



UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ - UNIOESTE

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

Colegiado de Ciência da Computação

Curso de Bacharelado em Ciência da Computação

Avaliação Prática de Comunicação e Levantamento dos Métodos de Segurança de LoRaWAN para Coleta de Dados de Sensores Sem-Fio

Trabalho de Conclusão de Curso

Willian Cavaller Faino



Cascavel-PR

2021

UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ - UNIOESTE

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

Colegiado de Ciência da Computação

Curso de Bacharelado em Ciência da Computação

Willian Cavaller Faino

**Avaliação Prática de Comunicação e Levantamento dos
Métodos de Segurança de LoRaWAN para Coleta de Dados de
Sensores Sem-Fio**

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação, do Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste do Paraná - Campus de Cascavel.

Orientador(a): Prof. Dr. Luiz Antonio Rodrigues

Cascavel-PR

2021

WILLIAN CAVALLER FAINO

**AVALIAÇÃO PRÁTICA DE COMUNICAÇÃO E LEVANTAMENTO DOS
MÉTODOS DE SEGURANÇA DE LORAWAN PARA COLETA DE DADOS
DE SENSORES SEM-FIO**

Monografia apresentada como requisito parcial para obtenção do Título de Bacharel em Ciência da Computação, pela Universidade Estadual do Oeste do Paraná, Campus de Cascavel, aprovada pela Comissão formada pelos professores:

Prof. Dr. Luiz Antonio Rodrigues (Orientador)
Colegiado de Ciência da Computação, UNIOESTE

Prof. Dr. Marcio Seiji Oyamada
Colegiado de Ciência da Computação, UNIOESTE

Prof. Dr. Edson Tavares de Camargo
UTFPR - Toledo

Cascavel, 28 de Julho de 2022

Dedico este trabalho a todos meus familiares, em especial meu pai Gilson da Silva Faino, minha mãe Lorinez de César Cavaller Faino, minha irmã Jaqueline Cavaller Faino e minha caçulinha Caroline Alexia Cavaller Faino, que sempre estiveram por perto me oferecendo motivação e ajudando de todas as formas possíveis. Dedico também a todos meus professores, que sempre estiveram presentes e se dispuseram a ajudar em qualquer momento e qualquer assunto, em especial ao professor Luiz Antonio Rodrigues, meu orientador tanto do TCC quanto de outros projetos, pois foi muito importante para meu desenvolvimento dentro do ambiente acadêmico. Por fim, dedico principalmente para a pessoa mais importante da minha vida, minha amada Gabrielle Marcondes Guimarães, que sua existência por si só sempre foi minha maior motivação para seguir em frente.

Agradecimentos

Agradeço primeiramente aos meus amigos Vinícius, Danielly, Ana, Eduardo, Lisandra e, principalmente, Lucas, que posso considerar como um professor à parte pelo tempo que utilizou me ajudando com trabalhos e listas de exercícios, agradeço a eles por tornarem a vida acadêmica mais leve e por sempre terem me prestado ajuda em qualquer dificuldade que eu apresentasse.

Agradeço também aos meus professores, que tanto investiram seu tempo em me ajudar com minhas dúvidas. Agradeço em especial ao professor Luiz Antonio Rodrigues, por me oferecer todo o suporte e confiança necessária nos projetos e neste trabalho que realizamos juntos.

*"Não sou corinthiano de coração
porque um dia ele para.
Sou corinthiano de alma
porque ela é eterna."
(Osmar Pereira Soares de Oliveira)*

Resumo

Redes sem fio de baixa potência e longo alcance têm sido empregadas na comunicação entre dispositivos para a solução de problemas relacionados a Internet das Coisas (IoT). Neste cenário, LoRaWAN têm sido uma opção bastante difundida, especialmente em ambientes de longa distância (WAN). O objetivo deste projeto é avaliar o funcionamento da tecnologia LoRa, a segurança na coleta de dados de sensores wireless e a sua aplicabilidade em soluções para Internet das Coisas para os ambientes internos e externos do campus da Unioeste – Cascavel. Como estudo de caso, serão utilizados sensores de umidade e temperatura. Para a avaliação da qualidade de comunicação, foi prototipado um ambiente que une um módulo Heltec ESP32 LoRa com um sensor de temperatura e umidade DHT11, e então foi implementado um software que controla este ambiente, à fim de realizar a coleta de dados com o sensor e o envio dos mesmos ao *gateway*, que por fim transmite estes dados para uma rede TTS (*The Things Stack*). Foram realizados diversos testes em duas localizações diferentes do campus, que possibilitaram verificar certos comportamentos relacionados à qualidade de comunicação na rede em tipos diferentes de ambientes, variando os parâmetros de *SF Spreading Factor* e *CR (Coding Rate)* para verificar a influência dos mesmos sobre a qualidade da comunicação. Como resultados, as melhores taxas de acerto no envio de mensagens foram obtidas utilizando $SF = 7$. Além disso, o valor do parâmetro CR não apresentou impactos sobre as taxas de envios com sucesso.

Palavras-chave: Internet das Coisas, IoT, Campus Inteligente, Segurança LoRa.

Lista de figuras

Figura 1 – Canais de envio e recebimento LoRa nos EUA e Brasil	15
Figura 2 – Arquitetura de comunicação LoRa	15
Figura 3 – Tela de cadastramento de aplicação na rede TTS	16
Figura 4 – Tela de monitoramento de um gateway cadastrado na rede TTS	17
Figura 5 – Diagrama de sequência do processo de <i>join</i> via OTAA	18
Figura 6 – Diagrama de sequência da ativação via ABP	19
Figura 7 – Módulo ESP32 LoRa SX1276 868/915Mhz com OLED (280,00 BRL)	20
Figura 8 – Sensor de Umidade e Temperatura DHT11 (15,00 BRL)	20
Figura 9 – Radioenge Gateway LoRaWAN	20
Figura 10 – Placa Raspberry Pi 3 (430,00 BRL)	20
Figura 11 – Protótipo montado usando o módulo ESP32 LoRa e o sensor DHT11 utilizando uma Protoboard de 1680 pontos	23
Figura 12 – Função <i>loop()</i> no código carregado para o módulo, é nesta seção de código onde as leituras de temperatura e umidade do ambiente são realizadas e exibidas no leitor OLED do módulo.	23
Figura 13 – Radioenge Gateway LoRaWAN e Raspberry Pi 3 anexados e criando um ambiente que possibilite a comunicação entre a fonte dos dados e seu local de armazenamento.	24
Figura 14 – Função <i>do_send()</i> no código carregado para o módulo, encarregada de montar o <i>payload</i> , organizando os dados as serem enviados em uma <i>array</i> de <i>bytes</i> e enviar os dados para o <i>gateway</i>	25
Figura 15 – Trecho do código fonte da biblioteca <i>lmic</i> onde se encontra o atributo que serve para modificar o valor do CR.	26
Figura 16 – Gráfico ilustrando o decaimento na taxa de acerto dos envios quando o SF é maior que 7.	29
Figura 17 – Gráfico mostrando a variação da razão entre sinal e ruído ao longo da execução dos testes.	29
Figura 18 – Gráfico ilustrando a variação da força do sinal ao longo da execução dos testes.	30
Figura 19 – Gráfico ilustrando o comportamento da taxa de acerto nos envios conforme se variam o SF e CR, para os testes feitos no bloco principal.	32
Figura 20 – Gráfico ilustrando o comportamento volátil da razão entre sinal e ruído para os testes feitos no bloco principal.	32
Figura 21 – Gráfico ilustrando a oscilação na força do sinal recebido para os testes feitos em sala.	33

Lista de tabelas

Tabela 1 – Taxas de acerto no envio e médias de SNR e RSSI variando os parâmetros de SF e CR no Laboratório de Redes de Computadores	28
Tabela 2 – Taxas de acerto no envio e médias de SNR e RSSI variando os parâmetros de SF e CR em uma sala de aula do bloco principal do campus	31

Lista de abreviaturas e siglas

ABP	<i>Activation by Personalization</i>
CR	<i>Coding Rate</i>
dB	<i>Decibéis</i>
dBm	<i>Decibéis por Miliwatt</i>
EUI	<i>Extended Unique Identifier</i>
IoT	<i>Internet of Things</i>
LPWAN	<i>Low Power Wide Area Network</i>
OTAA	<i>Over-The-Air Activation</i>
RSSI	<i>Received Signal Strength Indicator</i>
SF	<i>Spreading Factor</i>
SNR	<i>Signal-To-Noise Ratio</i>
TTS	<i>The Things Stack</i>
WAN	<i>Wide Area Network</i>

Sumário

1	Introdução	11
1.1	Objetivos	12
1.2	Metodologia	13
2	Levantamento Bibliográfico	14
2.1	A rede LoRa e suas especificações	14
2.2	A rede TTS (<i>The Things Stack</i>)	15
2.3	A Segurança em Redes LoRaWAN	17
2.3.1	Segurança do protocolo LoRaWAN na rede TTS	17
2.4	Componentes Eletrônicos para IoT	19
2.5	Bibliotecas Utilizadas	21
3	Resultados	22
3.1	Prototipação	22
3.2	Descrição dos Testes	27
3.3	Resultados dos Testes	27
4	Conclusões	35
	Referências	37

1

Introdução

Redes sem fio de baixa potência e longo alcance têm sido empregadas entre dispositivos para a comunicação relacionada a Internet das Coisas (IoT). O crescimento na demanda desse tipo de tecnologia tem movimentado o mercado e também as empresas de desenvolvimento.

