UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

IMARIO ALMEIDA BARBOSA

ANÁLISE DE VULNERABILIDADES EM REDES LORAWAN SOB ATAQUES DE NEGAÇÃO DE SERVIÇO

QUIXADÁ

2025

IMARIO ALMEIDA BARBOSA

ANÁLISE DE VULNERABILIDADES EM REDES LORAWAN SOB ATAQUES DE NEGAÇÃO DE SERVIÇO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Francisco Helder Candido dos Santos Filho.

QUIXADÁ

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B197a Barbosa, Imario Almeida.
Análise de vulnerabilidades em redes LoRaWAN sob ataques de negação de serviço / Imario Almeida Barbosa. – 2025.
43 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Engenharia de Computação, Quixadá, 2025.
Orientação: Prof. Dr. Francisco Helder Candido dos Santos Filho.

1. LoRaWAN. 2. DoS. 3. dispositivos. 4. fator de espalhamento. I. Título.

CDD 621.39

IMARIO ALMEIDA BARBOSA

ANÁLISE DE VULNERABILIDADES EM REDES LORAWAN SOB ATAQUES DE NEGAÇÃO DE SERVIÇO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Aprovada em: 27/02/2025.

BANCA EXAMINADORA

Prof. Dr. Francisco Helder Candido dos Santos Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Ricardo Reis Pereira
Universidade Federal do Ceará (UFC)

Prof. Me. Roberto Cabral Rabêlo Filho
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

Agradeço imensamente à minha família pelo apoio ao longo da minha jornada acadêmica.

Meus agradecimentos também ao meu orientador, Prof. Francisco Helder Candido dos Santos Filho, por aceitar contribuir com meu Trabalho de Conclusão de Curso (TCC). Sua paciência, disposição para esclarecer minhas dúvidas.

A universidade me proporcionou momentos de alegria e agradeço aos meus amigos por vivenciar bons momentos.

Agradeço aos meus professores por todo conhecimento repassado e apoio durante este período.

RESUMO

As aplicações de *IoT* vêm crescendo bastante em diversas áreas, como saúde, transporte, agricultura e industria. Entre as tecnologias de comunicação utilizadas nesse ecossistema, o *LoRaWAN* vem ganhando destaque por causa do seu longo alcance e do seu baixo consumo energético. Como em diversas outras tecnologias de comunicação sem fio, o *LoRaWAN* possui algumas falhas se segurança que podem ser exploradas para causar o mal funcionamento do sistema. O presente trabalho pretende avaliar o desempenho de uma rede *LoRaWAN* durante um ataque de negação de serviço, determinando o ponto em que a rede passa a perder bastante desempenho. Para simular a rede, foi utilizado o simulador de redes ns-3 em conjunto com o módulo *LoRa*, também foi necessário adaptar o módulo para a inserção de dispositivos maliciosos, que seriam responsáveis pelos ataques. O objetivo dos atacantes era imundar a rede, com o envio continuo de pacotes em um baixo intervalo, esse grande volume de pacotes na rede causaria o conflito entre pacotes, que acabaria causando a perca de pacotes uteis. Foram realizadas diversas simulações utilizando diversos parâmetros para abranger diversos cenários. Os fatores de espalhamento afetados pelos ataques foram o 7,9 e 12. Os resultados obtidos nas simulações e analises demonstram que no fator de espalhamento mais baixo a adição de poucos dispositivos atacantes é praticamente insignificante para o desempenho da rede, o que não acontece para fatores mais altos, que ao adicionar a mesma porcentagem de atacantes nesses fatores, o desempenho da rede caiu bastante.

Palavras-chave: LoRaWAN; DoS; dispositivos; fator de espalhamento.

ABSTRACT

IoT applications have been growing significantly in various areas such as healthcare, transportation, agriculture, and industry. Among the communication technologies used in this ecosystem, LoRaWAN has gained prominence due to its long range and low energy consumption. However, like many other wireless communication technologies, LoRaWAN has some security vulnerabilities that can be exploited to cause system malfunctions. This paper aims to evaluate the performance of a LoRaWAN network during a denial of service attack, determining the point at which the network begins to experience significant performance degradation. The network simulation was carried out using the ns-3 network simulator together with the LoRa module. Additionally, the module had to be adapted to include malicious devices responsible for the attacks. The attackers' goal was to flood the network by continuously sending packets at short intervals. This high volume of packets in the network would cause packet collisions, resulting in the loss of useful packets. Several simulations were conducted with varying parameters to cover different scenarios. The spreading factors affected by the attacks were 7, 9, and 12. The results obtained from the simulations and analyses demonstrate that, at the lowest spreading factor, the addition of a few attacking devices is practically insignificant for the network's performance. However, this is not the case for higher spreading factors, where adding the same percentage of attackers caused the network's performance to degrade significantly.

Keywords: LoRaWAN; DoS; devices; spread factor.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABP	*Activation By Personalization*
CPN	*Colored Petri Nets*
CSS	*Chirp Spread Spectrum*
DoS	*Denial of Service*
GSM	*Groupe Special Mobile*
IoT	*Internet of Things*
LPWAN	*Low Power Wide Area Network*
LTE-M	*Long-Term Evolution Machine*
LTE	*Long-Term Evolution*
LoRa	*Long Range*
NB-IoT	*NarrowBand IoT*
OTAA	*Over-The-Air Activation*
SF	*Spread Factor*
UMTS	*Universal Mobile Telecommunications Service*

SUMÁRIO

1 INTRODUÇÃO

O conceito de *Internet of Things* (*IoT*) motivou a criação de diversas aplicações em várias áreas, como na saúde, agricultura, transporte e indústria. A principal ideia desse conceito é conectar objetos, dispositivos e recursos do dia a dia na Internet.

Na área da saúde a *IoT* pode colaborar com o desenvolvimento de dispositivos vestíveis e sensores que capturam dados médicos. Esse dispositivos podem ajudar no monitoramento de idosos para a detecção de quedas, no monitoramento de pacientes em casa e em hospitais e no monitoramento das condições de temperatura em refrigeradores que armazenam medicamentos e vacinas (Sobin, 2020).

Na agricultura a *IoT* pode ser utilizada para monitorar a umidade do solo, controlar as condições climáticas, e regular o nível de umidade e temperatura para prevenir fungos. Também pode ser utilizada para o monitoramento das condições meteorológicas para a previsão de chuvas, formação de gelo, secas e outros fenômenos meteorológicos. Outro exemplo esta no uso de dispositivos inteligentes em gados para a coleta de informação sobre a movimentação do gado, comportamento, lactação e fertilidade, todas essas informações podem ser acessadas por meio de smarthphones, que ajudam a aumentar a produtividade (Sobin, 2020).

No transporte a *IoT* é utilizada para localizar itens em grandes armazéns e portos, verificar condições de qualidade durante o transporte da mercadoria e auxiliar nas rotas de produtos delicados, como medicamentos (Sobin, 2020). Diante disso a sociedade moderna se torna cada vez mais dependente dessas estruturas inteligentes, que possuem como principal desafio as redes de acesso de longa distância e baixa potência (*Low Power Wide Area Network* (*LPWAN*)). Com as principais tecnologias conhecidas como *Sigfox*, *NarrowBand IoT* (*NB-IoT*), *Long-Term Evolution Machine* (*LTE-M*) e *LoRaWAN* (Hessel *et al.*, 2020).

A *LPWAN* é uma rede projetada para longo alcance e baixo consumo energético. Ela é capaz de oferecer conectividade de longo alcance de 2 a 50 quilômetros, dependendo das condições da região onde for implantada. Outra característica desse tipo de rede é a longa duração da bateria. A taxa de dados oferecido pelo *LPWAN* é de 100bps a 250kbps e essa taxa é definida conforme os requisitos de alcance (Chacko; Job, 2018).

Dentre as tecnologias *LPWAN*, uma que ganhou bastante destaque foi a *LoRa*. A *LoRa* é uma tecnologia que modula sinais de radiofrequência para redes de longo alcance e baixa potência (*LPWAN*). Ela permite a comunicação entre dispositivos em até 5 quilômetros em áreas urbanas e em até 15 quilômetros em áreas rurais. A principal característica das soluções que uti-

lizam essa tecnologia é a necessidade de utilizar dispositivos de baixo consumo energético, esses dispositivos possuem baterias que podem durar até 10 anos. Um dos protocolos que utilizam a tecnologia *LoRa* é o *LoRaWAN*. O protocolo *LoRaWAN* foi desenvolvido pelo *LoRa Alliance*, ele oferece comunicação bidirecional segura, mobilidade e serviços de localização (Semtech, 2019). Uma questão muito importante a se abordar é a segurança em redes sem fio, particularmente em redes *LoRaWAN*. Redes sem fio geralmente não são confiáveis para uma operação segura de longo prazo, historicamente a maioria dos padrões sem fio apresentaram falhas na segurança. Isso inclui sistemas celulares como *Groupe Special Mobile* (*GSM*)/*Universal Mobile Telecommunications Service* (*UMTS*)/*Long-Term Evolution* (*LTE*) e tecnologias sem fio de curto alcance como *Wifi* e *Bluetooth* (Hessel *et al.*, 2023). Desde da primeira versão da especificação *LoRaWAN* em 2015, a segurança já estava presente. Mas como nos outros padrões sem fio, a *LoRaWAN* apresentou diversos problemas de segurança desde do inicio (Hessel *et al.*, 2023).

