

Elço João dos Santos Junior

**Análise do impacto de técnicas de diversidade na
comunicação entre dispositivos LoRa/LoRaWAN**

Florianópolis

2019

Elço João dos Santos Junior

**ANÁLISE DO IMPACTO DE TÉCNICAS DE DIVERSIDADE
NA COMUNICAÇÃO ENTRE DISPOSITIVOS
LORA/LORAWAN**

Trabalho de Conclusão de Curso submetido ao Departamento de Engenharia Elétrica e Eletrônica da Universidade Federal de Santa Catarina para a obtenção do título de Bacharel em Engenharia Eletrônica.

Orientador: Richard Demo Souza

Florianópolis

2019

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Santos Junior, Elço João dos

Análise do impacto de técnicas de diversidade na comunicação entre dispositivos LoRa/LoRaWAN / Elço João dos Santos Junior ; orientador, Richard Demo Souza, 2019.

93 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Tecnológico, Graduação em Engenharia Eletrônica, Florianópolis, 2019.

Inclui referências.

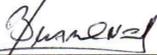
1. Engenharia Eletrônica. 2. Comunicações sem fio. 3. LoRaWAN. 4. Diversidade temporal. 5. Diversidade espacial. I. Souza, Richard Demo. II. Universidade Federal de Santa Catarina. Graduação em Engenharia Eletrônica. III. Título.

Elço João dos Santos Junior

**Análise do impacto de técnicas de diversidade na
comunicação entre dispositivos LoRa/LoRaWAN**

Este Trabalho foi julgado adequado para obtenção do Título de Bacharel em
Engenharia Eletrônica e aprovado em sua forma final pela sua Banca
Examinadora.

Florianópolis, 17 de maio de 2019.



Prof. Jefferson Luiz Brum Marques, Dr.
Coordenador do Curso

Banca examinadora:



Prof. Richard Demo Souza, Dr.
Orientador
Universidade Federal de Santa Catarina



Prof. Arliones Stevert Hoeller Jr., MSc.
Instituto Federal de Santa Catarina



Prof. Walter Antônio Gontijo, MSc.
Universidade do Vale do Itajaí

“Este trabalho é dedicado à minha família.”

AGRADECIMENTOS

Agradeço, primeiramente, à minha família por todo apoio durante estes anos de faculdade, sempre me fazendo acreditar que a educação é capaz de mudar vidas e nos levar a lugares que sempre sonhamos. À minha namorada, Ana Paula, por estar ao meu lado em todos os momentos, compartilhando os desafios e vitórias durante essa jornada que é a graduação. Ao meu colega de trabalho e amigo Fabiano, pela ajuda durante os testes de campo. E ao professor Richard pela orientação durante o trabalho, uma pessoa que tenho muita admiração, respeito e considero ser um profissional diferenciado no âmbito da educação.

Agradeço também ao Instituto Senai de Inovação em Sistemas Embarcados (ISI-SE), local no qual adquiri conhecimentos que foram de grande ajuda no desenvolvimento do trabalho, bem como às pessoas que lá trabalham. Também desejo agradecer ao financiamento parcial do trabalho através do projeto F-LOCO com recursos de P&D ANEEL/Grupo Energisa, código 00405-1804/2018, executado pelo INESC P&D Brasil.

“Dream big. Work hard. Stay humble.”
(Autor desconhecido)

RESUMO

Em redes de dispositivos que se comunicam por meio de uma tecnologia sem fio, como LoRa, os sinais que são transmitidos estão sujeitos a efeitos como *fading*, *shadowing* e *path loss*. Devido a isso, é preciso encontrar formas de se melhorar a confiabilidade da comunicação, aumentando a taxa de sucesso de entrega das mensagens. O protocolo LoRaWAN permite a utilização de mensagens de *uplink* confirmadas, que recebem uma mensagem de *downlink* atestando o recebimento, porém, esta técnica apresenta limitações quando utilizada em redes densas. Pode-se optar pela utilização de técnicas de diversidade, as quais foram investigadas neste trabalho, apresentando um resultado satisfatório em termos de probabilidade de conexão, ficando em torno de 90% a uma distância de 4 km no ambiente urbano, dentro do contexto de *smart cities*. Além disso, a diversidade faz com que o impacto dos efeitos citados acima seja reduzido, pois as diferentes versões de uma mesma mensagem experimentam versões não correlacionadas do canal. Os resultados mostraram que tanto a diversidade espacial quanto a temporal melhoraram a comunicação entre os dispositivos LoRa/LoRaWAN utilizados no trabalho, apresentando resultados praticamente iguais ao se utilizar duas antenas ou ao enviar uma mesma mensagem duas vezes. Porém, a diversidade temporal deve ser utilizada de forma controlada, pois pode aumentar a colisão entre pacotes em redes com um grande número de nós. O aumento da diversidade espacial é, por outro lado, sempre benéfica.

Palavras-chave: comunicações sem fio. diversidade. lora. lorawan.

ABSTRACT

In networks where devices communicate with each other through some wireless technology such as LoRa, transmitted signals are subject to effects such as fading, shadowing, and path loss. Because of this, it is necessary to find ways to improve the communication reliability, increasing message delivery. The LoRaWAN protocol allows the use of uplink confirmed messages, which receive a downlink message attesting the reception, but this technique has limitations when used in dense networks. It is possible to opt for the use of diversity techniques, which were investigated in this work, presenting a satisfactory result in terms of connection probability, being around 90% at a distance of 4 km in an urban environment, within the context of smart cities. In addition, the diversity reduced the impact caused by the effects mentioned above, since the different versions of the same message experience uncorrelated versions of the channel. The results showed that both spatial and temporal diversity improved the communication between the LoRa/LoRaWAN devices used in the work, presenting almost the same results when using two antennas or sending the same message twice. However, temporal diversity must be used in a controlled way, as it can increase the collision between packets in networks with a large number of nodes. Increased spatial diversity is, on the other hand, always beneficial.

Keywords: wireless communication. diversity. lora. lorawan.

LISTA DE FIGURAS

Figura 1 – Variáveis a serem monitoradas no contexto de <i>smart cities</i> .	25
Figura 2 – Topologia comum de uma rede LoRaWAN.	31
Figura 3 – Janelas de recebimento.	34
Figura 4 – Frequências do espectro utilizadas.	35
Figura 5 – Formato das mensagens. Tamanho dos campos está em <i>bits</i> .	38
Figura 6 – Cenário de utilização do modelo de dois raios.	43
Figura 7 – Distribuição <i>Rayleigh</i> .	46
Figura 8 – Distribuição <i>Rice</i> para diferentes valores de K .	47
Figura 9 – Distribuição <i>Nakagami</i> para diferentes valores de m .	47
Figura 10 – Variação da probabilidade de erro com o aumento da ordem da diversidade.	50
Figura 11 – Probabilidade de erro antes <i>vs</i> depois para diferentes ordens de diversidade.	51
Figura 12 – Placa B-L072Z-LRWAN1.	54
Figura 13 – Arquitetura do módulo CMWX1ZZABZ-091.	54
Figura 14 – Dispositivo resultante após montagem dos módulos.	56
Figura 15 – Máquina de estados do código do <i>end device</i> .	59
Figura 16 – Principais componentes de <i>hardware</i> e <i>software</i> do <i>gateway</i> .	61
Figura 17 – Topologia da rede montada para os testes.	63
Figura 18 – <i>Gateways</i> montados em campo.	64
Figura 19 – Exemplos de pontos de transmissão.	66
Figura 20 – Configuração da potência de transmissão segundo o padrão LoRaWAN.	67
Figura 21 – Valores de potência de transmissão obtidos pelo analisador de espectro.	69
Figura 22 – Exemplo da sequência de envio de mensagens.	70
Figura 23 – RSSI e RSSI médio para diferentes instantes de tempo.	73
Figura 24 – Variação instantânea da potência recebida para diferentes instantes de tempo.	74
Figura 25 – Distribuição do <i>fading</i> .	75
Figura 26 – RSSI e RSSI médio considerando diversidade espacial.	76

Figura 27 – Distribuição do <i>fading</i> considerando diversidade espacial.	77
Figura 28 – RSSI e RSSI médio considerando diversidade temporal.	78
Figura 29 – Distribuição do <i>fading</i> considerando diversidade temporal.	78
Figura 30 – RSSI e RSSI médio considerando ambas técnicas.	79
Figura 31 – Distribuição do <i>fading</i> considerando ambas técnicas.	80
Figura 32 – Probabilidade de conexão por ponto, por SF, sem considerar diversidade.	82
Figura 33 – Probabilidade de conexão por ponto, por SF, considerando diversidade espacial.	83
Figura 34 – Probabilidade de conexão por ponto, por SF, considerando diversidade temporal.	84
Figura 35 – Probabilidade de conexão por ponto, por SF, considerando ambas técnicas.	86
Figura 36 – Comparação do desempenho das técnicas para SF10.	87

LISTA DE TABELAS

Tabela 1	– Taxas de dados para diferentes valores de SF, $CR = \frac{4}{5}$ e $BW = 125$ KHz.	30
Tabela 2	– Exemplos de comandos AT.	58
Tabela 3	– Parâmetros do transmissor.	65
Tabela 4	– Sensibilidade do <i>gateway</i> para diferentes SFs.	71
Tabela 5	– Características dos canais entre cada ponto e o <i>gateway</i>	72
Tabela 6	– Valores de m para diferentes ordens de diversidade.	80

SUMÁRIO

1	INTRODUÇÃO	23
1.1	<i>Smart cities</i>	24
1.2	O porquê do uso de diversidade	26
1.3	Objetivos	26
1.3.1	Objetivo geral	26
1.3.2	Objetivos específicos	26
2	MODULAÇÃO LORA	29
2.1	Parâmetros da modulação	29
3	PROTOCOLO LORAWAN	31
3.1	Componentes da rede	31
3.2	Segurança na comunicação	32
3.3	Classes LoRaWAN	33
3.4	Frequências de utilização	34
3.5	Ativação dos <i>end devices</i>	35
3.5.1	OTAA	35
3.5.2	ABP	36
3.6	<i>Medium Access Control Layer</i>	36
3.6.1	Formato das mensagens	37
3.6.2	Tamanho das mensagens	38
4	COMUNICAÇÕES SEM FIO	41
4.1	O canal de comunicação e seus efeitos sobre o sinal	41
4.1.1	<i>Path Loss</i>	41
4.1.1.1	Modelos analíticos	42
4.1.1.2	Modelos empíricos	43
4.1.2	<i>Shadowing</i>	44
4.1.3	<i>Fading</i>	44
4.2	Diversidade	48
4.2.1	Tipos de diversidade	48
4.2.2	Efeito da diversidade na probabilidade de conexão	49

4.3	Colisões entre sinais	51
5	HARDWARE E FIRMWARE	53
5.1	Hardware	53
5.1.1	<i>End device</i>	53
5.1.2	<i>Gateway</i>	55
5.2	Firmware	57
5.2.1	<i>End device</i>	57
5.2.1.1	Detalhes do <i>firmware</i>	57
5.2.1.2	<i>Script</i> para controle do <i>end device</i>	60
5.2.2	<i>Gateway</i>	60
6	TESTES DE CAMPO	63
6.1	Metodologia dos testes	64
6.2	Parâmetros do transmissor	65
6.2.1	Verificação da potência de transmissão	65
6.3	Padrão das mensagens	68
6.3.1	Transmitidas	68
6.3.2	Recebidas	69
7	RESULTADOS	71
7.1	Sensibilidade	71
7.2	Medidas de RSSI, SNR e <i>Path Loss</i>	72
7.3	Modelagem do <i>fading</i>	72
7.3.1	Sem considerar diversidade	73
7.3.2	Considerando diversidade	75
7.3.2.1	Espacial	75
7.3.2.2	Temporal	77
7.3.2.3	Ambas técnicas	79
7.3.3	Comparação dos resultados	80
7.4	Probabilidade de conexão	81
7.4.1	Sem considerar diversidade	82
7.4.2	Considerando diversidade	83
7.4.2.1	Espacial	83

7.4.2.2	Temporal	84
7.4.2.3	Ambas técnicas	85
7.4.3	Comparação do desempenho para diferentes ordens de diversidade	87
8	CONCLUSÃO	89
	REFERÊNCIAS	91

1 INTRODUÇÃO

A quantidade de dados que trafega no mundo por meio de tecnologias de comunicação sem fio vem aumentando exponencialmente nos últimos anos. Segundo Cisco (2017), espera-se que este tráfego de dados chegue a 49 Exabytes por mês no ano de 2021. Algumas razões podem explicar este aumento de dados sendo utilizados, tais como: aumento do número de dispositivos conectados; avanço das tecnologias de comunicação sem fio; e novas aplicações que adotam este tipo de comunicação, tal como *Internet of Things* (IoT).

O termo IoT refere-se à troca de informações entre dispositivos ou sensores (MEKKI *et al*, 2018), caracterizando um tipo de comunicação *Machine-to-Machine* (M2M). Diversas aplicações práticas estão associadas à IoT, incluindo rastreamento de objetos, monitoramento de plantações, medição inteligente de energia elétrica e *smart cities*.

As principais formas de prover conectividade a dispositivos e fazê-los trocar informações são: i) por meio de redes *mesh*, onde os dados são levados por meio de saltos usando tecnologias de curto alcance, tais como ZigBee e Bluetooth, ou ii) através de tecnologias de longo alcance. Nesta segunda opção, pode-se adotar uma solução baseada em redes celulares (2G, 3G, 4G) ou por meio de *Low-Power Wide Area Networks* (LPWAN), fazendo uso de tecnologias como LoRa/LoRaWAN, SigFox ou NB-IoT.

Soluções de IoT baseadas em redes *mesh* tem a vantagem de possuir alta taxa de dados atrelada a um baixo consumo. Todavia, para cobrir uma grande área, seria necessário um grande número de dispositivos, tornando o sistema muito caro. Buscando então aumentar o alcance dos dispositivos, poderia-se optar por utilizar redes celulares, como citado anteriormente, porém estas tecnologias, apesar de proverem longo alcance, possuem um consumo energético excessivo. Isso se deve principalmente ao fato dos dispositivos serem projetados para lidarem com formas de onda complexas, otimizados para voz, texto e serviços com altas taxas de dados (RAZA; KULKARNI; SOORIYABANDARA, 2017).

Neste contexto, as LPWAN têm se tornado uma opção atrativa pois,

além do longo alcance e baixo consumo, utilizam *chips* de custo e complexidade reduzidos. Deve-se deixar claro que este longo alcance é possível graças à utilização de taxas de dados extremamente baixas, o que por sua vez implica em alta latência. Apesar disso, muitas aplicações necessitam apenas de poucos *bytes* para troca de informações não-críticas (tolerante a atrasos).

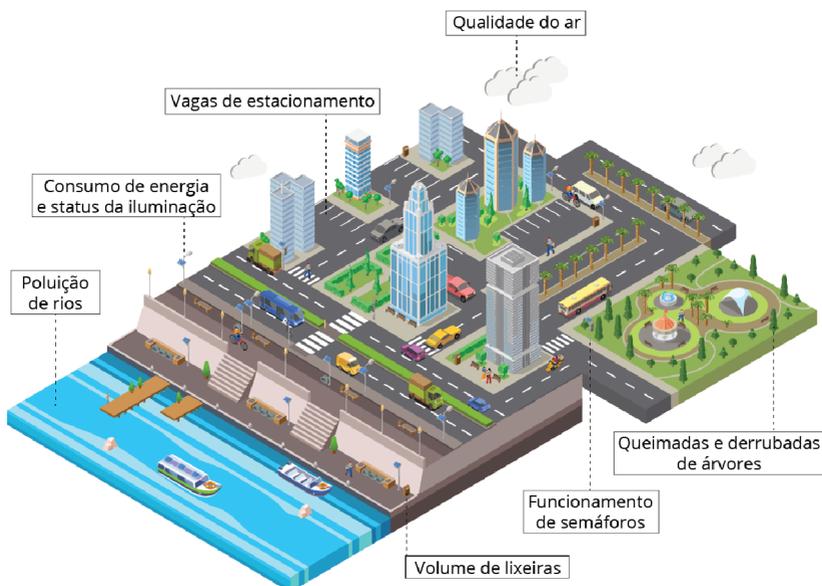
1.1 SMART CITIES

Aplicações de *smart cities* são um exemplo de soluções aderentes ao uso de LPWAN. Na Figura 1 pode-se observar algumas das variáveis que estas soluções visam monitorar. São elas:

- **Poluição de rios:** avaliar a qualidade da água de rios presentes nas cidades é um fator importante pois a poluição pode trazer doenças para a população.
- **Consumo de energia e status da iluminação:** verificar o consumo energético da iluminação pública para gerar indicadores para os órgãos responsáveis. Além disso, monitorar o funcionamento das lâmpadas, de modo que a manutenção possa ser agilizada.
- **Vagas de estacionamento:** a mobilidade urbana é um fator que as cidades modernas devem levar em consideração. Monitorar vagas de estacionamento e informar aos usuários (por meio de um aplicativo, por exemplo) onde há disponibilidade para parar seus carros pode contribuir.
- **Qualidade do ar:** assim como nos rios, monitorar a qualidade do ar é importante para garantir que as pessoas não sofram com doenças causadas pela poluição.
- **Queimadas e derrubadas de árvores:** esta aplicação visa monitorar áreas de preservação contra a exploração da vegetação.
- **Funcionamento de semáforos:** monitorar o correto funcionamento dos semáforos é um fator importante para contribuir com o trânsito e para realização de manutenção com agilidade.

- **Volume de lixeiras:** monitorar o volume de lixo em lixeiras públicas pode auxiliar aos prestadores de serviços a mapearem uma rota eficaz para coleta do lixo.

Figura 1 – Variáveis a serem monitoradas no contexto de *smart cities*.



Fonte: O autor (2019).

