Proteção de Dados em Dispositivos IoT em Redes LoRaWAN

Roni Rodrigues[1], Claudia Aparecida Martins[1], Nelcileno Virgílio de Souza Araújo[1], Constantino Dias da Cruz Neto[2]

[1]Instituto de Computação – Universidade Federal de Mato Grosso (UFMT)
CEP: 78060-900 – Cuiabá – MT – Brasil

[2]Instituto Federal de Educação Ciência e Tecnologia de Mato Grosso
CEP: 78005-200 – Cuiabá, MT - Brasil

roni.rodrigues@live.com, {claudia, nelcileno}@ic.ufmt.br,
constantino.neto@ifmt.edu.br

Abstract. *Low Power Wide Area Networks (LPWAN), such as LoRaWAN, are widely used in IoT applications but face significant security challenges. The objective of this study is to map the main vulnerabilities in LoRaWAN networks, identify the proposed solutions, and highlight existing gaps, contributing to the security and reliability of these networks. The results include the identification of vulnerabilities such as jamming, packet replay, spoofing, and DDoS attacks, as well as the analysis of solutions like dynamic key management (OTAA), the CRAM protocol, and the REBEB algorithm. Promising trends, such as the use of machine learning, are also highlighted for enabling more adaptive approaches.*

Resumo. *As redes de baixa potência e longo alcance (LPWAN), como o LoRaWAN, são amplamente usadas em aplicações IoT, mas enfrentam desafios em segurança. O objetivo do trabalho é mapear as principais vulnerabilidades em redes LoRaWAN, identificar as soluções propostas e destacar as lacunas existentes, contribuindo para a segurança e confiabilidade dessas redes. Os resultados incluem a identificação de vulnerabilidades como jamming, replay de pacotes, spoofing e DDoS, além da análise de soluções como o gerenciamento dinâmico de chaves (OTAA), o protocolo CRAM e o algoritmo REBEB. Destacam-se tendências promissoras, como o aprendizado de máquina, para abordagens mais adaptativas.*

1. Introdução

As redes de baixa potência e longa distância *Low Power Wide Area Network* (LPWAN) surgem como uma solução indispensável para a conectividade de dispositivos de Internet das Coisas (IoT), especialmente em aplicações que demandam grande cobertura geográfica aliada a baixo consumo de energia [LoRa Alliance 2024]. Entre as tecnologias LPWAN, o LoRaWAN se destaca pelo uso eficiente do espectro e pelo alcance estendido, sendo amplamente adotado em setores como indústrias, agricultura e cidades inteligentes. Além de sua eficiência energética, o LoRaWAN oferece comunicação bidirecional, segurança ponta a ponta, suporte à mobilidade e serviços de localização [LoRa Alliance 2024].

Essa tecnologia baseia-se na modulação *Chirp Spread Spectrum* (CSS), que proporciona resistência a interferências e viabiliza a transmissão de sinais fracos com

baixo consumo energético, tornando-a especialmente adequada para dispositivos IoT de longa duração [Chacko and Job 2018]. Em comparação com outras tecnologias sem fio, como *Wi-Fi* e *Bluetooth*, o LoRaWAN apresenta maior alcance e eficiência energética [Al-Shareeda et al. 2023]. Contudo, sua ampla cobertura e o uso de espectro não licenciado trazem desafios significativos em termos de segurança, como ataques de retransmissão e interferência por *jamming*[1].

Na Figura 1 é ilustrada a arquitetura típica de uma rede LoRaWAN, desde os nós sensores até as aplicações de usuário final. Essa estrutura destaca o fluxo de dados, que inicia nos dispositivos IoT conectados aos *gateways* via LoRa, é enviado para a nuvem utilizando protocolos TCP/IP e, finalmente, é acessado pelas aplicações de usuário. Essa arquitetura reflete a flexibilidade e escalabilidade da tecnologia em aplicações IoT [Ramos et al. 2020].