Recentemente alguns estudos foram publicados avaliando a segurança em redes que utilizam a pilha de protocolos *LoRaWAN*. O trabalho desenvolvido por (Es *et al.*, 2018) verifica as vulnerabilidades em relação a ataques de negação de serviço em redes *LoRaWAN*. Em (Hessel *et al.*, 2020) um *framework* foi desenvolvido para a avaliação da segurança, nele dois ataques de negação de serviço foram realizados.

Visto que redes *IoT* são amplamente utilizadas em diversas áreas e que cada vez mais as pessoas estão dependentes desse tipo de rede, é necessário que esses sistemas garantam uma proteção contra ataques de agentes maliciosos.

Diante disso, este trabalho tem como principal proposta realizar uma análise de vulnerabilidade em redes *LoRaWAN*, avaliando o desempenho da rede, durante um ataque de negação de serviço, essa análise será realizada por meio do simulador de rede NS-3. Com isso pretende-se verificar o comportamento dessa rede *LPWAN* após um ataque de negação de serviço, e analisar se é possível manter o mínimo de qualidade de serviço para o qual esse rede foi projetada.

1.1 Objetivos

O objetivo geral deste trabalho é avaliar o impacto de ataques de negação de serviço em redes *LoRaWAN* em diferentes cenários, utilizando o simulador NS-3. Este estudo busca contribuir para a análise da vulnerabilidade da rede *LoRaWAN* em diversas aplicações potenciais, como Indústria 4.0, cidades inteligentes, agricultura e saúde. Essas aplicações, por sua relevância,

podem se tornar alvos de ataques.

1.1.1 Objetivos específicos

a) Configurar a rede *LoRaWAN* no NS-3.
b) Implementar novas funcionalidades no módulo *LoRaWAN* do NS-3.
c) Realizar ataques de negação de serviço na rede.
d) Avaliar o desempenho da rede, antes e durante os vários cenários de ataque.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção tem como objetivo explanar os principais conceitos e tecnologias que serviram como base para o entendimento e para o desenvolvimento do trabalho proposto.

2.1 Tecnologia *LPWAN*

A tecnologia *LPWAN* abrange uma gama de tecnologias usadas para conectar dispositivos finais de baixa potência, como sensores e atuadores em comunicações MTC, podendo operar no espectro licenciado ou não licenciado, além de incluir opções proprietárias ou de padrão aberto. Logo, podemos descrever que as principais características das tecnologias LPWAN necessárias para alcançar todos os requisitos para implantação de um sistema ciber-físico IoT com sucesso são (Naik, 2018):

- Longo alcance de comunicação;
- Baixo consumo de energia;
- Baixa taxa de dados;
- Baixo custo dos dispositivos finais e de implantação;
- Topologia e implantação de rede simplificadas;
- Maior alcance de cobertura do sinal (maior capacidade de penetração do sinal);
- Alta capacidade de atualização da rede (baixa complexidade da infraestrutura).

A escolha de uma tecnologia LPWAN depende da área de aplicação em mente e de seus requisitos específicos, como taxa de dados, alcance, capacidade de energia, banda de frequência, transmissão bidirecional, custo da rede, escalabilidade e segurança.

As tecnologias LPWAN podem ser classificadas em duas categorias: tecnologias que utilizam o espectro licenciado (por exemplo, NB-IoT e LTE-M) e tecnologias que utilizam o espectro isento de licença ou não licenciado (por exemplo, Sigfox, Telensa, LoRa e RPMA), sendo utilizada na camada física as técnicas de modulação em NarrowBand (NB) ou Spread Spectrum (SS) para a maioria dessas tecnologias (Thomas; Eldhose, 2019).

2.2 Tecnologia LoRa e Rede LoRaWAN

LoRaWAN é um protocolo LPWAN que define os recursos de medium access control (MAC) e os formatos de mensagem que são entregues a uma camada física empregando tecnologia LoRa. O LoRaWAN foi desenvolvido e é atualizado continuamente pela LoRa

Alliance.

As redes LoRaWAN geralmente são implantadas em uma topologia estrela, na qual os gateways encaminham mensagens trocadas entre os dispositivos finais e um Network Server (NS). Por sua vez, o NS roteia os pacotes de cada dispositivo final para uma plataforma de serviços de aplicações. Os gateways e o NS são conectados através do protocolo de comunicação Internet Protocol (IP). Por outro lado, os dispositivos finais são conectados a um ou mais gateways usando LoRa (LoRa-Alliance, 2020). A seguir, são apresentados mais detalhes do LoRa e do LoRaWAN.

2.2.1 LoRa

Long Range (*LoRa*) é uma tecnologia de camada física que funciona em banda industrial, científica e médica (ISM) não licenciada que tem como base a técnica *Chirp Spread Spectrum* (*CSS*) (Chaudhari *et al.*, 2020). A tecnlogia *LoRa* realiza uma compensação entre sensibilidade e taxa de dados, enquanto opera em um canal de largura de banda fixa de 125 KHz ou 500 KHz (para canais de *uplink*) e 500KHz (para canais de *downlink*).

Ela também utiliza fatores de espalhamento ortogonais, que permite que a rede consiga preservar a duração da bateria dos dispositivos finais conectados, fazendo otimizações adaptáveis dos níveis energéticos e na taxa de dados de um dispositivo final individual. A modulação *LoRa* possui seis fatores de espalhamento, sendo eles do 7 ao 12 (SF7 a SF12). Quanto maior o fator de espalhamento, maior será a distância que o sinal poderá percorrer e ser recebido sem erros por um receptor de radio frequência.

A Figura 1 mostra quatro fatores de espalhamento diferentes que podem ser utilizados na transmissão de mensagens de *uplink* em um canal de 125KHz. Nela também é exibido a taxa de bits, o alcance estimado, que varia de acordo com o local, por exemplo, em locais rurais o alcance será maior do que em áreas urbanas, também é mostrado o tempo de permanência ou tempo no ar para um *payload* de 11 *bytes* (Semtech, 2019).

Os pacotes que utilizam diferentes fatores de espalhamento são ortogonais. Então, se dois pacotes chegarem ao mesmo tempo no mesmo canal de recepção e possuírem fatores de espalhamento diferentes, eles não irão colidir. Entretanto, caso dois pacotes cheguem ao mesmo tempo em um mesmo canal de recepção e seus fatores de propagação sejam idênticos os pacotes serão perdidos, caso os pacotes possuam sinais de diferentes intensidade, o pacote com sinal mais potente será preservado enquanto o outro será descartado (Aras *et al.*, 2017).

Figura 1 – Fatores de espalhamento LoRa

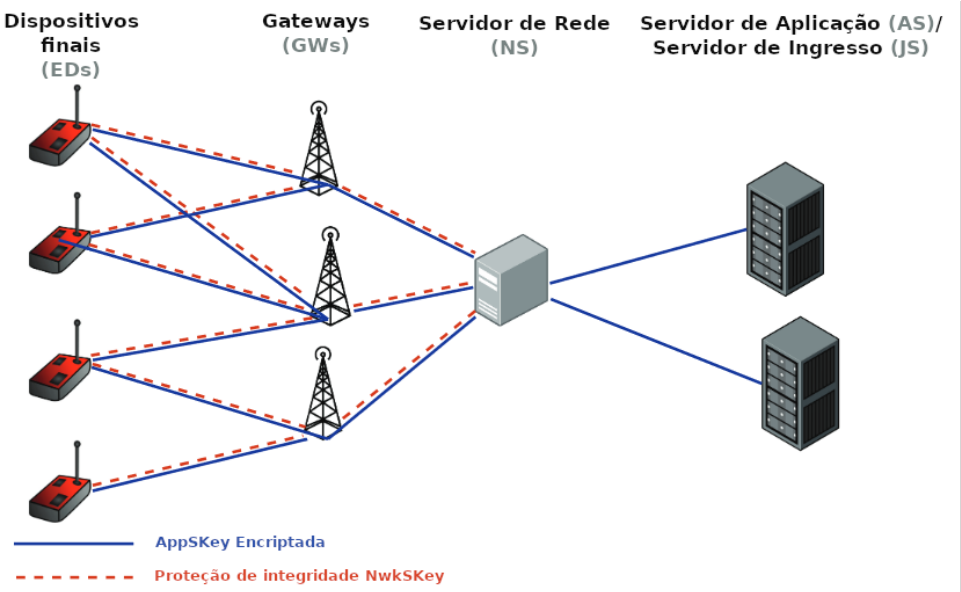
Fator de espalhamento	Taxa de bits (bps)	Alcance (Depende do terreno)	Tempo no ar para 11 bytes
SF10	980 bps	8 km	371 ms
SF9	1760 bps	6 km	185 ms
SF8	3125 bps	4 km	103 ms
SF7	5470 bps	2 km	61 ms

Fonte: Semtech (2019)(Adaptada).