Estas aplicações compactuam com envios de dados intermitentes e esporádicos, visto que suas variáveis tendem a não mudar tão rapidamente. Essa característica se torna fundamental na escolha do uso de tecnologias LPWAN, pois sua baixa taxa de dados não interfere no funcionamento da aplicação, trazendo o alcance como um ponto positivo.

Neste trabalho, optou-se pelo uso de LoRaWAN (protocolo que utiliza a modulação LoRa) devido ao fato de se ter recursos disponíveis para uso nos testes de campo (*gateways* e *end devices*). Além disso, por se ter acesso direto a diversas informações das mensagens trocadas pelos dispositivos, tais como: *Received Signal Strength Indicator* (RSSI), *Signal-to-Noise Ratio* (SNR), canal

utilizado, largura de banda, potência de transmissão, *Spreading Factor* (SF), dentre outros.

1.2 O PORQUÊ DO USO DE DIVERSIDADE

As características apresentadas acima acarretam, por outro lado, na necessidade dos dados serem transmitidos com alta confiabilidade de recebimento, pois como são enviados poucas vezes, uma perda de informação pode ser bastante prejudicial para quem irá gerenciar estes dados. Portanto, técnicas de diversidade se tornam interessantes, visto que possuem justamente a finalidade de aumentar a taxa de recebimento de pacotes.

1.3 OBJETIVOS

1.3.1 Objetivo geral

Avaliar experimentalmente o efeito do uso de técnicas de diversidade temporal e espacial na melhoria da taxa de recebimento de pacotes em redes sem fio empregadas em aplicações de IoT que utilizam a modulação LoRa e o protocolo LoRaWAN.

1.3.2 Objetivos específicos

- Montar *hardwares* protótipos por meio de módulos comerciais que atendam às necessidades dos testes de campo.
- Desenvolver o *firmware* que será executado nos dispositivos de testes, de modo que as configurações do transmissor e do receptor possam ser alteradas.
- Realizar testes de campo para obtenção de dados práticos a serem avaliados.
- Realizar os testes de campo em ambientes urbanos, de modo que a avaliação dos dados seja válida para aplicações de *smart cities*.

-
- Desenvolver um *script* para extração dos seguintes resultados dos dados armazenados nos testes de campo:
 - número mínimo de replicações (diversidade temporal) necessárias para comunicação com uma dada confiabilidade.
 - avaliação da confiabilidade no caso de diversidade na recepção (múltiplos gateways).
 - alcance máximo no ambiente urbano.
 - Modelar estatisticamente o canal sem fio, considerando efeitos de *fading*, *path loss* e *shadowing*, a partir dos dados extraídos das medidas.

2 MODULAÇÃO LORA

O termo LoRa (*Long Range*) diz respeito à camada física da tecnologia que foi desenvolvida e patenteada pela empresa Semtech (CENTENARO et al., 2016). Essa camada é responsável por modular o sinal utilizando uma técnica de espalhamento espectral na faixa de sub-gigahertz, que espalha o sinal sobre uma larga faixa de frequência. A esta técnica dá-se o nome de *chirp spread spectrum* (CSS) (RAZA; KULKARNI; SOORIYABANDARA, 2017).

Como o próprio nome da modulação já indica, a informação é codificada utilizando *chirps* de frequência com uma variação linear da frequência no tempo (sem variação de fase entre símbolos adjacentes). Devido a essa linearidade, *offsets* de frequência entre o transmissor e o receptor podem ser facilmente eliminados na decodificação. Esta característica auxilia no baixo custo do dispositivo, pois os cristais utilizados no transmissor não precisam ser fabricados com extrema precisão (AUGUSTIN et al., 2016).

Juntamente com a técnica de espalhamento espectral, a modulação utiliza a técnica de *Forward Error Correction* (FEC), o que aumenta a sensibilidade do receptor, além de tornar o sinal resistente a interferência e a ruídos externos (MEKKI et al, 2018). Não somente isso, com este esquema de modulação, espera-se que o sinal tenha robustez ao efeito *Doppler*, melhorando assim o desempenho da comunicação de dispositivos em movimento (MIKHAYLOV; PETAEJAEJAERVI; HAENNINEN, 2016).

2.1 PARÂMETROS DA MODULAÇÃO

Os principais parâmetros da modulação LoRa são: largura de banda (*BW*), *Spreading Factor* (*SF*) e *Code Rate* (*CR*). Todos eles podem ser customizados no dispositivo de forma a obter o melhor desempenho dependendo da situação.

O *SF* pode variar de 7 à 12. Porém, no Brasil, só é possível utilizar até o SF10 segundo normatizações. Este parâmetro define o número de *chirps* por símbolo, que é dado por 2^{SF} . Variando este parâmetro, varia-se o tempo de símbolo e a taxa de dados, tornando possível realizar o *trade-off* entre *throughput* e alcance da comunicação.

O parâmetro CR , utilizado pelo FEC, é dado por $\frac{4}{4+n}$, onde $n \in \{1, 2, 3, 4\}$. Os possíveis valores de BW para *uplink* são 125 KHz e 500 KHz e para *downlink* é 500 KHz (LORA ALLIANCE, 2019).

A taxa de dados pode ser obtida pela seguinte equação (AUGUSTIN et al., 2016):

$$R_b = SF \times \frac{BW}{2^{SF}} \times CR. \quad (2.1)$$

Para $CR = \frac{4}{5}$, $BW = 125$ KHz, pode-se calcular o valor da taxa de dados para diferentes valores de SF, como mostrado na Tabela 1.

Tabela 1 – Taxas de dados para diferentes valores de SF, $CR = \frac{4}{5}$ e $BW = 125$ KHz.

SF	R_b (bits/seg)
10	980
9	1760
8	3125
7	5470

No geral, com o aumento do parâmetro SF, a taxa de dados diminui e o tempo no ar da mensagem e o alcance da comunicação aumentam (HOELLER et al., 2018).

Ao se utilizar diferentes valores de SF, por estes serem praticamente ortogonais, é possível que diversos dispositivos transmitam pacotes em um mesmo canal, ao mesmo tempo, sem que haja grande degradação no sinal e o receptor consiga decodificar as mensagens (MIKHAYLOV; PETAEJAEJAEVI; HAENNINEN, 2016).

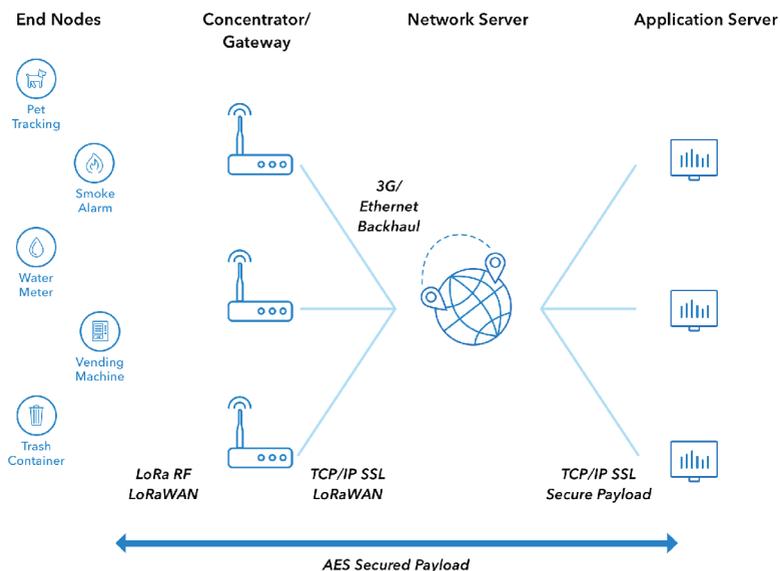
3 PROTOCOLO LORAWAN

O termo LoRaWAN (*Long Range Wide Area Network*) designa o protocolo da camada de rede das aplicações que utilizam a modulação LoRa na camada física. É responsável por gerenciar o funcionamento da rede, o cadastro de dispositivos, segurança, validação das mensagens, entre outros fatores. O protocolo é mantido aberto à comunidade e desenvolvido pela LoRa Alliance (CENTENARO et al., 2016).

3.1 COMPONENTES DA REDE

A Figura 2 mostra a arquitetura de uma rede LoRaWAN convencional.

Figura 2 – Topologia comum de uma rede LoRaWAN.



Fonte: THE THINGS NETWORK (2019).

Os *End Nodes*, também chamados de *End Devices*, são os dispositivos que ficam na camada mais externa da rede e são responsáveis por enviar, utilizando a tecnologia LoRa, dados de diferentes tipos de sensores. São dis-

positivos que possuem um *hardware* simples, de baixo custo e baixo consumo, ideal para aplicações que necessitam de longa duração de bateria.

Em um segundo nível, estão os *gateways*. Estes dispositivos são responsáveis por receber, armazenar e encaminhar os dados oriundos dos sensores para o componente *Network Server* via alguma tecnologia secundária, como GPRS (*General Packet Radio Services*) ou Wi-Fi. Possuem um *hardware* mais complexo, que possa receber mensagens de baixíssima potência devido às degradações sofridas pelo sinal. Do ponto de vista dos *end devices*, o *gateway* é um componente transparente, responsável apenas pelo encaminhamento de mensagens.

No *Network Server* as mensagens recebidas são validadas, verificando-se a integridade do pacote e se este foi enviado por um dispositivo que está cadastrado na rede. Além disso, é responsável por gerar os pacotes que serão enviados de volta aos *end devices*, contendo alguma configuração ou confirmação de recebimento.

Na próxima camada está o *Application Server*. Este elemento é responsável por prover uma interface na qual o usuário pode visualizar os dados que percorreram toda a rede desde os sensores, possibilitando um monitoramento da aplicação e auxiliando na tomada de decisão. Algoritmos de *machine learning* são comumente utilizados nesta etapa, com a finalidade de analisar e extrair características importantes a partir dos dados.

3.2 SEGURANÇA NA COMUNICAÇÃO

Em todas as camadas da rede, as mensagens são trocadas usando o algoritmo AES-128 para garantir a segurança das informações (LORA ALLIANCE, 2019). O protocolo LoRaWAN possui três chaves de segurança de 128 bits. São elas:

- *Application key* (AppKey): chave conhecida apenas pelo dispositivo e pela aplicação. É utilizada para gerar outras chaves de segurança.
- *Application session key* (AppSKey): chave utilizada pelo *end device* e pelo *network server* para criptografar e descriptografar o campo *payload* das mensagens.

- *Network session key* (NwkSKey): chave usada pelo *end device* e pelo *network server* no cálculo e verificação do código de integridade da mensagem (MIC) para garantir a integridade dos dados.

O protocolo LoRaWAN também utiliza um mecanismo de *Frame Counter* na segurança da informação. Esta variável é encriptada junto com a mensagem e tem seu valor incrementado a cada envio.

Por ser uma tecnologia de comunicação sem fio, qualquer dispositivo pode interceptar as mensagens sendo trocadas na rede. Porém, por não ter acesso às chaves AppSKey e NwkSKey, este dispositivo não conseguiria descriptografar as mensagens. Por outro lado, ele poderia retransmiti-las, podendo sobrecarregar os servidores de rede.

Quando uma mensagem é enviada com um *Frame Counter* inferior ao esperado pelo *network server*, essa mensagem é descartada. Deste modo, os ataques de replicação podem ser contornados.

Devido a isso, é necessário assegurar que um dispositivo da rede permaneça com o *Frame Counter* correto mesmo após ser reiniciado. Isso pode ser feito salvando esta variável em uma memória não-volátil do dispositivo, resgatando-a sempre que este for reiniciado. De outra maneira, ele se tornaria inútil, pois o *network server* ignoraria suas mensagens.

3.3 CLASSES LORAWAN

Os dispositivos da rede podem ser configurados em diferentes classes, cada uma com um tipo de funcionamento diferente. Normalmente, todos dispositivos de uma mesma rede possuem a mesma classe. Estas são:

- Classe A: os *end devices* desta classe realizam o envio de mensagens (*uplink*) a qualquer momento. Após o envio, duas janelas de recebimento são abertas com o intuito de receber mensagens de *downlink*, contendo alguma configuração ou confirmação de recebimento.
- Classe B: os dispositivos desta classe também realizam uma comunicação bidirecional, porém, além das janelas de recebimento após mensa-

gens de *uplink*, alguns *slots* no tempo são programados para recepção de mensagens.

- Classe C: nesta classe, os dispositivos possuem uma janela de recebimento contínua, fechando-a apenas nos momentos de envio.

As janelas de recebimento após o envio de mensagens, para o caso do Classe A, estão ilustradas pela Figura 3. Após cada envio, é realizado um *delay* para aguardar o recebimento e processamento da mensagem por parte do *network server*. Esse *delay* está representado na imagem por *RxDelay1*. Na sequência a primeira janela (RX1) é aberta. A segunda janela de recebimento (RX2) é aberta após *RxDelay2* segundos. O intervalo de tempo no qual estas janelas permanecerão abertas depende do *datarate* utilizado.

Figura 3 – Janelas de recebimento.



Fonte: (CHEONG et al., 2017).

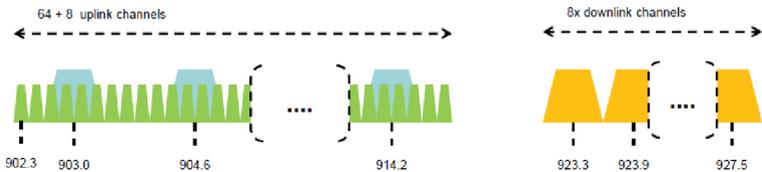
Como discutido em CHEONG et al. (2017), os dispositivos classe C possuem o maior consumo energético, devido ao fato de manterem a janela de recebimento sempre ativa. Por outro lado, a classe A é a que proporciona um menor consumo, podendo chegar a uma durabilidade de bateria superior a 10 anos, caso esta, em conjunto com os parâmetros da modulação, seja bem projetada.

3.4 FREQUÊNCIAS DE UTILIZAÇÃO

O protocolo LoRaWAN opera em uma faixa não-licenciada do espectro, o que significa que não é preciso pagar para utilizar tais frequências. Cada país possui restrições específicas no que tange tecnologias de longo alcance, devido a isso, o protocolo possui especificações para diferentes regiões. No Brasil, o LoRaWAN opera na faixa de frequência 902-928 MHz. A Figura 4

representa a divisão das frequências utilizadas. Nesta divisão, 64 canais de *uplink* (902.3 MHz a 914.9 MHz) são divididos em 8 sub-bandas, cada uma com 8 canais de 125 KHz de banda. Além disso, 8 canais de banda 500 KHz são utilizados para *downlink*, começando em 923.3 MHz indo até 927.5 MHz.

Figura 4 – Frequências do espectro utilizadas.



Fonte: LORA ALLIANCE (2019).

Quando o *end device* vai realizar uma transmissão, o protocolo escolhe o canal que será utilizado de forma aleatória dentro da sub-banda na qual o dispositivo está configurado. Além disso, segundo a regulamentação desta região, a potência de transmissão mínima que pode ser utilizada é 2 dBm, enquanto que a máxima é 30 dBm (LORA ALLIANCE, 2019).

3.5 ATIVAÇÃO DOS END DEVICES

Para que um dispositivo possa participar da rede e enviar mensagens, ele precisa realizar uma ativação. Isso pode ocorrer de duas formas, via *Over-The-Air-Activation* (OTAA) ou via *Activation By Personalization* (ABP).

3.5.1 OTAA

Neste método, o *end device* precisa realizar um procedimento de entrada na rede (*join procedure*) antes de enviar dados ao *network server*.

O *join procedure* inicia com o dispositivo enviando uma mensagem de *join request* em diferentes canais até obter uma resposta do *network server*. Isso é feito desta maneira pois não sabe-se a priori em quais canais o *gateway* opera. Esta mensagem enviada contém códigos identificadores do dispositivo (EUI). Caso o procedimento seja realizado com sucesso, o *network server*

envia uma mensagem (*join-accept message*) ao *end device* indicando que ele pode fazer parte da rede e passar a enviar pacotes. A partir das informações contidas nesta mensagem, o *end device* cria as chaves de segurança necessárias para a comunicação.

3.5.2 ABP

No método ABP, o cadastro de dispositivos na rede é feito salvando o endereço do dispositivo (*DevAddr*) e as chaves de autenticação (*AppKey*, *NwkSKey*, *NwkSEncKey* e *AppSKey*) no *network server*, que incluirá o *end device* na sua lista de dispositivos habilitados para realizar comunicação. Normalmente, os valores necessários para o cadastro são pré-definidos de fábrica e ficam salvos na memória do dispositivo. Caso esse não seja o caso, é possível gerar estas chaves no próprio *network server* e salvá-las no *end device*. Uma outra variável que deve ser conhecida com antecedência são os canais a serem utilizados, que devem ser os mesmos entre *end device* e *gateway*.

3.6 MEDIUM ACCESS CONTROL LAYER

O protocolo LoRaWAN possui uma camada MAC, responsável pelo gerenciamento de todo fluxo de dados. Esta camada define alguns comandos que são utilizados na comunicação bidirecional para realizar funções como: conferência de conectividade entre dispositivos (*LinkCheckReq*), solicitação de status (*DevStatusReq*), alteração do canal de comunicação (*NewChannelReq*), adaptação da taxa de dados (*LinkADRReq*), dentre outros. Cada comando possui um identificador (CID) específico que é enviado em um campo específico da mensagem juntamente com o pacote de dados.

O último comando citado, *LinkADRReq*, é utilizado em conjunto com a técnica de *Adaptive Data Rate* (ADR). Este é um mecanismo que busca reduzir o consumo de energia dos *end devices*, alterando sua configuração de taxa de dados e potência de transmissão a partir da qualidade do enlace do dispositivo com o *gateway*. Portanto, dispositivos mais próximos poderão utilizar uma taxa de dados maior e uma potência de transmissão menor, aumentando a durabilidade de suas baterias.

