, a adoção do protocolo no ambiente móvel e, principalmente, no mundo da Internet das Coisas. Justamente porque a heterogeneidade dos elementos, tanto no publish quanto no subscribe, é muito grande [57].

7.5.1.3. Contraponto

A dependência de um Broker e a utilização do TCP também pode ser um empecilho, pois ambos, assinantes e publicadores, necessitam de um certo poder computacional para funcionar, impossibilitando o uso MQTT em dispositivos mais simples. Por necessitar de um broker, este protocolo se torna uma boa opção para comunicação remota/cloud, pelo fato do servidor cloud atuar como o broker entre o dispositivo IoT e outros serviços [6].

7.5.2. SMQTT

SMQTT é uma extensão do MQTT, Secure MQTT, foi proposto para melhorar a segurança do MQTT. O algoritmo de criptografia consiste em 4 estágios principais: setup, cifração, publicação e decifração [7]. O SMQTT aumenta o recurso de segurança para o protocolo MQTT existente e suas variantes com base na Criptografia Baseada em Atributo (Attribute Based Encryption - ABE), sobre curvas elípticas. [60].

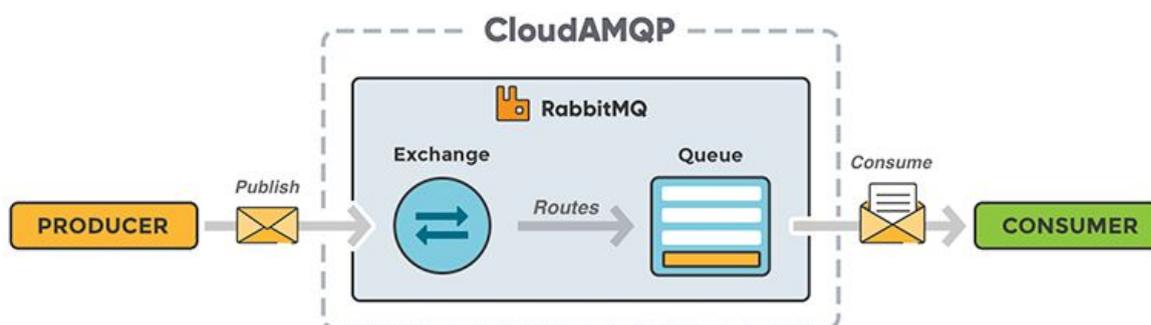
Essa abordagem funciona da seguinte maneira, o Publisher envia mensagem criptografada para o Broker do cluster ao qual pertence. Em seguida, Broker desse cluster encaminha mensagem criptografada para todos os assinantes no mesmo cluster, bem como Broker de outros clusters. Todos os assinantes, descriptografam mensagem usando as chaves fornecidas pelo PKG Global (Broker) da nuvem, o que torna esse processo complexo, onde o assinante recebe uma chave para decifrar os dados em que está inscrito [60].

Esse modelo, segundo os autores, se mostrou resistente a ataques de plaintext conhecido, ciphertext conhecido e de man-in-the-middle [59]. Por outro lado não se tem um estudo focado no impacto dos processos de criptografia nos dispositivos que capturam os dados, os publishers, e os enviam criptografados ao Broker e a descriptografia por parte dos clientes, os subscribers. No que tange os subscribers, em tese, o impacto não se torna muito impeditivo, porém por parte dos publishers, normalmente sensores e dispositivos de baixa potência e consumo de energia, pode afetar diretamente o consumo de energia e/ou a latência da entrega dos dados, quando a aplicação requer dados em tempo real.

7.5.3. AMQP

O AMQP, sigla para o inglês Advanced Message Queuing Protocol ou Protocolo de Enfileiramento de Mensagens Avançado em português, foi inicialmente projetado para o setor financeiro [25]. O AMQP é um projeto de código aberto para mensagens assíncronas por fio e permite mensagens criptografadas e interoperáveis entre organizações e aplicativos [64]. O protocolo fornece uma arquitetura de publicação / assinatura semelhante à do MQTT [25]. O protocolo tem um simples objetivo: definir a mecânica da transferência segura, confiável e eficiente de mensagens entre duas partes [64].