2.2.2 LoRaWAN

LoRaWAN é um protocolo de rede desenvolvido pela *LoRa Alliance*, que é uma organização sem fins lucrativos composta por diversas empresas do ramo da tecnologia. Esse protocolo foi otimizado para ser utilizado por dispositivos que requerem um baixo consumo de energia. Uma rede *LoRaWAN* possui alguns componentes fundamentais para o seu funcionamento, sendo eles, os *End Devices* (EDs), os *Gateways* (GWs), os *Network Servers* (NSs), os *Application Servers* (ASs) e os *Join Servers* (JSs) conforme é mostrado na Figura 2. Os EDs transmitem frame de dados para os GWs, que por sua vez transfere eles no seu estado bruto para o NS, por meio de uma conexão IP padrão. O NS tem como responsabilidade validar e decodificar os pacotes recebidos, após isso os pacotes são encaminhados para o AS (Kuntke *et al.*, 2022). A *LoRaWAN* especifica três tipo de classes diferentes, classe A, classe B e classe

Figura 2 – Arquitetura de rede LoRaWAN



Fonte: Kuntke *et al.* (2022, p. 3)(Adaptada).

C. Todos os dispositivos operam na classe A e alguns na classe B e classe C. Os dispositivos

que operam em mais de uma classe são comumente chamados de *"higher Class end-devices"* (LoRa-Alliance, 2020). A seguir serão apresentados os tipos de classes.

- **Classe A:** Os dispositivos finais classe A possuem a capacidade de se comunicar bi-direcionalmente, com uma transmissão de *uplink* que é seguida de duas janelas curtas de recibimento de *downlink*. O dispositivo final agenda uma transmissão conforme sua necessidade de comunicação. Essa é a classe que consome menos energia em cenários em que as aplicações necessitam de transmissões *downlink* somente depois do dispositivo final realizar transmissões *uplink*. (LoRa-Alliance, 2020)
- **Classe B:** Os dispositivos finais classe B, além de possuírem as janelas de recebimento da classe A, eles possuem janelas de recebimento extras em horários previamente determinados. Para as janelas abrirem nesse horário, o dispositivo recebe um *beacon* sincronizado com o horário do *gateway*. Isso permite que o *Network Server* sabia em que momento o dispositivo final está esperando o recebimento de pacotes.(LoRa-Alliance, 2020)
- **Classe C:** Os dispositivos finais que implementam classe C possuem janelas de recebimento abertas, fechando apenas em momentos de transmissão. Os dispositivos dessa classe são os que mais consomem energia e são os que possuem a menor latência na comunicação entre servidores e dispositivos finais. (LoRa-Alliance, 2020)

2.2.2.1 Pacotes camada física

A *LoRaWAN* possui duas terminologias a transmissão de dados na rede, *frames uplink* e *frames downlink*.

- **Uplink:** Pacotes *uplink* são enviados de dispositivos finais para um *Network Server* por meio de um ou mais *gateways*.
- **Downlink:** Pacotes *downlink* são enviados de um *Network Server* para um único dispositivo final por meio de um ou mais *gateways*.

2.2.2.2 Ativação na rede

Para que um dispositivo final possa participar de uma rede *LoRaWAN* é necessário que ele seja personalizado e ativado. Existem duas maneiras de ativar um dispositivo, a primeira é pelo o ar, chamada de *Over-The-Air Activation* (*OTAA*)) e a segunda é a *Activation By Personalization* (*ABP*).

2.2.2.3 Ativação pelo ar

Para os dispositivos finais começarem a trocar informações com um servidor de rede, eles devem passar por um processo chamado *Join Procedure* e um dispositivo final deve realizar um novo *Join Procedure* sempre que perder as informações sobre o contexto da sessão. Antes de iniciar um *Join Procedure* o dispositivo deve ser personalizado com um identificador globalmente exclusivo de dispositivo final (*DevEUI*), um identificador de *Join Server* (*JoinEUI*) e uma chave AES-128 (*AppKey*). Da perspectiva do dispositivo final, *Join Procedure* é apenas a troca de duas mensagens com o servidor, sendo elas, *Join Request* e *Join-Accept*. (LoRa-Alliance, 2020)

- **Join Request:** É a requisição realizada pelo dispositivo final para iniciar o *Join Procedure*. O *Join-Request frame* é composto pelo *JoinEUI*, por um *DevEUI* do dispositivo final e um *nonce* de dois octetos chamado de *DevNonce*. *DevNonce* é um contador iniciado em 0 assim que o dispositivo é ligado e ele é incrementado sempre que há uma requisição de *Join*. O *Join Server* armazena para cada dispositivo final o último valor *DevNonce* e ignora as solicitações de *Join* caso ele não seja incrementado.
- **Join-Accept:** É uma mensagem enviada da rede para o dispositivo final em resposta ao *Join Request*, caso o dispositivo tenha sido aceito na rede. O *Join-Accept frame* é composto por um *nonce* de três octetos, o *JoinNonce*, um identificador de rede chamado *NetID*, um endereço de dispositivo final (*DevAddr*), as configurações de *downlink* (*DLSettings*), um *delay* entre TX e RX (*RXDelay*) e uma lista de parâmetros de rede (*CFList*) que é opcional.

2.2.2.4 Ativação por personalização

A ativação por personalização associa um dispositivo final a uma rede, sem a necessidade do *Join Procedure*. Nesse tipo de ativação o dispositivo final armazena o *DevAddr* e as duas chaves de sessão *NwkSkey* e *AppSKey*, essas chaves devem ser exclusivas. Com isso o dispositivo final está pronto para participar da rede assim que é iniciado.

2.3 Segurança da informação

De acordo com Committee on National Security Systems (CNSS), a segurança da informação pode ser definida como a proteção da informação e de elementos vitais, como sistemas e hardware que acessam, armazenam e transmitem informação. (Whitman; Mattord, 2011) Essa proteção tem como objetivo assegurar que o sistema de informação siga integro,

disponível e confidencial. Essas características de segurança são conhecidas como tríade CIA (Confidentiality, Integrity and Avaiability) (Stalling, 2015).

- **Confidencialidade:** É a garantia de que as informações não serão expostas ou divulgadas para indivíduos, entidades ou processos sem autorização (ISO, 2018). Um exemplo prático da aplicação da confidencialidade está na autenticação de dois fatores (que requer um cartão físico e um código PIN) exigida pelos caixas eletrônicos. Nesse caso, o acesso aos dados é permitido somente quando ambas as condições são atendidas (Fruhlinger, 2020).
- **Integridade:** É a garantia de que as informações estão completas e que ninguém sem autorização possa modifica-las, seja por acidente ou maliciosamente (Fruhlinger, 2020). Uma forma de garantir a integridade das informações é por meio do hashing, que é a aplicação de um algoritmo que calcula um valor único chamado de hash, esse valor hash é utilizado como base para identificar se uma informação foi comprometida (Whitman; Mattord, 2011).
- **Disponibilidade:** É a garantia de que as informações estarão disponíveis de forma rápida e confiável (Stalling, 2015). Um exemplo da violação da disponibilidade é quando o sistema é alvo de um ataque de negação de serviço (CISA, 2021).

2.4 Ataques de negação de serviço

Um ataque de negação de serviço ou ataque *Denial of Service* (*DoS*), ocorre quando usuários são impedidos de acessar serviços, dispositivos ou outros recursos de rede por causa de algum agente malicioso. Os serviços negados podem ser email, sites, contas online (por exemplo, contas bancárias) ou outros serviços que dependem do dispositivo ou da rede atacada (CISA, 2021).

Existem diversos métodos para se realizar um ataque de negação de serviço. Um dos métodos é o de inundação, que ocorre quando o sistema sobrecarrega o *buffer* do servidor por causa de um alto tráfego, isso faz com que a velocidade do sistema seja drasticamente diminuída, até que por fim o sistema fique fora do ar (Networks, 2020).

2.5 Segurança em LoRaWAN

A segurança na rede LoRaWAN (Long Range Wide Area Network) é um aspecto crucial, especialmente porque essa rede é amplamente utilizada em soluções de Internet das

Coisas (IoT), onde dados sensíveis podem ser transmitidos. A LoRaWAN foi projetada com mecanismos de segurança robustos para garantir a confidencialidade, integridade e autenticidade dos dados transmitidos. Abaixo estão os principais aspectos de segurança na LoRaWAN (Butun *et al.*, 2018):

1. Criptografia de Dados
    - **Criptografia de Enlace de Rede** (Network Session Key - NwkSKey): Protege a comunicação entre o dispositivo final e o servidor de rede. Garante a autenticidade e a integridade das mensagens, evitando que dados sejam alterados durante o trânsito.
    - **Criptografia de Aplicação** (Application Session Key - AppSKey): Garante a confidencialidade das mensagens de dados da aplicação entre o dispositivo final e o servidor de aplicação. Isso impede que terceiros, incluindo o operador da rede, tenham acesso ao conteúdo das mensagens transmitidas.
2. Autenticação e Controle de Acesso
    - **Chave de Sessão** (AppKey): A chave de criptografia usada para derivar as chaves de sessão do dispositivo. Ela é exclusiva para cada dispositivo e é compartilhada entre o dispositivo e o servidor de rede. Isso garante que apenas dispositivos autorizados possam se conectar à rede.
    - **Identificação Única** (DevEUI): Cada dispositivo *LoRaWAN* possui um identificador exclusivo, o DevEUI, que é usado para autenticação na rede.
3. Métodos de Ativação
    - **Ativação por Personalização** (Activation by Personalization - ABP): Neste método, o dispositivo vem pré-configurado com as chaves de sessão. Embora mais simples, esse método é considerado menos seguro, pois as chaves são estáticas e podem ser comprometidas se interceptadas.
    - **Ativação Over-the-Air** (Over-the-Air Activation - OTAA): É o método mais seguro. Neste, o dispositivo se autentica dinamicamente com a rede e gera chaves de sessão únicas durante o processo de ativação, o que aumenta a segurança.