Desenvolvida pela Semtech, a tecnologia LoRa vem se destacando neste mercado, principalmente pelo seu baixo custo em relação às demais opções de mercado. Esta tecnologia se caracteriza pelo uso de comunicações sem fio de longo alcance com baixo consumo de energia (SEMTECH, 2022).

Essencial também para entender a tecnologia LoRa (camada física) é conhecer e compreender o funcionamento do protocolo que a mesma utiliza em suas comunicações: o protocolo LoRaWAN (camada de enlace/rede). LoRaWAN dita como funciona a comunicação entre dispositivos conectados através de uma rede LoRa e define a arquitetura da rede, influenciando diretamente em diversos fatores, como tempo de vida de um nó, capacidade da rede, qualidade do serviço, segurança e variedade de aplicações.

Nas comunicações usando LoRa, existem diversos fatores e parâmetros que influenciam na qualidade da transmissão e recepção de dados, dentre uma variedade de parâmetros, pode-se destacar o *Spreading Factor*, ou Fator de Espalhamento, e o *Coding Rate*, ou Taxa de Codificação. O primeiro determina a velocidade de um *chirp* (sinal cuja frequência oscila com o tempo), sendo determinante no alcance e na duração deste tipo de sinal. A velocidade de um *chirp* é aproximadamente igual à 2^{SF} , onde um *chirp* com maior velocidade apresenta mais mudanças de frequências do que um *chirp* mais lento (MACHINEQ, 2021). A Taxa de Codificação define a taxa de correção antecipada de erros, que provê proteção contra interferências aos pacotes transmitidos. Um maior CR implica em uma proteção melhor, ao custo de velocidade de transmissão, aumentando o tempo no ar dos pacotes (SOLAGNA et al., 2020).

Em redes de computadores, em cenários de conexões sem fio, existem diversos parâmetros que auxiliam na hora de verificar a qualidade de uma conexão. Os valores de SNR são a medida

da força do sinal desejado em relação ao ruído (sinal indesejado) e são medidos em decibéis (dB). O valor de SNR pode ser um valor positivo, um valor negativo ou até mesmo 0, sendo que quanto maior o valor, melhor é a qualidade do sinal (SHELDON; BURKE, 2021). O parâmetro RSSI é um indicador da força do sinal recebido, esse valor serve para determinar se o sinal recebido é forte o suficiente para estabelecer uma boa conexão com o transmissor. O valor do RSSI é medido em decibéis por miliwatt (dBm) e é um número negativo, quanto mais próximo de 0, mais forte é o sinal recebido (NETWORK, 2022).

As redes com LoRa têm sido empregadas em cada vez mais projetos, e ao pensar nessa tecnologia, é comum associá-la a soluções industriais e para o agronegócio, como monitoramento de armazéns ou de campos de colheita. Porém as redes LoRa se mostram muito eficientes em diversos outros cenários como monitoramento de ambientes internos e até informatização em esportes. Isto apenas torna a tecnologia ainda mais atrativa por ilustrar que a mesma não fica restrita a um nicho específico de problemas (FAINO, 2021).

Por ser uma tecnologia em constante crescimento e que ainda não se conhece todo o potencial de soluções, a LoRa se torna um objeto de estudo muito interessante a se abordar e exatamente por este motivo foi escolhida como tema central deste trabalho.

1.1 Objetivos

O objetivo geral do projeto é avaliar a qualidade de comunicação e fazer um levantamento das técnicas de segurança de dispositivos IoT que utilizam LoRa em ambientes internos e externos do campus da UNIOESTE-Cascavel utilizando sensores de umidade e temperatura como estudo de caso.

Como objetivos específicos, destacam-se:

- Fazer uma revisão de literatura sobre a tecnologia LoRa e suas características de comunicação e segurança
- Construir um protótipo usando um transmissor acoplado a um sensor de umidade e temperatura e um transmissor LoRa
- Verificar os níveis de segurança disponíveis na arquitetura LoRaWAN utilizada
- Avaliar o alcance da comunicação sem fio em ambientes internos e externos do campus variando os parâmetros de *Spreading Factor* e *Coding Rate* nos canais de comunicação
- Avaliar a qualidade da comunicação em termos de erros de transmissão dos dados enviados pelos sensores de umidade e temperatura

1.2 Metodologia

A partir de pesquisa bibliográfica foram definidos os módulos de processamento e comunicação mais adequados ao objetivo do monitoramento de umidade e temperatura para os ambientes internos e externos da Unioeste, campus de Cascavel. Um protótipo foi construído e testado em diferentes posições no campus, variando-se os parâmetros de comunicação do canal (SF e CR). Os resultados foram comparados considerando-se as taxas de envio e de erros de transmissão. Os dispositivos utilizados (placas, sensores, resistores, placas de prototipação) estavam disponíveis no LRC - Laboratório de Redes de Computadores do curso de Ciência da Computação.

O gateway utilizado ficou posicionado no LRC no bloco F do campus. A avaliação da qualidade de comunicação foi medida verificando a quantidade de mensagens enviadas com sucesso de um total de 100 envios. Para isso, foi verificado na rede TTS quantos pacotes foram recebidos ao fim de cada centena de envios. Foram avaliadas todas as combinações possíveis entre os parâmetros SF e CR, em duas localidades diferentes: no próprio Laboratório de Redes de Computadores (aproximadamente 6 metros de distância do *gateway*) e em uma sala de aula no bloco principal (aproximadamente 81 metros de distância do *gateway*), seriam executados também testes a partir da Biblioteca do campus (aproximadamente 180 metros de distância do *gateway*), porém a localização interna da antena e a grande quantidade de obstáculos no trajeto entre o ambiente de coleta e transmissão de dados e o *gateway* fizeram com que não fosse possível estabelecer uma conexão nesta localização. Foram levantadas as técnicas de segurança disponibilizadas pelo protocolo LoRaWAN. Após executados os testes, foram montadas tabelas e gráficos para apresentar e ilustrar o comportamento dos resultados.

2

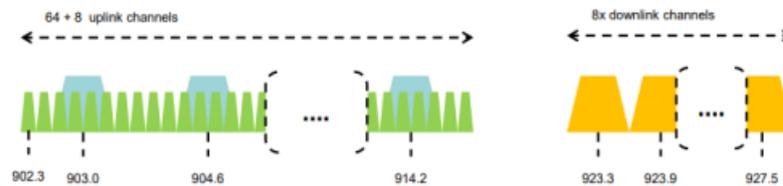
Levantamento Bibliográfico

Este Capítulo consiste de uma breve apresentação da rede LoRa e algumas de suas especificações (Seção 2.1). Em seguida, será apresentada a rede TTN, explicando seus conceitos e como um usuário pode utilizá-la de forma simples (Seção 2.2). O próximo passo consiste numa introdução ao funcionamento da segurança de uma rede LoRa (Seção 2.3), com uma aprofundamento nos aspectos da segurança do protocolo LoRaWAN em uma rede TTN (Subseção 2.3.1). Em sequência serão introduzidos os componentes eletrônicos que serão usados ao longo do desenvolvimento do ambiente de monitoramento de umidade e temperatura (Seção 2.4). Por fim, serão descritas as bibliotecas utilizadas na implementação do software que controlará o módulo ESP32 LoRa (Seção 2.5).

2.1 A rede LoRa e suas especificações

LoRa (Long Range, ou Longo Alcance, em português) é uma tecnologia que utiliza rádio frequência para a transmissão de dados a longas distâncias, podendo alcançar algumas dezenas de quilômetros em ambiente externo, e com baixo custo de energia (BARDYN et al., 2016). Para esta transmissão via rádio frequência, uma rede LoRa utiliza uma técnica chamada “Chirp Spread Spectrum” (CSS), que tem a capacidade de impedir que interferências atrapalhem a comunicação (ALLIANCE, 2015). Esse tipo de técnica tem como vantagem o seu longo alcance, mas fornece baixas taxas de transmissão e alta latência quanto a capacidade de comunicação entre um grande número de dispositivos do mesmo tipo. A largura de banda dos canais de comunicação pode ser de 125 kHz, 250 kHz ou 512 kHz, e é impactada por um parâmetro denominado fator de espalhamento espectral (SF - *Spreading Factor*), que pode variar entre 7 a 12, e pelo parâmetro CR (*Coding Rate*), que varia de 0 a 4 (ALLIANCE, 2015). Para as Américas, a faixa de frequência de operação da rede LoRa vai de 902 MHz a 928 MHz, dividida em canais de envio (*uplink*) e recebimento (*downlink*), conforme a Figura 1.