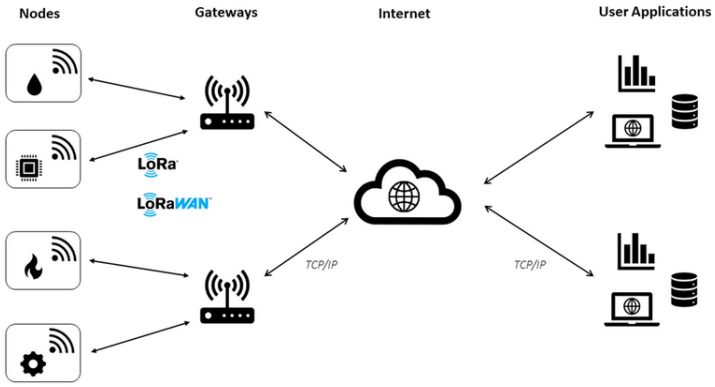

Figura 1. Arquitetura geral de comunicação LoRaWAN. Adaptado de Ramos et al. (2020) [Ramos et al. 2020].

Neste contexto, este artigo consiste na revisão e investigação sobre segurança em redes LoRaWAN, com o objetivo de identificar vulnerabilidades e soluções propostas na literatura. Além de mapear os principais desafios enfrentados, o estudo foca em algoritmos e abordagens que buscam mitigar riscos e aprimorar a segurança operacional desses dispositivos. Assim, espera-se contribuir para a consolidação de práticas que promovam maior confiabilidade no uso de redes LoRaWAN em aplicações IoT. Para garantir a reprodutibilidade desta revisão sistemática, o protocolo de busca e os dados extraídos foram disponibilizados em um repositório online público[2].

Este artigo está estruturado em seções que abordam de forma sistemática os aspectos fundamentais e aplicados da segurança em redes LoRaWAN. Na Seção de Metodologia são detalhados os critérios adotados para o levantamento sistemático da literatura e a seleção das soluções analisadas. Na Seção de Fundamentação Teórica, exploram-se os conceitos essenciais sobre redes LoRaWAN e seus desafios de segurança. Nas Seções de Vulnerabilidades Identificadas e Soluções Propostas são discutidas, respectivamente, as principais falhas de segurança observadas na literatura e as abordagens sugeridas para

[1]Ataques de *jamming* ocorrem quando um invasor transmite sinais de rádio potentes para interferir nas comunicações legítimas da rede [Chacko and Job 2018].

[2]Disponível em: `https://drive.google.com/drive/folders/1Xvj7SPnJ12OiXrUh45DFloSczlHsIbGi?usp=sharing`

mitigá-las. Na Seção de Discussão são analisadas as tendências, lacunas e soluções, enquanto na Seção de Conclusão e Trabalhos Futuros são sintetizados os resultados, destacando propostas para avanços na segurança de redes LoRaWAN.

2. Metodologia

Neste trabalho, adotou-se uma abordagem de revisão sistemática do estado da arte, inspirada no protocolo *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) [Moher et al. 2009], para identificar e analisar vulnerabilidades e soluções de segurança em redes LoRaWAN. O objetivo central é mapear as principais vulnerabilidades de segurança e identificar soluções propostas para mitigar esses problemas. Para isso, perguntas de pesquisa foram formuladas, como: quais são as vulnerabilidades mais comuns em redes LoRaWAN, quais soluções têm sido propostas para corrigi-las e quais lacunas ainda existem na segurança dessas redes.

Os critérios de inclusão abrangeram artigos publicados nos últimos cinco anos, com foco em segurança de redes LPWAN, especialmente LoRaWAN, revisados por pares e disponíveis em inglês ou português. Por outro lado, foram excluídos trabalhos que abordassem redes IoT fora do escopo LPWAN, como Wi-Fi e 5G, que carecessem de validação prática ou que não detalhassem soluções de segurança. Para a coleta de dados, foram utilizadas bases de dados renomadas, como IEEE Xplore, ACM Digital Library e ScienceDirect. A busca foi realizada com termos como ”LoRaWAN security”, ”LoRa vulnerabilities”e ”LPWAN security solutions”.

O processo de seleção incluiu filtragem dos artigos por título, resumo e texto completo, e a extração dos dados abrangeu informações como vulnerabilidades identificadas, soluções propostas e seus impactos sobre desempenho e segurança. Os dados extraídos foram então analisados e sintetizados, categorizando os artigos por tipo de vulnerabilidade abordada, solução proposta e validação prática. Essa análise buscou identificar padrões, lacunas e tendências emergentes na segurança de redes LoRaWAN.

