INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS TERESINA CENTRAL
CURSO TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ARTHUR VIEIRA MELO SILVA

ANÁLISE DE DISPONIBILIDADE E EFICIÊNCIA ENERGÉTICA EM REDES LORAWAN SOB ATAQUE DE JAMMING REATIVO: UMA ABORDAGEM VIA SIMULAÇÃO NO NS-3

TERESINA, PIAUÍ
2026

ARTHUR VIEIRA MELO SILVA

ANÁLISE DE DISPONIBILIDADE E EFICIÊNCIA ENERGÉTICA EM REDES LORAWAN SOB ATAQUE DE JAMMING REATIVO: UMA ABORDAGEM VIA SIMULAÇÃO NO NS-3

Trabalho de Conclusão de Curso (Artigo Científico) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina.

Orientador: Prof. Me. Francisco Marcelino Almeida de Araújo

TERESINA, PIAUÍ
2026

ANÁLISE DE DISPONIBILIDADE E EFICIÊNCIA ENERGÉTICA EM REDES LORAWAN SOB ATAQUE DE JAMMING REATIVO: UMA ABORDAGEM VIA SIMULAÇÃO NO NS-3

Arthur Vieira Melo Silva[1]
Francisco Marcelino Almeida de Araújo[2]

RESUMO

A expansão da Internet das Coisas (IoT) tem impulsionado a adoção do protocolo LoRaWAN em infraestruturas críticas devido ao seu longo alcance e baixo consumo energético. No entanto, a operação em espectro não licenciado torna essas redes suscetíveis a ataques de Negação de Serviço na camada física, especificamente o jamming reativo. Este trabalho apresenta uma análise quantitativa do impacto desses ataques na disponibilidade e na eficiência energética de redes LoRaWAN, com foco no cenário regulatório brasileiro (faixa AU915, Anatel). Por meio de simulações no Network Simulator 3 (NS-3), modelou-se um nó interferente com latência de reação baseada em dados experimentais de hardware SDR real. Os resultados demonstram que o ataque reduz a taxa de entrega de pacotes (PDR) em até 24,7 pontos percentuais em SF7 no experimento com SF fixo, e até 22,6 pontos percentuais em SF8 no ambiente rural com ADR ativo. O algoritmo Adaptive Data Rate (ADR) eleva o fator de espalhamento em resposta às perdas, aumentando o consumo energético médio em até 51% — fenômeno denominado espiral de degradação energética. O experimento com SF fixo comprovou que o jammer é energeticamente inócuo na ausência do ADR, isolando esse algoritmo como o único vetor de exaustão energética. O estudo evidencia a urgência de mecanismos anti-jamming adaptados à realidade nacional.

Palavras-chave: LoRaWAN; segurança de redes; jamming reativo; NS-3; disponibilidade; eficiência energética.

ABSTRACT

The expansion of the Internet of Things (IoT) has driven the adoption of the LoRaWAN protocol in critical infrastructures due to its long range and low energy consumption. However, operation in unlicensed spectrum makes these networks susceptible to Denial of Service attacks at the physical layer, specifically reactive jamming. This work presents a quantitative analysis of the impact of these attacks on the availability and energy efficiency of LoRaWAN networks, focusing on the Brazilian regulatory scenario (AU915 band, Anatel). Through simulations in Network Simulator 3 (NS-3), an interfering node was modeled with reaction latency based on experimental data from real SDR hardware. The results demonstrate that the attack reduces the packet delivery rate (PDR) by up to 24.7 percentage points in SF7 in the experiment with fixed SF, and up to 22.6 percentage points in SF8 in the rural environment with active ADR. The Adaptive Data Rate (ADR) algorithm increases the spreading factor in response to losses, increasing

[1] Discente do curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal do Piauí (IFPI). E-mail: aarthur.vieira.contato@gmail.com.
[2] Professor Mestre do Instituto Federal do Piauí (IFPI). E-mail: Francisco.marcelino@ifpi.edu.br .

average energy consumption by up to 51% – a phenomenon known as the energy degradation spiral. The experiment with fixed SF proved that the jammer is energetically innocuous in the absence of ADR, isolating this algorithm as the sole vector of energy depletion. The study highlights the urgency of anti-jamming mechanisms adapted to the national reality.

Keywords: LoRaWAN; network security; reactive jamming; NS-3; availability; energy efficiency.