Apesar de o *network server*, que é quem executa o algoritmo do ADR, ter a capacidade de controlar os parâmetros de todos os dispositivos da rede, o uso desta técnica não é obrigatório. Como discutido por Reynders, Meet e Pollin (2016), há dois tipos diferentes de redes, i) as passivas, que não utilizam o mecanismo do ADR, ficando a cargo dos próprios *end devices* definirem seus parâmetros, e ii) as ativas, que enviam parâmetros de configuração sempre que necessário.

Além disso, a camada MAC do LoRaWAN aceita dois tipos de mensagens: confirmadas e não confirmadas. Ao utilizar mensagens do tipo confirmadas, o *end device* irá transmitir o mesmo pacote no máximo 8 vezes até receber uma confirmação por *downlink*.

3.6.1 Formato das mensagens

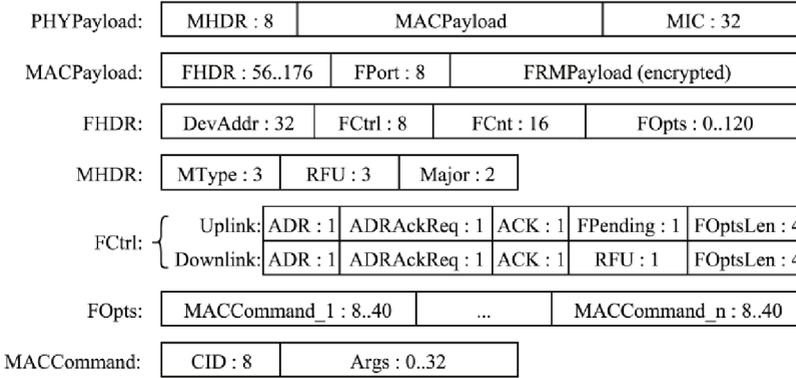
O protocolo LoRaWAN possui um formato de mensagem específico tanto para mensagens de *uplink* quanto para mensagens de *downlink*. A principal diferença entre elas é que nas mensagens de *downlink* não há um campo de CRC (*Cyclic Redundancy Check*).

O formato das mensagens está apresentado na Figura 5. Todas mensagens possuem um *PHYPayload*, que é dividido em um cabeçalho de 8 bits chamado *MHDR*, seguido do *MACPayload* de tamanho variável, terminando em um código de integridade de mensagem (*MIC*) de 32 bits.

O campo *MHDR* é composto por 3 *bits* que indicam o tipo da mensagem (*MType*), podendo esta ser uma mensagem de *uplink*, *downlink*, do tipo confirmada, não confirmada, entre outras opções (LORA ALLIANCE, 2019). Além disso, possui 3 *bits* reservados para uso futuro (*RFU*) e 2 *bits* que indicam a versão da camada LoRaWAN que está sendo utilizada (*Major*).

O campo *MACPayload* contém os seguintes subcampos: i) *FHDR*, o qual é composto pelo endereço do dispositivo (*DevAddr*), o *Frame Control* (*FCtrl*) que possui algumas informações para controle do ADR, o *Frame Counter* (*FCnt*) que indica o número de mensagens que o *end device* enviou ao *network server*, e 15 bytes utilizados para transportar comandos MAC (*FOpts*); ii) *FPort*, que é um campo que está presente quando o campo (*FRMPayload*) do pacote contém dados; iii) *FRMPayload*, também é um campo opcional e é

Figura 5 – Formato das mensagens. Tamanho dos campos está em *bits*.



Fonte: AUGUSTIN et al. (2016).

onde os dados em si (valores de sensores, por exemplo) são criptografados e enviados.

3.6.2 Tamanho das mensagens

O tamanho máximo de uma mensagem é, como discutido pela LoRa Alliance (2019), uma variável derivada do tempo em que tal mensagem fica no ar. Isso quer dizer que, quanto menor é a taxa de dados (a que proporciona maior alcance e fica mais tempo no ar), menor é a quantidade de *bytes* que podem ser enviados.

Segundo o Ato 14448, Seção 10.4.1, desenvolvido pela Anatel, o tempo de ocupação do espectro de um sinal de radiofrequência que utiliza espalhamento espectral na faixa de frequência em questão deve ser no máximo 400 ms. Utilizando a calculadora disponível em LoRaTools (2019), é possível calcular o tempo que um sinal modulado usando LoRa ocupa. Para o SF10 (*Spreading Factor* 10), considerando uma banda de 125 KHz, *coderate* 4/5, um tamanho de pacote de 11 *bytes* e um preambulo de 8 *bytes*, tem-se que o tempo no ar da mensagem é de 288,77 ms.

Tomando como exemplo novamente o SF10, que resulta em uma taxa de dados de 980 *bits* por segundo (como mostrado na Tabela 1), o tamanho

máximo do campo *MACPayload* é de 19 bytes (LORA ALLIANCE, 2019). Considerando que o campo *FHDR* possui 7 bytes (quando *FOpts* não é utilizado) e o campo *FPort* possui 1 byte, o tamanho do campo *FRMPayload* deve ser no máximo 11 bytes. Ou seja, os dados extraídos da aplicação, como leitura de sensores, devem totalizar no máximo 11 bytes por pacote enviado quando se utiliza SF10.

Além disso, o protocolo LoRaWAN não possui um mecanismo de fragmentação de mensagens (AUGUSTIN et al., 2016), porém, isso poderia ser resolvido na aplicação fazendo uma verificação do tamanho da mensagem antes de realizar o envio, dividindo-a quando este tamanho for maior que o especificado no protocolo. Portanto, deve-se sempre respeitar as limitações de tamanho de mensagem, pois, caso isso não seja feito, o *network server* irá descartar a mensagem recebida.

4 COMUNICAÇÕES SEM FIO

Este capítulo tem o objetivo de fazer uma discussão acerca do canal de comunicação sem fio e os efeitos aos quais os sinais transmitidos estão submetidos, apresentando as formas presentes na literatura para modelar tais efeitos.

Esta é uma discussão importante pois, ao utilizar uma tecnologia de comunicação como LoRa/LoRaWAN, os sinais serão atenuados em decorrência destes efeitos, sendo interessante, portanto, entender como isso acontece e ser capaz de modelar seu comportamento.

Além disso, serão apresentados conceitos sobre as técnicas de diversidade utilizadas neste trabalho. É fundamental entender como estas são aplicadas na prática e qual é o seu efeito na melhoria da comunicação.

4.1 O CANAL DE COMUNICAÇÃO E SEUS EFEITOS SOBRE O SINAL

Em um canal de comunicação sem fio, os sinais transmitidos estão sujeitos a ruído, interferência e outros fenômenos que variam com o tempo, devido, por exemplo, à movimentação do dispositivo (GOLDSMITH, 2004).

Pode-se modelar a variação na potência do sinal recebido entendendo os efeitos que agem sobre ele, tais como: perda de percurso (*path loss*), sombreamento (*shadowing*) e desvanecimento (*fading*).

4.1.1 *Path Loss*

O *path loss* refere-se à dissipação da potência radiada pelo transmissor devido à propagação do sinal no meio. Variações da potência do sinal devido a este fenômeno irão aparecer sobre longas distâncias, na casa de centenas e milhares de metros. Devido a isso, este efeito é classificado como sendo de larga escala (GOLDSMITH, 2004).

A equação (4.1) mostra que a perda de percurso é uma razão entre a potência transmitida e recebida, que indica o quanto de potência foi absorvida

pelo canal. Considera-se que o valor de P_t é conhecido.

$$PL_{dB} = 10 \log_{10} \left(\frac{P_t}{P_r} \right). \quad (4.1)$$

Existem alguns modelos que podem ser utilizados para entender melhor o *path loss* e prever as variações na potência média do sinal. Estes são classificados em modelos analíticos e empíricos.

4.1.1.1 Modelos analíticos

Um tipo de modelo analítico é o modelo de propagação no **espaço livre**, o qual busca entender o efeito da perda de percurso considerando que não há atenuação e nem reflexões do sinal entre os dois pontos (transmissão e recepção).

O valor de P_r utilizado no cálculo do *path loss* pode ser obtido pela equação de Friis:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}, \quad (4.2)$$

onde o parâmetro G_t refere-se ao ganho da antena de transmissão, G_r representa o ganho da antena de recepção, λ é o comprimento de onda da portadora, d é a distância entre o transmissor e o receptor, e L representa outras perdas.

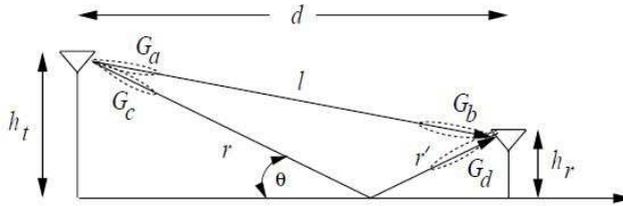
Um outro modelo também do tipo analítico, é o **modelo de dois raios**, utilizado quando considera-se que o sinal transmitido é refletido no solo uma vez. Portanto, o sinal recebido será uma soma de duas componentes: um sinal transmitido considerando espaço livre, sem atenuação, e um sinal que foi refletido no chão com um determinado ângulo. A Figura 6 mostra a situação descrita acima.

Para estimar a potência de recepção, pode-se utilizar a equação:

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4}. \quad (4.3)$$

Dividindo ambos os lados de (4.3) por P_t e invertendo, tem-se que a

Figura 6 – Cenário de utilização do modelo de dois raios.



Fonte: GOLDSMITH (2004).

perda de percurso (P_t/P_r), em decibéis, é dada por:

$$PL_{dB} = 40 \log_{10}(d) - [10 \log_{10}(G_t) + 10 \log_{10}(G_r) + 20 \log_{10}(h_t) + 20 \log_{10}(h_r)]. \quad (4.4)$$

Nota-se que agora o *path loss* também irá variar de acordo com a altura das antenas de transmissão (h_t) e recepção (h_r).

4.1.1.2 Modelos empíricos

Os modelos explicados anteriormente são baseados em fenômenos físicos, obtidos a partir das equações de Maxwell. Desenvolver um modelo completo que capte o comportamento de determinado *link* de comunicação seria uma tarefa muito árdua, pois muitas variáveis e aproximações teriam que ser levadas em consideração.

Devido a isso, criou-se modelos empíricos que tem o objetivo de descrever a perda de percurso baseando-se em medidas a uma determinada distância, faixa de frequência e em uma geografia particular.

O modelo **Log Distância** é um do tipo empírico. De equacionamento simples, busca capturar o comportamento da propagação do sinal em função da distância, sendo que a perda de percurso pode ser determinada como

$$PL(d) = PL(d_0) + 10\alpha \log_{10} \left(\frac{d}{d_0} \right), \quad (4.5)$$

onde $PL(d_0)$ representa a perda de percurso a uma determinada distância conhecida, que pode ser calculada a partir das medidas, α é o coeficiente de

perda de propagação do canal e seu valor depende do ambiente no qual as transmissões estão sendo realizadas. No espaço livre, por exemplo, tem-se que $\alpha = 2$. Porém, seu valor também pode ser encontrado a partir das medidas.

Quando estas medidas são feitas em um ambiente em que há outros efeitos de atenuação no sinal além da distância, o modelo **Log Normal** pode ser utilizado, o qual é definido por

$$PL(d) = PL(d_0) + 10\alpha \log_{10} \left(\frac{d}{d_0} \right) + \phi_{dB}. \quad (4.6)$$

Como pode ser observado em (4.6), este modelo é uma extensão do modelo anterior, e insere na modelagem o efeito do sombreamento através de ϕ_{dB} , uma variável aleatória Gaussiana de média zero e variância $\sigma_{\phi_{dB}}^2$.

Outros modelos como **Okumura** e **Hata** também são utilizados para modelar a perda de percurso a partir de medidas. Este segundo é uma extensão do primeiro, onde se tem uma formulação empírica para cálculo da perda.

4.1.2 Shadowing

O efeito do *shadowing* é causado por obstáculos entre o transmissor e o receptor, os quais atenuam a potência do sinal. Pode ocorrer a distâncias proporcionais ao tamanho dos objetos causadores do efeito (dezenas ou centenas de metros), sendo assim considerado como de larga escala (GOLDSMITH, 2004).

Pode ser modelado, como discutido anteriormente, por meio de uma variável aleatória Gaussiana de média zero e variância $\sigma_{\phi_{dB}}^2$.

4.1.3 Fading

Este efeito descreve o comportamento da potência instantânea vista pelo receptor (valor de RSSI). Este valor pode sofrer variações consideráveis pois, quando o sinal transmitido é refletido e refratado no meio, o sinal que chega à antena receptora é resultante de uma combinação (construtiva ou destrutiva) de sinais que percorreram multipercursos (*multipaths*), que nada mais são que diversas versões com amplitude e fase distintas do sinal original.

As variações na potência devido a este efeito ocorrem em distâncias muito curtas, na ordem do comprimento de onda do sinal. Devido a isso, o *fading* é classificado como sendo de pequena escala (GOLDSMITH, 2004).

Desenvolver um modelo que descreva este fenômeno de forma determinística é uma tarefa muito difícil pois seria necessário ter um conhecimento muito detalhado sobre o comportamento do sinal no canal de comunicação.

Uma opção mais interessante é modelar o *fading* de forma estatística. A partir disso, pode-se definir a potência de recepção instantânea como

$$P_r = h^2 \times \bar{P}_r, \quad (4.7)$$

onde \bar{P}_r é a potência média recebida, enquanto que h é o *fading*. Vale salientar que este modelo descarta as variações de fase.

Nota-se portanto que a potência instantânea recebida é uma variável aleatória que está em função do *fading*, logo, pode ser modelada por uma distribuição de probabilidade.

As distribuições de probabilidade mais usadas para modelar o *fading* são *Rayleigh*, *Rice* e *Nakakami-m*.

A distribuição *Rayleigh* é usada para modelagem quando se tem uma comunicação sem linha de visada (NLOS). Neste caso, a *pdf* de h é

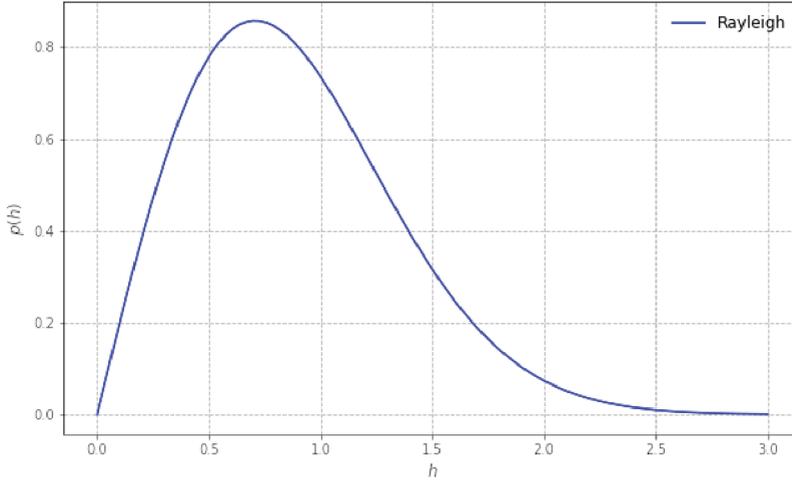
$$p(h) = \frac{2h}{\bar{P}_r} \exp\left(-\frac{h^2}{\bar{P}_r}\right). \quad (4.8)$$

Nota-se a distribuição está em função do *fading* e da potência média recebida. A Figura 7 mostra o gráfico da distribuição.

Já a distribuição *Rice* é mais utilizada quando se tem uma forte linha de visada (LOS). Irá variar, além do *fading*, em função do parâmetro K , que indica a forma da distribuição e representa a razão entre a potência da componente LOS e das componentes NLOS. Neste caso,

$$p(h) = \frac{2h(K+1)}{\bar{P}_r} \exp\left(-K - \frac{h^2(K+1)}{\bar{P}_r}\right) I_0\left(2h\sqrt{\frac{K(K+1)}{\bar{P}_r}}\right), \quad (4.9)$$

onde I_0 é a função de Bessel de ordem zero. Para $K = 0$, a distribuição *Rice*

Figura 7 – Distribuição *Rayleigh*.

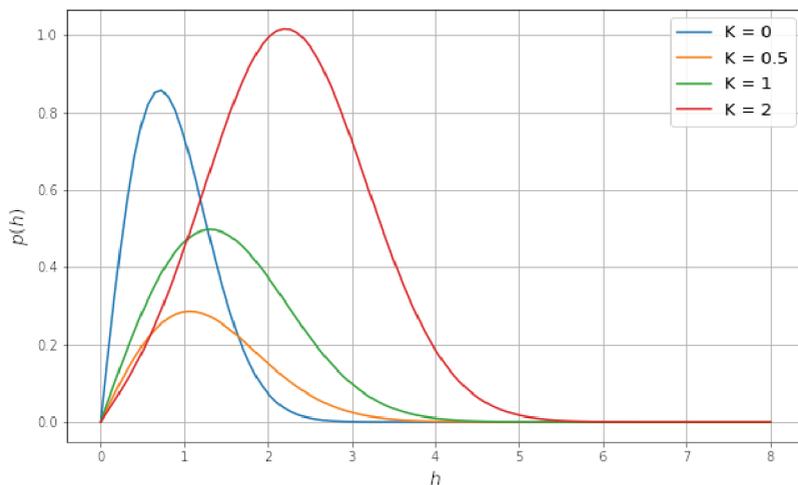
Fonte: O autor (2019).

fica igual a de *Rayleigh*. A Figura 8 apresenta o formato desta distribuição para diferentes valores de K .