AMQP é tudo sobre filas. Ele envia mensagens transacionais entre os servidores. Como um middleware centrado na mensagem que surgiu do setor bancário, ele pode processar milhares de transações enfileiradas com confiabilidade [65]. A central, equivalente ao broker do MQTT, é responsável por receber mensagens do editor e distribuí-las em filas com base em funções e condições predefinidas. As filas representam basicamente os tópicos e são assinados pelos assinantes que receberão os dados sensoriais sempre que estiverem disponíveis na fila [25].



Fonte: <https://www.cloudamqp.com/docs/amqp.html>

7.5.3.1. Segurança e Interoperabilidade

O AMQP está focado em não perder mensagens. As comunicações dos editores para as trocas e das filas para os assinantes usam o TCP, que fornece conexão ponto-a-ponto estritamente confiável. Além disso, os endpoints devem reconhecer a aceitação de cada mensagem. O padrão também descreve um modo de transação opcional com uma sequência formal de confirmação de várias fases. Fiel às suas origens no setor bancário, o middleware AMQP se concentra no rastreamento de todas as mensagens e garante que cada uma delas seja entregue como pretendido, independentemente de falhas ou reinicializações [65].

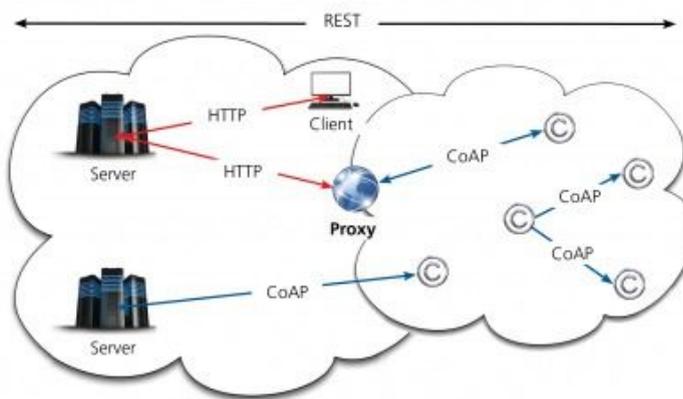
Este protocolo é eficiente, portátil, multicanal e seguro. O protocolo binário oferece autenticação e criptografia por meio de SASL ou TLS, contando com um protocolo de transporte como o TCP. O protocolo de mensagens é rápido e oferece entrega garantida com reconhecimento de mensagens recebidas. O AMQP funciona bem em ambientes de múltiplos clientes e fornece um meio para delegar tarefas e fazer com que os servidores lidem com solicitações imediatas mais rapidamente. Como o AMQP é um sistema de mensagens binárias transmitido com um comportamento de mensagens altamente obrigatório, a interoperabilidade de clientes de diferentes fornecedores é garantida [64].

O AMQP é um protocolo de enquadramento e transferência. O enquadramento significa que ele fornece a estrutura para fluxos de dados binários que fluem em qualquer direção de uma conexão de rede. A estrutura oferece delimitação para que blocos de dados distintos, chamados de *quadros* sejam trocados entre as partes conectadas. Os recursos de transferência garantem que ambas as partes da comunicação possam estabelecer uma compreensão geral sobre quando os quadros deverão ser transferidos e quando as transferências deverão ser consideradas concluídas [63].

7.5.4. CoAP

O CoAP, do inglês Constrained Application Protocol ou Protocolo de Aplicação Restrita, representa o protocolo para a camada de sessão para redes e nós com restrições. É definido para aplicações M2M e, assemelha-se ao HTTP. Utiliza de comandos GET, PUT, POST e DELETE, do modelo REST, e faz uso de conceitos da web como URIs [59]. CoAP foi projetado pelo grupo de trabalho IETF RESTful Environment (Core) para fornecer uma interface RESTful (HTTP) leve [25] e para permitir que sensores de baixa potência usem serviços RESTful enquanto atendem às restrições de energia [25].

Este protocolo utiliza o modelo 'cliente/servidor', o qual disponibiliza interação 'request/response' um-para-um, podendo também suportar multicast. Diferente do MQTT, o CoAP surgiu para suprir a necessidade em protocolos IoT, desenvolvido para interoperar com HTTP e com arquiteturas RESTful, através de simples proxies, tornando-se compatível com a Internet [6]. O CoAP se difere do conceito do REST padrão por usar o protocolo UDP, o que o coloca como mais adequado para aplicações em IoT [45].