1 INTRODUÇÃO

A sociedade moderna vivencia uma transformação digital impulsionada pelo paradigma da Internet das Coisas (IoT). Para suportar a comunicação massiva de sensores restritos em bateria, o protocolo LoRaWAN consolidou-se como um padrão dominante nas redes LPWAN (Low Power Wide Area Networks). Entretanto, a natureza aberta do meio sem fio torna essa tecnologia inerentemente vulnerável a ataques de Negação de Serviço (DoS), em especial o Jamming (PIRAYESH; ZENG, 2022).

A segurança dessas infraestruturas deve ser analisada sob a tríade Confidencialidade, Integridade e Disponibilidade (CIA): enquanto o LoRaWAN endereça os dois primeiros pilares via criptografia AES-128 e códigos de autenticação (MIC), o terceiro permanece um desafio crítico. A natureza aberta do meio sem fio expõe essas redes a ataques de Negação de Serviço (DoS), em especial o jamming reativo — um atacante furtivo que permanece em escuta e só emite ruído ao detectar o preâmbulo de pacotes legítimos (PIRAYESH; ZENG, 2022). No contexto regulatório brasileiro (banda AU915), onde não há limitação estrita de *Duty Cycle* como no modelo europeu EU868, os dispositivos retransmitem pacotes de forma quase ininterrupta sob ataque contínuo, característica que atua como catalisador do esgotamento prematuro da bateria.

Neste contexto, este artigo tem como objetivo analisar quantitativamente a disponibilidade e a eficiência energética de redes LoRaWAN sob ataque de jamming reativo via simulação no NS-3, avaliando especificamente como o Fator de Espalhamento (SF) afeta a letalidade do ataque.

2 DESENVOLVIMENTO

2.1. FUNDAMENTAÇÃO TEÓRICA E TRABALHOS RELACIONADOS

A camada física LoRa utiliza a modulação *Chirp Spread Spectrum* (CSS), permitindo configurar o Fator de Espalhamento (SF) de 7 a 12. O aumento do SF melhora a sensibilidade do receptor, mas eleva proporcionalmente o tempo de transmissão (*Time-on-Air* – ToA), tornando cada pacote mais longo e mais exposto no canal (ADELANTADO *et al.*, 2017; BOR *et al.*, 2016). Essa janela de tempo estendida é o alvo principal do Jamming Reativo.

A viabilidade desse ataque foi comprovada experimentalmente por Aras *et al.* (2017)

com hardware SDR de baixo custo, e aprofundada por Hou, Xia & Zheng (2023), que demonstraram que chirps de jamming sincronizados com o mesmo SF da vítima são capazes de contornar mecanismos de recuperação de colisão existentes. A não ortogonalidade entre SFs distintos pode causar perdas mesmo quando o interferente não opera no mesmo SF da vítima (CROCE *et al.*, 2018). Perković *et al.* (2021) demonstraram que hardware de baixo custo é suficiente para paralisar uma rede LoRaWAN via jamming reativo, propondo contramedidas iniciais baseadas em espalhamento de canal. Martinez, Tanguy & Nouvel (2019) avaliaram o desempenho de redes LoRaWAN sob jamming via NS-3, reportando reduções expressivas no throughput — resultados que o presente trabalho estende ao incorporar latência realista de hardware SDR e ao contextualizar a análise no cenário regulatório brasileiro (AU915), onde a ausência de *Duty Cycle* amplifica o impacto energético sob ataque contínuo. Kuaban *et al.* (2023) modelaram matematicamente o esgotamento de bateria em dispositivos IoT sob ataques de negação de serviço, e Pirayesh & Zeng (2022) apresentam uma revisão abrangente de estratégias anti-jamming em redes sem fio. A escassez de trabalhos focados no contexto regulatório brasileiro motivou a adaptação das metodologias existentes para o padrão AU915, diferenciando esta pesquisa das anteriores ao correlacionar de forma integrada o SF com a taxa de sucesso do ataque e o custo energético — análise ausente nos trabalhos citados.