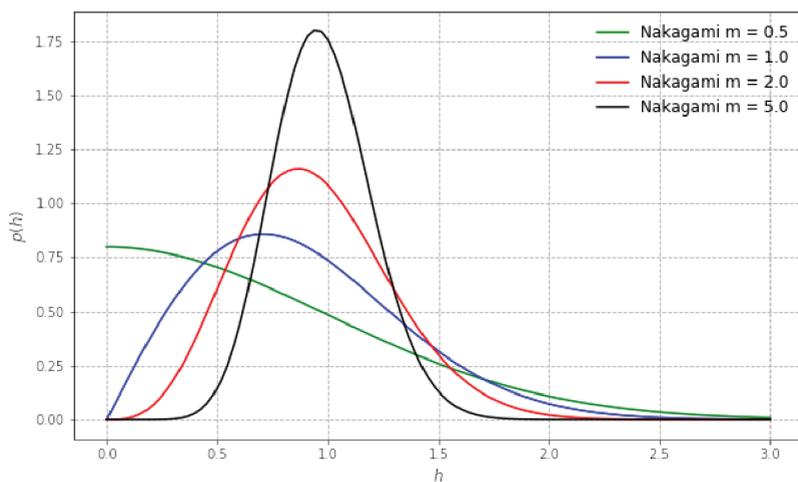
Por outro lado, a distribuição *Nakagami- m* é genérica, podendo ser utilizada para ambos os casos ou quando se tem cenários com LOS parcial. A *pdf Nakagami- m* é

$$p(h) = \frac{2m^m h^{2m-1}}{\Gamma(m)\bar{P}_r^m} \exp\left(-\frac{mh^2}{\bar{P}_r}\right), \quad (4.10)$$

onde $\Gamma(m)$ é a função Gama calculada em m , que é o parâmetro de *Nakagami* e dá uma ideia de quão severo é o *fading*. A Figura 9 mostra o formato da distribuição para diferentes valores de m . Para $m = 1$, a distribuição é a mesma que a *Rayleigh*.

Figura 8 – Distribuição *Rice* para diferentes valores de K .

Fonte: O autor (2019).

Figura 9 – Distribuição *Nakagami* para diferentes valores de m .

Fonte: O autor (2019).

4.2 DIVERSIDADE

Como pôde-se perceber após a discussão realizada na seção anterior, quando um sinal é transmitido por um canal de comunicação sem fio, diversos efeitos que podem degradar a potência de transmissão atuam sobre ele.

Em algumas aplicações, onde deseja-se que a comunicação seja feita com determinada confiabilidade, se torna necessário o emprego de algumas técnicas para garantir maior probabilidade de sucesso no recebimento das mensagens. Uma técnica que pode ser utilizada é a *Automatic Repeat Request* (ARQ), presente no protocolo LoRaWAN, na qual o transmissor reenvia até 8 vezes uma mesma mensagem até que uma confirmação através de um *downlink* seja recebida. Contudo, como discutido por POP et al. (2017), com o aumento do número de dispositivos na rede, esta técnica se torna não confiável pois os receptores não são capazes de suportar um grande fluxo de mensagens de confirmação por *downlink* devido a limitações regulamentárias.

Uma outra opção seria utilizar então técnicas de **diversidade**, que proveem melhorias no *link* de comunicação a um custo (monetário e de complexidade dos dispositivos) relativamente baixo.

Através da diversidade, receptores podem enxergar diferentes versões de uma mesma mensagem com um *fading* de baixa correlação entre estas versões. Assim, se em um destes canais uma forte degradação é imposta ao sinal, no outro o mesmo pode não ocorrer.

4.2.1 Tipos de diversidade

Diferentes tipos de técnicas de diversidade podem ser utilizadas. Alguns exemplos são:

- **Espacial:** na diversidade espacial utiliza-se múltiplas antenas, sejam elas em um mesmo dispositivo ou em dispositivos diferentes. Esta multiplicidade de antenas pode ser considerada tanto no transmissor quando no receptor. Caso seja utilizada em ambos, tem-se o caso de *Multiple-Input and Multiple-Output* (MIMO).
- **Temporal:** neste caso, realizam-se transmissões repetidas de uma

mesma mensagem, com um intervalo entre envios sendo maior que o tempo de coerência do canal, de modo que as cópias da mensagem estejam sujeitas a *fadings* independentes.

- **Frequência:** ao utilizar diversidade em frequência, a mesma mensagem é transmitida em portadoras independentes, de modo que os dados enviados não estejam sujeitos ao mesmo *fading*. Para que estas portadoras em frequência não sejam correlacionadas, é necessário que a separação entre elas seja pelo menos a banda de coerência do canal.
- **Polarização:** neste tipo de diversidade, utiliza-se antenas com diferentes polaridades (horizontal e vertical, por exemplo). Deste modo, ao enviar uma mesma mensagem através destas antenas, o receptor irá enxergar diferentes versões do sinal, gerando diversidade.

Neste trabalho, os três primeiros tipos de diversidade citados acima foram utilizados. Destaca-se que a diversidade em frequência é feita pelo próprio protocolo LoRaWAN, definindo de forma randômica um canal dentro da sub-banda configurada para enviar os dados. Portanto, serão consideradas apenas as diversidades de tempo e espaço, pois estas eram as variáveis sobre as quais se tinha controle.

4.2.2 Efeito da diversidade na probabilidade de conexão

Um receptor será capaz de decodificar um sinal se a potência instantânea (RSSI) for maior ou igual a uma RSSI mínima, também chamada de sensibilidade. Esta variável pode ser obtida através do *datasheet* do componente utilizado ou por meio de medidas. Diferentes SFs resultam em diferentes valores de sensibilidade.

A probabilidade de conexão, definida como a probabilidade de recebimento de uma determinada mensagem, pode então ser calculada como

$$P_{con} = P_r[RSSI \geq RSSI_{min}], \quad (4.11)$$

ou seja, a probabilidade de conexão é igual à probabilidade da potência instantânea recebida ser maior ou igual à sensibilidade. Além disso, o valor de RSSI

deve ser maior que a potência de ruído, assim, a equação (4.11) poderia ser reescrita em termos da SNR do sinal, ficando $P_{con} = P_r[SNR \geq SNR_{min}]$, onde SNR_{min} é a SNR de *threshold* do receptor.

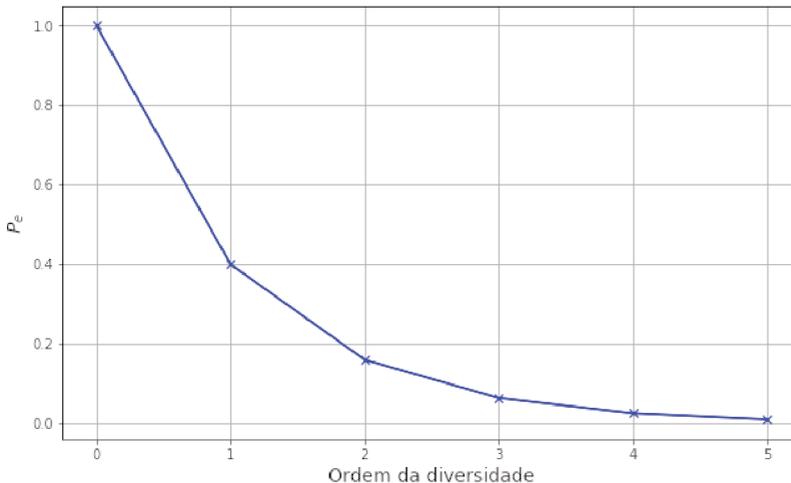
Ao se aplicar algum tipo de diversidade na transmissão, pode-se observar um aumento na probabilidade conexão, como discutido em Hoeller et al. (2018), de acordo com

$$P_{con,D} = 1 - (1 - P_{con})^D, \quad (4.12)$$

onde D indica a ordem da diversidade (podendo ser de qualquer tipo) e considera-se que as diferentes versões da mensagem possuem *fading* independentes.

A mesma análise pode ser feita em termos da probabilidade de erro ($P_e = 1 - P_{con}$ e $P_{e,D} = 1 - P_{con,D}$). A Figura 10 mostra o efeito do aumento da ordem da diversidade na probabilidade de erro. Considerando inicialmente que $P_e = 0.4$, obteve-se que para $D = 5$ a probabilidade de erro resultante é praticamente nula (praticamente 100% de chance de a mensagem ser recebida).

Figura 10 – Variação da probabilidade de erro com o aumento da ordem da diversidade.

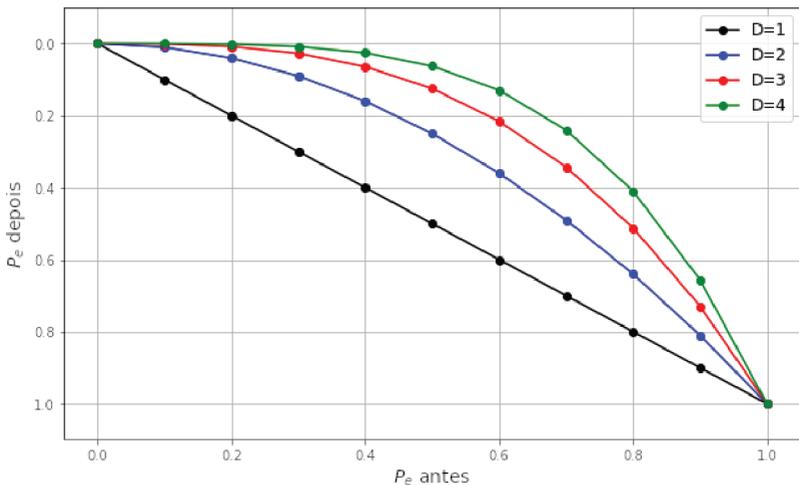


Fonte: O autor (2019).

Já a Figura 11 mostra uma relação entre a probabilidade de erro antes e depois de se aplicar diversidade de diferentes ordens. Por exemplo, para $D = 1$ tinha-se inicialmente $P_e = 0.6$, após aplicar diversidade de ordem 3, a probabilidade de erro resultante é $P_{e,3} \approx 0.2$.

Esta é uma análise interessante pois pode-se definir uma probabilidade de erro (ou de conexão) mínima que deseja-se obter, e então escolher a menor ordem que atende ao requisito, de modo a reduzir fatores como número de transmissões ou número de receptores (diminuindo o consumo energético ou o custo monetário da solução, respectivamente).

Figura 11 – Probabilidade de erro antes vs depois para diferentes ordens de diversidade.



Fonte: O autor (2019).

4.3 COLISÕES ENTRE SINAIS

Em uma aplicação real, espera-se que um grande número de dispositivos sejam instalados em campo para realizar o monitoramento das variáveis de interesse. Não somente isso, mas em um cenário como o de *smart cities*, outras aplicações podem dividir o espectro, gerando interferência.

Apesar de a modulação LoRa aumentar a resistência à interferência usando a técnica de espalhamento espectral, em uma rede com uma alta densidade de nós podem haver colisões entre pacotes, o que gera perda de informação. Este trabalho não analisa este quesito, visto que os testes de campo foram feitos com apenas um nó devido a uma limitação de recursos. Por outro lado, trabalhos como Hoeller et al. (2018), Raza, Kulkarni e Sooriyabandara (2017), Augustin et al. (2016), Yu, Zhu e Fan (2017), Ferre (2017) e Vejlgard et al. (2017) realizaram um estudo sobre colisões e interferência a partir de simulações computacionais.

Os resultados mostram que, mesmo sob interferência, dispositivos LoRa conseguem se comunicar com uma baixa probabilidade de erro. Porém, à medida que o número de dispositivos conectados aumenta, a probabilidade de erro tende a aumentar também.

A escolha do SF é importante, pois quanto maior o valor deste parâmetro, mais tempo o sinal fica no ar e maior é a probabilidade de haver uma colisão. Por isso, uma boa estratégia seria configurar os dispositivos próximos ao *gateway* com SF de valor mais baixo.

O uso de mensagens não confirmadas é interessante em redes de alta densidade, pois isso diminui o fluxo de mensagens de *uplink* e *downlink*. Mas para garantir determinada probabilidade de conexão, caso deseje-se utilizar diversidade temporal, o número de retransmissões deve ser controlado, para não aumentar o carregamento da rede, o que pode aumentar as colisões, e preservar a durabilidade da bateria. Neste caso poderia-se optar por outros tipos de diversidade, como a espacial, que é sempre benéfica.

5 HARDWARE E FIRMWARE

Os principais componentes físicos de uma rede LoRa/LoRaWAN são *end devices* e *gateways*. Um é responsável por fazer a leitura de sensores e enviar estas informações, enquanto o outro é responsável pelo recebimento e encaminhamento das mensagens ao *network server*, onde estas são validadas e a configuração dos dispositivos cadastrados na rede é solicitada por meio de mensagens de *downlink* enviadas através do *gateway*.

O *gateway* é um componente geralmente mais caro, complexo e de maior consumo energético. Tem a característica de possuir uma potência mínima de recepção (sensibilidade) baixa, de modo a possibilitar o recebimento de sinais bastante atenuados.

Durante o projeto de implantação de uma rede, quesitos como localização e altura dos dispositivos necessitam serem estudados com atenção, pois isso pode ter influência direta no desempenho da comunicação.

Como exposto nos objetivos do trabalho, testes de campo foram realizados em uma rede LoRaWAN para que a avaliação acerca do impacto das técnicas de diversidade na comunicação pudesse ser feita a partir de dados práticos.

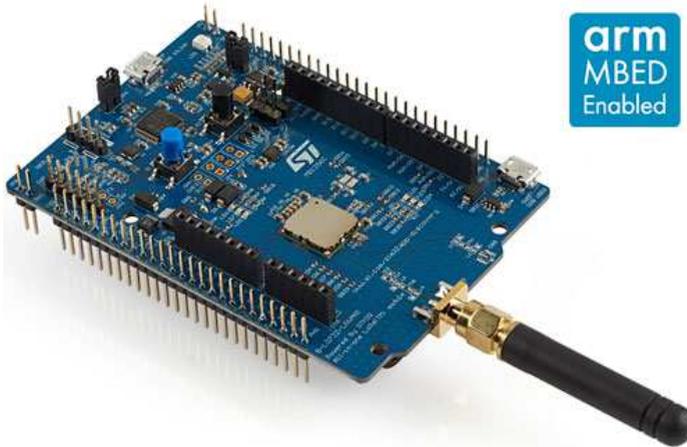
Para realizar tais testes de campo, montou-se um *end device* e dois *gateways* a partir de componentes de prateleira. Após isso, desenvolveu-se o *firmware* a ser executado nestes dispositivos.

5.1 HARDWARE

5.1.1 *End device*

Como *end device*, utilizou-se o *kit* de desenvolvimento da *STMicroelectronics* chamado B-L072Z-LRWAN1, o qual está mostrado na Figura 12. Esta placa possui um módulo desenvolvido pela empresa *Murata* chamado CMWX1ZZABZ-091. Este módulo, por sua vez, possui integrado o *chip* STM32L072CZ (o qual possui um processador ARM Cortex-M0+ de 32 *bits* com 32 MHz de *clock*) e o transceiver SX1276 (desenvolvido pela *Semtech*).

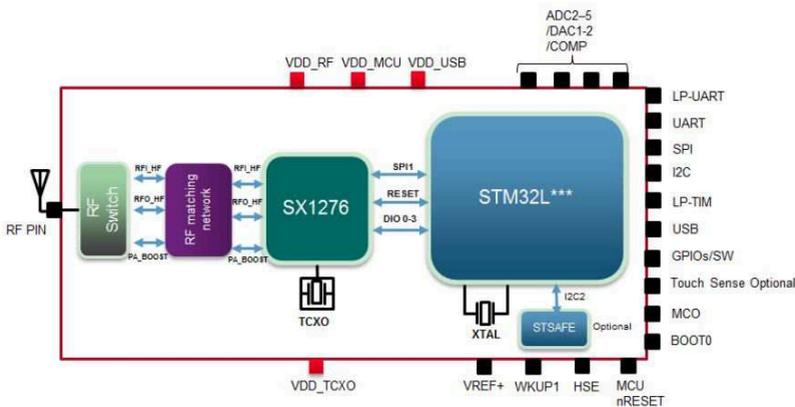
Figura 12 – Placa B-L072Z-LRWAN1.



Fonte: STMicroelectronics (2019).

A Figura 13 mostra o diagrama de ligações internas do módulo CMWX1ZZABZ-091. A comunicação entre o processador e o transceiver SX1276 (responsável pela modulação do sinal) é feita pela *Serial Peripheral Interface* (SPI), além de pinos de interrupção (DIO) e o pino de *reset*.

Figura 13 – Arquitetura do módulo CMWX1ZZABZ-091.



Fonte: MURATA (2019).

Nota-se que toda instrumentação da parte de rádio frequência, como casamento de impedâncias e o roteamento de múltiplos sinais para uma única linha de transmissão (*switch*), já é feita internamente no módulo. Esse fator é muito importante pois reduz o custo e a complexidade do desenvolvimento de uma aplicação real, diminuindo o *time-to-market*.

A potência máxima de transmissão do módulo é de 20 dBm (MURATA, 2019), parâmetro que é limitado pelo fabricante. Esse valor é 10 dBm a menos que o valor máximo permitido pelo protocolo LoRaWAN no Brasil.

Além disso, o processador ARM contido no *chip* STM32L072CZ possui modos de operação de baixo consumo, sendo eles: *sleep*, *stop* e *standby mode*. Esse fator é muito importante pois as aplicações as quais o dispositivo é destinado necessitam de baixo consumo de energia para operar durante longos períodos usando uma mesma bateria.

5.1.2 Gateway

Os receptores utilizados nos testes de campo são compostos pelos seguintes componentes:

- Raspberry Pi 3 Model B V1.2
- Módulo Gateway LoRaWAN (RHF0M301) RISINGHF
- Adaptador de pinos para módulo Gateway LoRaWAN
- SD Card
- Antena 915 MHz

A Figura 14 mostra o dispositivo resultante após a montagem dos componentes supracitados, faltando apenas a antena.

Foram montados dois *gateways*, de modo que a avaliação da diversidade espacial pudesse ser realizada. Ambos foram colocados em uma caixa com isolamento de alumínio, com a antena na parte externa.

Figura 14 – Dispositivo resultante após montagem dos módulos.



Fonte: TOKOPEDIA (2019).