Após a escrita do artigo, visando melhorar a clareza e a qualidade da redação do texto final, foi utilizado um modelo de inteligência artificial generativa para correção textual, incluindo verificação de consistência, gramática e estilo acadêmico. Essa etapa visou otimizar a apresentação dos resultados, assegurando que a comunicação das ideias já escritas fosse precisa e alinhada às melhores práticas editoriais.

3. Fundamentação Teórica

A segurança em redes de longa distância e baixa potência, como o LoRaWAN, é um tema cada vez mais relevante no contexto da Internet das Coisas (IoT). Essas redes têm se destacado por seu alcance estendido e consumo energético reduzido, permitindo a conexão de dispositivos em larga escala em áreas urbanas e rurais [LoRa Alliance 2024]. O LoRaWAN, em particular, utiliza a modulação *Chirp Spread Spectrum* (CSS), que proporciona uma alta resistência a interferências e torna a tecnologia ideal para aplicações que exigem comunicação confiável em distâncias maiores [Chacko and Job 2018].

Apesar de suas vantagens, o LoRaWAN enfrenta desafios significativos relacionados à segurança. A comunicação em espectro não licenciado e a ausência de mecanismos robustos de autenticação e criptografia tornam a rede suscetível a ataques como *jamming*

e *replay* de pacotes [Al-Shareeda et al. 2023]. Estudos como os de Hayati et al. (2022) propõem soluções para mitigar essas vulnerabilidades, como a atualização dinâmica de chaves na camada física, utilizando algoritmos leves para atender às limitações de processamento e energia dos dispositivos IoT [Hayati et al. 2022].

Outra abordagem relevante é a integração de *Blockchain* em redes LoRaWAN, como discutido por Saputro e Sari (2022). Essa tecnologia adiciona uma camada de segurança ao fornecer integridade de dados e autenticação descentralizada, reduzindo o risco de manipulação de pacotes e de ataques maliciosos [Saputro and Sari 2022]. Por sua vez, em Wong et al. (2024) é mostrado o uso de aprendizado de máquina para a detecção de anomalias e otimização de rotas em redes LoRa *multi-hop*, abordando vulnerabilidades relacionadas à escalabilidade e ao gerenciamento de tráfego [Wong et al. 2024].

Portanto, na literatura é evidenciado que, embora existam soluções promissoras para melhorar a segurança em redes LoRaWAN, ainda há lacunas importantes a serem exploradas. Este trabalho busca sintetizar essas contribuições, identificando as principais vulnerabilidades e as abordagens mais eficazes para enfrentá-las, promovendo um avanço nas práticas de proteção para redes IoT baseadas em LoRaWAN.

4. Vulnerabilidades Identificadas em Redes LoRaWAN

As redes LoRaWAN, amplamente utilizadas em aplicações IoT, enfrentam vulnerabilidades significativas que podem comprometer a segurança e a confiabilidade das comunicações. Um dos problemas mais críticos é o ataque de *jamming*, como destacado por Szewczyk et al. (2022). Esse ataque explora o longo tempo de transmissão das mensagens em LoRaWAN, que pode variar de 900 milissegundos a 1,2 segundos. Durante esse intervalo, a rede torna-se suscetível a interferências deliberadas, onde um invasor transmite sinais de alta potência para bloquear ou interromper a comunicação. Essa vulnerabilidade é ainda mais problemática em cenários de alta densidade de dispositivos, nos quais a interrupção de um único *gateway* pode comprometer a conectividade de múltiplos nós IoT [Szewczyk et al. 2022].

As vulnerabilidades identificadas podem ser classificadas em níveis conforme sua criticidade: de alto impacto (*jamming*, *spoofing*, DDoS), médio impacto (*replay* de pacotes, vazamento de informações) e baixo impacto (interferência por ADR). Essa categorização visa auxiliar na priorização de medidas de mitigação em projetos com restrições de recursos.