No contexto regulatório brasileiro, a operação de dispositivos LoRaWAN é regida pelo Ato Anatel nº 14.448/2017 (Agência Nacional de Telecomunicações (Anatel), 2017), que define o plano de frequências AU915 (915–928 MHz) sem impor restrições de *Duty Cycle* — diferentemente do modelo europeu EU868, que limita o uso do canal a 1% do tempo. Essa ausência tem implicações críticas para a segurança: dispositivos sob ataque de jamming reativo podem retransmitir pacotes de forma quase ininterrupta, transformando uma falha de disponibilidade em um vetor acelerado de esgotamento energético (PIRAYESH; ZENG, 2022). Ademais, o modelo de consumo energético adotado contabiliza a energia dissipada nos estados de transmissão (TX), recepção (RX) e hibernação (*Sleep*), com valores típicos de transceptores LoRa de baixo custo: $P_{TX} = 90$ mW, $P_{RX} = 56$ mW e $P_{Sleep} = 0{,}015$ mW (RAJAB *et al.*, 2023; TALEB *et al.*, 2023)..

2.2. METODOLOGIA DE SIMULAÇÃO

O experimento foi modelado utilizando o Network Simulator 3 (NS-3) versão 3.45 (CAMPANILE *et al.*, 2020), em ambiente Linux, integrando o módulo LoRaWAN desenvolvido por Abeele *et al.* (2017). Para garantir fidelidade com as regulamentações nacionais, a simulação operou na faixa de frequências AU915 (915–928 MHz), conforme o Ato Anatel nº 14.448/2017 (Agência Nacional de Telecomunicações (Anatel), 2017), sem restrição de *Duty Cycle* — característica que distingue o cenário brasileiro do europeu e amplifica o impacto energético sob ataque contínuo (LoRa Alliance Technical

Committee, 2023).

O cenário base consistiu em um *gateway* central e 30 nós sensores distribuídos aleatoriamente em disco de raio variável (1.000 a 5.000 m), com modelo de propagação `LogDistancePropagationLossModel` e expoente de perda de caminho $\alpha = 2{,}8$ (rural) e $\alpha = 3{,}5$ (urbano). O tráfego foi configurado com envios periódicos a cada 3 minutos, totalizando 24 horas de simulação por cenário, com semente aleatória fixa para garantir reprodutibilidade. Devido às limitações de implementação do módulo LoRaWAN no ns-3.45, desenvolvido originalmente para a região europeia, a simulação adotou 3 canais de uplink na faixa 915 MHz (915,2; 915,4; 915,6 MHz) como aproximação do plano AU915 — simplificação que representa um cenário conservador, tendendo a maximizar o impacto do jammer nos resultados.

Essa redução, embora drástica em relação aos 64 canais oficiais do AU915, configura deliberadamente um *worst-case scenario*: com apenas 3 canais disponíveis para os 30 nós sensores, a probabilidade de colisão entre transmissões legítimas já é estruturalmente elevada, maximizando a janela de atuação do jammer. Em uma rede real operando com os 64 canais do plano AU915, a dispersão do tráfego entre os canais reduziria naturalmente a probabilidade de colisão — o que significa que os impactos de PDR e consumo energético aqui reportados representam um limite superior conservador. A gravidade dos resultados obtidos nessa configuração adversa não é, portanto, atenuada pela limitação do módulo, mas reforçada.

Dois experimentos complementares foram conduzidos: (1) **SF fixo** (SF7 e SF12), travando o Fator de Espalhamento para isolar o ToA como variável crítica; e (2) **SF adaptativo** com ADR ativo, permitindo observar a degradação energética causada pela reação do protocolo às perdas (FINNEGAN; FARRELL; BROWN, 2020).

Para assegurar a validade estatística dos resultados, cada cenário foi executado com 5 sementes de aleatoriedade distintas (*seeds* 1 a 5), variando a distribuição espacial dos nós sensores. Os resultados apresentados correspondem à média das 5 execuções, acompanhada do intervalo de confiança de 95% calculado via distribuição t de Student (CAMPANILE *et al.*, 2020).

O nó atacante (*jammer* reativo) foi posicionado a 50 m do *gateway* com raio de escuta de 2.500 m. Ao detectar um pacote legítimo, agenda o disparo de ruído com latência modelada por distribuição normal, com parâmetros extraídos de dados experimentais de hardware SDR real (Šabić, Edin *et al.*, 2025): SF7 ($\mu = 14{,}1$ ms, $\sigma = 3{,}0$ ms) a SF12 ($\mu = 126{,}6$ ms, $\sigma = 19{,}3$ ms).