Fonte: <https://www.u-blox.com/en/ip-versus-coap-iot-communications>

7.5.4.1. Arquitetura

A implementação do CoAP, se comporta tanto como servidor como cliente em uma comunicação M2M. O modelo de mensagem do CoAP é baseado na troca de mensagem, sobre UDP, entre dois pontos em que um cliente requisita uma ação (utilizando um código de método), de um recurso (identificado por uma URI),

localizado em um servidor, que retorna uma resposta com um código de resposta. As mensagens são trocadas de maneira assíncrona e, como é realizada sobre UDP, o protocolo fornece um mecanismo leve para a confiabilidade [59].

Por utilizar o protocolo UDP, o CoAP apresenta menor consumo computacional e energético. Seu uso permite um menor tempo de resposta quando acionado, pois mantém uma conexão ativa entre nodos. Este protocolo é mais indicado para envio de comandos para nodos locais, por se tratar de uma arquitetura semelhante a HTTP [6].

A arquitetura CoAP é dividida em duas subcamadas principais: mensagem e solicitação/resposta. A subcamada de mensagens é responsável pela confiabilidade e duplicação de mensagens, enquanto a subcamada de solicitação/resposta é responsável pela comunicação. O CoAP possui quatro modos de mensagens: confirmable, non-confirmable, piggyback e separate. Os modos confirmable e non-confirmable representam as transmissões confiáveis e não confiáveis, respectivamente, enquanto os outros modos são usados para solicitação/resposta. Piggyback é usado para comunicação direta cliente/servidor, onde o servidor envia sua resposta diretamente após receber a mensagem, ou seja, dentro da mensagem de confirmação. Por outro lado, o modo separado é usado quando a resposta do servidor vem em uma mensagem separada da confirmação e pode levar algum tempo para ser enviada pelo servidor. [25].

7.5.5. XMPP

O XMPP, do inglês Extensible Messaging and Presence Protocol ou Mensagens Extensíveis e Protocolo de Presença, foi originalmente chamado de “Jabber” [65] e é um protocolo de comunicação para middleware orientado a mensagens [66], projetado originalmente para bate-papo e troca de mensagens e foi padronizado pela IETF. É muito conhecido e provou ser altamente eficiente através da internet [25]. Recentemente, ele foi reutilizado para aplicativos IoT, bem como um protocolo para SDN. Essa reutilização do mesmo padrão se deve ao uso do XML, que o torna facilmente extensível. O XMPP suporta a arquitetura de

publicação/assinatura e solicitação/resposta, e cabe ao desenvolvedor do aplicativo escolher qual arquitetura usar. Ele é projetado para troca de dados estruturados, em um modelo que se aproxima de tempo-real enviando pequenos pedaços de mensagem conhecidos por “XML Stanzas” [59], portanto, suporta eficientemente mensagens pequenas de baixa latência.

O principal recurso do XMPP é: Core [XMPP-CORE]. Esse recurso, principalmente os fluxos de XML, fornecem os blocos de construção para muitos tipos de eventos, quase reais, que podem ser colocados em camadas no topo do núcleo enviando dados específicos do aplicativo qualificados por espaços de nomes XML específicos [XML-NAMES] [66].

No contexto da IoT, o XMPP oferece uma maneira fácil de endereçar um dispositivo. Isso é especialmente útil se esses dados estiverem entre pontos distantes. Não é projetado para ser rápido. Na verdade, a maioria das implementações usa pesquisa ou verificação de atualizações apenas sob demanda. O "tempo real" para o XMPP está em escalas humanas, medido em segundos [65].

7.5.5.1. Contraponto

O XMPP não fornece nenhuma garantia de qualidade de serviço e, portanto, não é prático para comunicações M2M. Além disso, as mensagens XML criam uma sobrecarga adicional devido a muitos cabeçalhos e formatos de tag que aumentam o consumo de energia que é crítico para o aplicativo IoT. Por isso, o XMPP é raramente usado em IoT, mas ganhou algum interesse para melhorar sua arquitetura, a fim de suportar aplicativos IoT [25].

7.5.5.2. Segurança

O XMPP utiliza da segurança provida pelo TLS. No RFC 7590 são especificadas recomendações da utilização do TLS pelo protocolo de maneira segura. O documento provê também informações relativas ao que já está definido no padrão do protocolo (RFC 6120) em termos de segurança, como a obrigatoriedade de que clientes autentiquem servidores, servidores autentiquem clientes e que servidores não devem autenticar outros servidores [59].