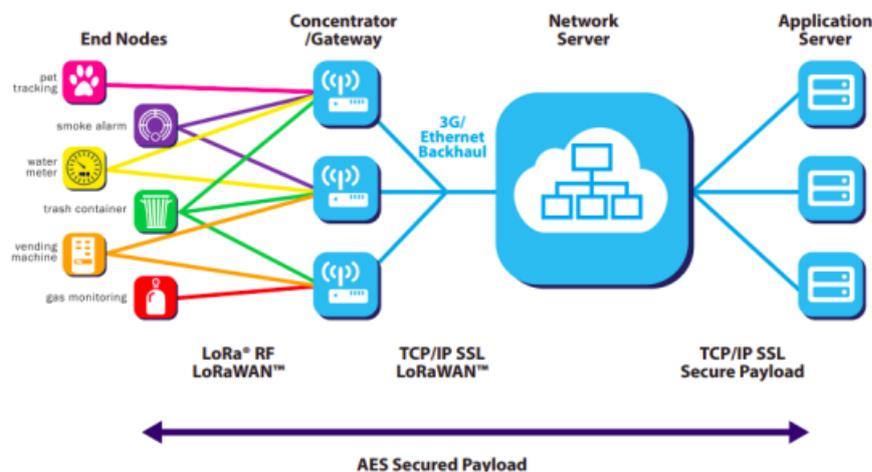
Figura 1 – Canais de envio e recebimento LoRa nos EUA e Brasil



Fonte: LoRa Alliance (2015)

Para a comunicação entre dispositivos que utilizam LoRa, é empregado o protocolo LoRaWAN, que apresenta uma topologia estrela que inclui dispositivos finais (*end-nodes*, geralmente sensores), concentradores (*gateways*) e servidores de aplicação, onde um servidor pode estar conectado a múltiplos *gateways*, que por sua vez estão conectados a múltiplos dispositivos finais Figura 2.

Figura 2 – Arquitetura de comunicação LoRa



Fonte: LoRa Alliance (2015)

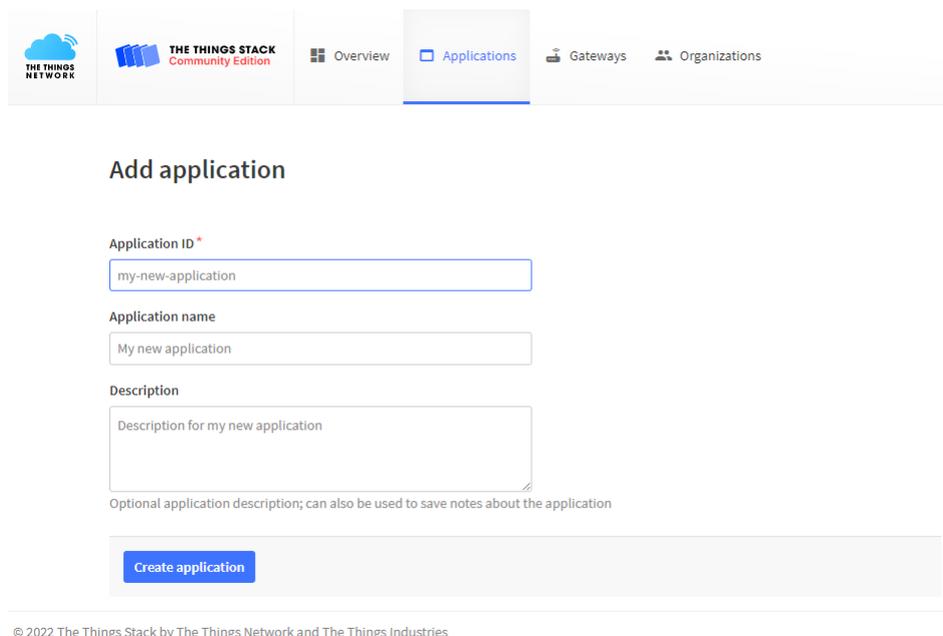
2.2 A rede TTS (*The Things Stack*)

A The Things Stack (TTS) é uma solução colaborativa para *Network Server* que possibilita a comunicação dos gateways com o Servidor de Aplicação. A TTS é uma rede baseada em servidores na nuvem que estabelecem conexão entre diversos gateways LoRaWAN ao redor do planeta. Esta rede adota o protocolo LoRaWAN com objetivo de oferecer uma cobertura mais ampla, o que a caracteriza como uma WAN (*Wide Area Network*). Além disso, como se caracteriza também pelo baixo consumo de energia, a rede TTS é mais do que apenas uma WAN, mas uma LPWAN (*Low Power Wide Area Network*). Mas não apenas isso destaca a rede TTS: Ela também é uma rede *open source* e colaborativa, o que permite que qualquer usuário possa contribuir apenas instalando um gateway em sua residência. Com um gateway cadastrado no

console de usuário da rede TTS, é possível monitorar a comunicação entre os dispositivos e o servidor, assim como configurá-lo ou deletá-lo.

Para cadastrar um gateway ou uma aplicação na rede TTS, primeiramente é necessário ter um cadastro pessoal na plataforma TTS, o que pode ser feito facilmente acessando o endereço <<https://www.thethingsnetwork.org>> e clicando na opção *Sign Up* e preenchendo os campos requisitados, e então com o cadastro finalizado e o usuário logado, clicar em cima do nome de usuário no canto superior direito da tela e selecionar a opção *Console*. Será aberta uma página com um globo e algumas opções, onde será escolhido em qual *cluster* da rede será adicionado o dispositivo ou aplicação. A partir daí, podemos ver os dispositivos e aplicações já registradas pelo usuário naquele *cluster*, para cadastrar um novo é necessário apenas selecionar a aba de aplicação ou de gateways, de acordo com o que se desejar registrar, preencher os campos requisitados e finalizar o processo selecionando a opção *Create gateway/application*. A Figura 3 mostra a tela de cadastramento de uma aplicação no cluster australiano da rede TTS.

Figura 3 – Tela de cadastramento de aplicação na rede TTS

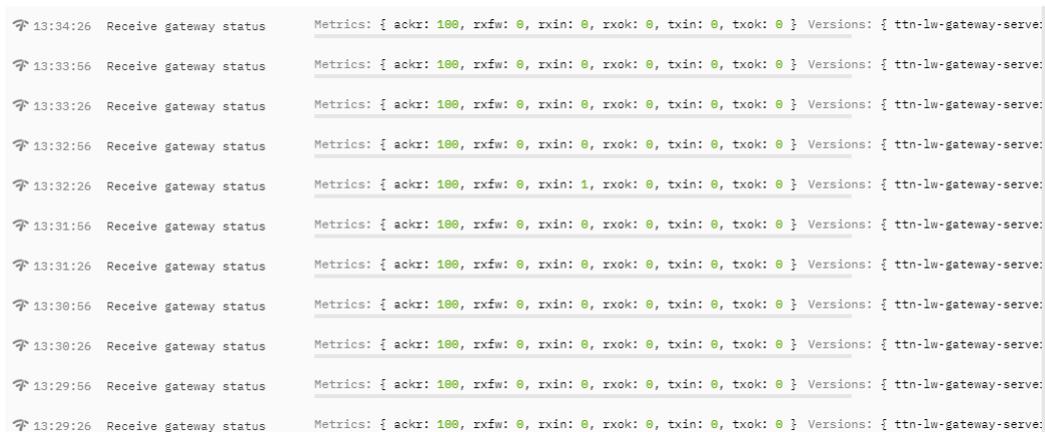


The screenshot displays the 'Add application' interface in the TTS console. At the top, there is a navigation bar with the following items: 'THE THINGS NETWORK' logo, 'THE THINGS STACK Community Edition', 'Overview', 'Applications' (highlighted with a blue underline), 'Gateways', and 'Organizations'. Below the navigation bar, the main heading is 'Add application'. The form contains three input fields: 'Application ID*' with the value 'my-new-application', 'Application name' with the value 'My new application', and 'Description' with the value 'Description for my new application'. Below the description field, there is a small note: 'Optional application description; can also be used to save notes about the application'. At the bottom of the form, there is a blue button labeled 'Create application'. The footer of the page reads '© 2022 The Things Stack by The Things Network and The Things Industries'.

Fonte: <https://au1.cloud.thethings.network/console/applications/add>

Com as suas aplicações e gateways cadastrados, é possível monitorar as atividades recentes deles usando o *Console* de usuário da rede TTS. Na Figura 4 vemos o monitoramento das atividades do gateway que foi usado no desenvolvimento deste trabalho.