Outro aspecto crítico é a fragilidade da criptografia AES128, que, embora amplamente utilizada por sua eficiência, apresenta limitações quando aplicada a redes LoRaWAN. A implementação padrão com mensagens de tamanho fixo facilita ataques direcionados, uma vez que adversários podem explorar padrões previsíveis na comunicação. Dispositivos IoT conectados a redes LoRaWAN, frequentemente limitados em capacidade de processamento, não conseguem implementar versões mais robustas do AES, tornando-se alvos fáceis de ataques como força bruta e intercepção [Szewczyk et al. 2022]. Esse cenário é agravado em redes onde os dispositivos têm recursos computacionais mínimos, o que restringe a aplicação de técnicas de segurança avançadas.

A vulnerabilidade a ataques de repetição, ou *replay*, também é um problema recorrente. Nesse tipo de ataque, invasores capturam pacotes legítimos transmitidos na rede

e os retransmitem para explorar a previsibilidade das comunicações. Segundo Szewczyk et al. (2022), essa prática compromete tanto a integridade quanto a autenticidade das mensagens, permitindo que invasores manipulem dados ou até mesmo assumam controle de dispositivos IoT [Szewczyk et al. 2022]. Essa vulnerabilidade é exacerbada pela falta de mecanismos de autenticação robusta, o que impede a rede de verificar a origem dos pacotes recebidos.

A função *Adaptive Data Rate* (ADR), projetada para otimizar a eficiência e a cobertura das redes LoRaWAN, apresenta vulnerabilidades específicas. Dispositivos mais distantes do *gateway* precisam aumentar o tempo de transmissão para alcançar a cobertura necessária, o que cria uma maior janela de exposição a ataques. Como observado por Szewczyk et al. (2022), esse comportamento não apenas amplifica os riscos de *jamming*, mas também pode ser explorado por atacantes para sobrecarregar a rede com tráfego falso ou mensagens manipuladas [Szewczyk et al. 2022]. Além disso, o ADR não incorpora verificações de segurança suficientes para mitigar essas ameaças, deixando a rede ainda mais exposta.

Hayati et al. (2022) apontam para a reutilização de chaves de sessão e a baixa aleatoriedade na geração dessas chaves como outra vulnerabilidade crítica em redes LoRaWAN. Essas práticas expõem os dispositivos IoT a vazamentos de dados sensíveis, já que chaves previsíveis podem ser facilmente exploradas por invasores para interceptar e decodificar comunicações [Hayati et al. 2022]. A reutilização de chaves em várias sessões aumenta a probabilidade de comprometimento, especialmente em redes de grande escala, onde o gerenciamento seguro de chaves é mais desafiador.

Por fim, vulnerabilidades como ataques de *spoofing*, *wormholes* e *flooding* foram amplamente discutidas por Wong et al. (2024) no contexto de redes LoRaWAN *multi-hop* e em malha. Esses ataques aproveitam falhas no gerenciamento de tráfego e nas rotas para manipular os dados transmitidos ou sobrecarregar os recursos da rede. O *spoofing*, por exemplo, permite que invasores se passem por dispositivos legítimos, enquanto ataques de *wormholes* criam rotas maliciosas para redirecionar pacotes e comprometer a integridade dos dados. O *flooding*, por sua vez, inunda a rede com tráfego falso, resultando em consumo excessivo de energia e degradação do desempenho [Wong et al. 2024]. Esses problemas refletem a necessidade de soluções mais robustas e integradas para proteger as redes LoRaWAN contra múltiplos vetores de ataque.

As vulnerabilidades mencionadas não apenas evidenciam os desafios das redes LoRaWAN, mas também apontam para a necessidade de avanços na implementação de soluções que conciliem segurança com as limitações de recursos dos dispositivos IoT.

5. Soluções Propostas na Literatura

Diversas soluções têm sido propostas para mitigar as vulnerabilidades presentes em redes LoRaWAN, cada uma com diferentes abordagens para resolver problemas específicos de segurança. Szewczyk et al. (2022) destacam o uso do método de ativação *Over-the-Air Activation* (OTAA) como uma solução robusta para a atualização dinâmica de chaves de sessão. Essa técnica reduz consideravelmente a vulnerabilidade a ataques de interceptação e *replay*, pois as chaves são renovadas a cada nova conexão, dificultando que invasores explorem dados capturados anteriormente. Além disso, os autores recomendam o uso do gerenciamento de chaves baseado na camada física (PHYSEC), que utiliza as proprieda-

des físicas do canal de comunicação para gerar e autenticar chaves. Essa abordagem não apenas aumenta a segurança, mas também minimiza o impacto no consumo energético dos dispositivos IoT, um aspecto crítico em redes LoRaWAN, onde a eficiência energética é essencial [Szewczyk et al. 2022].