8. CONCLUSÃO

Durante este trabalho foram apresentados alguns dos principais protocolos de comunicação utilizados em internet das coisas. Não é a maioria, pelo contrário, existem diversos outros protocolos, cada um com foco em uma finalidade, desde economia de energia, capacidade de alcance até minimização de tráfego de dados.

O ponto chave que determina quais protocolos podem se adequar corretamente as necessidade de um projeto é a etapa de levantamento de requisitos. As decisões tomadas neste processo dão o correto direcionamento sobre quais protocolos são melhores, ou possuem um melhor custo/benefício.

É interessante notar que não se pode ter o melhor de todos os mundos. Quando um dos requisitos principais é a aquisição de dados a longas distâncias, o consumo energético ou a taxa de transferência de dados são diretamente afetados. Enquanto que se o consumo energético for vital para aplicações que envolvam bateria, tanto taxa de transferência quanto distância alcançadas podem ser diretamente afetados.

Ainda em projetos com aquisição de dados de longo alcance, onde se tem vários dispositivos coletando dados pode-se considerar utilizar hardwares e protocolos capazes de construir uma rede tal que possam se comunicar, de modo a transferir e centralizar os dados em um nó com maior poder de processamento e comunicação, que ficará responsável pelo armazenamento local e envio posterior a um servidor.

Neste cenário torna-se possível utilizar hardwares mais discretos e dedicados, possibilitando assim um menor custo com aquisição dos dispositivos, economia ainda maior de energia, e maior coleta de dados em consequência da possível compra de mais dispositivos sensores por exemplo, devido ao preço reduzido dos mesmos.

Os protocolos das camadas de enlace e de rede tem grande influência neste tipo de análise. Estes podem implementar diversas estratégias de comunicação ponto a ponto a fim de encontrar a melhor rota possível para que a informação chegue a um nó centralizador ou outro nó qualquer de destino.

Em redes onde os nós responsáveis por efetivamente sincronizar os dados obtido com servidores utilizam planos de dados, normalmente utilizando redes móveis como o 3G e 4G, é importante considerar a utilização dos protocolos das camadas mais superiores como encapsulamento e sessão capazes de minimizar gasto de banda reduzindo o *overhead* de informação neste processo.

Em resumo, a etapa de definição de requisitos de um projeto em internet das coisas onde é discutido o modo como as informações são trafegadas é, ou pode ser, bem mais do que um simples envio para web das informações adquiridas de sensores ou outros meios de conectar as coisas. Desde o nível mais baixo, onde se tem preocupações com consumo e alcance até as mais superiores, onde grande parte do foco na internet se converte, existem diversos tipo de protocolos que podem tornar a viabilidade de um projeto muito mais atraente a um potencial cliente.

9. BIBLIOGRAFIA

[1] INFOPEDIA. **Protocolos de comunicação**. Disponível em: <https://keep.google.com/#NOTE/1zvRryGpriHLFcskwct3-hB-SL8GQ3a5-7HW-fgPPT0nHWIjtnxvr_mNjBj_FrA>. Acesso em 01/08/2018.

[2] SUYAMA, MARIA. **Protocolos de comunicações**. Disponível em: <<http://www.criarweb.com/artigos/533.php>>. Acesso em 01/08/2018.

[3] FLORÊNCIO, HEITOR MEDEIROS. **Redes Industriais**. Disponível em: <https://www.dca.ufrn.br/~heitor/aulasDCA/dca0107/aula03_RedesIndustriais-old.pdf>. Acesso em 01/08/2018.

[4] VIDAL, VITOR. **10 protocolos de IoT que você deveria conhecer**. Disponível em: <<https://www.professionaisti.com.br/2017/11/10-protocolos-de-iot-que-voce-deveria-conhecer/>>. Acesso em 01/08/2018.

[5] MOMOTE, VICTOR. **Modelos de comunicação para IoT**. Disponível em: <<https://www.embarcados.com.br/modelos-de-comunicacao-para-iot/>>. Acesso em 01/08/2018.

[6] ROTTA, GIOVANNI. CHARÃO, Andrea. DANTAS, MARIO. **Um Estudo sobre Protocolos de Comunicação para Ambientes de Internet das Coisas**. Disponível em: <<http://www.lbd.dcc.ufmg.br/colecoes/erad/2017/091.pdf>>. Acesso em 01/08/2018.

[7] PATRICIO, NATHALIA SAUTCHUK. **Protocolos de Rede para Internet das Coisas**. Disponível em: <<https://pt.slideshare.net/nathaliapatricio/protocolos-de-rede-para-internet-das-coisas>>. Acesso em 01/08/2018.