Figura 4 – Tela de monitoramento de um gateway cadastrado na rede TTS



🔔 13:34:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:33:56	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:33:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:32:56	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:32:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 1, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:31:56	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:31:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:30:56	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:30:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:29:56	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:
🔔 13:29:26	Receive gateway status	Metrics: { ackr: 100, rxfw: 0, rxin: 0, rxok: 0, txin: 0, txok: 0 } Versions: { ttn-lw-gateway-serve:

Fonte: <https://au1.cloud.thethings.network/console/>

2.3 A Segurança em Redes LoRaWAN

A segurança de uma rede LoRaWAN possui dois fatores chave, sendo eles do procedimento de ingresso na rede e a autenticação de mensagem. O procedimento de ingresso faz uma autenticação mútua entre o dispositivo e a rede LoRa à qual o dispositivo esteja conectado. Apenas dispositivos autorizados tem permissão para ingressar na rede. As mensagens de MAC LoRaWAN e de aplicações possuem autenticação de origem, proteção de integridade e criptografia ponta a ponta. Esse sistema de segurança garante que:

- O tráfego da rede não tenha sido alterado
- Apenas dispositivos autorizados estejam conectados à rede
- O tráfego da rede não seja ouvido (não há *eavesdropping*)
- O tráfego da rede não seja capturado e reproduzido (ataques de reprodução)

2.3.1 Segurança do protocolo LoRaWAN na rede TTS

O principal mecanismo de segurança dentro das redes TTS consiste na troca de chaves de segurança. O protocolo LoRaWAN 1.0 especifica algumas chaves de segurança, sendo elas *NwkSKey*, *AppSKey* e *AppKey*, todas tendo comprimento de 128 bits. O algoritmo usado neste processo é o AES-128, que se assemelha ao algoritmo usado pelo padrão 802.15.4 (NETWORK, 2021). Quando um dispositivo se conecta à rede, são geradas duas chaves, uma para a sessão da aplicação (*AppSKey*) e outra para a sessão da rede (*NwkSKey*). Ambas as chaves serão usadas apenas enquanto durar a conexão, sendo que a primeira mantém-se privada enquanto a segunda é compartilhada com a rede. Estas duas chaves são únicas para cada dispositivo e para cada sessão.

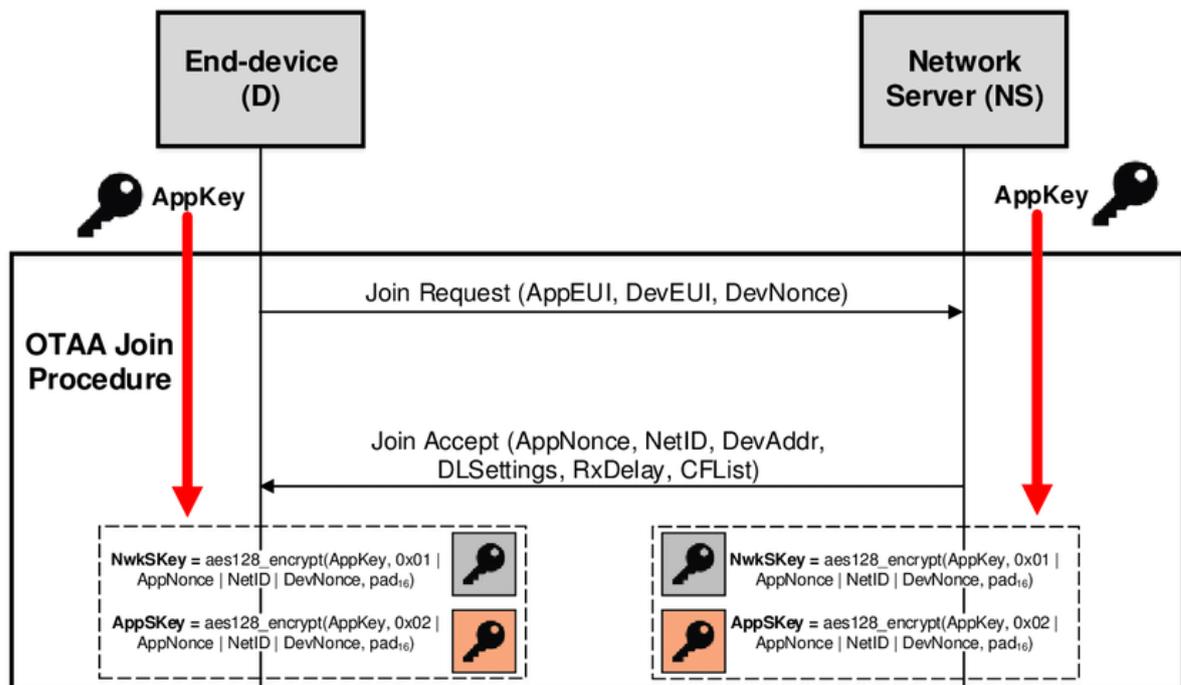
A *NwksKey* é usada na interação entre o nó e o servidor de rede. Esta chave é responsável pela validação da integridade de cada mensagem, realizada pelo seu *Message Integrity Code*, que se assemelha a um *checksum*, porém com algumas verificações adicionais.

Já a *AppSKey* é encarregada de criptografar e descriptografar os pacotes de dados que trafegam entre a aplicação e a rede, os quais são completamente criptografados entre o nó e o servidor TTS. Ou seja, ninguém além de quem envia os dados é capaz de lê-los, pois como já mencionado, esta chave é mantida privada.

Por fim, a *AppKey* é conhecida apenas pelo dispositivo e pela aplicação. Dispositivos que são ativados dinamicamente utilizam a *AppKey* para gerar as duas chaves de sessão durante o processo de ativação.

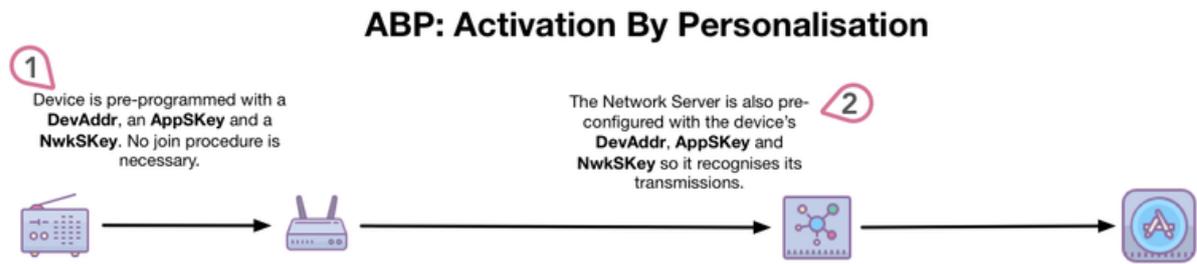
O protocolo LoRaWAN oferece dois tipos de ativação: a *Over-The-Air Activation* e a *Activation by Personalization*. Na ativação OTAA (Figura 5), o dispositivo recebe uma EUI do dispositivo, uma EUI da aplicação e uma *AppKey*, que é usada para gerar as duas chaves *AppSKey* e *NwksKey*. Para que o dispositivo se conecte, ele deve enviar uma solicitação de *join*, e utilizar a resposta da solicitação para derivar as duas chaves. A ativação ABP não requer as EUIs de dispositivo e aplicação e também a *AppKey*, uma vez que as chaves *AppSKey* e *NwksKey* são programadas diretamente no dispositivo, o qual já foi previamente registrado na rede. O procedimento é ilustrado na Figura 5.

Figura 5 – Diagrama de sequência do processo de *join* via OTAA



Fonte: https://www.researchgate.net/figure/Overview-of-the-OTAA-join-procedure_fig1325570245

Figura 6 – Diagrama de sequência da ativação via ABP



Fonte: <https://www.robocore.net/tutoriais/lorawan-conceitos-basicos>

2.4 Componentes Eletrônicos para IoT

Existe hoje uma enorme variedade de dispositivos que suportam a tecnologia LoRa, desde módulos programáveis até sensores e gateway, e dentre essa vasta biblioteca de itens, foram escolhidos três em específico para a criação do protótipo que foi usado ao longo do desenvolvimento deste projeto. O módulo programável Heltec WiFi Lora 32 Figura 7 é equipado com um chip ESP32 e foi usado para obter e transmitir os dados obtidos para um gateway conectado a um servidor TTN. Um Sensor DHT11 Figura 8 foi utilizado para a obtenção dos dados de temperatura e umidade do ambiente, este estará conectado com o módulo ESP32 LoRa, para que os dados obtidos pelo sensor possam ser transmitidos para o gateway e conseqüentemente para o servidor TTN. Por fim, o gateway escolhido foi o modelo Radioenge Gateway LoRaWAN Figura 9, que foi integrado com uma placa Raspberry Pi 3 Figura 10, estes dois dispositivos ficarão encarregados de estabelecer a comunicação entre o protótipo contendo o módulo ESP32 LoRa e sensor DHT11 e o servidor TTN, recebendo os dados obtidos pelo primeiro e transmitindo para o segundo (CAMARGO et al., 2021).

Figura 7 – Módulo ESP32 LoRa SX1276 868/915Mhz com OLED (280,00 BRL)



Fonte: www.filipeflop.com

Figura 9 – Radioenge Gateway LoRaWAN



Fonte:
<https://www.radioenge.com.br/produto/gateway-lorawan/>

Figura 8 – Sensor de Umidade e Temperatura DHT11 (15,00 BRL)



Fonte: www.filipeflop.com

Figura 10 – Placa Raspberry Pi 3 (430,00 BRL)



Fonte: www.filipeflop.com

2.5 Bibliotecas Utilizadas

Para o desenvolvimento do software que faz a leitura dos dados e a comunicação entre o módulo ESP32 e o *gateway*, foi utilizada uma série de bibliotecas:

- *DHT sensor library by Adafruit* (versão 1.3.4): inclui funções de leitura de temperatura e umidade do sensor DHT11;
- *MCCI LoRaWAN LMIC library by Terry Moore* (versão 4.1.1): provê implementações das Classes A e B de dispositivos compatíveis com o protocolo LoRaWAN, com suporte para as faixas EU-868, US-915, AU-921, AS-923 e IN-866;
- *Heltec ESP32 Dev-Boards by HelTec* (versão 1.1.0): fornece o material necessário para programar a placa Heltec ESP32;
- *Arduino Built-In library*: biblioteca padrão do Arduino, fornece as funções básicas da linguagem.