2.5.1 Proteção contra Rejogos (Replay Attacks)

Para evitar ataques de repetição, onde mensagens antigas são retransmitidas, a LoRaWAN utiliza um contador de quadros (Frame Counter) para cada dispositivo. Se o contador de quadros de uma mensagem for inferior ao último valor conhecido, a mensagem é descartada.

2.5.2 Canais de Comunicação

A LoRaWAN opera em frequências de rádio públicas (como 868 MHz na Europa e 915 MHz nas Américas), o que significa que qualquer dispositivo pode tentar se conectar à rede. No entanto, a autenticação e criptografia garantem que apenas dispositivos autorizados possam acessar a rede e os dados.

2.5.3 Desafios e Vulnerabilidades

Apesar de seus mecanismos de segurança, existem desafios:

- **Chaves mal gerenciadas:** Se as chaves não forem bem gerenciadas (por exemplo, compartilhamento inadequado ou chaves fracas), a rede pode ser vulnerável.
- **Ataques físicos:** Como muitos dispositivos LoRaWAN são implantados em áreas remotas ou abertas, existe o risco de ataques físicos ao hardware do dispositivo, como extração de chaves de criptografia.

O padrão LoRaWAN está em evolução, e novas versões aprimoram os aspectos de segurança, além de incorporar boas práticas para evitar vulnerabilidades conhecidas.

Portanto, a segurança na LoRaWAN é bastante sólida, mas depende muito de uma boa implementação, especialmente no gerenciamento das chaves e na configuração dos dispositivos.

2.6 Simulador NS-3

O NS-3 é um simulador de redes de computadores que utiliza a simulação de eventos discretos. Nele, cada evento é associado a um tempo de execução e a simulação executa os eventos na ordem temporal do tempo de simulação. Quando um evento é executado, ele pode gerar zero, um ou mais eventos. Conforme a simulação é processada, os eventos são concluídos, podendo gerar ou não novos eventos. A simulação irá parar quando a fila de eventos estiver vazia ou quando o evento *"Stop"* for executado (Simulator, 2023).

O NS-3 foi desenvolvido para ser utilizado em pesquisa, ele promove um modelo de colaboração baseado na comunidade, tanto para ajudar no desenvolvimento de novos módulos quanto para realizar atividades de validação (Campanile *et al.*, 2020).

O simulador NS-3 implementa modelos para diversos elementos presentes em redes de computadores. Os modelos existentes são:

- **Nós:** representam os dispositivos finais, como computadores, notebooks, hubs, switches e

roteadores.

- **Dispositivos de rede:** representam o dispositivos físicos que tem como função realizar a conexão entre um nó e um canal de comunicação. Por exemplo a placa de rede *Ethernet*.
- **Canais de comunicação:** representam o meio utilizado para a comunicação entre dispositivos.
- **Protocolos de comunicação:** modelam a implementação de protocolos de rede, também podem estar presentes protocolos experimentais que ainda não foram padronizados.
- **Cabeçalhos de protocolo:** são subconjuntos de dados encontrados em pacotes de rede, eles possuem um formato específico para cada objeto de protocolo associado.
- **Pacotes de rede:** são a unidade fundamental na troca de informações em redes de computadores (Riley; Henderson, 2010).

3 TRABALHOS RELACIONADOS

Nesta seção alguns trabalhos que possuem alguma relação com o trabalho desenvolvido são apresentados.

3.1 Denial-of-Service Attacks on LoRaWAN

Em (Es *et al.*, 2018), foi realizado uma análise de segurança na especificação do protocolo *LoRaWAN* tendo como foco as possibilidades de ataques de negação de serviço contra dispositivos finais. Nessa análise foram encontradas três vulnerabilidades que permitiam ataques do tipo negação de serviço, sendo uma vulnerabilidade de *beaconing*, uma de *downlink routing* e uma na ativação de dispositivo final. A vulnerabilidade na ativação de dispositivo final já foi mitigada na versão 1.1 do LoRaWAN.

A vulnerabilidade de *beaconing* foi detectada pela a falta de mecanismos de segurança na transmissão de *beacons* entre dispositivos de classe B e o gateway. Os *beacons* são usados para sincronizar dispositivos de classe B com a rede, essa sincronização permite o agendamento de janelas de transmissão para o envio de dados. Por causa dessa falha na segurança é possível manipular o intervalo de tempo da recepção de dados, com isso os dispositivos ficam dessincronizados causando a indisponibilidade da rede.

A vulnerabilidade de *downlink routing* explora a ausência da confirmação se um dispositivo final ainda é acessível apos a atualização do banco de dados de rota de *donwlink* feita pela o servidor de rede.

A vulnerabilidade na ativação de dispositivos finais esta presente no processo de ativação pelo ar (*OTAA*). Esse tipo de ativação utiliza duas mensagens principais, o *Join-Request* e o *Join-Accept*. A falta de uma referencia a mensagem de *Join-Request* na mensagem *Join-Accept* possibilita que mensagens antigas de *Join-Accept* possam ser reaproveitadas, com isso um *Join-Accept* pode ser retransmitido para um dispositivo final a partir de um dispositivo malicioso, causando assim uma falha de comunicação entre o dispositivo final e o servidor de rede.

Para validar as falhas de segurança encontradas, foram criados modelos formais das partes mais relevantes do protocolo *LoRaWAN* por meio do *Colored Petri Nets* (*CPN*). Esses modelos foram utilizados para a simulação e análise das vulnerabilidades encontradas por meio do *CPNtools*, que foram confirmadas.

A principal diferença entre o trabalho (Es *et al.*, 2018) e o nosso trabalho é que (Es

et al., 2018) utiliza o *CPNTools* para realizar os testes de vulnerabilidade e o nosso trabalho pretende verificar as vulnerabilidades de protocolo *LoRaWAN* utilizando o simulador NS-3. Outro diferencial é que o nosso trabalho irá realizar uma análise de desempenho da rede antes e durante os ataques de negação de serviço.

3.2 ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation

Em (Hessel *et al.*, 2020) foi desenvolvido um *framework* para a avaliação de segurança de redes *LoRaWAN* chamado *ChirpOTLE*. Nele dois ataques que afetam a disponibilidade do sistema são testados, sendo eles o *ADR Spoofing* e *Beacon Spoofing*. Após os testes, algumas contramedidas para cada ataque foram apresentadas e foi concluído que sem a alteração na especificação do protocolo os ataques não podem ser evitados, apenas dificultados.

A principal diferença entre o trabalho de (Hessel *et al.*, 2020) e o nosso é que o nosso trabalho não irá realizar testes no mundo real. A utilização de um simulador possibilita o uso de diversos dispositivos finais, visto que no trabalho de (Hessel *et al.*, 2020) são utilizados poucos dispositivos em seus testes. Outra diferença é que no nosso trabalho será realizada uma verificação de desempenho da rede antes e durante os ataques propostos.

3.3 Security Vulnerabilities in LoRaWAN

Em (Yang *et al.*, 2018), foi feita uma analise da segurança do protocolo *LoRaWAN* v1.0.2, e cinco vulnerabilidades foram exploradas. Para cada vulnerabilidade, um ataque foi desenvolvido e testado em um ambiente *LoRaWAN* controlado.

A primeira vulnerabilidade explorada permitia a repetição de mensagens anteriores. Isso possibilitou o envio de mensagens maliciosas com o objetivo de modificar o valor do contador utilizado para sincronizar as mensagens de uplink e downlink. Ao alterar o valor desse contador, a sincronização da rede é comprometida, resultando em uma indisponibilidade temporária e, consequentemente, causando uma interrupção no serviço (quebra de disponibilidade).

O segundo ataque explora a implementação da confidencialidade no protocolo LoRaWAN, que utiliza criptografia AES no modo contador (CTR). A vulnerabilidade está na reutilização do fluxo de chaves, durante um reinício, o valor do contador é reiniciado, mas a chave permanece a mesma. Isso faz com que o cifrador de blocos gere o mesmo material de chave, resultando na reutilização do fluxo de chaves.

No terceiro ataque, são exploradas vulnerabilidades na implementação da verificação de integridade dos pacotes. Nesse cenário, o autor consegue interceptar e alterar os pacotes, comprometendo a integridade das informações transmitidas.

O quarto ataque explora o fato de que a mensagem de ACK (confirmação) não contém uma referência explícita à mensagem que está confirmando. Neste cenário, o atacante utiliza um gateway malicioso para capturar e armazenar os ACKs enviados pelo servidor de rede. Quando o servidor de rede transmite um ACK, o gateway malicioso intercepta e armazena a mensagem. Posteriormente, o gateway seleciona seletivamente um pacote enviado pelo dispositivo e, ao invés de entregar o ACK correto, o atacante retransmite o ACK previamente capturado, fazendo com que o dispositivo acredite que a mensagem foi confirmada pela rede, mesmo que não tenha sido processada.

A quinta vulnerabilidade explorada é a integridade fraca dos frames beacons utilizados por dispositivos de classe B, essenciais para agendar envios de mensagens e enviar a localização dos dispositivos. O autor descreve dois ataques: o primeiro altera as informações de localização nos beacons, comprometendo a integridade das notificações do servidor de rede. O segundo ataque altera as janelas de envio de mensagens para o gateway, podendo dessincronizar os dispositivos e, se o intervalo de envio for drasticamente reduzido, drenar a bateria e comprometer prematuramente a rede. Por fim, o autor apresenta algumas medidas preventivas de segurança para mitigar as vulnerabilidades identificadas.