2.3. RESULTADOS E DISCUSSÕES

2.3.1. Disponibilidade sob SF Fixo

Para quantificar o impacto direto do jamming na disponibilidade, a rede foi submetida a cenários sem ataque (“Limpo”) e com ataque (“Atacado”), mantendo o SF fixo. Essa configuração isola o ToA como variável crítica, eliminando a influência adaptativa do ADR.

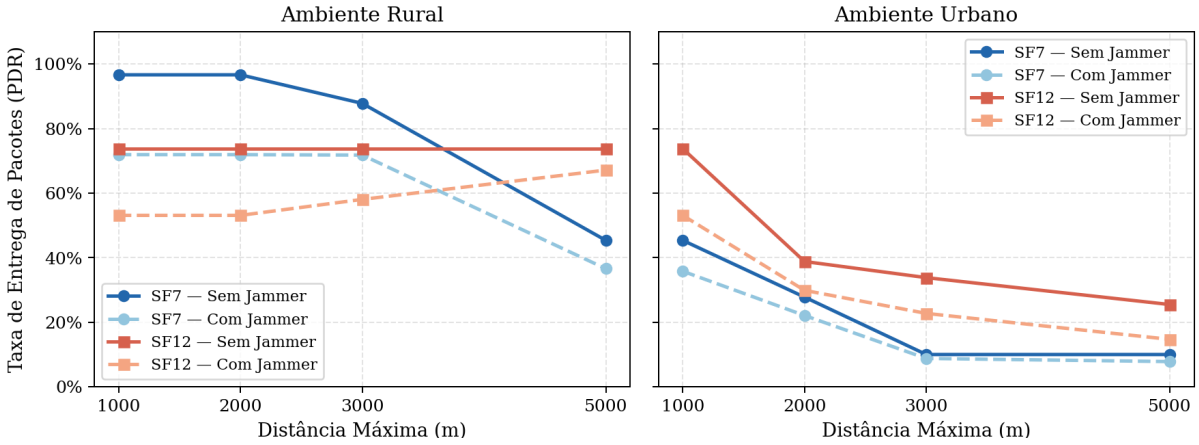

Figura 1 – PDR sob ataque de jamming reativo: SF7 vs SF12.

A Figura 1 ilustra a diferença de resiliência entre SF7 e SF12 em função da distância, nos ambientes rural e urbano. No ambiente rural a 1.000 m e 2.000 m, SF7 sofreu queda de 24,7 pontos percentuais no PDR (de 96,7% para 71,9% sob ataque), enquanto SF12 apresentou redução de 20,7 pontos percentuais (de 73,8% para 53,1%). SF7, com ToA de aproximadamente 56 ms, consegue em muitos casos concluir a transmissão antes que o jammer processe o preâmbulo e dispare o ruído (Šabić, Edin *et al.*, 2025). SF12, com ToA superior a 1,4 segundos, oferece janela de colisão amplamente suficiente para qualquer hardware reativo reagir, tornando-o sistematicamente vulnerável mesmo a jammers com latência elevada (ARAS *et al.*, 2017).

Esse fenômeno evidencia um paradoxo de segurança crítico: embora o SF12 seja projetado para ser a configuração mais robusta contra ruídos naturais, o seu longo *Time-on-Air* torna-o estruturalmente mais exposto ao jamming reativo do que o SF7 em transmissões próximas ao *gateway*. A 5.000 m, ambos os SFs apresentam quedas menores (8,8 e 6,6 pontos percentuais respectivamente), pois as perdas por propagação já limitam o PDR base independentemente do ataque.

Um resultado igualmente relevante é que, no experimento com SF fixo, as variações de consumo energético entre os cenários com e sem jammer situam-se entre -7% e $+1\%$ — dentro da margem estatística esperada. Isso comprova que, na ausência do algoritmo ADR, o jammer reativo é energeticamente neutro para os dispositivos vítimas,

isolando o ADR como o único mecanismo responsável pela transformação de uma falha de disponibilidade em exaustão energética.

2.3.2. Impacto Energético e o Comportamento do ADR

A Figura 2 evidencia o fenômeno denominado *espiral de degradação energética*: ao detectar perdas consecutivas causadas pelo *jammer*, o algoritmo ADR eleva o SF em busca de maior robustez, aumentando proporcionalmente o ToA e o consumo energético por transmissão (FINNEGAN; FARRELL; BROWN, 2020).