3

Resultados

Neste capítulo será abordado o estágio de prototipação, com explicações do processo de montagem do protótipo e da implementação do software que controlará o ambiente criado, juntamente com imagens que ilustram parte do processo de desenvolvimento desta etapa do trabalho (Seção 3.1). Em seguida, será apresentada uma descrição dos testes que foram realizados, explicando quais parâmetros foram levados em consideração para a avaliação da comunicação (Seção 3.2). Por fim, foram apresentados os resultados obtidos, utilizando também tabelas e gráficos para ilustrar melhor o comportamento da comunicação em cada cenário de teste (Seção 3.3).

3.1 Prototipação

A fase de prototipação foi realizada usando os dispositivos anteriormente citados, em conjunto com uma Protoboard de 1680 pontos, usada para conectar a placa ESP32 LoRa ao sensor DHT11 e realizar a coleta dos dados, como mostrado na Figura 11.

Com o protótipo devidamente montado, o próximo passo foi iniciar a implementação do software que seria carregado no módulo ESP32 LoRa e controlaria o funcionamento do protótipo, que até esta fase consiste em configurar a obtenção dos dados de temperatura e umidade do sensor DHT11 e exibi-los no leitor OLED presente no módulo LoRa. Esta implementação foi feita na linguagem Arduino, que é compatível com o módulo utilizado e dispõe de uma grande biblioteca de materiais de estudo, o que facilitou o aprendizado da linguagem. A Figura 12 exemplifica uma parte do código que foi carregado no módulo, esta função *loop()* é executada em um laço indeterminadas vezes, até que a alimentação do módulo seja desligada ou que seja feita algum novo carregamento de código para a placa, na função mostrada, são executados os passos que realizam as coletas e exibição dos dados do ambiente.

Figura 11 – Protótipo montado usando o módulo ESP32 LoRa e o sensor DHT11 utilizando uma Protoboard de 1680 pontos

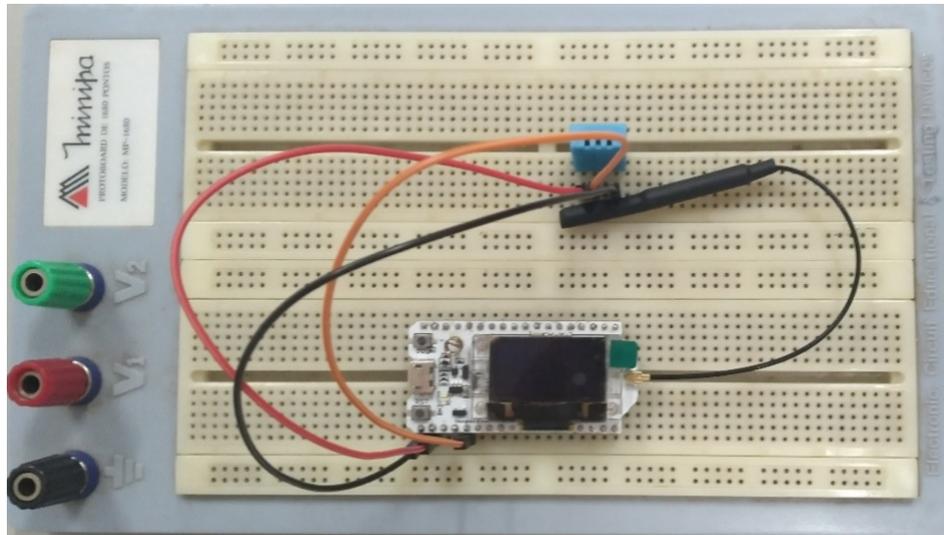


Figura 12 – Função `loop()` no código carregado para o módulo, é nesta seção de código onde as leituras de temperatura e umidade do ambiente são realizadas e exibidas no leitor OLED do módulo.

```
void loop() {
    Heltec.display->drawString(0,0,"Dados: \n");
    float h = dht.readHumidity();
    float t = dht.readTemperature();

    String humMessage = "Umidade : ";
    String temMessage = "Temperatura: ";

    humMessage.concat(h);
    temMessage.concat(t);
    humMessage.concat("%");
    temMessage.concat("°C");
    Heltec.display->drawString(0,10,humMessage);
    Heltec.display->drawString(0,20,temMessage);
    Heltec.display->display();
    Serial.println("Ok");
    delay(3000);
    Heltec.display->clear();
}
```

O gateway LoRaWAN e a placa Raspberry Pi 3 foram montados juntos para que, além de poder receber os dados através do Gateway, também seja possível transmiti-los para o servidor TTS, usando a Raspberry Pi. Essa integração permite que seja estabelecida a ponte entre a coleta de dados e o local onde os mesmos foram armazenados. A Figura 13 mostra como ficou o ambiente formado pelo anexo do gateway com a placa Raspberry.

Figura 13 – Radioenge Gateway LoRaWAN e Raspberry Pi 3 anexados e criando um ambiente que possibilite a comunicação entre a fonte dos dados e seu local de armazenamento.



A última etapa da prototipação consistiu da implementação da comunicação entre o módulo LoRa ESP32 e o *gateway*. Neste passo, foi implementada a função *do_send()*, que é encarregada de criar um *payload* de *bytes*, onde são alojados os dados coletados e um contador de tentativas de envios, cada dado alocado em um *byte* deste *payload*, e em seguida realizando o envio. É dentro desta função também que é chamada a função *LMIC_setDrTxpow()*, usada para definir o valor do SF do envio a ser realizado. Esta função recebe 2 parâmetros, sendo o primeiro usado para alterar o valor do SF, e o segundo teoricamente deveria alterar a potência de transmissão, porém internamente no código este segundo parâmetro não altera realmente valor da potência de transmissão, portanto a função serve apenas para realizar a alteração do SF.

Figura 14 – Função *do_send()* no código carregado para o módulo, encarregada de montar o *payload*, organizando os dados as serem enviados em uma *array* de *bytes* e enviar os dados para o *gateway*.

```
void do_send(osjob_t *j)
{
    // Check if there is not a current TX/RX job running
    if (LMIC.opmode & OP_TXRXPEND)
    {
        Serial.println(F("OP_TXRXPEND, not sending"));
    }
    else
    {
        // Codificação da mensagem em bytes, dividindo um inteiro em 2 bytes
        payload[0] = highByte(mydata);
        payload[1] = lowByte(mydata);
        payload[2] = highByte(tempIntPart);
        payload[3] = lowByte(tempIntPart);
        payload[4] = highByte(tempDecPart);
        payload[5] = lowByte(tempDecPart);
        payload[6] = highByte(humIntPart);
        payload[7] = lowByte(humIntPart);
        payload[8] = highByte(humDecPart);
        payload[9] = lowByte(humDecPart);

        // Prepare upstream data transmission at the next possible time.
        LMIC_setDrTxpow(DR_SF11, 14);
        LMIC_setTxData2(1, payload, sizeof(payload), 0);
        Serial.println("Packet queued " + String(mydata));
    }
    // Next TX is scheduled after TX_COMPLETE event.
}
```

A variação dos parâmetros SF e CR são feitas em locais diferentes do código. O primeiro é modificado logo antes do envio, como mostrado acima na Figura 14. Já para alterar o valor do CR, é necessário modificar o arquivo fonte da biblioteca LMIC, portanto é necessário abrir o arquivo *lmic.c* e modificar o atributo *LMIC.errcr*, alternando o valor entre *CR_4_5*, *CR_4_6*, *CR_4_7* e *CR_4_8* para definir o valor do parâmetro CR, como mostrado na Figura 15

Figura 15 – Trecho do código fonte da biblioteca *lmic* onde se encontra o atributo que serve para modificar o valor do CR.

```
C lmic.c X
C: > Users > willi.DESKTOP-REK1S4P > Documents > Arduino > libraries > MCCI_LoRaWAN_LMIC
2770         e_.info = EV_RESET));
2771     os_radio(RADIO_RST);
2772     os_clearCallback(&LMIC.osjob);
2773
2774     // save callback info, clear LMIC, restore.
2775     do {
2776         lmic_client_data_t client = LMIC.client;
2777
2778         os_clearMem((xref2u1_t)&LMIC,SIZEOFEXPR(LMIC));
2779
2780         LMIC.client = client;
2781     } while (0);
2782
2783     // LMIC.devaddr = 0; // true from os_clearMem().
2784     LMIC.devNonce = os_getRndU2();
2785     LMIC.opmode = OP_NONE;
2786     LMIC.errcr = CR_4_8;
2787     LMIC.adrEnabled = FCT_ADREN;
2788     resetJoinParams();
2789     LMIC.rxDelay = DELAY_DNW1;
```

3.2 Descrição dos Testes

Os testes consistem no envio de 100 mensagens para o *gateway*, cada mensagem contendo os dados de umidade e temperatura da leitura em questão e um contador exibindo o número da tentativa do envio da mensagem em questão. Entre cada tentativa de envio, foi definido um intervalo de 5 segundos.