A diferença presente entre o trabalho de (Yang *et al.*, 2018) e o nosso é que o (Yang *et al.*, 2018) realiza os testes em um ambiente real e controlado, utilizando apenas um *gateway* e um dispositivo malicioso, enquanto nosso trabalho pretende realizar os testes em um ambiente simulado, onde é possível realizar testes com uma grande quantidade de dispositivos. O trabalho do (Yang *et al.*, 2018) também se diferencia do nosso no quesito análise de desempenho da rede, visto que o nosso trabalho irá realizar essa análise.

3.4 Análise comparativa

A Tabela 1 faz um comparativo entre os trabalhos relacionados apresentados anteriormente e o trabalho proposto. Os pontos que foram levados em consideração na comparação, são, se o trabalho utiliza algum simulador, se o trabalho realiza testes de carga e se o trabalho realiza uma análise de desempenho da rede. A principal diferença entre este trabalho e os demais é a execução de testes de carga, que visa monitorar o comportamento da rede em situações de

estresse.

Tabela 1 – Análise comparativa

Trabalhos	**Utiliza simulador**	**Realiza testes de carga**	**Analisa o desempenho da rede**
(Es *et al.*, 2018)	Sim	Não	Não
(Hessel *et al.*, 2020)	Não	Não	Sim
(Yang *et al.*, 2018)	Não	Não	Não
Trabalho proposto	Sim	Sim	Sim

Fonte: Elaborado pelo autor

4 METODOLOGIA

Nesta seção, são apresentados os procedimentos metodológicos adotados para alcançar os objetivos propostos neste trabalho. As etapas seguidas incluem a configuração da rede LoRaWAN no simulador, a implementação dos cenários, a realização dos ataques, a análise dos dados obtidos e, por fim, a comparação dos resultados.

4.1 Configurações da Rede LoRaWAN no simulador NS-3

Para as simulações na rede *LoRa*, um módulo *LoRa* no simulador de eventos discretos NS-3, foi utilizado. Esse módulo foi desenvolvido por um grupo de pesquisa da Universidade de Padova (Magrin *et al.*, 2017), e foi alterado para que algumas novas funcionalidades pudessem ser adicionadas e utilizadas neste trabalho. Dentre elas, a implementação de uma aplicação para simular dispositivos intrusos na rede, incluindo a geração de pacotes associados a esses invasores.

4.1.1 Modificações no módulo

Para atingir os objetivos propostos, foi necessário implementar novas funcionalidades no módulo *LoRa* do simulador NS-3. Primeiramente, os parâmetros de entrada foram ajustados para aceitar novas configurações, incluindo o número de dispositivos atacantes e o período de envio de seus pacotes. Além disso, o módulo foi adaptado para suportar os dispositivos maliciosos, uma função foi desenvolvida para distribuir os dispositivos maliciosos no ambiente simulado e o contador de pacotes foi modificado para contabilizar corretamente os pacotes maliciosos.

As principais modificações realizadas foram:

- Adição de novos parâmetros de entrada: Número de dispositivos atacantes; Período de envio dos pacotes maliciosos;
- Adaptação do módulo para suportar dispositivos atacantes;
- Implementação de uma função para distribuir os dispositivos maliciosos na simulação;
- Modificação do contador de pacotes para contabilizar pacotes maliciosos;
- Ajuste no *Network Server* para suportar os dispositivos maliciosos;
- Configuração do tamanho do pacote enviado pelos dispositivos maliciosos;

O código-fonte das modificações foi disponibilizado em um repositório no GitHub[1].

4.1.2 Parâmetros

As descobertas deste trabalho, baseadas na variação de parâmetros como o número de usuários e atacantes, são utilizadas para avaliar o desempenho em quatro cenários distintos, detalhados na próxima seção. Esses cenários podem representar situações reais, como aquelas encontradas em ambientes que adotam os conceitos de Fábricas do Futuro ou Indústria 4.0.

Os valores de taxa de sucesso e da vazão foram obtidos por meio de simulações computacionais no programa NS-3 para uma rede *LoRaWAN*, utilizando as seguintes configurações:

- Cenários com n dispositivos finais, com $n \in (0, 1000]$
- Cenários sem atacantes e com atacantes variando de 10%, 30% e 50% de n;
- Dispositivos finais espalhados aleatoriamente na área circular de $max = 8000\ m$;
- Potência de transmissão 14 dBm;
- Largura de banda $BW = 125\ kHz$;
- Oito canais distintos (frequências igualmente espaçadas entre 867.1 MHz e 868.5 MHz);
- Taxa de codificação $CR = 1$;
- *Duty Cycle* (DC = 10%).

Foram executadas cinco campanhas de simulação em cada estratégia. O principal objetivo é avaliar, em cenários de rede *LoRaWAN*, taxa de sucesso das transmissões dos usuários em casos sem ataque e com ataque de *DoS*.

4.2 Implementação dos cenários para a realização dos ataques

A posição do *gateway* é predeterminada, localizada no centro de um círculo de raio de 8000 m. Todos os dispositivos finais são de classe A e suas posições são estabelecidas de forma diferente dependendo se são dispositivos usuários legítimos ou maliciosos. Os dispositivos legítimos são colocados aleatoriamente (distribuídos uniformemente ao longo da área da célula), mas são mantidos fixos durante o tempo de execução da simulação, e cada dispositivos gera pacotes de 28 $bytes$, transmitindo periodicamente em intervalos de 600 s, e a primeira transmissão de cada dispositivo é decidida por atraso aleatório por meio de uma variável aleatória uniforme, ou seja, $\sim U([0, 600])$. Os dispositivos maliciosos também são mantidos fixos durante todo o tempo de execução da simulação, mas são distribuídos espacialmente de três maneiras diferentes:

[1] Acessar: https://github.com/imarioa/ns3-tcc2

i Distribuição uniforme na área do fator de espalhamento 7;

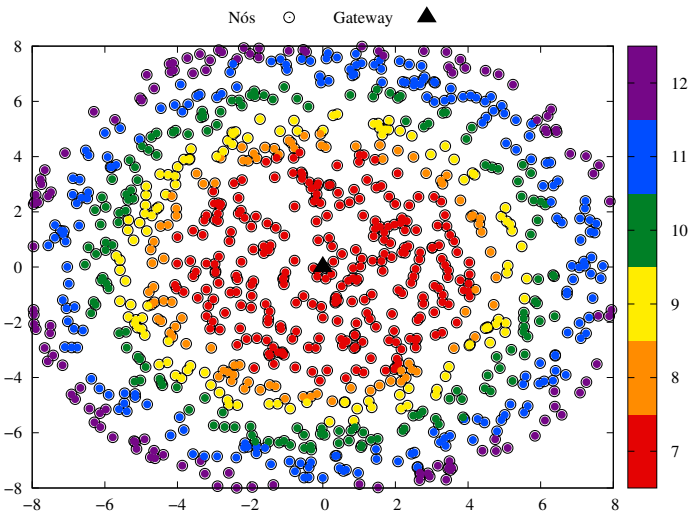
ii Distribuição uniforme na área do fator de espalhamento 9;

iii Distribuição uniforme na área do fator de espalhamento 12.

Os dispositivos atacantes geram pacotes de 14 *bytes* e transmitem em intervalos de tempo aleatórios, seguindo uma distribuição exponencial com média de 60 s, ou seja, $\sim Exp(\frac{1}{60})$. Cada cenário foi definido com base no desempenho da rede *LoRaWAN* em relação aos fatores de espalhamento (SFs). No total, foram configurados quatro cenários, considerando os seguintes parâmetros:

Cenário 1: O primeiro cenário é aquele que não haverá nenhum dispositivo malicioso operando na rede, ele serve como base para comparações de desempenho. Na Figura 3 temos um exemplo de simulação no cenário 1, com 1000 dispositivos finais operando na rede. A figura apresenta uma barra lateral colorida, em que cada cor representa um *SF* e essas cores são refletidas nos dispositivos finais e nos atacantes. Os eixos x e y, representam a área em quilômetros, tendo como centro o *gateway*.

Figura 3 – Cenário 1 - Distribuição de 1000 dispositivos finais simulados, alocados com 5 fatores de espalhamento (SFs).