Ahmar et al. (2022) propõem o protocolo *Cryptographic Frequency Hopping Medium Access Control* (CRAM), que se destaca por sua capacidade de mitigar ataques de *jamming* seletivo. O protocolo utiliza uma técnica de *hopping* de frequência criptográfica, onde os dados são transmitidos em diferentes frequências de forma aleatória e sincronizada. Isso dificulta a previsão dos canais de comunicação pelos invasores, reduzindo significativamente a eficácia dos ataques. Além de melhorar a resistência contra *jamming*, o CRAM também aumenta a escalabilidade da rede em ambientes densos, evitando colisões de mensagens e otimizando o uso do canal [Ahmar et al. 2023].

Para solucionar vulnerabilidades relacionadas à geração e gerenciamento de chaves, Hayati et al. (2022) introduzem um esquema baseado no algoritmo Photon-256 truncado. Essa abordagem visa resolver problemas como a baixa aleatoriedade e a reutilização de chaves, fatores que comprometem a confidencialidade das comunicações em LoRaWAN. O Photon-256 gera chaves únicas para cada sessão, reduzindo drasticamente o risco de vazamento de informações e a possibilidade de ataques de interceptação e *replay*. Essa técnica é especialmente relevante em cenários de grande escala, no qual o gerenciamento seguro de chaves é mais desafiador [Hayati et al. 2022].

Saputro e Sari (2022) sugerem o uso de *blockchain* integrado a uma topologia de névoa para autenticação descentralizada e proteção contra ataques DDoS. O modelo conhecido como *Lightweight Multi-Fog* (LMF) utiliza contratos inteligentes para autenticar dispositivos e controlar o tráfego de dados de forma eficiente. Essa abordagem torna a rede mais resiliente a sobrecargas, mantendo a integridade e disponibilidade dos serviços, mesmo em cenários de ataques de alta intensidade. A descentralização proporcionada pelo *blockchain* também elimina pontos únicos de falha, melhorando a segurança geral da rede [Saputro and Sari 2022].

Entre as soluções mais inovadoras, Zhihan et al. (2022) propõem o algoritmo REBEB, que combina codificação de dados com aprendizado de máquina para detectar padrões de tráfego anômalos. Essa abordagem é eficaz contra ataques de interceptação, *replay* e *jamming*, utilizando técnicas de aprendizado supervisionado para identificar desvios nos padrões esperados de comunicação. O REBEB se mostrou particularmente eficiente em aplicações críticas, como em cidades inteligentes, onde a confiabilidade e resiliência das redes LPWAN são essenciais [LyuLiang et al. 2021].

Mousavi et al. (2022) introduzem o protocolo C-LoRa, que combina espectro licenciado e não licenciado com alocação cognitiva de espectro. Essa solução otimiza o uso dos canais disponíveis, reduzindo interferências e melhorando a eficiência espectral, um problema comum em redes LoRaWAN densas. A abordagem também aumenta a qualidade do serviço (QoS) ao priorizar tráfegos críticos, como em aplicações de tempo real [Mousavi et al. 2022].

Han et al. (2022) apresentam um esquema inovador de geração de chaves seguras baseado no indicador de força do sinal recebido (RSSI). Esse método explora as propriedades do canal de comunicação para gerar chaves dinâmicas, protegendo contra ataques

de interceptação e melhorando a segurança em comunicações veículo-a-veículo (V2V) e veículo-a-infraestrutura (V2I). O esquema também utiliza um protocolo aprimorado de acordo de chaves, chamado Cascade, que aumenta a taxa de geração de chaves enquanto minimiza vazamentos de informações [Han et al. 2021].