A placa de adaptação de pinos possui um *jumper* amarelo no qual pode-se selecionar a fonte de alimentação da placa RHF0M301. Se posicionado à esquerda, como na Figura 14, a alimentação será oriunda de uma fonte externa, de modo que esta placa e a *Raspberry Pi* possuam alimentação separada. A outra opção, quando o *jumper* está posicionado no pino à direita, é alimentar o RHF0M301 utilizando os pinos de alimentação da *Raspberry Pi*. A opção mais recomendada é a primeira.

A placa RHF0M301 é responsável por realizar o recebimento dos sinais de rádio frequência. Já possui um *hardware* próprio encapsulado que entrega as mensagens recebidas através da interface SPI. Deste modo, não é necessário fazer nenhuma programação neste dispositivo. Um fator extremamente importante é conectar a ele uma antena que seja projetada para sua frequência de operação, que está na faixa de 915 MHz.

A *Raspberry Pi* é responsável por executar algumas aplicações de *software* que rodam no sistema operacional Linux da placa. Estas aplicações são configuradas como serviços, deste modo, são executadas a todo momento.

5.2 FIRMWARE

5.2.1 *End device*

A *STMicroelectronics* disponibiliza uma biblioteca denominada I-CUBE-LRWAN que possui alguns códigos exemplo para o *kit* de desenvolvimento B-L072Z-LRWAN1.

Um dos exemplos da biblioteca é o *AT Slave*, o qual propõe uma solução a partir do recebimento e envio de comandos AT por meio da interface serial *low power* UART (LPUART). Um dispositivo auxiliar é necessário para controle deste *slave*, podendo este possuir algum outro tipo de tecnologia de comunicação, o que resultaria em um dispositivo multi-protocolo que pode ser encaixado em diversas aplicações.

Dentro do contexto de *smart cities* por exemplo, poderia-se propor uma solução na qual todas as variáveis de interesse, como mostrado na Figura 1, fossem monitoradas a partir de sensores que possuem conectividade *Bluetooth*. Dividindo a cidade em áreas, poderia-se colocar um dispositivo concentrador que lê estes sensores através do *Bluetooth* em cada área, e encaminha esta informação por longas distâncias através do LoRa para um *gateway*.

Portanto, o desenvolvimento de um dispositivo *slave* que recebe comandos AT é pertinente pois este pode ser acoplado a outros dispositivos criando soluções variadas. O *Bluetooth* citado anteriormente poderia ser substituído por outras tecnologias como *ZigBee*, *6LoWPAN* e *RFID*, tornando possível aumentar o alcance de soluções que anteriormente poderiam se comunicar apenas na ordem de metros, mantendo o baixo consumo.

5.2.1.1 *Detalhes do firmware*

A *stack* LoRaWAN utilizada no código foi desenvolvida pela *Semtech* e é compatível com a versão 1.0.3 do protocolo. A partir dela, todos comandos AT recebidos são processados seguindo as especificações do LoRaWAN.

Todos os parâmetros do dispositivo podem ser configurados via comando AT, por exemplo: taxa de dados, potência de transmissão, tempo das janelas de recebimento, tipo das mensagens (confirmadas ou não confirmadas), tipo de autenticação (ABP ou OTAA), uso do ADR ou não, dentre outros.

A partir deste código base, implementou-se novas funcionalidades como: salvamento dos parâmetros do dispositivo na memória EEPROM, de modo que após sua reinicialização sua configuração não seja perdida; criação de um novo comando AT para configurar a sub-banda de operação do rádio; operação em modo de baixo consumo enquanto mensagens não são recebidas na serial.

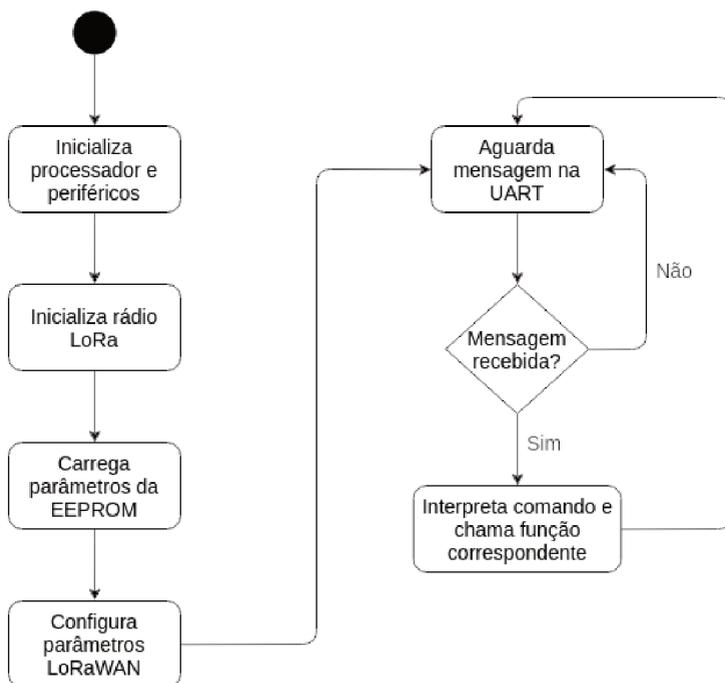
Alguns exemplos de comandos AT e suas utilidades estão mostrados na Tabela 2. Outros exemplos de comandos podem ser vistos no *Application Note* disponibilizado por STMicroelectronics AN4967 (2019).

Tabela 2 – Exemplos de comandos AT.

AT+SEND=1:mensagem	Comando para realizar o envio de mensagens através do protocolo LoRaWAN. O valor antes dos dois pontos é a porta (<i>FPort</i>) utilizada no envio.
AT+TXP=[0,1,2,3,...,15] AT+TXP=?	Configurar ou ler a potência de transmissão. Os valores permitidos estão, como especificado no protocolo, dentro do intervalo de 0 a 15.
AT+SUBBAND=[0,1,2,3,...,8] AT+SUBBAND=?	Configurar ou ler a sub-banda. Se configurado com o valor zero, todas as frequências são utilizadas. Os demais valores aceitos estão na faixa de 1 a 8, representando 8 sub-bandas de canais contíguos na faixa de 915 MHz.
AT+DR=[0,1,2,3,4,5,6,7] AT+DR=?	Configurar ou ler a taxa de dados. Os possíveis valores estão entre 0 e 7.
AT+ADR=[0,1] ou AT+ADR=?	Configurar ou ler o parâmetro binário que indica o uso do mecanismo de ADR.

A Figura 15 mostra a máquina de estados do *firmware* do *end device*. O primeiro passo é a inicialização do processador e periféricos. Na sequência, o rádio LoRa tem seus parâmetros iniciais configurados, enquanto que os demais são configurados após a leitura de seus valores da memória EEPROM. Também da memória, são resgatadas informações pertinentes ao protocolo. Após estas etapas de configuração, o dispositivo permanece em estado de baixo consumo enquanto um *byte* não é recebido na interface UART. Assim que um valor é recebido, uma interrupção é gerada e o processador volta a executar plenamente, recebendo todos os *bytes* do comando AT e processando-o de acordo com o tipo do comando.

Figura 15 – Máquina de estados do código do *end device*.



Fonte: O autor (2019).

5.2.1.2 *Script para controle do end device*

Como comentado anteriormente, o *end device* se comporta como um componente passivo, um *slave*, que necessita de uma intervenção externa para realizar alguma ação.

Para realização dos testes de campo, desenvolveu-se um *script* em *Python* para realizar o controle do *end device*. Este *script* é executado em um computador que é levado a campo e conectado ao dispositivo pela porta serial.

O que ele faz é, inicialmente, setar alguns parâmetros do *end device*. Após isso, realiza de forma sequencial o envio do comando AT+SEND, variando o SF configurado no dispositivo. Todas mensagens enviadas são salvas no próprio computador para avaliação futura.

5.2.2 *Gateway*

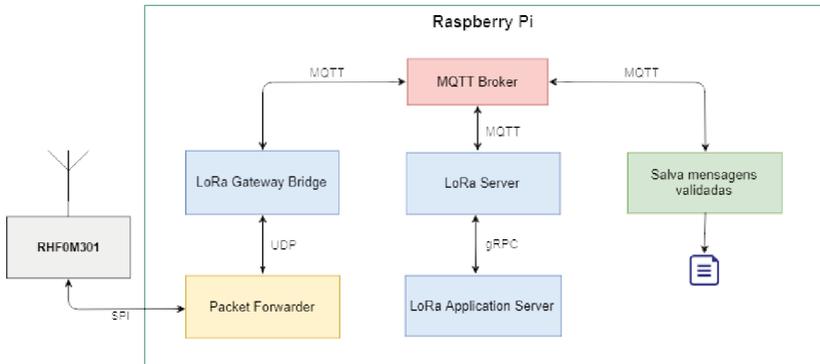
Na seção 3.1, com o auxílio da Figura 2, discutiu-se os componentes de uma rede LoRaWAN, que são: *end devices*, *gateways*, *network server* e *application server*. Estes dois últimos elementos normalmente são executados na nuvem, recebendo mensagens do *gateway* através de uma comunicação *Ethernet* ou rede celular. Porém, neste trabalho, desenvolveu-se uma solução na qual a rede é composta apenas por *end devices* e *gateways*, sendo que o *network server* e o *application server* são executados no próprio dispositivo que contém o *gateway*, eliminando a necessidade de comunicação com o mundo externo.

O *firmware* do *gateway* é executado na *Raspberry Pi* através de processos do sistema operacional que estão continuamente ativos. A Figura 16 mostra os principais processos e como as conexões entre eles é realizada. Também está ilustrada a conexão física entre os componentes de *hardware*, antena, RHF0M301 e *Raspberry Pi*.

Os detalhes sobre o funcionamento e origem de cada serviço executado na *Raspberry Pi* estão mostrados na sequência.

- **Packet forwarder**: este processo é responsável por fazer a comunicação com a placa RHF0M301 através da interface SPI. Em um *gateway* tradicional, os pacotes recebidos são encaminhados para um servidor na

Figura 16 – Principais componentes de *hardware* e *software* do *gateway*.



Fonte: O autor.

nvem usando o protocolo IP/UDP. No caso deste projeto, as mensagens recebidas são encaminhadas ao bloco *LoRa Gateway Bridge*.

O *software* do *Packet forwarder* é de código aberto e foi desenvolvido pela *Semtech*, detentora dos direitos da tecnologia LoRa.

- **LoRa Gateway Bridge:** este componente é responsável por converter o padrão de comunicação UDP do *Packet Forwarder* para pacotes do tipo *JSON* e enviá-los a um *broker* MQTT. Com esta conversão, toda troca de mensagens entre os serviços fica centralizada em um *broker*, tornando a comunicação mais simples.

O *LoRa Gateway Bridge* é um *software* de código aberto e foi desenvolvido como parte do projeto *LoRa Server*.

- **MQTT broker:** elemento central do *gateway* responsável por gerenciar o fluxo dos dados. Por ele passam todas as mensagens recebidas e enviadas pelo *gateway*. O protocolo MQTT é baseado em *publishers* e *subscribers*. Sempre que um *publisher* envia uma mensagem ao *broker*, todos os *subscribers* recebem esta informação.
- **LoRa Server:** este componente é o *network server* da rede LoRaWAN implementada. É responsável por fazer a validação das mensagens recebidas seguindo o padrão LoRaWAN. Sempre que o bloco *LoRa*

Gateway Bridge publica no *broker* MQTT, o *LoRa Server* recebe esta informação e verifica se ela é válida (ou seja, se o dispositivo que a enviou está cadastrado na rede, se o tamanho da mensagem está dentro dos limites impostos pelo protocolo LoRaWAN, dentre outros aspectos).

Este componente de *software* também faz parte do projeto *LoRa Server*, sendo de código aberto.

- **LoRa Application Server:** o *LoRa Application Server* é o *application server* da rede desenvolvida. Sempre que uma mensagem é validada pelo *LoRa Server*, ela é encaminhada ao *LoRa Application Server*.

Esta aplicação é responsável por salvar os dispositivos cadastrados na rede, bem como realizar o gerenciamento das mensagens de *uplink* e *downlink* (criptografar e descriptografar, por exemplo).

Além disso, esta aplicação provê uma interface gráfica para gerenciamento da rede. Nela, pode-se observar as mensagens sendo recebidas e enviadas, realizar o cadastro e exclusão de dispositivos da rede, entre outras configurações.

O *LoRa Application Server* também faz parte do projeto *LoRa Server*, sendo de código aberto.

- **Salva mensagens validadas:** este serviço foi desenvolvido pelo autor e tem a finalidade de salvar em um arquivo de texto as mensagens que foram validadas pelo *LoRa Server*. Este arquivo gerado é utilizado posteriormente para avaliar a comunicação entre os dispositivos.

Mais informações sobre o projeto *LoRa Server* podem ser vistas no site do desenvolvedor¹.

O procedimento para geração da imagem do sistema operacional a ser utilizada na *Raspberry Pi* com toda funcionalidade do *gateway* está apresentado no repositório² do autor.

¹ <<https://www.loraserver.io/>>

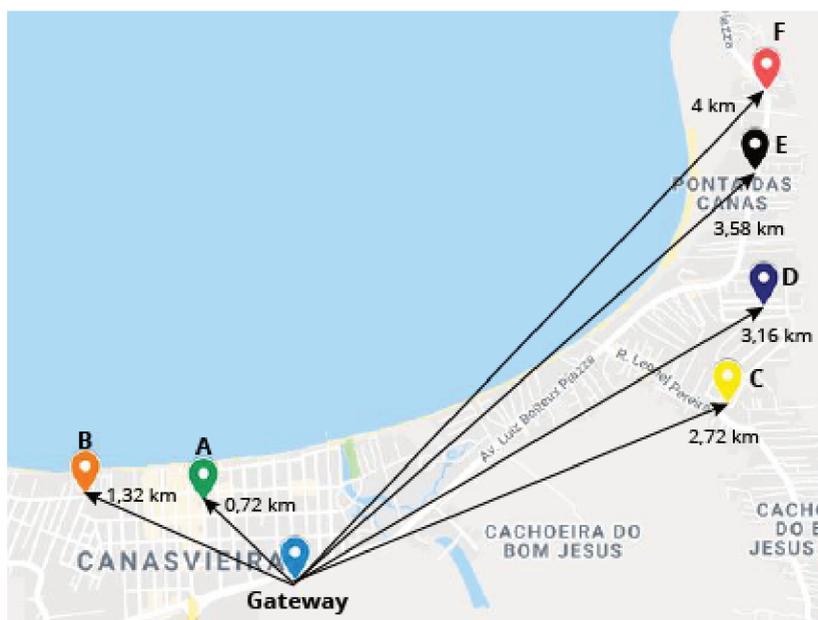
² <<https://github.com/esantosjr/tcc/blob/master/gateway-installation.md>>

6 TESTES DE CAMPO

Para realizar uma avaliação acerca do impacto da utilização de técnicas de diversidade no desempenho da comunicação em redes LoRa/LoRaWAN, uma rede contendo um *end device* e dois *gateways* foi montada na região do norte da ilha de Florianópolis, em uma área urbana, englobando os bairros Canasvieiras, Cachoeira do Bom Jesus e Ponta das Canas.

Foram escolhidos seis pontos diferentes para realizar a transmissão dos pacotes. A Figura 17 mostra a topologia da rede resultante utilizada nos testes, indicando a distância entre cada ponto e o *gateway*.

Figura 17 – Topologia da rede montada para os testes.



Fonte: O autor (2019).

Os testes foram realizados em dois dias diferentes (3 pontos em cada dia), e buscou-se uma condição climática semelhante entre eles, para que isso não fosse um fator que influenciasse nos resultados dos testes.

6.1 METODOLOGIA DOS TESTES

Os *gateways* foram posicionados em um ponto fixo do mapa, separados a uma distância de 80 centímetros. Através de uma estrutura de canos, foram elevados à 5 metros de altura, sendo alimentados por uma bateria estacionária de 12 Volts e 7Ah. A Figura 18 mostra os *gateways* montados para os testes.

Figura 18 – *Gateways* montados em campo.



Fonte: O autor (2019).

O *end-device* foi deslocado a pontos específicos, transmitindo pacotes apenas nestes pontos (o dispositivo permanecia desligado nos deslocamentos).

Assim como no *gateway*, foi utilizada uma estrutura de canos durante os testes de campo com o *end device*, o mantendo a 3 metros de altura durante as transmissões. A Figura 19 mostra a utilização desta configuração em campo.

Uma sacola foi usada para cobrir o dispositivo, para preveni-lo de sujeira e de uma possível chuva.

Como já comentado anteriormente, o *end device* é controlado por um *script* em *Python* sendo executado em um *notebook* conectado via porta serial. O fio que pode ser visto nas imagens é quem faz essa conexão.

6.2 PARÂMETROS DO TRANSMISSOR

Para testar o desempenho dos diferentes SFs, o mecanismo de ADR foi desativado, resultando em um fluxo unidirecional de dados, apenas com mensagens de *uplink*. Além disso, o modo de autenticação utilizado foi o ABP.

A Tabela 3 mostra os parâmetros que foram configurados no *end device*. A potência de transmissão máxima suportada pelo *hardware* foi utilizada e mantida fixa. Variou-se o SF, usando os valores permitidos no Brasil. Optou-se por utilizar a primeira sub-banda de frequência do espectro, que engloba as frequências de 902,3 a 903,7 MHz. A largura de banda do sinal é de 125 KHz.

Tabela 3 – Parâmetros do transmissor.

Parâmetro	Valor
Potência de transmissão	16 dBm
SF	$\in \{10, 9, 8, 7\}$
Faixa de frequência	902,3 a 903,7 MHz
Largura de banda	125 KHz
Classe	A
Modo de autenticação	ABP

6.2.1 Verificação da potência de transmissão

Realizou-se testes com um analisador de espectro para verificar se a potência de transmissão irradiada na antena era coerente com a configurada via *firmware*.