[8] ROSA, DAYANE. **Modelo OSI, o que é, quem criou e como funciona**. Disponível em: <<https://www.linkedin.com/article/modelo-osi-o-que-%C3%A9-quem-criou-como-funciona-dayane-rosa?originalSubdomain=pt>>. Acesso em 01/08/2018.

[9] TELECO. **Modelo OSI: Camada 1: Física**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialosi/pagina_5.asp>. Acesso em 01/08/2018.

[10] TELECO. **Modelo OSI: Camadas 2 a 7**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialosi/pagina_6.asp>. Acesso em 01/08/2018.

- [11] MELO, PABLO. **Padrão IEEE 802.15.4 - A base para as especificações Zigbee, WirelessHart e MiWi.** Disponível em: <<https://www.embarcados.com.br/padrao-ieee-802-15-4/>>. Acesso em 04/08/2018.
- [12] ANASTASI, GIUSEPPE. **IEEE 802.15.4e Standard. A Building Block for the Internet of (Relevant) Things.** Disponível em: <<http://info.iet.unipi.it/~anastasi/talks/2016-MST.pdf>>. Acesso em 04/08/2018.
- [13] UFRJ. **IEEE 802.11ah.** Disponível em: <https://www.gta.ufrj.br/grad/15_1/802.11ah/ieee80211ah.html>. Acesso em 04/08/2018.
- [14] UFRJ. **IEEE 802.11ah.Aplicações.** Disponível em: <https://www.gta.ufrj.br/grad/15_1/802.11ah/aplicacao.html>. Acesso em 04/08/2018.
- [15] GOMEZ, CARLES. OLLER, JOAQUIM. PARADELLS, JOSEP. **Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology.** Disponível em: <<https://www.mdpi.com/1424-8220/12/9/11734/htm>>. Acesso em 08/08/2018.
- [16] PESSOA, LEANDRO. **Introdução ao Bluetooth Smart (BLE).** Disponível em: <<https://www.embarcados.com.br/bluetooth-smart-ble/>>. Acesso em 08/08/2018.
- [17] BARBOSA, THIAGO. CARVALHO, FABRÍCIO BRAGA SOARES. **Rede de Comunicação de Medidores Inteligentes Sem Fio.** Disponível em: <https://www.researchgate.net/publication/269059045_Rede_de_Comunicacao_de_Medidores_Inteligentes_Sem_Fio>. Acesso em 09/08/2018.
- [18] AZEVEDO, MÓNICA SOFIA REI **Monitorização da Qualidade do Ar utilizando Redes de Sensores Sem Fios Oportunistas.** Disponível em: <https://paginas.fe.up.pt/~ee05143/Diss/documentos/MQAUWSNO_5Mar.docx>. Acesso em 09/08/2018.
- [19] AMÂNCIO, ANDERSON. **Algumas Perguntas Frequentes Sobre o Zigbee** Disponível em: <<http://wireengenharia.com.br/br/tag/zigbee/>>. Acesso em 10/08/2018.
- [20] ECIL ENERGIA, **Smart Grid** Disponível em: <<http://www.ecilenergia.com.br/download/Smart%20Grid%20-%20Inovcity%20Aparecida.pdf>>. Acesso em 10/08/2018.