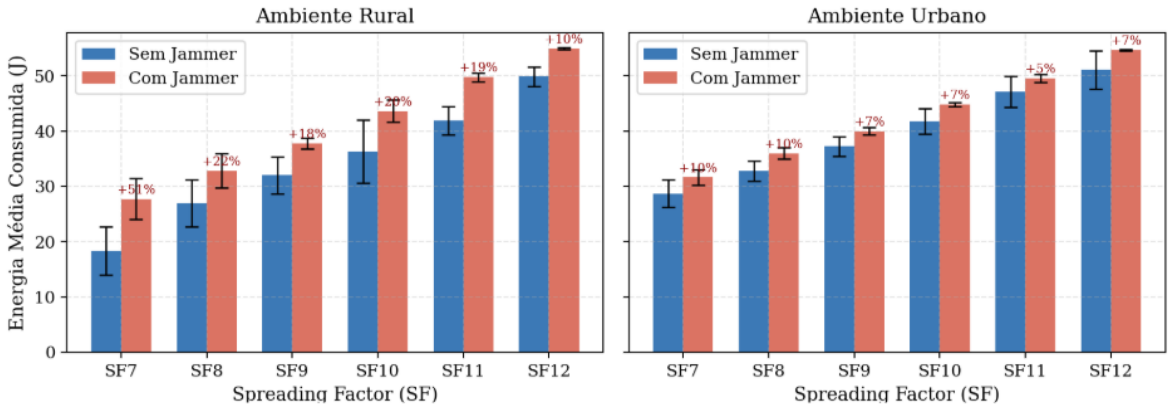

Figura 2 – Consumo energético médio com ADR sob ataque de jamming reativo (distância 2.000 m).

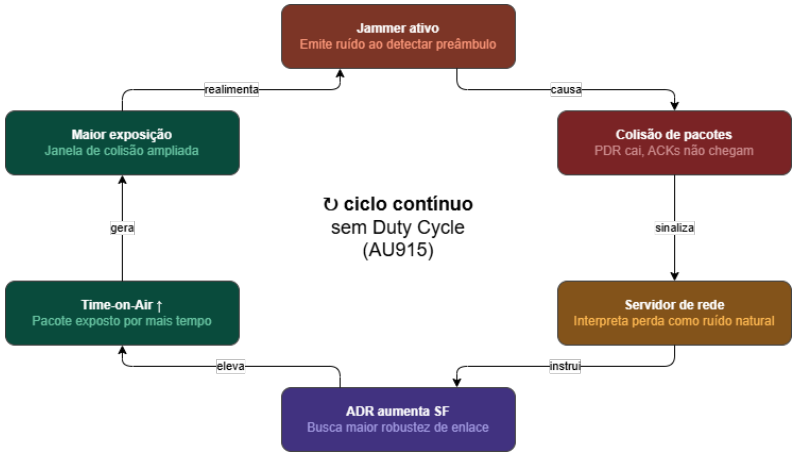

Figura 3 – Espiral de degradação energética induzida pelo jamming reativo em redes LoRaWAN com ADR ativo no contexto regulatório brasileiro (AU915).

A Figura 3 ilustra esse mecanismo de forma cíclica: ao causar colisões nos pacotes legítimos, o jammer induz o servidor de rede a interpretar as perdas como degradação do canal; o algoritmo ADR responde aumentando o SF do dispositivo em busca de maior robustez; o SF elevado amplia o *Time-on-Air* (ToA), expondo o pacote por mais

tempo à interferência; essa maior exposição resulta em novas colisões, reiniciando o ciclo. No contexto brasileiro, a ausência de restrição de *Duty Cycle* no plano AU915 elimina qualquer pausa obrigatória entre retransmissões, tornando o ciclo contínuo e o dreno energético irreversível.

No ambiente rural, esse efeito foi consistente em todos os SFs avaliados, confirmado pela agregação de 5 cenários de simulação com sementes distintas. O SF7 apresentou o maior aumento relativo de consumo, com acréscimo de 51% sob ataque (de 15,1 J para 22,4 J). Os demais SFs seguiram padrão similar: SF8 com $+22$%, SF9 com $+18$%, SF10 com $+20$%, SF11 com $+19$% e SF12 com $+10$%. A agregação das 5 *seeds* eliminou o comportamento anômalo de redução de consumo anteriormente identificado no SF8 em execuções isoladas, revelando que tal resultado decorria da variação natural entre execuções e não de um comportamento estrutural do algoritmo ADR.