Para os testes, foram realizadas combinações entre 2 parâmetros *in code* e 1 parâmetro geográfico, sendo os parâmetros de SF e CR, que resumidamente afetam a velocidade e alcance do envio, e a proteção contra interferência dos pacotes, ao custo de velocidade de envio. O parâmetro geográfico foi a localização do módulo de obtenção de dados, sendo posicionado no Laboratório de Redes de Computadores, com uma distância aproximada de 6 metros do *gateway*, e em sala de aula no bloco principal, há aproximadamente 81 metros de distância do *gateway*.

As variações foram feitas da seguinte maneira:

- SF = {7, 8, 9, 10, 11, 12}
- CR = $\{\frac{4}{5}, \frac{4}{6}, \frac{4}{7}, \frac{4}{8}\}$
- Localização = Laboratório de Redes de Computadores, Sala de Aula

totalizando 48 testes no total, sendo 24 em cada localização e 4 testes para cada um dos 6 valores de SF, variando o valor de CR em cada caso.

3.3 Resultados dos Testes

Após realizados todos os testes, foram montadas tabelas exibindo os resultados de cada caso de teste para melhor visualização dos mesmos.

Os primeiros testes foram realizados no Laboratório de Redes de Computadores, no Bloco F do campus da Unioeste. Nessa localização, a distância entre o módulo ESP32 e o *gateway* é de aproximadamente 6 metros, portanto esses testes servirão como parâmetro para avaliar a qualidade de uma conexão *indoor* utilizando LoRa.

Os testes no Laboratório de Redes de Computadores apresentaram resultados (apresentados na Tabela 1) que indicam que, para comunicações de curto alcance, o ideal é utilizar o SF igual a 7, obtendo taxas de sucesso no envio sempre acima de 90%, independentemente do valor do CR utilizado. Neste cenário, notamos que aumentar o valor do SF diminui drasticamente a porcentagem de envios com sucesso, não ultrapassando os 53% de taxa de acerto quando o valor do SF é maior do que 7, como mostrado na Figura 16, isso ocorre pelo aumento na oscilação da frequência de um *chirp* decorrente do aumento da sua velocidade ao elevar o SF.

Tabela 1 – Taxas de acerto no envio e médias de SNR e RSSI variando os parâmetros de SF e CR no Laboratório de Redes de Computadores

Local	SF	CR	Taxa de envios com sucesso (%)	Média SNR (10 envios)	Média RSSI (10 envios)
Laboratório	7	4/5	93	8,87	-51,14
		4/6	92	9,29	-53,86
		4/7	92	9,06	-51,5
		4/8	92	9,20	-52,38
	8	4/5	53	10,72	-54
		4/6	51	10,65	-52,8
		4/7	51	11,76	-51,5
		4/8	50	11,04	-50,5
	9	4/5	48	12,07	-53,2
		4/6	49	12,05	-56,4
		4/7	49	12,76	-53,1
		4/8	49	12,81	-79,9
	10	4/5	49	10,83	-70,1
		4/6	49	10,5	-65,6
		4/7	49	11,7	-57,9
		4/8	49	10,97	-56
	11	4/5	49	10,96	-53,8
		4/6	45	11,87	-58,6
		4/7	48	11,54	-55,4
		4/8	49	11,26	-53,3
	12	4/5	49	10,01	-59,6
		4/6	50	9,10	-65
		4/7	49	9,63	-60,8
		4/8	49	10,22	-60,3

Observando as médias de SNR de todos os testes, podemos afirmar que mesmo com alguns momentos em que a razão entre sinal e ruído é maior, as taxas de envio não aumentam ou diminuem com base nesse parâmetro, isso é ilustrado na Figura 17. Em relação ao RSSI, podemos observar que não há grandes variações ditadas pelos valores do SF e CR, havendo sim um pico em certo momento, porém que logo se estabiliza novamente, com podemos observar na Figura 18.

Figura 16 – Gráfico ilustrando o decaimento na taxa de acerto dos envios quando o SF é maior que 7.

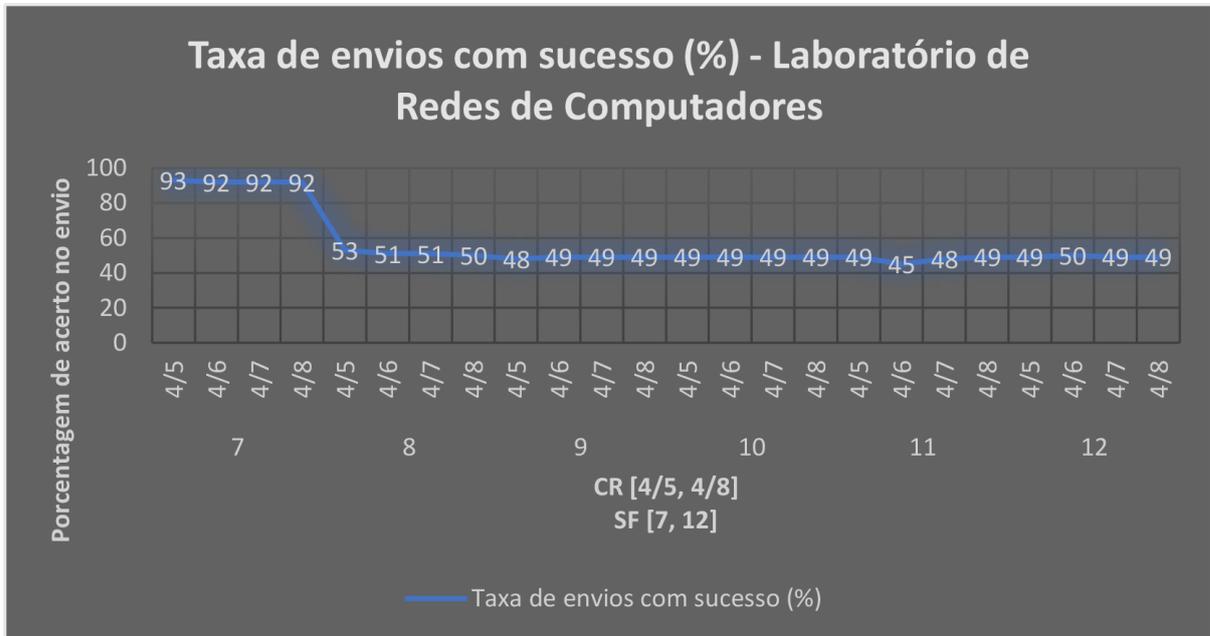


Figura 17 – Gráfico mostrando a variação da razão entre sinal e ruído ao longo da execução dos testes.

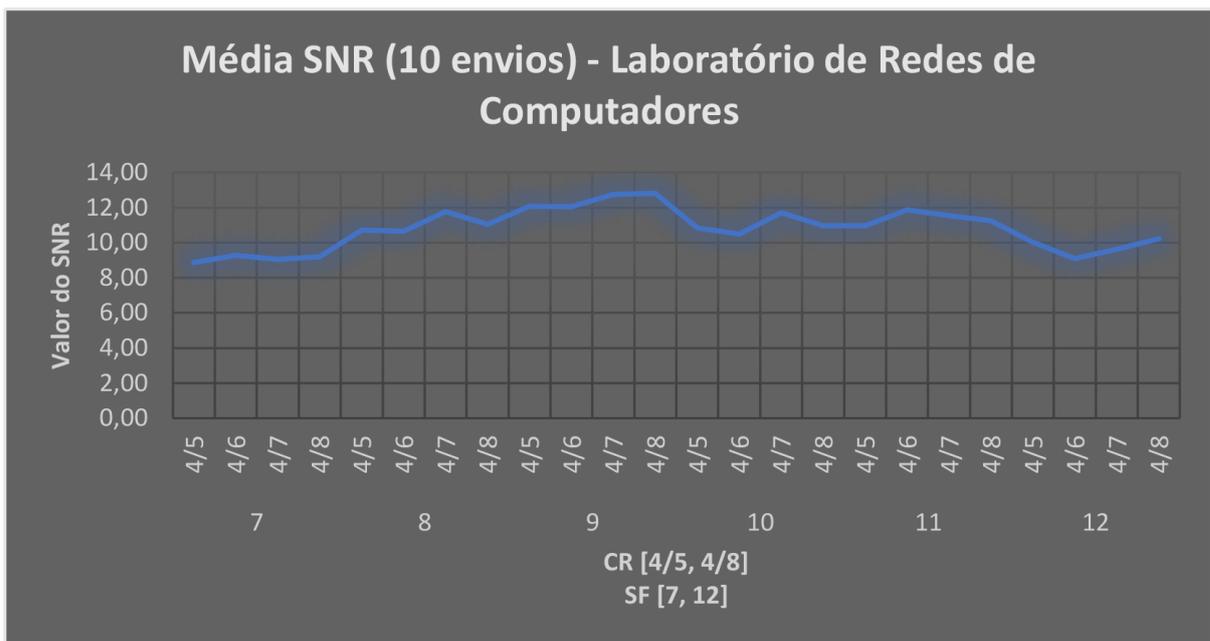
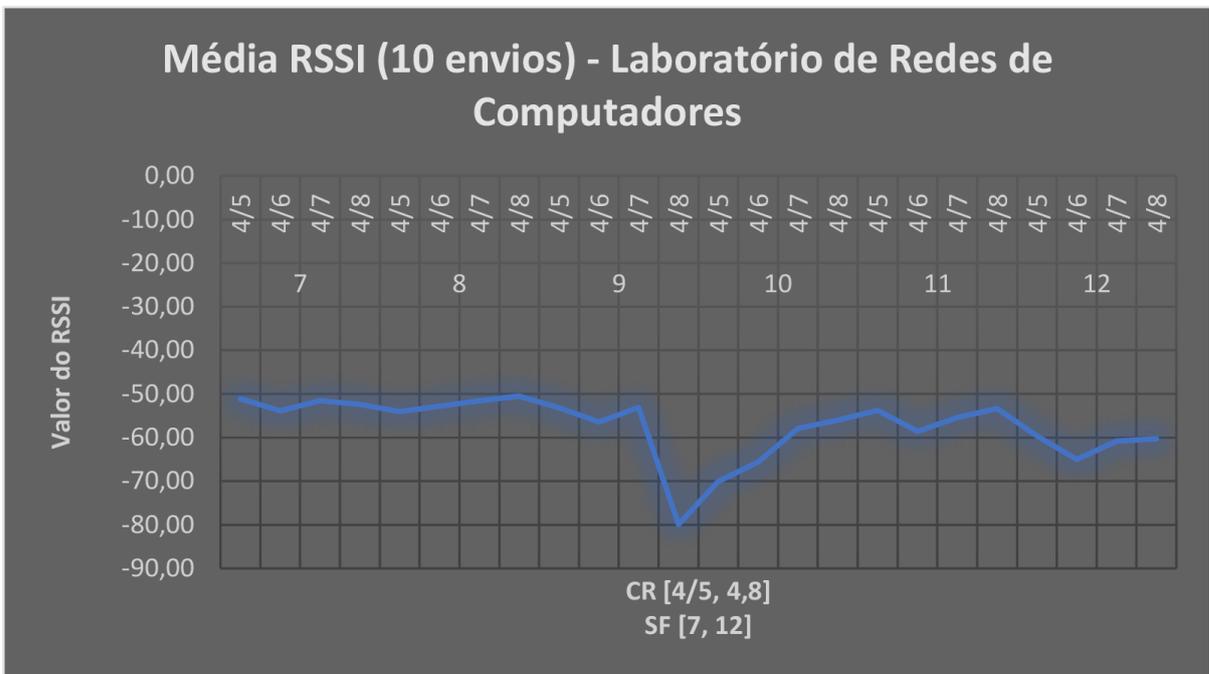