Por fim, Wong et al. (2024) sugerem o uso de aprendizado de máquina para melhorar a segurança e a eficiência em redes *multi-hop*. A técnica permite a detecção de tráfego anômalo e otimiza a seleção de rotas, mitigando vulnerabilidades como ataques de *wormholes* e *flooding*. Mai et al. (2022) complementam essa abordagem com uma arquitetura de fatiamento de rede baseada em *Software-Defined Networking* (SDN), que melhora a alocação de recursos, garantindo maior eficiência energética e confiabilidade [Wong et al. 2024, Mai et al. 2022].

Essas soluções refletem o avanço da literatura na busca por abordagens diversificadas para proteger redes LoRaWAN. No entanto, muitas delas ainda carecem de validação prática e integração em sistemas unificados, o que representa uma lacuna significativa na área. A escolha da solução ideal deve considerar não apenas sua eficácia contra vulnerabilidades específicas, mas também sua viabilidade de implementação em cenários reais.

6. Discussão

A análise das soluções propostas na literatura revela avanços importantes na segurança de redes LoRaWAN, mas também evidencia desafios significativos, conforme mostrado na Tabela 1. Entre as soluções, destaca-se o algoritmo REBEB, proposto por Zhihan et al. (2022), como uma das abordagens mais abrangentes. O REBEB utiliza aprendizado de máquina para detectar padrões anômalos no tráfego da rede e combina essa capacidade com codificação de dados, o que lhe permite lidar com múltiplas vulnerabilidades, como *jamming*, *replay* de pacotes, *spoofing* e vazamento de informações. Sua abordagem integrada é particularmente valiosa para cenários de alta criticidade, como cidades inteligentes, considerando que a confiabilidade e segurança são essenciais. Ao corrigir mais vulnerabilidades que outras soluções, o REBEB se posiciona como um exemplo promissor de como técnicas de aprendizado de máquina podem ser aplicadas em redes IoT.

Outras soluções seguem abordagens mais especializadas. Por exemplo, o protocolo CRAM de Ahmar et al. (2022) foi projetado especificamente para mitigar ataques de *jamming* seletivo, utilizando *hopping* de frequência criptográfico para aumentar a resistência da rede contra interferências. Já o OTAA, discutido por Szewczyk et al. (2022), é uma solução eficiente para lidar com ataques de *replay*, proporcionando a atualização dinâmica de chaves de sessão. Embora eficiente em seu propósito, o OTAA não aborda outras vulnerabilidades, como *spoofing* ou ataques de DDoS. Da mesma forma, o Photon-256, proposto por Hayati et al. (2022), reforça a segurança contra vazamento de informações e *replay* ao gerar chaves únicas, mas carece de uma aplicação mais ampla para múltiplas vulnerabilidades.

Na Tabela 2 é possível perceber que, embora algumas soluções como o *Blockchain* LMF de Saputro e Sari (2022) apresentem potencial para mitigar várias vulnerabilidades (como DDoS e *spoofing*), outras são limitadas a cenários específicos. Por exemplo, a abordagem baseada em RSSI de Han et al. (2022) é eficaz para mitigar *spoofing*, mas não aborda ataques como *flooding* ou *wormholes*. Soluções que combinam múltiplas técnicas,

Tabela 1. Comparativo de Vulnerabilidades e Soluções em Redes LoRaWAN

Vulnerabilidade	Solução	Cobertura do Problema
Jamming	Protocolo CRAM (Ahmar et al., 2022), REBEB (Zhihan et al., 2022)*, Aprendizado de Máquina (Wong et al., 2024)*	Reduz ataques seletivos com *hopping* criptográfico, aprendizado de máquina e análise de tráfego anômalo.
Replay de pacotes	OTAA (Szewczyk et al., 2022), Photon-256 (Hayati et al., 2022)*, REBEB (Zhihan et al., 2022)*	Atualização dinâmica de chaves e geração de chaves únicas reduzem previsibilidade e vulnerabilidade a interceptações.
Interferência por ADR	C-LoRa (Mousavi et al., 2022)*	Alocação cognitiva de espectro reduz interferências e otimiza comunicação.
Spoofing e falsificação	*Blockchain* LMF (Saputro e Sari, 2022)*, REBEB (Zhihan et al., 2022)*	A autenticação descentralizada e técnicas de aprendizado de máquina melhoram a integridade dos dispositivos conectados.
Ataques DDoS	*Blockchain* LMF (Saputro e Sari, 2022)*	Resiliência a sobrecarga em dispositivos e comunicação de dados.
Vazamento de informações	Photon-256 (Hayati et al., 2022)*, REBEB (Zhihan et al., 2022)*	Geração de chaves seguras e aprendizado de máquina protegem contra acessos não autorizados.
Wormholes e *flooding*	Aprendizado de Máquina (Wong et al., 2024)*	Melhora a detecção de tráfego anômalo e identifica ataques de manipulação de rotas.