- [21] Rane, U. A. PATIL, ANIKET V. **A Review on ZIGBEE Smart Energy Implementation for Energy Efficient Building**. Disponível em: <http://www.ijera.com/papers/Vol4_issue3/Version%201/DW4301735740.pdf>. Acesso em 10/08/2018.
- [22] FERREIRA, ISRAEL V. GODOY, EDUARDO P. **INTEGRAÇÃO DE INTERNET DAS COISAS E ZIGBEE NO CONTEXTO DE EFICIÊNCIA ENERGÉTICA E AUTOMAÇÃO PREDIAL**. Disponível em: <<https://ssl4799.websiteseuro.com/swge5/PROCEEDINGS/PDF/CBA2016-0415.pdf>>. Acesso em 10/08/2018.
- [23] LIM, JAE-HYUN. HAN, DAE-MAN. **Design and implementation of smart home energy management systems based on zigbee**. Disponível em: <<https://ieeexplore.ieee.org/document/5606278>>. Acesso em 10/08/2018.
- [24] DIAS, RENATA RAMPIM DE FREITAS. **ZigBee e a Internet das Coisas**. Disponível em: <<http://brasil.rfidjournal.com/artigos/vision?14126/>>. Acesso em 10/08/2018.
- [25] SALMAN, TARA **Internet of Things Protocols and Standards**. Disponível em: <https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/>. Acesso em 11/08/2018.
- [26] ITU-T. **Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications**. Disponível em: <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9959-201501-!!!PDF-E&type=items>. Acesso em 11/08/2018.
- [27] IETF. **Transmission of IPv6 Packets over ITU-T G.9959 Networks**. Disponível em: <<https://tools.ietf.org/html/rfc7428>>. Acesso em 11/08/2018.
- [28] ITU. **Sector Members, Associates and Academia**. Disponível em: <<https://www.itu.int/en/membership/Pages/sector-members.aspx>>. Acesso em 11/08/2018.
- [29] AGÊNCIA EFE. **Z-Wave fortalece a sua liderança como tecnologia preferida para a Internet of Things for Smart Home**. Disponível em: <https://www.efe.com/efe/brasil/comunicado-imprensa/z-wave-fortalece-a-sua-lideranca-como-tecnologia-preferida-para-internet-of-things-for-smart-home/50000252-MULTIMEDIAE_2503926>. Acesso em 11/08/2018.

[30] ROHDE-SCHWARZ. **Conceitos Básicos de LTE / LTE-Advanced**. Disponível em: <https://www.rohde-schwarz.com/br/tecnologias/celular/lte/tecnologia-lte/informacoes-sobre-lte_52292.html>. Acesso em 12/08/2018.

[31] TELECO. **Redes 4G: LTE Advanced**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredes4gev/pagina_5.asp>. Acesso em 12/08/2018.

[32] MELO, PABLO. **Tecnologias celulares aplicadas em IoT**. Disponível em: <<https://www.embarcados.com.br/tecnologias-celulares-aplicadas-em-iot/>>. Acesso em 12/08/2018.

[33] LSR. **Technical Overview of DECT ULE** Disponível em: <<https://www.lsr.com/white-papers/technical-overview-of-dect-ule>>. Acesso em 12/08/2018.

[34] ETSI. **DECT ULE** Disponível em: <<https://www.etsi.org/technologies-clusters/technologies/dect/dect-ule>>. Acesso em 12/08/2018.

[35] THE CROW GROUP. **DECT-ULE Peripherals**. Disponível em: <http://www.thecrowgroup.com/Products_Systems/dect_ule_peripherals/dect_ule_peripherals/>. Acesso em 12/08/2018.

[36] RF WIRELESS WORLD. **DECT ULE Tutorial**. Disponível em: <<http://www.rfwireless-world.com/Tutorials/DECT-ULE-tutorial.html>>. Acesso em 12/08/2018.

[37] BUSH, STEVE. **DECT ULE connects homes for IoT** Disponível em: <<https://www.electronicweeky.com/news/design/communications/dect-ule-connects-homes-iot-2015-09/>>. Acesso em 12/08/2018.

[38] ALECRIM, EMERSON. **O que é Internet das Coisas (Internet of Things)?** Disponível em: <<https://www.infowester.com/iot.php>>. Acesso em 13/08/2018.

[39] ZAMBARDA, PEDRO. **‘Internet das Coisas’: entenda o conceito e o que muda com a tecnologia**. Disponível em: <<https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>>. Acesso em 13/08/2018.

[40] MAGNUS, TIAGO. **O que é IoT (Internet das Coisas)? Futuro ou Presente?** Disponível em: <<https://transformacaodigital.com/o-que-e-iot-internet-das-coisas/>>. Acesso em 13/08/2018.

[41] sas. **Internet das Coisas (IoT) O que é e qual sua importância?** Disponível em: <https://www.sas.com/pt_br/insights/big-data/internet-das-coisas.html>. Acesso em 13/08/2018.

[42] PROOF. **INTERNET DAS COISAS E SEUS DESAFIOS DE SEGURANÇA.** Disponível em: <<https://www.proof.com.br/blog/iot-internet-das-coisas/>>. Acesso em 13/08/2018.

[43] COTRIM, JEFERSON RODRIGUES. **Protocolo de Roteamento RPL** Disponível em: <<http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/rsf2016/rpl.pdf>>. Acesso em 14/08/2018.