Figura 18 – Gráfico ilustrando a variação da força do sinal ao longo da execução dos testes.



A outra etapa dos testes foi realizada em uma sala de aula localizada no bloco principal de aulas do campus, onde a distância para o *gateway* é de aproximadamente 81 metros, havendo diversos obstáculos no caminho, como paredes de concreto e janelas.

Os resultados, compilados na Tabela 2, mostraram um comportamento diferente dos obtidos nos testes realizados no laboratório, sendo possível obter taxas razoáveis de transmissão com alguns valores de SF maiores que 7.

Tabela 2 – Taxas de acerto no envio e médias de SNR e RRSI variando os parâmetros de SF e CR em uma sala de aula do bloco principal do campus

Local	SF	CR	Taxa de envios com sucesso (%)	Média SNR (10 envios)	Média RRSI (10 envios)
Sala de Aula	7	4/5	92	-4,38	-117,90
		4/6	98	-0,49	-114,40
		4/7	99	1,42	-113,8
		4/8	99	-1,64	-115,20
	8	4/5	92	-1,8	-116,4
		4/6	94	6,38	-108,2
		4/7	99	4,32	-110,6
		4/8	96	4,51	-110,5
	9	4/5	91	-0,37	-116
		4/6	95	1,87	-113,2
		4/7	95	2,75	-113,7
		4/8	92	5,56	-111,7
	10	4/5	87	-3,49	-116
		4/5	91	1,79	-113
		4/7	89	1,2	-113,8
		4/8	87	-1,02	-115,00
	11	4/5	60	1,47	-114
		4/6	56	2,95	-113,7
		4/7	54	3,84	-112,2
		4/8	56	3,12	-112,5
12	4/5	53	3,63	-110,4	
	4/6	50	3,93	-109,1	
	4/7	49	4,22	-109,6	
	4/8	50	0,32	-113,5	

Mesmo com o aumento na oscilação de frequência dos *chirps* conforme se eleva o valor do SF, a distância mais de 10 vezes maior contribui para que não se percam tantos pacotes como nos testes do laboratório.

Apesar de apresentar taxas de envio aceitáveis com valores diferentes de SF, os melhores resultados também foram obtidos com SF = 7, como nos testes feitos em laboratório, se mostrando a melhor opção para comunicações de menor alcance. É possível observar este comportamento no gráfico da Figura 19.

Um detalhe a se ressaltar nos resultados dos testes em sala, é a enorme variação no valor do SNR (Figura 20), o que indica que a razão entre sinal e ruído, por diversas vezes, era afetada mais significativamente por ruídos gerados durante o trajeto dos envios. Quanto ao RRSI, foi observado que não houve grandes oscilações, portanto a força do sinal manteve-se

consideravelmente estável durante o período dos testes. Isso pode ser observado na Figura 21.

Figura 19 – Gráfico ilustrando o comportamento da taxa de acerto nos envios conforme se variam o SF e CR, para os testes feitos no bloco principal.

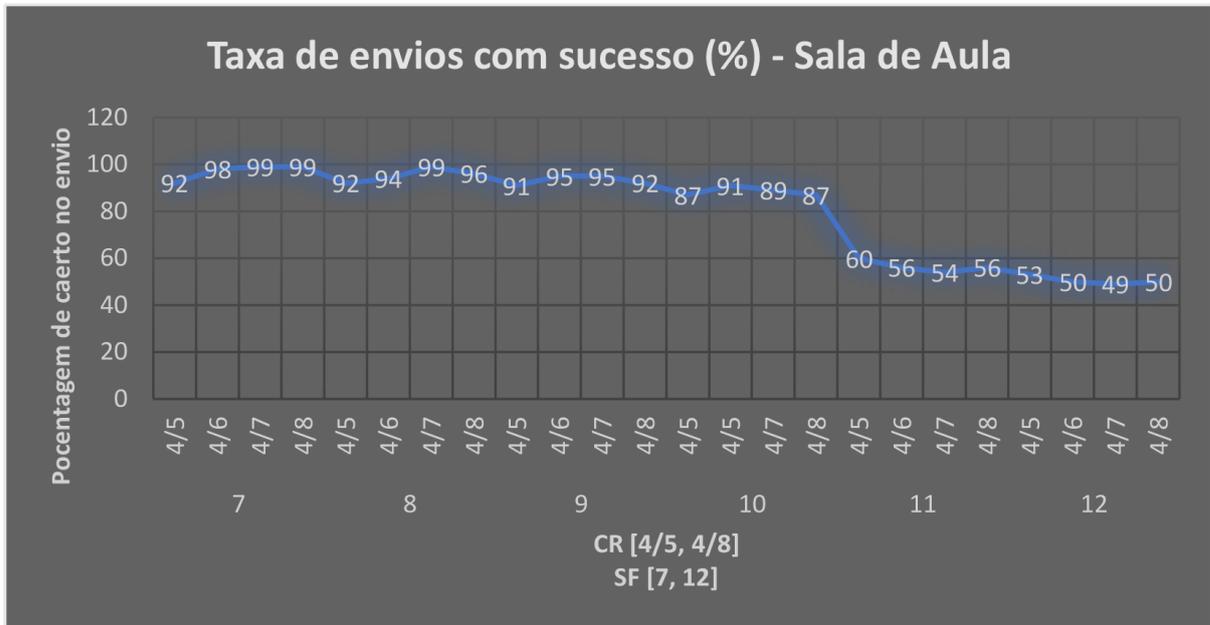


Figura 20 – Gráfico ilustrando o comportamento volátil da razão entre sinal e ruído para os testes feitos no bloco principal.