como o C-LoRa de Mousavi et al. (2022), que otimiza espectro e reduz interferências, mostram que abordagens integradas têm grande potencial para resolver múltiplos problemas, embora ainda careçam de validação prática em ambientes reais.

Tabela 2. Relação entre Vulnerabilidades e Soluções em Redes LoRaWAN

Vulnerabilidade	CRAM (Ahmar)	OTAA (Szewczyk)	Photon-256 (Hayati)	C-LoRa (Mousavi)	Blockchain LMF (Saputro)	ML (Wong)	REBEB (Zhihan)	RSSI (Han)
Jamming	X			X		X	X	
Replay de pacotes		X	X				X	
Interferência por ADR				X				
Spoofing e falsificação					X		X	X
Ataques *DDoS*					X			
Vazamento de informações			X				X	
Wormholes e *flooding*						X		

Além disso, as lacunas na pesquisa continuam significativas. Apesar do avanço em técnicas de aprendizado de máquina, como as destacadas por Wong et al. (2024), sua implementação prática em dispositivos IoT é limitada devido aos recursos computacionais restritos. A necessidade de integrar essas abordagens em um modelo unificado permanece evidente, já que a maioria das soluções atuais aborda vulnerabilidades de forma isolada. Por exemplo, enquanto o REBEB se destaca por sua abrangência, ele ainda depende de testes mais amplos para validar sua eficiência energética e viabilidade operacional em redes LoRaWAN reais.

A discussão reflete que, embora soluções como REBEB e *Blockchain* LMF demonstrem alto potencial, os desafios de integração e validação prática permanecem críticos. O desenvolvimento de abordagens mais unificadas, que combinem o melhor de

cada técnica sem sobrecarregar os dispositivos IoT, é uma direção promissora para pesquisas futuras. Além disso, a necessidade de abordar vulnerabilidades emergentes, como ataques de DDoS distribuído e manipulação de rotas, reforça a urgência de soluções mais robustas e adaptativas.

Uma direção promissora seria a combinação de abordagens complementares, como a integração do CRAM com o REBEB, que pode unir a mitigação eficiente de *jamming* com a detecção de tráfego anômalo. Arquiteturas híbridas que combinem aprendizado de máquina com técnicas de autenticação baseadas em *Blockchain* também podem oferecer maior robustez frente a múltiplos vetores de ataque, especialmente em cenários de alta densidade e criticidade.

7. Conclusão

O levantamento realizado identificou sete principais vulnerabilidades em dispositivos IoT conectados a redes LoRaWAN, incluindo ataques de *jamming*, *replay* de pacotes, *spoofing* e vazamento de informações. Foram encontradas e discutidas nove soluções propostas na literatura, como o gerenciamento dinâmico de chaves, o uso de aprendizado de máquina para detecção de anomalias e protocolos especializados como o CRAM e o REBEB. Essas soluções representam avanços significativos, mas ainda enfrentam desafios para validação prática e integração em sistemas reais.

Apesar de algumas abordagens, como o *Blockchain* LMF [Saputro and Sari 2022] e o Photon-256 [Hayati et al. 2022], apresentarem a capacidade de mitigar múltiplas vulnerabilidades, sua eficácia foi amplamente avaliada apenas em ambientes simulados, sem levar em conta restrições energéticas e operacionais de dispositivos IoT em redes LoRaWAN reais. Além disso, soluções como o CRAM [Ahmar et al. 2023], embora eficazes contra ataques de *jamming*, não abordam problemas como vazamento de informações ou ataques de repetição, o que ressalta a necessidade de modelos mais abrangentes. A falta de integração entre abordagens distintas também limita o desenvolvimento de sistemas unificados e eficientes.