[44] COTRIM, JEFERSON RODRIGUES. KLEINSCHMIDT JOÃO HENRIQUE. **Avaliação de Desempenho do Protocolo RPL em Ambientes com Mobilidade.** Disponível em: <https://www.researchgate.net/publication/307980622_Avaliacao_de_Desempenho_do_Protocolo_RPL_em_Ambientes_com_Mobilidade>. Acesso em 14/08/2018.

[45] SANTOS, BRUNO P. SILVA, LUCAS A. M. CLAYSON S. F. S. CELES. NETO, JOÃO B. BORGES. PERES, BRUNA S. VIEIRA, MARCOS AUGUSTO M. VIEIRA, LUIZ FILIPE M. GOUSSEVSKAIA, OLGA N. LOUREIRO, ANTONIO A. F. . **Internet das Coisas: da Teoria à Prática.** Disponível em: <<https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>>. Acesso em 14/08/2018.

[46] GRENOBLE. **A Internet e a Rede das coisas: desafios e oportunidades.** Disponível em: <<http://grenoble.ime.usp.br/~gold/cursos/2013/movel/mono1st/2305-Straus.pdf>>. Acesso em 14/08/2018.

[47] GONZÁLES, AGUSTÍN ROCHA. **Modelado y simulación de redes de sensores inalámbricas subacuáticas.** Disponível em: <<https://riunet.upv.es/bitstream/handle/10251/54029/ROCA%20-%20Modelado%20y%20simulaci%F3n%20de%20redes%20de%20sensores%20inal%20mbricas%20subacu%20ticas..pdf?sequence=2>>. Acesso em 15/08/2018.

[48] RF WIRELESS WORLD. **RPL vs CORPL vs CARP-difference between RPL,CORPL,CARP IoT.** Disponível em: <<http://www.rfwireless-world.com/Terminology/RPL-vs-CORPL-vs-CARP.html>>. Acesso em 15/08/2018.

[49] AIJAZ, ADNAN. SU, HONGJIA. AGHVAMI, A. HAMI. **CORPL: A routing protocol for cognitive radio enabled AMI networks.** Disponível em:

<https://www.researchgate.net/publication/265709173_CORPL_A_routing_protocol_for_cognitive_radio_enabled_AMI_networks>. Acesso em 15/08/2018.

[50] GRAM-HANSEN, RIKKE. **Internet of Things and Data Analytics Handbook**. Disponível em: <<https://books.google.com.br/books?id=V3mYDQAAQBAJ&pg=PA224&lpg=PA224&dq=CORPL%20iot&source=bl&ots=QsoRVJpfNX&sig=bKKoHG8mbmy0K99vYocKcQMUtBk&hl=pt-BR&sa=X&ved=2ahUKEwji2o2ZiPDcAhVBHJAKHY3IDTgQ6AEwEnoECFoQAQ&authuser=0#v=onepage&q=CORPL%20iot&f=false>>. Acesso em 15/08/2018.

[51] GRAM-HANSEN, RIKKE. **Internet of Things and Data Analytics Handbook**. Disponível em: <<https://books.google.com.br/books?id=V3mYDQAAQBAJ&pg=PA224&lpg=PA224&dq=CORPL%20iot&source=bl&ots=QsoRVJpfNX&sig=bKKoHG8mbmy0K99vYocKcQMUtBk&hl=pt-BR&sa=X&ved=2ahUKEwji2o2ZiPDcAhVBHJAKHY3IDTgQ6AEwEnoECFoQAQ&authuser=0#v=onepage&q=6LoWPAN&f=false>>. Acesso em 15/08/2018.

[52] DATA TRACKER. **IPv6 over Networks of Resource-constrained Nodes (6lo)**. Disponível em: <<https://datatracker.ietf.org/wg/6lo/charter/>>. Acesso em 20/08/2018.

[53] ØVREBEKK, TORBJØRN. **Why run IPV6 over Bluetooth low energy?** Disponível em: <<https://blog.nordicsemi.com/getconnected/why-run-ipv6-over-blue-tooth-low-energy>>. Acesso em 20/08/2018.

[54] MQTT.ORG. **MQTT**. Disponível em: <<http://mqtt.org/>>. Acesso em 21/08/2018.

[55] YUAN, MICHAEL. **Conhecendo o MQTT**. Disponível em: <<https://www.ibm.com/developerworks/br/library/iot-mqtt-why-good-for-iot/index.html>>. Acesso em 21/08/2018.