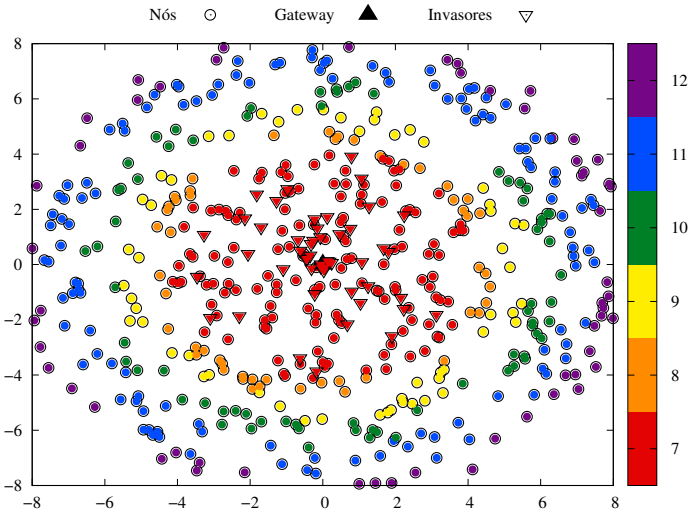


Fonte: Elaborado pelo autor

Cenário 2: No segundo cenário, todos os dispositivos maliciosos operam com o fator de espalhamento (*SF*) 7. Esse *SF* foi escolhido por proporcionar a maior taxa de transferência, permitindo que os dispositivos maliciosos enviem um grande volume de pacotes em um curto período de tempo, aumentando a taxa de ocupação do canal e o impacto do ataque. A Figura 4 ilustra uma simulação desse cenário, considerando 500 dispositivos finais legítimos, 50 dispositivos

maliciosos e um *gateway* central.

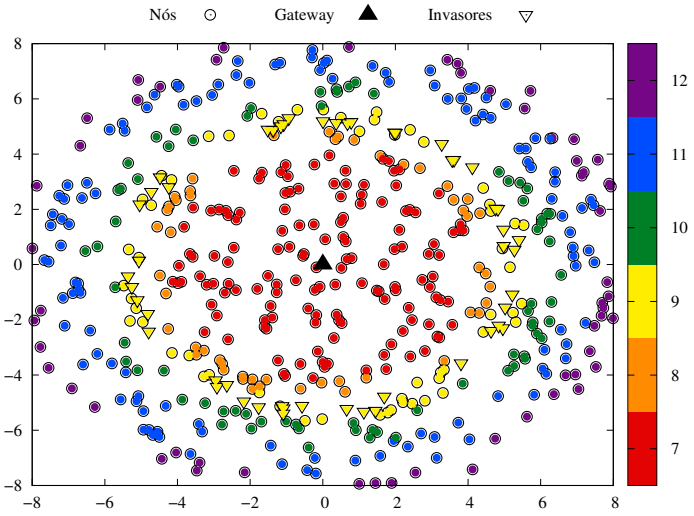
Figura 4 – Cenário 2 - Distribuição de 500 dispositivos legítimos e 50 dispositivos maliciosos operando no *SF* 7, com um *gateway* central.



Fonte: Elaborado pelo autor

Cenário 3: O terceiro cenário consiste em todos os dispositivos maliciosos operando no *SF* 9. Esse *SF* foi escolhido por ser um meio-termo entre a taxa de transferência e alcance, permitindo que os dispositivos maliciosos afetem tanto dispositivos próximos quanto distantes, aumentando a interferência em uma área maior da rede. Na Figura 5 é apresentada a topologia da rede com 500 dispositivos finais e 50 dispositivos maliciosos, correspondendo a 10% dos dispositivos finais.

Figura 5 – Cenário 3 - Distribuição de 500 dispositivos finais legítimos e 50 dispositivos maliciosos operando no *SF* 9.



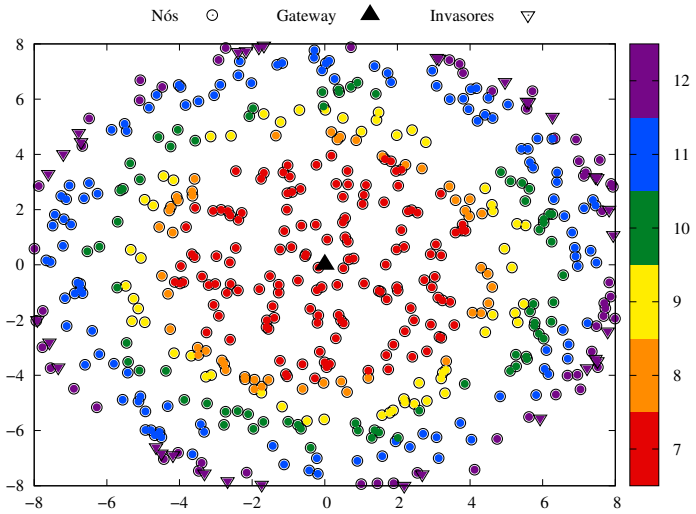
Fonte: Elaborado pelo autor

Cenário 4: No último cenário, todos os dispositivos invasores operam no *SF* 12. Esse *SF* foi escolhido por possuir o maior tempo de transmissão, ocupando o canal por tempos mais longos e reduzindo a disponibilidade da rede para outros dispositivos. Além disso, por possuir o maior alcance entre os fatores de espalhamento, esse *SF* permite que os dispositivos maliciosos afetem uma área ainda maior da rede, aumentando o impacto do ataque. A Figura 6 ilustra a disposição dos dispositivos finais e invasores, com um total de 500 dispositivos finais e 50 dispositivos atacantes.

4.3 Realização dos ataques

Nesta etapa, foram realizados os ataques em cada cenário definido na seção 4.2. Durante as simulações, dados como a quantidade de pacotes enviados, a quantidade de pacotes perdidos e o número de dispositivos conectados à rede, foram capturados para análise posterior. Para coletar os dados, foi utilizada a ferramenta *LoraPacketTracker*, disponível no módulo

Figura 6 – Cenário 4 - Distribuição espacial de 500 dispositivos legítimos, alocados com 5 fatores de espalhamento (SFs) e 50 dispositivos maliciosos operando no *SF* 12.



Fonte: Elaborado pelo autor

LoRaWAN do ns-3. Essa ferramenta contabiliza os pacotes transmitidos tanto por dispositivos legítimos quanto por dispositivos maliciosos, além de registrar os pacotes recebidos, permitindo a análise do desempenho da rede durante.

4.4 Análise estatística e visualização dos dados

Com base nos dados coletados nas simulações, foram calculadas métricas estatísticas, como a taxa de pacotes perdidos, a taxa de pacotes recebidos com sucesso e a vazão da rede em cada cenário. Utilizando os dados das simulações, também foram montados gráficos para facilitar a análise dos dados. O primeiro dado calculado foi a quantidade de pacotes perdidos, que pode ser expressado pela equação 4.1, onde P_L representa a quantidade de pacotes perdidos, P_s são os pacotes enviados e P_r os pacotes recebidos.

$$P_L = P_s - P_r \tag{4.1}$$

A segunda métrica calculada foi o *throughput* (vazão), que representa a taxa de pacotes recebidos com sucesso durante a simulação. O *throughput* é definido pela equação 4.2, onde o T_{hr} é o *throughput*, o P_r é a quantidade de pacotes recebidos e S_t é o tempo de simulação, em segundos.

$$T_{hr} = \frac{P_r}{S_t} \tag{4.2}$$

O terceiro dado calculado foi a taxa de sucesso dos pacotes. Para isso foi utilizada a equação 4.3, onde R_{suc} representa a taxa de sucesso, enquanto P_r representa a quantidade de pacotes recebidos com sucesso e P_s a quantidade de pacotes enviados.

$$R_{suc} = \frac{P_r}{P_s} \tag{4.3}$$

Para cada cenário, foram executadas cinco simulações independentes. Os valores obtidos em cada simulação foram agrupados e tratados estatisticamente, sendo a média aritmética utilizada como medida central para consolidar os dados. Essa média foi calculada para cada métrica apresentada.

Por fim, os valores médios foram utilizados para a construção dos gráficos, permitindo a comparação entre os diferentes cenários simulados.

4.5 Comparação dos dados obtidos

Após a análise dos dados, foi realizada uma comparação entre os resultados obtidos antes e durante os ataques. O objetivo dessa comparação é identificar o impacto dos ataques no desempenho da rede e determinar em que momento a degradação se tornou significativa.

5 RESULTADOS

Esta seção apresenta os resultados obtidos por meio das simulações e as análises realizadas. São discutidos os impactos dos ataques *DoS* sobre a rede, levando em consideração diferentes proporções de atacantes e variando o número de dispositivos. Os principais indicadores analisados incluem a taxa de sucesso na transmissão de pacotes e a vazão da rede, buscando identificar os pontos críticos em que o desempenho da rede é significativamente degradado. Um dos principais objetivos da análise é identificar o ponto em que os ataques as redes passam a causar dano suficiente para degradar o desempenho da rede.

A análise dos impactos dos ataques *DoS* será realizada para cada *Spread Factor* (*SF*) dentro dos cenários definidos na Seção 4.1. O *SF* é um dos principais parâmetros no funcionamento de uma rede *LoRaWAN*, influenciando diretamente a taxa de transmissão, a cobertura e a robustez contra interferências.

Cada *SF* define uma taxa de transmissão diferente: *SFs* mais baixos correspondem a taxas de transmissão mais altas, enquanto *SFs* mais altos oferecem maior alcance, mas com menor taxa de transmissão. Os dados analisados incluirão a probabilidade de sucesso, que determina a chance de um pacote enviado chegar ao *gateway*, e a taxa de transferência.