Como explicado na seção 5.2.1.1, a potência de transmissão é setada utilizando o comando $AT+TXP=TXPower$, onde *TXPower* pode assumir valores na faixa de 0 a 15, como especificado no protocolo LoRaWAN e mostrado na Figura 20. A potência de transmissão é sempre calculada da seguinte forma:

Figura 19 – Exemplos de pontos de transmissão.



(a) Ponto A.



(b) Ponto B.



(c) Ponto C.



(d) Ponto F.

Fonte: O autor (2019).

$30 - 2 \times TXPower$, em dBm. Apesar de ser possível obter 30 dBm através do cálculo ($TXPower = 0$) o rádio limita a potência de saída em 20 dBm, como discutido na seção 5.1.1.

Figura 20 – Configuração da potência de transmissão segundo o padrão LoRaWAN.

TXPower	Configuration (conducted power)
0	30 dBm – 2*TXpower
1	28 dBm
2	26 dBm
3 : 13
14	2 dBm
15	Defined in LoRaWAN

Table 13: US902-928 TX power table

Fonte: LORA ALLIANCE (2019).

O primeiro valor atribuído à variável $TXPower$ durante o teste foi 9, de modo que uma potência de 12 dBm é esperada na saída do rádio. A Figura 21a mostra o resultado obtido pelo analisador de espectro, onde pode-se observar o sinal transmitido na frequência de 902,5 MHz.

Observa-se uma potência de transmissão de 10,76 dBm, 1,24 dB a menos do que esperado. Esta perda pode ser causada por algum descasamento de impedância no circuito, ou até mesmo devido ao conversor SMA/BNC usado para conectar a placa ao analisador de espectro.

O teste foi repetido setando o parâmetro $TXPower$ para 7, o que resulta em uma potência de transmissão esperada de 16 dBm. A Figura 21b mostra o valor encontrado na prática, onde pode-se observar o sinal transmitido na frequência de 903,3 MHz.

Bem como no resultado anterior, a potência observada foi abaixo da esperada, ficando em 14,66 dBm, 1,34 dB a menos do que o valor teórico. Esta diferença é semelhante à encontrada anteriormente, e pode ser explicada pelas mesmas razões.

Na sequência, buscou-se analisar a potência de transmissão máxima que o dispositivo consegue alcançar. Para isso, o parâmetro foi setado em um

primeiro momento para 3, o que resultaria em uma potência de 24 dBm. O resultado observado na prática está mostrado na Figura 21c.

Observa-se que a potência de transmissão foi de 16,06 dBm. Segundo o *datasheet* do *chip* Murata, a potência máxima de saída que pode ser utilizada é 20 dBm. Apesar dessa limitação física imposta pelo fabricante, a potência de transmissão máxima encontrada foi de 16,06 dBm. O mesmo foi observado ao setar o parâmetro *TXPower* para 0, como mostrado na Figura 21d.

Devido a isso, pode-se afirmar que a máxima potência de transmissão que poderia ser utilizada nos testes de campo é de 16,06 dBm. Além disso, observou-se que as frequências mostradas pelo *firmware* no momento da transmissão eram as mesmas observadas no analisador de espectro, indicando que o circuito estava bem tunado e possui confiabilidade no que tange este parâmetro.

6.3 PADRÃO DAS MENSAGENS

6.3.1 Transmitidas

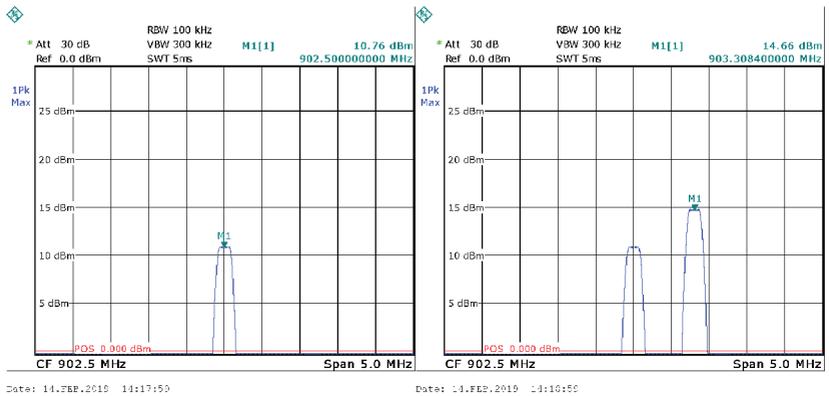
A cada 1,65 segundos, o *end device* transmite uma mensagem que contém um contador, a área na qual a transmissão está sendo feita, e um *payload* fictício de 5 *bytes*. Estes campos são separados por vírgula, o que faz que cada mensagem enviada tenha no máximo 10 *bytes* (quando o contador passa a ter dois dígitos).

A Figura 22 exemplifica um ciclo completo de envio de mensagens. Após cada transmissão, é informada a frequência (escolhida de forma randômica pelo protocolo) e o SF utilizados, bem como o instante de envio. Uma mesma mensagem é enviada 12 vezes, 3 vezes em cada SF. O intervalo de tempo entre o envio de pacotes com mesmo SF é de 6,6 segundos.

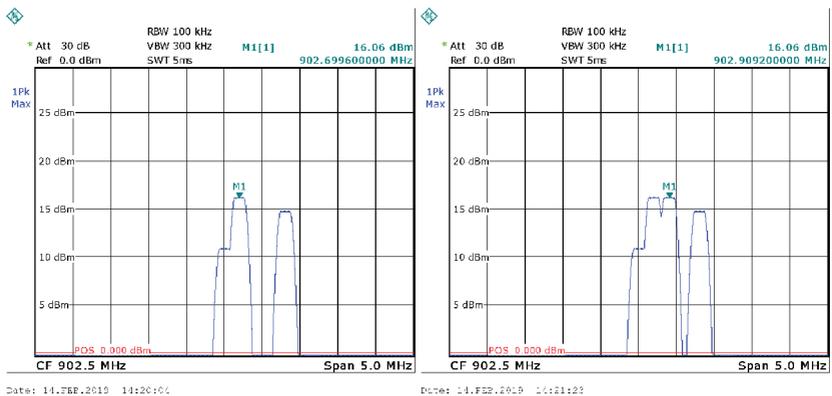
Em cada ponto do mapa dos testes de campo, o contador é variado de 0 a 15. Como são feitas 12 transmissões de uma mesma mensagem (12 vezes o mesmo contador), tem-se que $16 \times 12 = 192$ mensagens foram transmitidas por ponto, totalizando $192 \times 6 = 1152$ pacotes ao fim do teste.

Todas informações mostradas na Figura 22 são salvas em um arquivo para serem analisadas posteriormente.

Figura 21 – Valores de potência de transmissão obtidos pelo analisador de espectro.



(a) $TXPower = 9$. Valor teórico: 12 dBm. (b) $TXPower = 7$. Valor teórico: 16 dBm.



(c) $TXPower = 3$. Valor teórico: 24 dBm. (d) $TXPower = 0$. Valor teórico: 30 dBm.

Fonte: O autor (2019).

6.3.2 Recebidas

A cada sinal recebido que foi validado pelo *network server*, o *gateway* salva em um arquivo na memória interna: a mensagem em si, que contém o contador, a área e o *payload* fictício (sequência de 1's); o RSSI; a SNR; o

Figura 22 – Exemplo da sequência de envio de mensagens.

```
[SENT] AT+SEND=1:0,A,11111#
freq: 902900000 / sf: 10 / time:10:55:11.842928
[SENT] AT+SEND=1:0,A,11111#
freq: 902300000 / sf: 9 / time:10:55:13.495090
[SENT] AT+SEND=1:0,A,11111#
freq: 903700000 / sf: 8 / time:10:55:15.147230
[SENT] AT+SEND=1:0,A,11111#
freq: 903100000 / sf: 7 / time:10:55:16.799379
[SENT] AT+SEND=1:0,A,11111#
freq: 903300000 / sf: 10 / time:10:55:18.451504
[SENT] AT+SEND=1:0,A,11111#
freq: 902500000 / sf: 9 / time:10:55:20.103641
[SENT] AT+SEND=1:0,A,11111#
freq: 903500000 / sf: 8 / time:10:55:21.755795
[SENT] AT+SEND=1:0,A,11111#
freq: 902700000 / sf: 7 / time:10:55:23.407916
[SENT] AT+SEND=1:0,A,11111#
freq: 902700000 / sf: 10 / time:10:55:25.060028
[SENT] AT+SEND=1:0,A,11111#
freq: 902500000 / sf: 9 / time:10:55:26.712158
[SENT] AT+SEND=1:0,A,11111#
freq: 903100000 / sf: 8 / time:10:55:28.364307
[SENT] AT+SEND=1:0,A,11111#
freq: 903500000 / sf: 7 / time:10:55:30.016443
```

Fonte: O autor (2019).

canal de recepção e o SF.

Um exemplo de uma mensagem que é salva neste arquivo está mostrado abaixo. Neste caso, uma mensagem enviada do ponto B, com contador 6, que utilizou a frequência de 902,9 MHz e SF8, foi recebida com RSSI = -108 dBm e SNR = -3,5 dB.

6,B,11111,-108,-3.5,902900000,SF8

Com estas informações, é possível realizar uma comparação entre as informações salvas no transmissor e no receptor, gerando resultados como a quantidade de pacotes recebidos de cada ponto, fazendo uma distinção por SF, o RSSI mínimo recebido pelo *gateway*, o que caracteriza sua sensibilidade, dentre outras variáveis, as quais serão abordadas no capítulo seguinte.

7 RESULTADOS

Neste capítulo, serão apresentados os resultados obtidos a partir da avaliação dos dados extraídos dos testes de campo. Para tal, um *script* em *Python* foi desenvolvido, por onde foi possível processar as mensagens salvas no *notebook* que controlava o *end device* e na memória interna do *gateway*.

Durante o capítulo, a variável *A* denotará o número de antenas (*gateways*) sendo consideradas, enquanto que *M* refere-se ao número de vezes que uma mesma mensagem foi enviada.

7.1 SENSIBILIDADE

O primeiro resultado observado a partir das medidas feitas foi a sensibilidade do *gateway* para diferentes valores de SF. Para tal, as mensagens recebidas foram separadas por SF, resultando em quatro grupos de mensagens. A partir disso, pegou-se o valor de RSSI mínimo de cada grupo, resultando na sensibilidade observada.

Os valores obtidos estão apresentados na Tabela 4. Como pode ser observado, um aumento no valor do SF acarreta em uma melhor sensibilidade, apesar de que ao mudar de SF9 para SF10 isso não tenha sido observado, provavelmente pela insuficiência estatística do teste.

Tabela 4 – Sensibilidade do *gateway* para diferentes SFs.

SF	Sensibilidade (dBm)
7	-114
8	-115
9	-117
10	-117

Os valores obtidos na prática divergem dos apresentados no *datasheet* do componente RHF0M301, que indica que ao utilizar o SF7 a sensibilidade esperada é de -125 dBm, por exemplo. Isso se deve ao fato de que o fabricante realiza testes de bancada com cabos de resistência variável (ao aumentar a resistência simula-se um canal com maior atenuação, por exemplo), porém, na prática o comportamento é diferente pois podem haver sinais interferentes

na mesma faixa, entre outros motivos, resultando nesta discrepância. Apesar disso, os valores encontrados são satisfatórios.

7.2 MEDIDAS DE RSSI, SNR E *PATH LOSS*

O próximo passo foi separar os pacotes recebidos pelo *gateway* por área, usando o campo da mensagem que indica de qual região ela foi enviada. A partir disso, calculou-se os valores de RSSI médio e SNR média destes sub-conjuntos de dados. Os resultados estão mostrados na Tabela 5.

Tabela 5 – Características dos canais entre cada ponto e o *gateway*.

Ponto	$\overline{\text{RSSI}}$ (dBm)	$\overline{\text{SNR}}$ (dB)	$\overline{\text{Path Loss}}$ (dB)
A	-108,55	-5	131,05
B	-110,75	-8,72	133,25
C	-113,5	-8,11	136
D	-113,04	-9,79	135,54
E	-113,2	-8,52	135,7
F	-113,16	-10,77	135,66

Também na Tabela 5, mostra-se o valor do *Path Loss* do canal de cada ponto. Usando os valores de RSSI médio mostrados na tabela, o cálculo deste parâmetro é feito a partir de

$$PL_{dB} = P_{t_{dBm}} - \overline{\text{RSSI}}_{dBm} + G_t + G_r, \quad (7.1)$$

onde P_t vale 16 dBm. As variáveis G_t e G_r são os ganhos da antena de transmissão (3 dBi) e recepção (3,5 dBi), respectivamente.

7.3 MODELAGEM DO *FADING*

Como discutido na primeira seção do Capítulo 4, quando um sinal é transmitido por um canal de comunicação sem fio, ele está sujeito a diversos efeitos que atenuam e degradam a qualidade da comunicação.

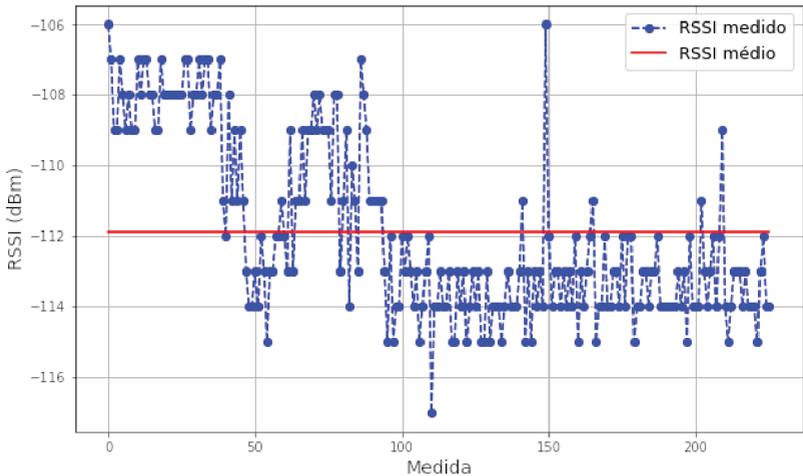
Um destes efeitos é o *fading*, que pode ser modelado a partir dos dados coletados em campo. Esta análise foi feita considerando apenas as mensagens transmitidas usando o SF10.

7.3.1 Sem considerar diversidade

Inicialmente, o *fading* foi modelado sem considerar a diversidade. Para tal, todas as mensagens recebidas por um dos *gateways* foram consideradas, ignorando o fato de haver diferentes versões de uma mesma mensagem.

Na Figura 23, os pontos em azul representam o valor do RSSI no instante em que as mensagens foram recebidas, sendo que o intervalo de tempo entre recebimentos é de $\approx 6,6$ segundos. O valor da potência instantânea média foi calculado e está representado por uma reta vermelha. O resultado encontrado foi de $-111,86$ dBm.

Figura 23 – RSSI e RSSI médio para diferentes instantes de tempo.

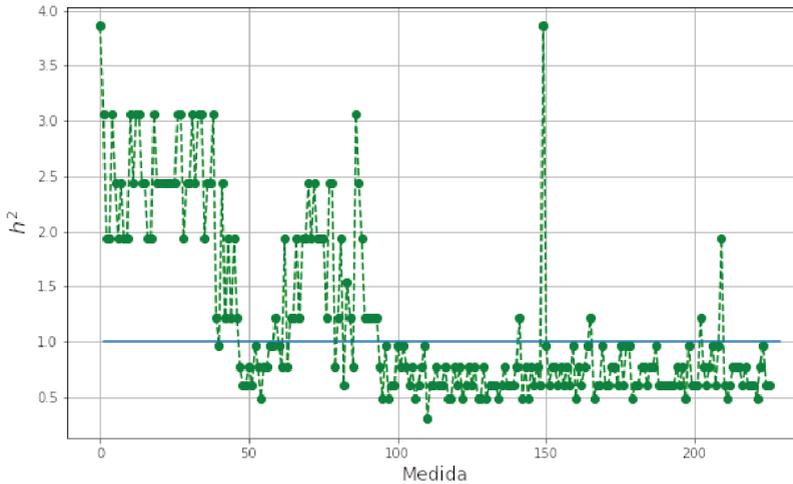


Fonte: O autor (2019).

Tendo os valores de RSSI em cada instante de tempo e o valor do RSSI médio, pode-se modelar o *fading* utilizando (4.7). Na Figura 24 pode-se observar o valor de h^2 para cada instante de tempo. Observa-se a variação dos valores em torno de 1, como esperado.

Com o valor de h^2 , é possível calcular o *fading* por meio de uma simples raiz quadrada: $h = \sqrt{h^2}$. Como o *fading* é uma variável aleatória, pode-se modelá-lo por meio de uma das funções densidade de probabilidade discutidas

Figura 24 – Variação instantânea da potência recebida para diferentes instantes de tempo.



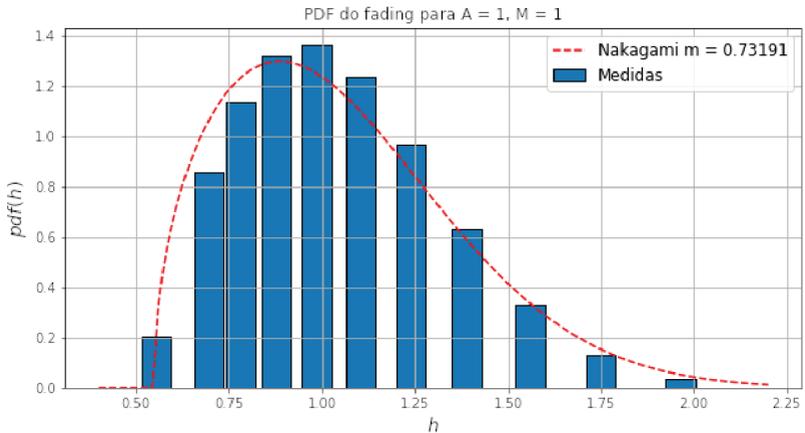
Fonte: O autor (2019).

no Capítulo 4. Com isso, é possível se ter uma ideia melhor do seu impacto sobre o sinal, gerando algum entendimento sobre o canal de comunicação.