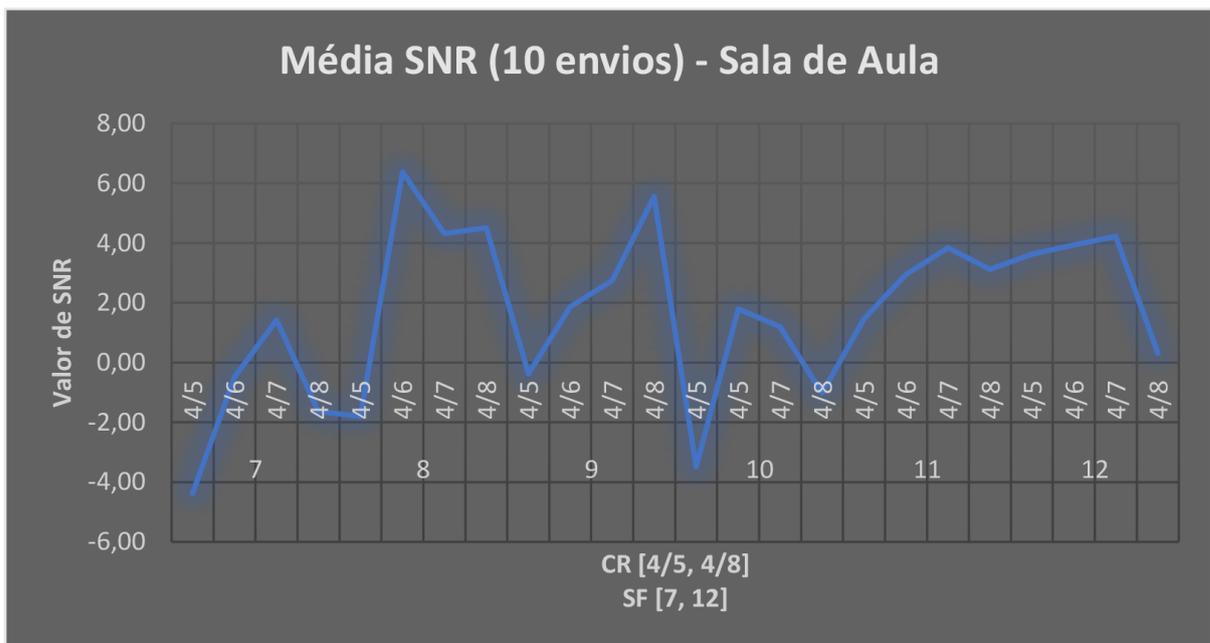
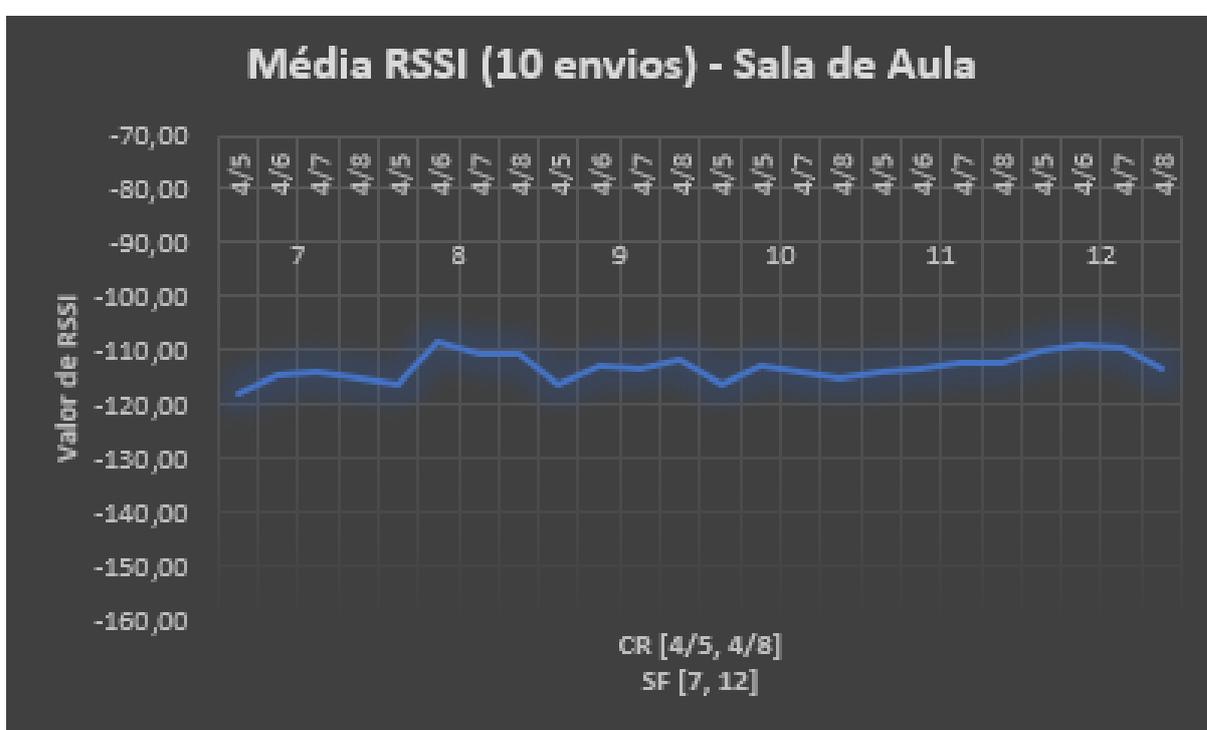


Figura 21 – Gráfico ilustrando a oscilação na força do sinal recebido para os testes feitos em sala.



Ao fim de todos os testes, além de observado que as melhores taxas de acerto no envio de mensagens foram obtidas utilizando $SF = 7$, também concluiu-se que, para os cenários apresentados, o valor do parâmetro CR não apresentou impactos significantes sobre as taxas de envios com sucesso.

4

Conclusões

Este trabalho foi realizado visando fazer uma avaliação da comunicação utilizando redes LoRa dentro do campus da Unioeste de Cascavel/PR, de forma a estudar a possibilidade da implantação de sistemas IoT na universidade utilizando estas redes. Foi também objetivo deste trabalho realizar levantamentos bibliográficos sobre a tecnologia LoRa, seus aspectos de comunicação e arquitetura, o protocolo LoRaWAN e seus níveis de segurança disponibilizados.

Durante o desenvolvimento deste trabalho foram levantados alguns aspectos em relação à segurança provida pelo protocolo LoRaWAN e seu funcionamento. Foi realizada uma revisão bibliográfica sobre a tecnologia LoRa e algumas de suas características de comunicação e segurança, com objetivo de melhor compreender o funcionamento desta rede. A avaliação da comunicação foi realizada variando os parâmetros de SF e CR, possibilitando verificar o impacto dos mesmos sobre a qualidade de comunicação da rede. O *gateway* ficou posicionado no Laboratório de Redes de Computadores, no Bloco F do campus, enquanto o módulo de leitura e transmissão de dados foi disposto em duas localizações diferentes para a realização dos testes: no próprio laboratório onde foi montado o *gateway*, a cerca de 6 metros do mesmo, e em uma sala de aula no bloco principal do campus, distanciando cerca de 81 metros do *gateway*.

Os testes realizados permitiram concluir que a melhor opção para os cenários planejados é utilizar um SF = 7, sendo inviável o uso de valores maiores que este para envios muito próximos (teste no laboratório) e tendo resultados razoáveis com SF ≤ 10, porém não tão satisfatórios quanto aos obtidos com SF = 7. Após a realização dos testes também foi possível perceber que, para os cenários escolhidos, o parâmetro CR não possui impacto significativo. Ao fim das execuções, foram levados em consideração também os valores médios de SNR e RSSI dos envios, com isso foi possível notar que nos testes em laboratório a qualidade do sinal era consideravelmente razoável e estável, apresentando também uma boa e estável razão entre sinal e ruído. Já nos testes feitos na sala de aula, foi possível observar que diversos ruídos eram gerados ao longo dos testes, isso pois o valor do SNR oscilou bruscamente enquanto o a força do sinal

(RSSI) se manteve mais estável.

A realização deste trabalho abre um leque de possibilidades futuras. Utilizar uma antena de maior porte e posicionada externamente possibilitará que seja feita uma cobertura muito maior, cobrindo possivelmente o campus por completo e parcialmente seus arredores. Com isso, o desenvolvimento de aplicações que ajudem na manutenção do campus será possível.

Referências

- ALLIANCE, L. *Technical Overview of LoRa and LoRaWAN*. 2015. Disponível em: <<https://www.tuv.com/content-media-files/master-content/services/products/1555-tuv-rheinland-lora-alliance-certification/tuv-rheinland-lora-alliance-certification-overview-lora-and-lorawan-en.pdf>>. Citado na página 14.
- BARDYN, J.-P. et al. IOT: The era of LPWAN is starting now. *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, 2016. Citado na página 14.
- CAMARGO, E. T. d. et al. Fundamentos de LoRaWAN – teoria e prática. In: *Anais do ERRC 2021*. [S.l.: s.n.], 2021. Citado na página 19.
- FAINO, W. C. Estudo da utilização de redes LoRa-WAN na implementação de soluções para internet das coisas. In: *Anais do VII EAICTI*. [S.l.: s.n.], 2021. Citado na página 12.
- MACHINEQ. *What is the Spreading Factor (SF)?* 2021. Disponível em: <<https://support.machineq.com/s/article/What-is-the-Spreading-Factor-SF>>. Citado na página 11.
- NETWORK, T. T. *Security*. 2021. Disponível em: <<https://www.thethingsnetwork.org/docs/lorawan/security/>>. Citado na página 17.
- NETWORK, T. T. *RSSI and SNR*. 2022. Disponível em: <<https://www.thethingsnetwork.org/docs/lorawan/rssi-and-snr/>>. Citado na página 12.
- SEMTECH. *What is Lora®?* 2022. Disponível em: <<https://www.semtech.com/lora/what-is-lora>>. Citado na página 11.
- SHELDON, R.; BURKE, J. *What is signal-to-noise ratio and how is it measured?* TechTarget, 2021. Disponível em: <<https://www.techtarget.com/searchnetworking/definition/signal-to-noise-ratio>>. Citado na página 12.
- SOLAGNA, E. A. et al. Análise de perdas de pacotes de uma rede LoRaWAN. Universidade de Passo Fundo, 2020. Citado na página 11.