Embora este estudo tenha um enfoque técnico, destaca-se que a adoção dessas soluções em países como o Brasil pode enfrentar desafios relacionados à infraestrutura de conectividade, heterogeneidade de dispositivos e limitações energéticas em áreas remotas. Esses fatores reforçam a necessidade de desenvolver abordagens que considerem não apenas a robustez das soluções, mas também sua viabilidade operacional em contextos diversos e em cenários de conectividade limitada.

Para trabalhos futuros, recomenda-se a implementação prática de soluções como o PHYSEC e o aprendizado de máquina em ambientes reais, permitindo a avaliação de sua eficácia, impacto no consumo energético e viabilidade operacional. O desenvolvimento de uma solução integrada, que combine o gerenciamento dinâmico de chaves com detecção inteligente de anomalias, também se mostra promissor, possibilitando maior robustez e adaptabilidade. Além disso, propõe-se a criação de uma biblioteca de segurança de fácil uso, desenvolvida em C, voltada para microcontroladores amplamente utilizados, como Arduino e ESP. Essa biblioteca poderia simplificar a adoção de protocolos de segurança avançados, democratizando a proteção de redes IoT e tornando-as mais acessíveis para desenvolvedores de aplicações práticas.

Referências

Ahmar, A.-U.-H., Aras, E., Nguyen, T. D., Michiels, S., Joosen, W., and Hughes, D. (2023). Design of a robust mac protocol for lora. *International Journal of Sensor Networks*, 38(2):133–146.

Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., and Manickam, S. (2023). Long range technology for internet of things: review, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics*, 12(6):3758 a 3767.

Chacko, S. and Job, D. (2018). Security mechanisms and vulnerabilities in lpwan. In *IOP Conference Series: Materials Science and Engineering*, volume 396, page 012027.

Han, B., Peng, S., Wu, C., Wang, X., and Wang, B. (2021). Lora-based physical layer key generation for secure v2v/v2i communications. *IEEE Internet of Things Journal*, 9(14):11803–11815.

Hayati, N., Windarta, S., Suryanegara, M., Pranggono, B., and Ramli, K. (2022). A novel session key update scheme for lorawan. *Journal of Information Security and Applications*, 68:103210.

LoRa Alliance (2024). About lorawan®. `https://lora-alliance.org/about-lorawan/`. Acesso em: 5 nov. 2024.

LyuLiang, Z., Kumar, Q., Singh, S. K., and Wang, Q. (2021). AI-empowered IoT Security for Smart Cities. *ACM Transactions on Internet Technology*, 21(4):Article 99.

Mai, T., Yao, H., Zhang, N., He, W., Guo, D., and Guizani, M. (2022). Transfer reinforcement learning aided distributed network slicing optimization in industrial iot. *IEEE Internet of Things Journal*, 9(17):16572–16585.

Moher, D., Liberati, A., Tetzlaff, J., and Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The prisma statement. *PLoS Medicine*, 6(7):e1000097.

Mousavi, S. M., Khademzadeh, A., and Rahmani, A. M. (2022). Cognitive long-range: Towards efficient public communication infrastructure for internet of things. *Journal of Network and Computer Applications*, 200:103367.

Ramos, C., Moreira, A., and Santos, J. (2020). An autonomous low-power lora-based flood-monitoring system. *ResearchGate*, 10(2):45–57.

Saputro, M. Y. A. and Sari, R. F. (2022). Performance evaluation of broadcast domain on the lightweight multi-fog blockchain platform for a lora-based internet of things network. *Journal of Communications and Networks*, 24(2):145–156.

Szewczyk, J., Nowak, M., Remlein, P., and Głowacka, A. (2022). Lorawan communication implementation. *International Journal of Electronics and Telecommunications*, 68(4):841–854.

Wong, A. W.-L., Goh, S. L., Hasan, M. K., and Fattah, S. (2024). Multi-hop and mesh for lora networks: Recent advancements, issues, and recommended applications. *ACM Computing Surveys*, 56(6):1–43.