[56] FIWARE LAB . **Apresentação do protocolo MQTT como alternativa para comunicação IoT**. Disponível em: <<http://fiwarelabsp.org/2016/07/apresentacao-do-protocolo-mqtt/>>. Acesso em 21/08/2018.

[57] OGLIARI, RICARDO. **Popularização do padrão Publisher/Subscriber no mobile e na IoT**. Disponível em: <<https://imasters.com.br/desenvolvimento/popularizacao-do-padrao-publishersubscriber-no-mobile-e-na-iot>>. Acesso em 21/08/2018.

[58] VICENZI, ALEXANDRE. **MQTT Parte 1: O que é MQTT?** Disponível em: <<https://butecoopopensource.github.io/mqtt-parte-1-o-que-e-mqtt/>>. Acesso em 21/08/2018.

[59] MAGALHÃES, GABRIEL G. M. S. **Estudo de segurança nos principais protocolos da Internet das Coisas.** Disponível em: <http://bdm.unb.br/bitstream/10483/14252/1/2016_GabrielGonzagaMartinsSoutodeMagalhaes.pdf>. Acesso em 21/08/2018.

[60] NEVES, FLÁVIO DA SILVA. **Uma Abordagem de Segurança para os Dados Transmítidos por Dispositivos em Internet das Coisas.** Disponível em: <<https://repositorio.ufpe.br/bitstream/123456789/24888/1/DISSERTA%C3%87%C3%83O%20FI%C3%A1vio%20da%20Silva%20Neves.pdf>>. Acesso em 21/08/2018.

[61] SIMAS, LUIS GABRIEL NASCIMENTO. **Introdução ao AMQP com RabbitMQ.** Disponível em: <<https://www.devmedia.com.br/introducao-ao-amqp-com-rabbitmq/33036>>. Acesso em 25/08/2018.

[62] PELLURU, SREEDHAR. **Suporte ao AMQP 1.0 no Barramento de Serviço.** Disponível em: <<https://docs.microsoft.com/pt-br/azure/service-bus-messaging/service-bus-amqp-overview>>. Acesso em 25/08/2018.

[63] VASTERS, CLEMENS. **AMQP 1.0 no guia de protocolo do Barramento de Serviço e dos Hubs de Eventos do Azure.** Disponível em: <<https://docs.microsoft.com/pt-br/azure/service-bus-messaging/service-bus-amqp-protocol-guide>>. Acesso em 25/08/2018.

[64] ROUSE, MARGARET. **Advanced Message Queuing Protocol (AMQP).** Disponível em: <<https://whatis.techtarget.com/definition/Advanced-Message-Queuing-Protocol-AMQP>>. Acesso em 25/08/2018.

[65] SCHNEIDER, STAN. **Understanding The Protocols Behind The Internet Of Things.** Disponível em: <<https://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things>>. Acesso em 25/08/2018.

[66] AMÂNCIO, ANDERSON. **Protocolos Envolvidos na IoT.** Disponível em: <<http://wireengenharia.com.br/br/tag/xmpp/>>. Acesso em 26/08/2018.

[67] JÚNIOR, VIDAL PEREIRA DA SILVA. **Conheça a tecnologia LoRa® e o protocolo LoRaWAN.** Disponível em: <<https://www.embarcados.com.br/conheca-tecnologia-lora-e-o-protocolo-lorawan/>>. Acesso em 28/08/2018.

[68] HATTON, MATT. **The global M2M market is set to reach 27 billion connections in 2024, generating US\$1.6 trillion in revenue.** Disponível em: <<https://www.iot-now.com/2015/06/24/34330-the-global-m2m-market-is-set-to-reach>>

27-billion-connections-in-2024-generating-usd1-6-trillion-in-revenue/>. Acesso em 30/08/2018.

[69] AMÂNCIO, ANDERSON.. **O Protocolo Sigfox**. Disponível em: <<http://wireengenharia.com.br/br/o-protocolo-sigfox/>>. Acesso em 30/08/2018.

[70] ENBARCADOS. **Uma visão técnica da Rede Sigfox**. Disponível em: <<https://www.embarcados.com.br/uma-visao-tecnica-da-rede-sigfox/>>. Acesso em 30/08/2018.

[71] FAGUNDES, EDUARDO. **Sigfox uma plataforma para IoT**. Disponível em: <<http://efagundes.com/blog/sigfox-uma-plataforma-para-iot/>>. Acesso em 30/08/2018.