5.1 Análise no fator de espalhamento 7

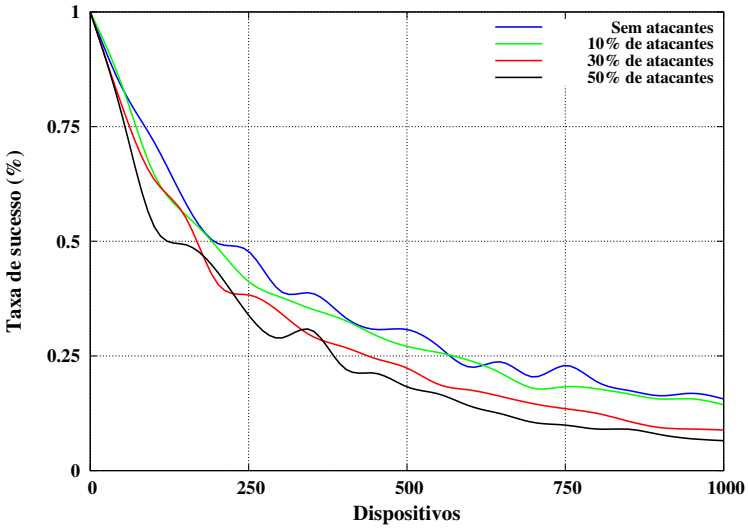
No gráfico da Figura 7, é apresentada a taxa de sucesso no *SF* 7 em dois cenários: o cenário 1 (sem atacantes) e o cenário 2 (com atacantes no *SF* 7). As porcentagens na legenda do gráfico representam a proporção de atacantes em relação ao número total de dispositivos finais utilizados no cenário 2. Observa-se que, quando 10% dos dispositivos são atacantes, a taxa de sucesso é levemente inferior ao cenário sem atacantes. Isso sugere que uma proporção de 10% de atacantes não causa um impacto significativo no desempenho da rede.

As proporções de 30% e 50% resultam em uma redução considerável na taxa de sucesso. Esse declínio ocorre porque o número de atacantes é suficientemente elevado para prejudicar o desempenho da rede. A perda de desempenho ocorre devido ao envio contínuo de pacotes pelos atacantes, o que gera congestionamento, aumentando a probabilidade de colisões e, consequentemente, a perda de pacotes.

De acordo com o gráfico, a partir de 30% de atacantes, a rede começa a perder desempenho de forma significativa, especialmente nas simulações com grande quantidade de

dispositivos.

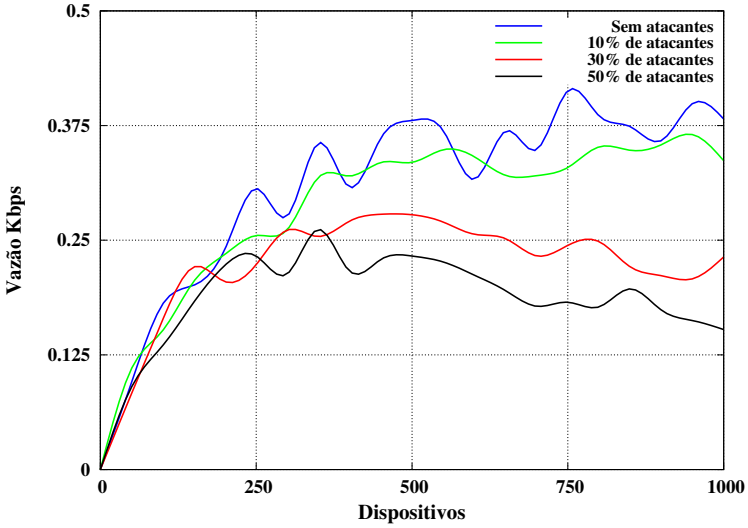
Figura 7 – Taxa de sucesso no SF 7



Fonte: Elaborado pelo autor

No gráfico da Figura 8 a vazão nos cenários que possuem a proporção de atacantes igual a 30% e 50% é menor em comparação ao cenário sem atacantes. Essa diferença se da ao grande número de dispositivos invasores no SF 7, que enviam pacotes maliciosos de forma constante, sobrecarregando a rede e reduzindo sua capacidade de transmitir dados de forma eficiente.

Figura 8 – Vazão no SF 7



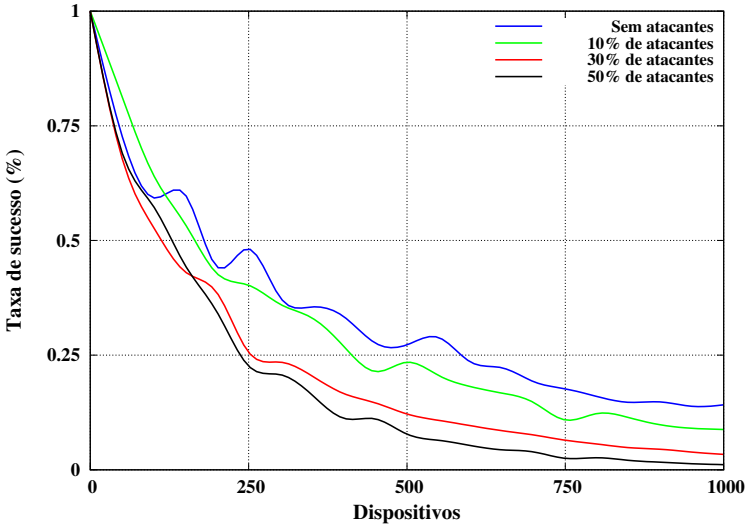
Fonte: Elaborado pelo autor

5.2 Análise no fator de espalhamento 9

No gráfico da Figura 9, o cenário com 10% de atacantes foi significativamente mais eficiente em degradar a rede se comparado ao mesmo cenário no SF 7. Isso indica que, no SF 9, os ataques foram capazes de aumentar drasticamente a taxa de colisão de pacotes, reduzindo a taxa de sucesso da rede.

Como discutido anteriormente na análise do SF 7, o envio constante de pacotes realizados pelos agentes maliciosos nesse SF, reduz consideravelmente a taxa de sucesso, devido ao aumento da possibilidade de colisões e causando a perda de pacotes.

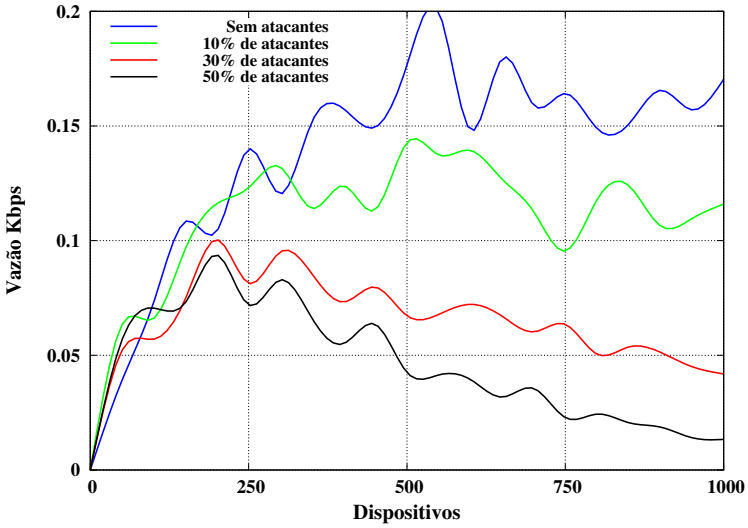
Figura 9 – Taxa de sucesso no SF 9



Fonte: Elaborado pelo autor

No gráfico da Figura 10 a vazão nos cenários que possuem atacantes é ligeiramente menor em relação ao cenário sem atacantes. Isso ocorre por causa da presença de invasores no SF 9, que enviam pacotes constantemente, sobrecarregando a rede e reduzindo seu desempenho.

Figura 10 – Vazão no SF 9

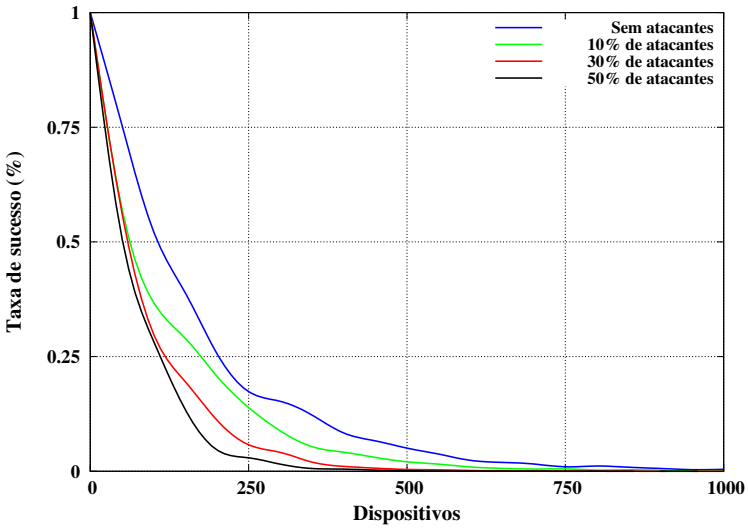


Fonte: Elaborado pelo autor

5.3 Análise no fator de espalhamento 12

Por ser o maior fator de espalhamento, o SF 12 possui o maior tempo de transmissão. No entanto, devido à duração prolongada das mensagens, a chance de colisão aumenta. Isso pode ser observado no gráfico da Figura 11, onde, mesmo na ausência de atacantes, a taxa de sucesso permaneceu baixa. Além disso, assim como no gráfico da taxa de sucesso do SF 9, a Figura 11 também mostra uma degradação significativa na taxa de sucesso à medida que a proporção de atacantes aumenta. Esse comportamento pode ser explicado pelo grande volume de pacotes enviados pelos dispositivos maliciosos, que intensificam a ocupação do canal aumentando a chance de colisões.