Realizou-se um *fit* nos valores encontrados para h , considerando a distribuição *Nakagami-m* (4.10), por esta ser genérica. A Figura 25 mostra o resultado obtido.

O valor do parâmetro m da distribuição *Nakagami* indica o quão severo é o *fading*, sendo que quanto menor seu valor, maior tende a ser o efeito deste fenômeno sobre o sinal. O mínimo valor que este parâmetro pode assumir é 0,5 e o máximo, idealmente, é $m = \infty$, que é o caso quando não há *fading* (GOLDSMITH, 2004).

Observa-se que o valor de m encontrado foi de 0,73191, indicando uma forte degradação no canal por parte do *fading*.

Figura 25 – Distribuição do *fading*.

Fonte: O autor (2019).

7.3.2 Considerando diversidade

A mesma análise pode ser feita considerando agora diferentes tipos e ordens de diversidade. Os dados utilizados nesta parte são extraídos dos dados obtidos nos testes de campo, pegando a melhor versão de cada mensagem recebida. Ou seja, o conjunto de dados é separado em sub-conjuntos que contêm as diferentes versões de uma mesma mensagem, escolhendo-se a versão com o maior RSSI para realizar a análise.

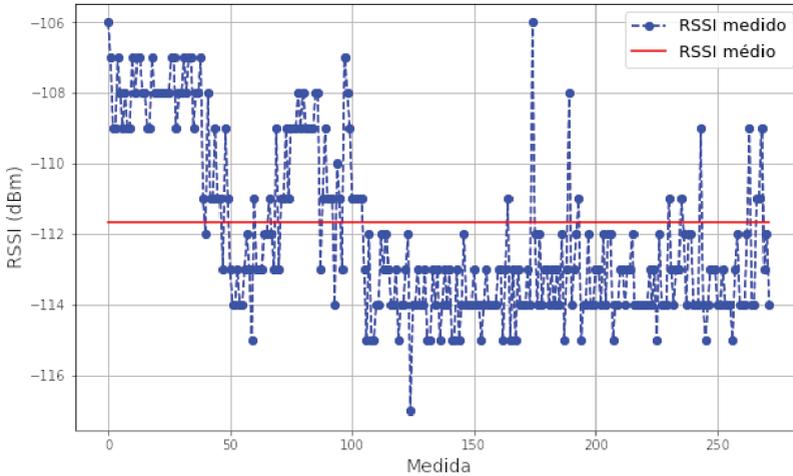
O intuito disso é, através da diversidade, analisar qual é a melhoria obtida nos efeitos que o canal impõe sobre os sinais transmitidos. Os resultados obtidos estão apresentados abaixo.

7.3.2.1 Espacial

Inicialmente, a análise foi refeita considerando a diversidade espacial, fazendo uso dos pacotes salvos nos dois *gateways* ($A = 2$) que foram utilizados nos testes de campo. Dessa maneira, cada sub-conjunto de dados obtido possuía no máximo duas mensagens, que é quando ambos os *gateways* receberam a mesma mensagem.

Na Figura 26 pode-se observar os valores de RSSI medidos para diferentes instantes de tempo, bem como o valor do RSSI médio calculado. O valor obtido foi de -111,65 dBm.

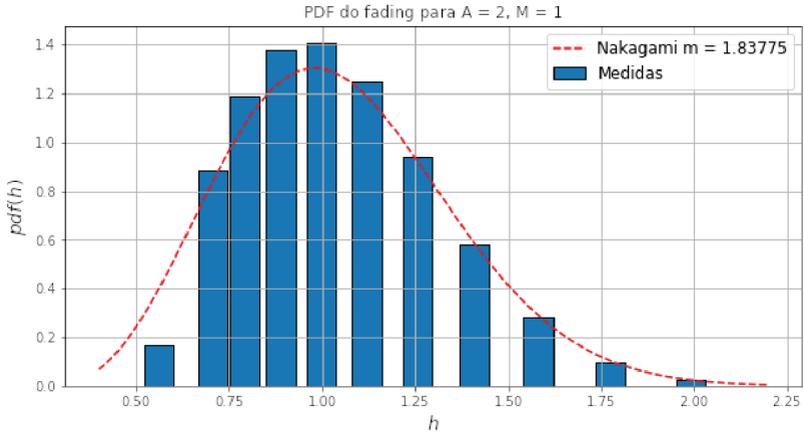
Figura 26 – RSSI e RSSI médio considerando diversidade espacial.



Fonte: O autor (2019).

A partir destes valores, é possível modelar o *fading* seguindo o mesmo procedimento feito anteriormente. A distribuição resultante pode ser visualizada no gráfico da Figura 27. Observa-se que o parâmetro m de *Nakagami* obtido agora foi 1,83775, valor que é 2,5 vezes maior que o obtido quando não considerou-se diversidade.

Figura 27 – Distribuição do *fading* considerando diversidade espacial.



Fonte: O autor (2019).

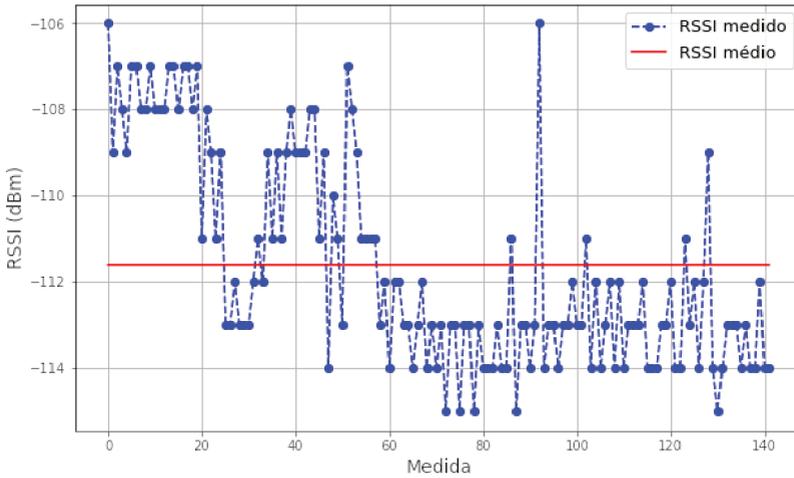
7.3.2.2 Temporal

No próximo passo, a análise foi feita para a diversidade temporal, considerando-se 1 replicação por mensagem, ou seja, uma mesma mensagem é enviada duas vezes ($M = 2$).

Novamente, os valores de RSSI e RSSI médio (calculado considerando as melhores versões das mensagens) foram traçados, resultando na Figura 28, onde o RSSI médio vale -111,60 dBm.

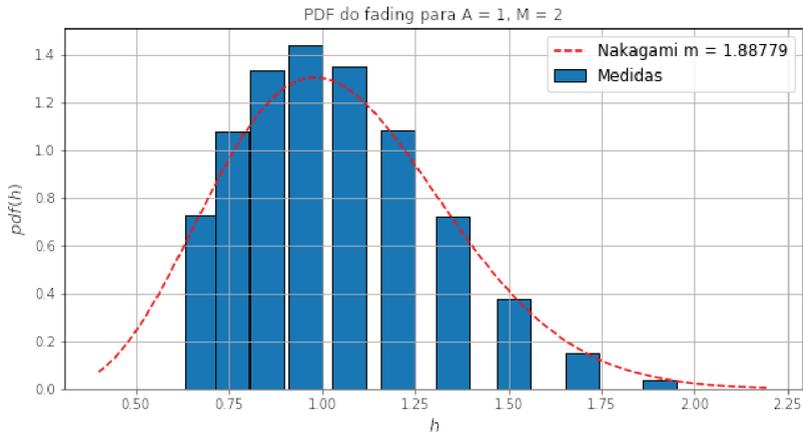
A distribuição de probabilidade do *fading* pode ser observada na Figura 29. Nota-se que agora o valor do parâmetro m encontrado foi 1,88779.

Figura 28 – RSSI e RSSI médio considerando diversidade temporal.



Fonte: O autor (2019).

Figura 29 – Distribuição do *fading* considerando diversidade temporal.



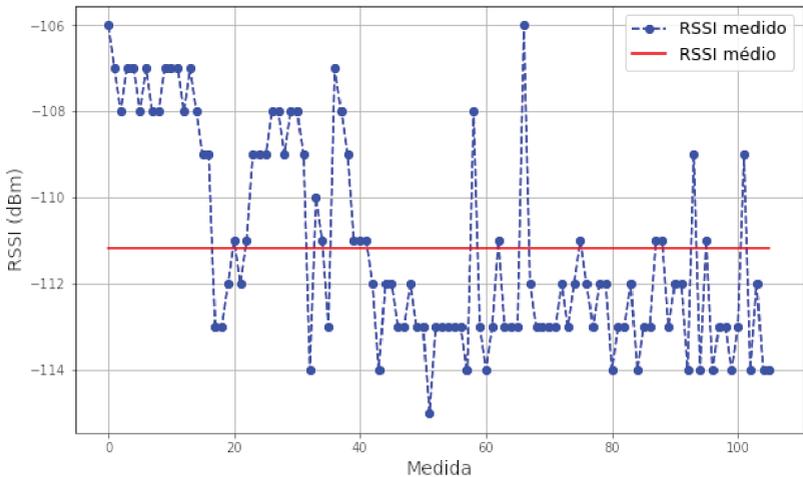
Fonte: O autor (2019).

7.3.2.3 Ambas técnicas

A última análise feita para modelagem do *fading* foi considerando as técnicas de diversidade temporal e espacial simultaneamente, resultando em uma ordem de diversidade igual a 4 ($A = 2$ e $M = 2$).

Novamente, considerando as melhores versões das mensagens em termos de potência instantânea, os valores de RSSI e RSSI médio foram traçados, resultando na Figura 30, onde o RSSI médio vale $-111,17$ dBm.

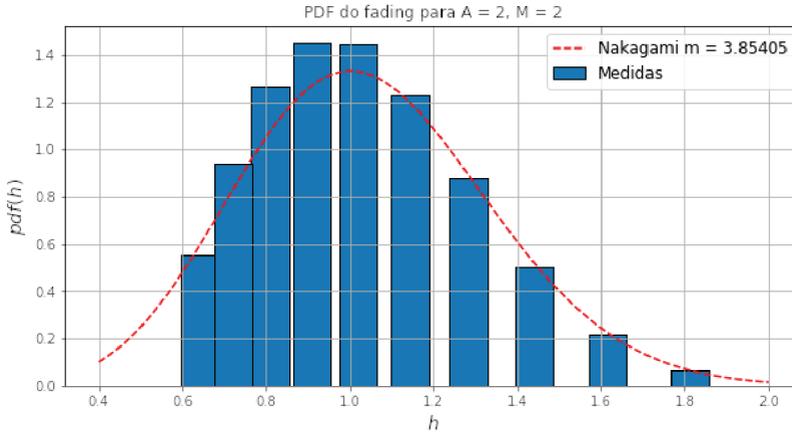
Figura 30 – RSSI e RSSI médio considerando ambas técnicas.



Fonte: O autor (2019).

A distribuição de probabilidade do *fading* pode ser observada na Figura 31. Como mostrado na figura, o valor de m encontrado neste caso foi de 3,85405.

Figura 31 – Distribuição do *fading* considerando ambas técnicas.



Fonte: O autor (2019).

7.3.3 Comparação dos resultados

A Tabela 6 resume os resultados apresentados acima, mostrando o valor do parâmetro m da distribuição *Nakagami* para diferentes ordens de diversidade¹.

Tabela 6 – Valores de m para diferentes ordens de diversidade.

Esquema	Ordem	m
A=1, M=1	1	0,73191
A=2, M=1	2	1,83775
A=1, M=2	2	1,88779
A=2, M=2	4	3,85405

Observa-se que, à medida que a ordem da diversidade aumenta (mais receptores sendo utilizados ou mais réplicas de mensagens sendo enviadas) o valor do parâmetro m aumenta.

Esse comportamento indica que ao utilizar diversidade, é possível enxergar versões dos sinais transmitidos que são menos degradadas pelo canal,

¹ Essa ordem refere-se à diversidade inserida no sistema (A x M).

ou seja, que estão sob efeito de um *fading* menos severo, fazendo com que se tenha uma comunicação de melhor qualidade. Além disso, à medida que a ordem da diversidade aumenta, a distribuição de probabilidade do *fading* se torna mais uniforme em torno de 1.

Em um caso ideal, poderia-se transmitir uma mensagem infinitas vezes, ou utilizar infinitos receptores, de modo que o valor de m tendesse ao infinito. Porém, na prática, observa-se que a probabilidade de conexão satura para uma determinada ordem de diversidade, ou até mesmo tem seu valor reduzido devido às colisões, como mostrado em Hoeller et al. (2018), quando se utiliza diversidade temporal.

Deve-se optar por uma estratégia na qual um número mínimo de mensagens são transmitidas (ou um número mínimo de receptores são utilizados) para uma dada confiabilidade desejada, com intuito de reduzir o consumo de energia e a ocupação do canal. Esta discussão é feita na próxima seção.

7.4 PROBABILIDADE DE CONEXÃO

Nesta seção, a probabilidade de conexão obtida nos testes de campo, para cada ponto do mapa da Figura 17, fazendo discriminação por SF, será mostrada a partir de gráficos. Este parâmetro é um indicativo da qualidade da comunicação em cada ponto, mostrando o porcentual das mensagens enviadas que foram recebidas.

Em uma aplicação real, por exemplo, poderia-se utilizar o valor da probabilidade de conexão para decidir se o ponto do qual mensagens estão sendo enviadas é adequado para se manter o dispositivo.

A partir deste valor é possível identificar o impacto das técnicas de diversidade na qualidade da comunicação, observando que a probabilidade de conexão aumenta quando se faz replicações de mensagens ou utiliza-se múltiplos *gateways*. Vale lembrar que o protocolo LoRaWAN realiza a variação do canal de envio das mensagens de forma automática, escolhendo uma das oito frequências configuradas no *end device*. Deste modo, uma mensagem nunca é enviada na mesma frequência da anterior, fator que contribui para a melhoria da comunicação, gerando diversidade em frequência.

7.4.1 Sem considerar diversidade

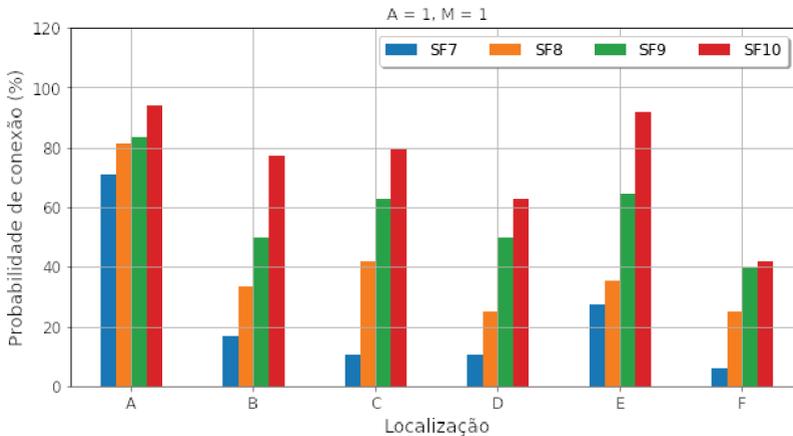
O cálculo da probabilidade de conexão é feito, inicialmente, sem considerar diversidade. Para tal, as mensagens, tanto transmitidas quanto recebidas, são divididas por área e por SF. Deste modo, a probabilidade de conexão é calculada diretamente a partir de uma divisão entre o número de mensagens recebidas e o número de mensagens transmitidas.

O resultado obtido está mostrado na Figura 32. Observa-se que os maiores valores da probabilidade de conexão são obtidos ao utilizar SF10. Isso já era esperado, visto que ao configurar o rádio com este parâmetro, uma taxa de dados menor é utilizada e com isso consegue-se um alcance maior.

Porém, mesmo para o SF10, um resultado satisfatório só foi obtido nos pontos A e E. Nos demais, a probabilidade de conexão é menor ou igual a 80%, o que ainda é uma perda de pacotes muito grande para a maioria das aplicações.

Ao utilizar os outros SFs, os resultados não foram muito relevantes, ficando acima de 80% apenas no ponto A, para o SF9 e SF8.

Figura 32 – Probabilidade de conexão por ponto, por SF, sem considerar diversidade.



Fonte: O autor (2019).

7.4.2 Considerando diversidade

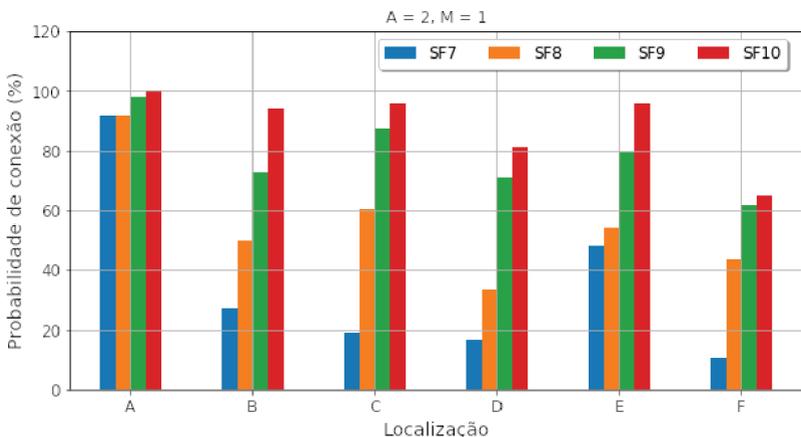
No próximo passo, a probabilidade de conexão foi recalculada, considerando agora a diversidade. Nesta parte, o valor não é calculado de uma forma direta, fazendo apenas uma divisão. Um pré-processamento é realizado nos dados para que as diferentes versões de uma mesma mensagem sejam consideradas.