No ambiente urbano, as variações de consumo sob ataque são substancialmente menores — entre $+7$% e $+10$% para SF7 a SF9 — reflexo do fato de que o canal urbano severo já força o ADR a operar em SFs elevados mesmo sem a presença do jammer, deixando pouca margem adicional para degradação induzida pelo ataque. A ausência de restrição de *Duty Cycle* no plano AU915 elimina o mecanismo natural de contenção presente no modelo europeu, transformando uma falha de disponibilidade em um Ataque de Esgotamento de Energia capaz de drenar baterias projetadas para anos em prazos muito menores (PIRAYESH; ZENG, 2022).

2.3.3. Estimativa de Vida Útil da Bateria

O impacto energético pode ser traduzido em uma métrica concreta: a estimativa de vida útil da bateria, calculada com base em uma fonte típica de 2$\times$AA (aproximadamente 15.000 J) dividida pelo consumo médio diário observado nas simulações de 24 horas.

No ambiente rural, o resultado mais severo ocorre em SF7: sem jammer, a vida útil estimada é de 995 dias ($\approx$2,7 anos), caindo para 669 dias ($\approx$1,8 anos) sob ataque — uma redução de 33%. Para SF8, a redução foi de 18%, consistente com o aumento de 22% no consumo energético identificado na seção anterior. Para SF9 e SF10, as reduções são de 22% e 24% respectivamente. SF11 e SF12 apresentam reduções menores, de 12% e 13%, consistentes com a menor margem de adaptação do ADR nesses SFs.

Cabe ressaltar que este modelo assume descarga linear da bateria. Na prática, baterias eletroquímicas reais apresentam quedas de tensão não lineares, especialmente sob o estresse de transmissões contínuas com correntes de pico elevadas. Em hardware físico, a exaustão tenderia a ocorrer ainda mais rapidamente — o que torna as estimativas aqui apresentadas limites superiores conservadores, reforçando a gravidade do impacto do ataque. Dispositivos LoRaWAN são tipicamente dimensionados para operar por 5 a 10 anos sem substituição de bateria (SCHWAB, 2016). A redução de

33% na vida útil projetada em SF7 pode transformar um investimento planejado para uma década em um sistema que requer manutenção em menos de dois anos.

3 CONCLUSÃO

Este trabalho analisou o impacto do jamming reativo na disponibilidade e eficiência energética de redes LoRaWAN no contexto regulatório brasileiro, por meio de simulações no NS-3 com modelo de latência de atacante baseado em dados experimentais reais de hardware SDR (Šabić, Edin *et al.*, 2025). Em relação à literatura existente, este trabalho avança sobre Martinez, Tanguy & Nouvel (2019) ao incorporar latência realista de hardware SDR e ao contextualizar a análise no plano AU915, complementando a modelagem de Kuaban *et al.* (2023) com dados quantitativos que correlacionam SF, disponibilidade e custo energético de forma integrada — análise ausente nos trabalhos anteriores.

Os resultados confirmam um paradoxo de segurança crítico: configurações com SF elevado, embora necessárias para coberturas de longa distância, apresentam maior *Time-on-Air*, tornando-se alvos estruturalmente mais vulneráveis ao jamming reativo. Em contrapartida, SF7 sofre maior degradação energética quando o ADR é habilitado, pois possui maior margem para elevar o fator de espalhamento em resposta às perdas, culminando na espiral de degradação energética com aumento de até 51% no consumo médio. O experimento com SF fixo provou que o jammer reativo é energeticamente inócuo na ausência do ADR — variações entre -7% e $+1\%$ foram observadas, dentro da margem estatística — isolando esse algoritmo como o único mecanismo responsável pela transformação de uma falha de disponibilidade em exaustão energética.

A ausência de restrição de *Duty Cycle* no plano AU915 brasileiro amplifica o dreno energético sob ataques contínuos, uma vez que os dispositivos retransmitem sem limitação temporal. Esse aspecto regulatório diferencia o cenário nacional e reforça a necessidade de mecanismos de proteção específicos para a realidade brasileira.

Como trabalhos futuros, destacam-se o desenvolvimento de algoritmos de detecção baseados em Inteligência Artificial para diferenciar interferências naturais de ataques de jamming, bem como modificações no ADR que permitam ao servidor de rede identificar padrões de ataque antes de instruir o aumento do consumo energético dos dispositivos (FINNEGAN; FARRELL; BROWN, 2020; PIRRI *et al.*, 2025). Estudos experimentais com hardware real na faixa AU915 também são necessários para validar os resultados de simulação aqui apresentados (PERKOVIć *et al.*, 2021).