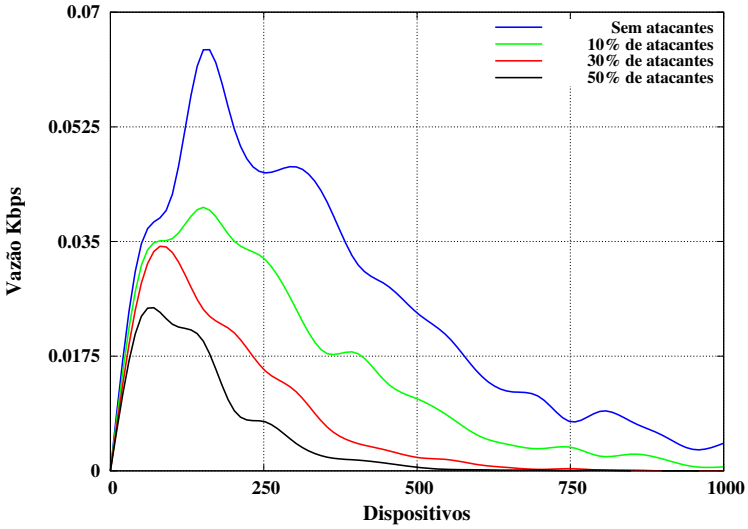
Figura 11 – Taxa de sucesso no SF 12



Fonte: Elaborado pelo autor

No gráfico da Figura 12 os cenários com atacantes possuem uma vazão consideravelmente menor. Essa queda na vazão pode ser explicada pela presença de dispositivos maliciosos no SF 12. Como foi citado anteriormente, o SF 12 possui um tempo maior de transmissão e isso o torna mais vulnerável a ataques, o que explica a drástica redução na vazão. Essa degradação significativa impacta diretamente a eficiência da rede.

Figura 12 – Vazão no SF 12



Fonte: Elaborado pelo autor

6 CONCLUSÕES

Este trabalho apresentou a simulação e análise de cenários que utilizam a tecnologia *LoRaWAN*, amplamente empregada atualmente devido ao seu longo alcance e baixo consumo de energia. No entanto, justamente por seu baixo consumo de energia, essa tecnologia carece de implementações robustas de medidas de segurança que garantam o bom funcionamento de seus dispositivos em caso de ataques. Diante disso, este trabalho realizou simulações em que diversos dispositivos maliciosos enviavam pacotes constantemente para a rede em um curto intervalo de tempo, com o objetivo de gerar congestionamento e, consequentemente, a perda de pacotes.

Para as simulações, o número de dispositivos finais foi aumentado gradualmente em incrementos de 50 até atingir o limite de 1000 dispositivos. Já o número de dispositivos maliciosos foi definido como uma proporção dos dispositivos finais, sendo utilizadas as proporções de 10%, 30% e 50%.

Para realizar a simulação descrita foi utilizado o simulador de redes de computadores ns-3 em conjunto com o módulo *LoRa*, que foi desenvolvido por um grupo de pesquisa da Universidade de Padova (Magrin *et al.*, 2017). Esse módulo também foi adaptado nesse trabalho para a adição de dispositivos maliciosos. Após a simulação foram coletados dados relacionados ao desempenho da rede, como a taxa de sucesso dos pacotes e a vazão, essas métricas foram apresentadas para cada SF.

A análise concluiu que, para o SF 7, a presença de 10% de dispositivos atacantes foi praticamente insignificante para o desempenho da rede. No entanto, isso não se repetiu para os demais SFs, onde a mesma porcentagem de atacantes já causou uma queda no desempenho. Também foi possível concluir que a proporção mínima de atacantes que começa a impactar significativamente o desempenho da rede é de 30%. Em todos os SFs atacados, ficou evidente que a partir dessa proporção de atacantes o desempenho da rede sofreu uma queda acentuada.

REFERÊNCIAS

ARAS, E.; SMALL, N.; RAMACHANDRAN, G. S.; DELBRUEL, S.; JOOSEN, W.; HUGHES, D. Selective jamming of lorawan using commodity hardware. **MobiQuitous 2017: Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services**, Association for Computing Machinery, New York, NY, USA, p. 363–372, 2017.

BUTUN, I.; PEREIRA, N.; GIDLUND, M. Analysis of lorawan v1. 1 security. **Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects**. [*S. l.*: *s. n.*], 2018. p. 1–6.

CAMPANILE, L.; GRIBAUDO, M.; IACONO, M.; MARULLI, F.; MASTROIANNI, M. Computer network simulation with ns-3: A systematic literature review. **Electronics**, v. 9, n. 2, 2020. ISSN 2079-9292.

CHACKO, S.; JOB, M. D. Security mechanisms and vulnerabilities in lpwan. **IOP Conference Series: Materials Science and Engineering**, IOP Publishing, v. 396, n. 1, p. 012027, aug 2018.

CHAUDHARI, B. S.; ZENNARO, M.; BORKAR, S. Lpwan technologies: Emerging application characteristics, requirements, and design considerations. **Future Internet**, v. 12, n. 3, 2020. ISSN 1999-5903.

CISA. **Understanding Denial-of-Service Attacks**. CISA, 2021. Disponível em: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks. Acesso em: Acesso em: 25 abr. 2023.

ES, E. van; VRANKEN, H.; HOMMERSOM, A. Denial-of-service attacks on lorawan. **Proceedings of the 13th International Conference on Availability, Reliability and Security**. New York, NY, USA: Association for Computing Machinery, 2018. (ARES 2018). ISBN 9781450364485.

FRUHLINGER, J. **The CIA triad**: Definition, components and examples. Josh Fruhlinger, 2020. Disponível em: https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html. Acesso em: Acesso em: 10 out. 2024.

HESSEL, F.; ALMON, L.; ÁLVAREZ, F. Chirpotle: A framework for practical lorawan security evaluation. **Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks**. New York, NY, USA: Association for Computing Machinery, 2020. (WiSec '20), p. 306–316. ISBN 9781450380065.

HESSEL, F.; ALMON, L.; HOLLICK, M. Lorawan security: An evolvable survey on vulnerabilities, attacks and their systematic mitigation. **ACM Trans. Sen. Netw.**, Association for Computing Machinery, New York, NY, USA, v. 18, n. 4, mar 2023. ISSN 1550-4859.

ISO. **Security techniques — Information security management systems**. ISO/IEC 27000:2018(en). Vernier, Geneva, Switzerland: International Organization for Standardization, 2018. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en. Acesso em: Acesso em: 10 out. 2024.

KUNTKE, F.; ROMANENKO, V.; LINSNER, S.; STEINBRINK, E.; REUTER, C. Lorawan security issues and mitigation options by the example of agricultural iot scenarios. **Transactions on Emerging Telecommunications Technologies**, v. 33, n. 5, p. e4452, 2022.

LORA-ALLIANCE. **LoRaWAN L2 1.0.4 Specification**. Lora Alliance, 2020. Disponível em: https://lora-alliance.org/wp-content/uploads/2021/11/LoRaWAN-Link-Layer-Specification-v1.0.4.pdf. Acesso em: Acesso em: 10 abr. 2023.

MAGRIN, D.; CENTENARO, M.; VANGELISTA, L. Performance evaluation of lora networks in a smart city scenario. IEEE. **2017 IEEE International Conference on Communications (ICC)**. [*S. l.*], 2017. p. 1–7.

NAIK, N. Lpwan technologies for iot systems: choice between ultra narrow band and spread spectrum. IEEE. **2018 IEEE international systems engineering symposium (ISSE)**. [*S. l.*], 2018. p. 1–8.

NETWORKS, P. **What is a denial of service attack (DoS) ?** Paloalto Networks, 2020. Disponível em: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. Acesso em: Acesso em: 25 abr. 2023.

RILEY, G. F.; HENDERSON, T. R. The ns-3 network simulator. **Modeling and Tools for Network Simulation**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. cap. 2, p. 15–34. ISBN 978-3-642-12331-3.

SEMTECH. **LoRa® and LoRaWAN®**: A technical overview. Semtech, 2019. Disponível em: https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf. Acesso em: Acesso em: 10 abr. 2023.

SIMULATOR, N. **ns-3 Tutorial**. Network Simulator, 2023. Disponível em: https://www.nsnam.org/docs/release/3.38/tutorial/ns-3-tutorial.pdf. Acesso em: Acesso em: 10 mai. 2023.

SOBIN, C. C. A survey on architecture, protocols and challenges in iot. **Wireless Personal Communications**, v. 112, n. 3, p. 1383–1429, June 2020. ISSN 1572-834X.

STALLING, W. **Criptografia e segurança de redes**: princípios e práticas. SP, Brasil: Pearson Education do Brasil, 2015. 6–34 p. ISBN 978-85-430-1450-0.

THOMAS, A.; ELDHOSE, N. Scalability concerns of chirp spread spectrum for lpwan applications. **IJASUC**, v. 10, p. 1–11, 2019.

WHITMAN, M. E.; MATTORD, H. J. Principles of information security, fourth edition. **Principles of Information Security, Fourth Edition**. Boston, MA: Course Technology, 2011. p. 8–34. ISBN 978-1-111-13821-9.

YANG, X.; KARAMPATZAKIS, E.; DOERR, C.; KUIPERS, F. Security vulnerabilities in lorawan. **2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)**. [*S. l.*: *s. n.*], 2018. p. 129–140.