7.4.2.1 Espacial

Inicialmente, a probabilidade de conexão é calculada considerando diversidade espacial ($A = 2$). Ou seja, se uma mensagem é recebida em pelo menos um dos *gateways*, ela é considerada como recebida.

O resultado obtido está mostrado na Figura 33. Observa-se que em todos os pontos e em todos os SFs houve um aumento no valor da probabilidade de conexão. Levando em consideração o SF10 nos pontos A, B, C e E, obteve-se um valor acima dos 90%, sendo que no ponto A os SF7, 8 e 9 também chegaram nesse nível.

Figura 33 – Probabilidade de conexão por ponto, por SF, considerando diversidade espacial.



Fonte: O autor (2019).

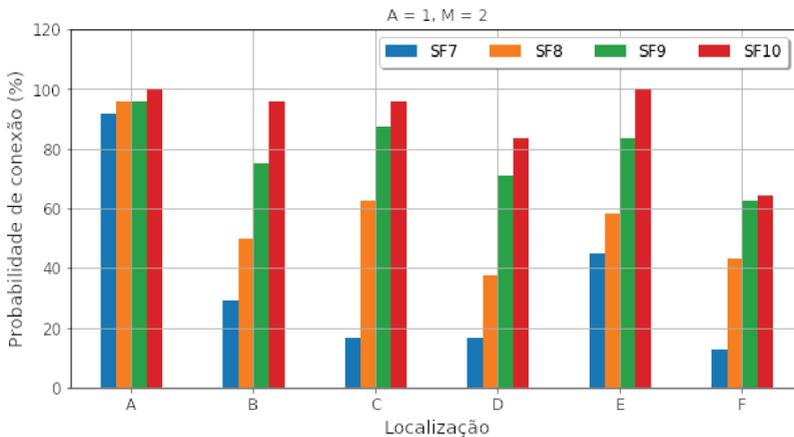
Isso mostra que, ao utilizar um segundo *gateway*, idêntico ao primeiro, é possível tornar a comunicação viável em pontos onde antes a qualidade não era satisfatória, como nos pontos B e C, ou viabilizar a utilização de um SF menor, que ocupa menos o canal, como no ponto A. Porém, isso ainda não é suficiente para se ter uma confiabilidade elevada em todos os casos, como no ponto F, onde obteve-se uma probabilidade de conexão de $\approx 65\%$.

7.4.2.2 Temporal

Na análise seguinte, considerou-se o efeito da diversidade temporal na qualidade da comunicação ao se realizar uma replicação de cada mensagem ($M = 2$). Para isso, considerando as mensagens recebidas por um dos *gateways*, se uma mensagem é recebida pelo menos uma vez, ela é considerada como recebida.

O resultado obtido pode ser visualizado na Figura 34. Assim como no caso da diversidade espacial, houve um acréscimo no valor da probabilidade de conexão em todas as ocasiões, chegando a 100% nos pontos A e E ao utilizar SF10.

Figura 34 – Probabilidade de conexão por ponto, por SF, considerando diversidade temporal.



Fonte: O autor (2019).

Apesar desse aumento na probabilidade de conexão, nos pontos D e F, ainda não se tem uma confiabilidade satisfatória. Além disso, ainda é necessário utilizar SF10 na maioria dos casos. Devido a isso, ainda deve-se explorar mais o uso da diversidade neste cenário.

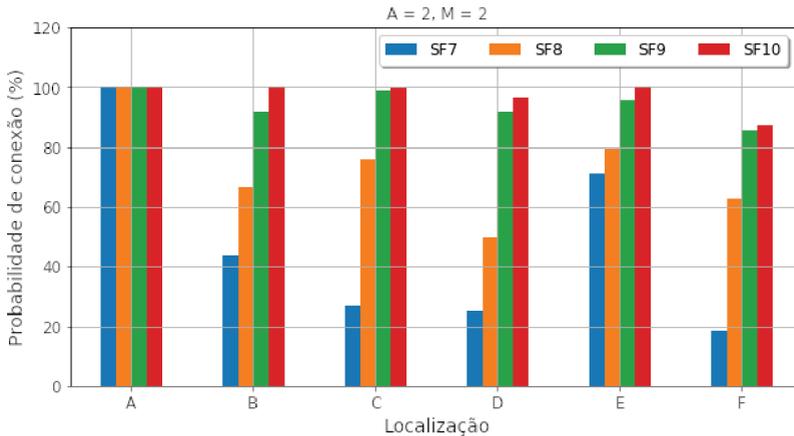
Observa-se que os resultados obtidos ao se considerar diversidade temporal são semelhantes aos alcançados com o uso de diversidade espacial. Isso era esperado de acordo com a teoria, visto que em ambos os casos tinha-se uma ordem de diversidade igual a 2.

7.4.2.3 Ambas técnicas

Neste momento, a análise do impacto da diversidade será feita considerando as técnicas espacial e temporal atuando de forma simultânea. A utilização de diferentes técnicas de diversidade em um mesmo cenário se torna interessante pois, neste caso, pode-se obter uma ordem de diversidade igual a 4 sem precisar transmitir uma mensagem 4 vezes, visto que 2 *gateways* estão sendo utilizados. Com isso, é possível reduzir o consumo energético do módulo e a ocupação do canal.

O resultado para o caso de $A = 2$ e $M = 2$ pode ser visualizado na Figura 35. Observa-se que em todos os pontos obteve-se uma probabilidade de conexão $\geq 90\%$. Por meio deste resultado, é possível identificar qual configuração do *end device* é necessária em cada ponto, dada uma confiabilidade mínima. Nos pontos B, C, D e E é possível utilizar SF9, diminuindo a ocupação do canal. Além disso, no ponto A, pode-se utilizar SF7, o que é ideal para pontos mais próximos do receptor. Poderia-se optar também por uma potência de transmissão menor, para diminuir o consumo. No ponto F é preciso utilizar SF10, o que é razoável devido à distância de 4 km entre transmissor e receptor. Poderia-se optar também por utilizar um fator $M = 3$ neste ponto, procurando melhorar ainda mais a probabilidade de conexão.

Figura 35 – Probabilidade de conexão por ponto, por SF, considerando ambas técnicas.



Fonte: O autor (2019).

Com os resultados acima, os quais apresentam uma alta confiabilidade em todos os pontos, pode-se afirmar que o alcance máximo obtido considerando o ambiente urbano no qual os testes foram feitos foi de 4 km. Este é um resultado satisfatório quando comparado aos apresentados na literatura. Em Augustin et al. (2016), obteve-se uma probabilidade de conexão de 90% a uma distância máxima de 2,8 km, utilizando SF12 (valor que é permitido na Europa) e uma potência de transmissão de 14 dBm. Já em Petajajarvi et al. (2015), a probabilidade de conexão obtida foi de 88% em uma faixa de 0 à 2 km e de 85% de 2 a 5 km, ambas utilizando SF12 e 14 dBm. Com estas mesmas configurações, o trabalho de Centenaro et al. (2016) obteve um alcance de 1,2 km.

Nestes trabalhos, as técnicas de diversidade não foram investigadas, o que pode explicar esta diferença no resultado obtido. Esse fator reafirma a utilidade das técnicas de diversidade. Além disso, apesar de as topologias utilizadas terem sido diferentes (principalmente altura dos dispositivos), os testes feitos nos artigos possuem semelhança com o deste trabalho pois foram feitos dentro de um contexto de *smart cities*, em uma área urbana, de modo que a comparação seja cabível.

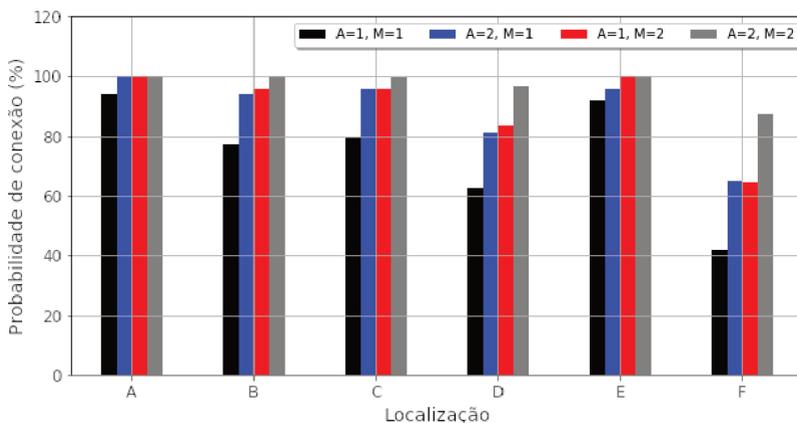
7.4.3 Comparação do desempenho para diferentes ordens de diversidade

Nesta seção, será discutido o real ganho obtido no valor da probabilidade de conexão ao se utilizar técnicas de diversidade.

A Figura 36 mostra, levando em consideração o parâmetro SF10, em preto, o valor da probabilidade de conexão sem considerar diversidade, em azul, considerando duas antenas, em vermelho, considerando uma replicação, e em cinza, considerando ambas técnicas.

Observa-se que ao utilizar uma ordem de diversidade igual a 2 ($A = 2$ ou $M = 2$), consegue-se um aumento por volta de 20 pontos percentuais nos melhores casos, chegando a até ≈ 40 pontos percentuais ao se considerar $A = 2$ e $M = 2$, como no ponto F.

Figura 36 – Comparação do desempenho das técnicas para SF10.



Fonte: O autor (2019).

Como mostrado na equação (4.12), espera-se que uma mesma ordem de diversidade resulte em um mesmo ganho na probabilidade de conexão, independente do tipo da diversidade sendo utilizada. Isso pode ser observado na maioria dos pontos mostrados na Figura 36, na qual as barras azuis e vermelhas são praticamente as mesmas em todos os casos, mostrando que os resultados obtidos na prática são coerentes e aderentes à teoria. Para os demais

SFs o mesmo pode ser concluído.

Todavia, em uma aplicação com um grande número de nós, esse resultado seria diferente, pois o aumento de M acarretaria em um aumento nas colisões entre sinais. Logo, aumentar o valor de A traria melhores resultados em uma situação como essa.

8 CONCLUSÃO

A utilização de técnicas de diversidade possui o objetivo de melhorar o desempenho da comunicação sem fios em ambientes pouco favoráveis para tal prática. Através da modulação LoRa e do protocolo LoRaWAN, é possível encontrar um conjunto de parâmetros especial para cada cenário, que irão influenciar em fatores como consumo de energia do dispositivo, tempo de ocupação do canal, alcance da comunicação, entre outros.

Os resultados apresentados no trabalho mostram que através da diversidade e dos parâmetros dos dispositivos, é possível tornar uma comunicação viável em pontos onde antes não se tinha um desempenho aceitável, a um baixo custo de complexidade, monetário e até mesmo energético.

Se a topologia de rede apresentada durante os testes fosse utilizada em uma aplicação real, os resultados obtidos poderiam servir como uma fonte de decisão para configurar os *end devices* no que tange potência de transmissão, SF e número de replicações de mensagens necessário.

Levando em consideração a diversidade espacial, ao se utilizar múltiplos *gateways*, além de haver uma melhoria na qualidade da comunicação, o uso desta técnica pode tornar uma rede escalável, como discutido por Bor et al. (2016). Assim, a diversidade espacial é sempre benéfica, ao contrário da diversidade temporal, onde deve-se utilizar o mínimo de replicações possíveis para diminuir o consumo de energia e a probabilidade de colisões entre pacotes. Deste modo, há um compromisso entre a densidade da rede (número de nós) e a quantidade de replicações. Além disso, deve-se procurar utilizar sempre o mínimo SF possível (maior taxa de dados), para que o tempo em que os sinais fiquem no ar diminua, o que faz com que a probabilidade de colisões também diminua.

Os resultados apresentados, como o da Figura 32 por exemplo, deixou claro que não é apenas a distância que influencia a qualidade da comunicação. O ponto E que está a 3,58 km, por exemplo, apresentou um resultado melhor do que o ponto B, a 1,32 km. Isso se deve ao fato de o canal ser diferente em cada ponto, como por exemplo pelo relevo do solo ou obstáculos que geram sombreamento. Isso implica que uma solução deve ser desenvolvida para um

ambiente específico.

Apesar desse fator, os resultados obtidos podem ser utilizados de base para outros trabalhos ou alguma aplicação prática que busque implantar uma rede de dispositivos LoRa em um ambiente urbano, pois foram satisfatórios ao se utilizar técnicas de diversidade, tanto no quesito alcance quando em relação à probabilidade de conexão.

Sabendo que a arquitetura de uma rede LoRaWAN é do tipo estrela, o alcance de 4 km poderia ser obtido também em outras direções, e se fosse possível criar diversas células como essa, a cobertura da rede poderia abranger outros bairros além dos três apresentados no trabalho.

Por fim, pode-se concluir que os objetivos levantados no começo do trabalho foram alcançados, sendo possível verificar o impacto positivo do uso de técnicas de diversidade em redes LoRa/LoRaWAN.

REFERÊNCIAS

- AUGUSTIN, Aloÿs; YI, Jiazi; CLAUSEN, Thomas; TOWNSLEY, William Mark. **A study of Lora: Long range & low power networks for the internet of things**. Sensors (Switzerland), 2016.
- BOR, Martin Christiaan; ROEDIG, Utz; VOIGT, Thiemo; ALONSO, Juan M. **Do LoRa Low-Power Wide-Area Networks Scale?**. Association for Computing Machinery (ACM), pp. 59–67. 2016.
- CENTENARO, Marco; VANGELISTA, Lorenzo; ZANELLA, Andrea; ZORZI, Michele. **Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios**. IEEE Wireless Communications, vol. 23, no. 5, pp. 60-67, 2016.
- CHEONG, Phui San; BERGS, Johan; HAWINKEL, Chris; FAMAHEY, Jeroen. **Comparison of LoRaWAN classes and their power consumption**. 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT), Leuven, 2017, pp. 1-6.
- CISCO. **Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2016-2021**. White Pap., 2017.
- FERRE, Guillaume. **Collision and packet loss analysis in a LoRaWAN network**. 2017 25th European Signal Processing Conference (EUSIPCO), Kos, 2017, pp. 2586-2590.
- GOLDSMITH, Andrea. **Wireless Communications**. Stanford University, 2004.
- HOELLER, Arliones; SOUZA, Richard Demo; López, O. L. Alcaraz; ALVES, Hilrey; NORONHA NETO, Mário; BRANTE, Glauber. **Analysis and Performance Optimization of LoRa Networks With Time and Antenna Diversity**. IEEE Access, vol. 6, pp. 32820-32829, 2018.
- LORA ALLIANCE. **LoRaWAN Specification v1.1**. Disponível em: <https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf>. Acesso em: 5 fev. 2019.

LORA ALLIANCE. **LoRaWAN Regional Parameters v1.1**. Disponível em: <https://loro-alliance.org/sites/default/files/2018-04/lorawanm_regional_parameters_v1.1rb_-_final.pdf>. Acesso em: 8 fev. 2019.

LORA TOOLS. **Calculate the air time of your LoRa frame**. Disponível em: <<https://www.loratools.nl/#/airtime>>. Acesso em: 30 março 2019.

MEKKI, Kais; BAJIC, Eddy; CHAXEL, Frederic; MEYER, Fernand. **A comparative study of LPWAN technologies for large-scale IoT deployment**. ICT Express, 2018.

MIKHAYLOV, Konstantin; PETAEJAEJAERVI, Juha; HAENNINEN, Tuomo. **Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology**. European Wireless 2016; 22th European Wireless Conference, Oulu, Finland, 2016, pp. 1-6.

MURATA. **Sub-G Module Data Sheet**. Disponível em: <https://wireless.murata.com/RFM/data/type_abz.pdf>. Acesso em: 6 março 2019.

PETAJAJARVI, Juha; MIKHAYLOV, Konstantin; ROIVAINEN, Antti; HANNINEN, Tuomo; PETTISSALO, Marko. **On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology**. 2015 14th International Conference on ITS Telecommunications (ITST), Copenhagen, 2015, pp. 55-59.

POP, Alexandru-Ioan; RAZA, Usman; KULKARNI, Parag; SOORIYABANDARA, Mahesh. **Does Bidirectional Traffic Do More Harm Than Good in LoRaWAN Based LPWA Networks?**. 2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings.

RAZA, Usman; KULKARNI, Parag; SOORIYABANDARA, Mahesh. **Low Power Wide Area Networks: An Overview**. IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855-873, 2017.

REYNDERS, Brecht; MEERT, Wannes; POLLIN, Sofie. **Range and coexistence analysis of long range unlicensed communication**. 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, 2016, pp. 1-6.

STMicroelectronics. **B-L072Z-LRWAN1**. Disponível em: <<https://www.st.com/en/evaluation-tools/b-l072z-lrwan1.html>>. Acesso em: 6 março 2019.

STMicroelectronics AN4967. **Examples of AT commands on I-CUBE-LRWAN**. Disponível em: <<https://bit.ly/2VN924S>>. Acesso em: 8 março 2019.

THE THINGS NETWORK. **LoRaWAN Overview**. Disponível em: <<https://www.thethingsnetwork.org/docs/lorawan/>>. Acesso em: 4 fev. 2019.

TOKOPEDIA. **LoRa Gateway / Concentrator Module Kit - RHF0M301 915MHz**. Disponível em: <<https://www.tokopedia.com/altrosurabaya/lora-gateway-concentrator-module-kit-rhf0m301-915mhz>>. Acesso em: 6 março 2019.

VEJLGAARD, Benny; LAURIDSEN, Mads; NGUYEN, Huan; KOVACS, Istvan Z.; MOGENSEN, Preben; SORENSEN, Mads. **Interference Impact on Coverage and Capacity for Low Power Wide Area IoT Networks**. 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, 2017, pp. 1-6.

YU, Fanghao; ZHU, Ziming; FAN, Zhong. **Study on the feasibility of LoRaWAN for smart city applications**. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, 2017, pp. 334-340.