REFERÊNCIAS

ABEELE, F. Van den *et al.* Scalability analysis of large-scale lorawan networks in ns-3. **IEEE Internet of Things Journal**, v. 4, n. 6, p. 2186–2198, 2017. Citado na página 4.

ADELANTADO, F. *et al.* Understanding the limits of lorawan. **IEEE Communications Magazine**, v. 55, n. 9, p. 34–40, 2017. Citado na página 3.

Agência Nacional de Telecomunicações (Anatel). **Ato nº 14.448, de 04 de dezembro de 2017**. 2017. Regulamentação técnica para equipamentos de radiocomunicação de radiação restrita. Disponível em: <https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2017/1139-ato-14448>. Citado na página 4.

ARAS, E. *et al.* Selective jamming of lorawan using commodity hardware. In: **Proceedings of the 11th Workshop on Challenged Networks**. [S.l.]: Association for Computing Machinery, 2017. Citado 2 vezes nas páginas 3 e 6.

BOR, M. C. *et al.* Do lora low-power wide-area networks scale? In: **Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems**. [S.l.]: Association for Computing Machinery, 2016. Citado na página 3.

CAMPANILE, L. *et al.* Computer network simulation with ns-3: A systematic literature review. **Electronics**, v. 9, n. 2, 2020. Citado 2 vezes nas páginas 4 e 5.

CROCE, D. *et al.* Impact of LoRa imperfect orthogonality: Analysis of link-level performance. **IEEE Communications Letters**, v. 22, n. 4, p. 796–799, 2018. Citado na página 4.

FINNEGAN, J.; FARRELL, R.; BROWN, S. Analysis and enhancement of the lorawan adaptive data rate scheme. **IEEE Internet of Things Journal**, v. 7, n. 8, p. 6904–6915, 2020. Citado 3 vezes nas páginas 5, 7 e 9.

HOU, N.; XIA, X.; ZHENG, Y. Jamming of LoRa PHY and countermeasure. **ACM Transactions on Sensor Networks**, v. 19, n. 4, p. 1–27, 2023. Citado na página 4.

KUABAN, G. S. *et al.* Modelling of the energy depletion process and battery depletion attacks for battery-powered internet of things (iot) devices. **Sensors**, v. 23, n. 13, 2023. Citado 2 vezes nas páginas 4 e 9.

LoRa Alliance Technical Committee. **LoRaWAN L2 Specification**. [S.l.], 2023. Citado na página 5.

MARTINEZ, I.; TANGUY, P.; NOUVEL, F. On the performance evaluation of LoRaWAN under jamming. In: **2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)**. [S.l.: s.n.], 2019. p. 141–145. Citado 2 vezes nas páginas 4 e 9.

PERKOVIć, T. *et al.* Low-cost implementation of reactive jammer on LoRaWAN network. **Electronics**, v. 10, n. 7, p. 864, 2021. Citado 2 vezes nas páginas 4 e 9.

PIRAYESH, H.; ZENG, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. **IEEE Communications Surveys & Tutorials**, v. 24, n. 2, p. 767–809, 2022. Citado 3 vezes nas páginas 3, 4 e 8.

PIRRI, M. *et al.* Comparative assessment of adaptive data rate algorithms for LoRaWAN IoT applications. In: **2025 10th International Workshop on Advances in Sensors and Interfaces (IWASI)**. [S.l.: s.n.], 2025. p. 1–6. Citado na página 9.

RAJAB, H. *et al.* Evaluation of energy consumption of LPWAN technologies. **EURASIP Journal on Wireless Communications and Networking**, v. 2023, n. 1, 2023. Citado na página 4.

SCHWAB, K. **A quarta revolução industrial**. São Paulo: Edipro, 2016. ISBN 978-8572839785. Citado na página 8.

TALEB, H. *et al.* Energy efficient selection of spreading factor in LoRaWAN-based WBAN medical systems. **Internet of Things**, v. 24, p. 100896, 2023. Citado na página 4.

Šabić, Edin *et al.* **Reactive Jamming of LoRa Networks: Latency Characterization with SDR Hardware**. 2025. Dados experimentais do Cenário II utilizados para modelagem da latência do jammer. Citado 3 vezes nas páginas 5, 6 e 9.