Empregos da Tecnologia *LoRa* para Comunicações no Cenário Tático

Marcelo Silva de Souza, Gabriel Sousa Silva, Iury Justo de Barros
Centro de Apoio a Sistemas Operativos (CASOP), Niterói/RJ – Brasil

***Resumo* – Este artigo apresenta um estudo sobre a aplicação da tecnologia *LoRa* em ambientes militares, destacando sua comunicação de longo alcance, baixo consumo energético e resistência a interferências. São exp*LoRa*das redes mesh descentralizadas para rastreamento de tropas, monitoramento de perímetros e controle de sistemas autônomos em cenários sem infraestrutura convencional. Integrada a arquiteturas híbridas, *LoRa* oferece resiliência e segurança essenciais para operações táticas e logísticas. O trabalho aponta tendências futuras em soberania tecnológica.**

***Palavras-Chave* – *LoRa*, Comunicação Militar, Comunicação e Controle, Arquitetura Híbrida**

I. INTRODUÇÃO

A comunicação é um dos pilares da operação de sistemas modernos, sejam civis, industriais ou militares. Transmitir informações de forma eficiente em ambientes remotos, com pouca infraestrutura, muita interferência de campo e severas restrições energéticas ou logísticas, permanece um desafio técnico relevante.

Soluções tradicionais de comunicação à longa distância — como rádios VHF/UHF ou redes celulares — apresentam limitações. Enquanto os primeiros exigem equipamentos específicos e operadores treinados, as redes móveis dependem de infraestrutura e cobertura, além de consumo energético elevado, o que inviabiliza seu uso em dispositivos portáteis por longos períodos.

No ambiente agrícola e sensoriamento ambiental, o *LoRa* (Long Range) possibilita a implantação de redes de sensores distribuídos para monitoramento contínuo de variáveis críticas como umidade do solo, temperatura, luminosidade, níveis de irrigação, o acompanhamento em tempo real da qualidade do ar, níveis de poluição, condições meteorológicas e detecção de incêndios florestais, promovendo uma gestão ambiental proativa e eficiente [1]. Nesse contexto, a tecnologia *LoRa*, baseada na modulação *Chirp Spread Spectrum* (CSS), se destaca por oferecer longo alcance (até 15 km em ambientes abertos), operação em bandas ISM (*Industrial, Scientific and Medical*) — faixas de frequência reservadas internacionalmente para aplicações industriais, científicas e médicas que não exigem licença específica de uso —, baixo consumo energético e custo reduzido. Isso a torna uma base tecnológica promissora para aplicações em Internet das Coisas (IoT), redes de sensores e comunicações portáteis em locais remotos.

II. FUNDAMENTOS TEÓRICOS

A. Tecnologia LoRa

LoRa (Long Range) é uma modulação proprietário baseada em chirp-spread-spectrum que opera nas bandas ISM sub-GHz (EU868, US915, AS923, entre outras). Ao variar dinamicamente o spreading factor (SF7–SF12) a tecnologia pode entrega um enlace acima de 160 dB, cobrindo algumas dezenas de quilômetros com baixa potência — ideal para sensores alimentados a bateria. A família mais recente de transceptores SX126x da Semtech reduz a corrente de recepção (< 5 mA) e adiciona modos de "stand-by" ultrabaixo, prolongando a autonomia para mais de dez anos em campo. O relatório anual da *LoRa* Alliance mostra que, em 2024, o ecossistema ultrapassou 300 milhões de nós ativos e 200 operadoras globais, com forte adoção nos setores marítimo, agrícola e de cidades inteligentes [2].

B. Análise Tecnológica

Devido a natureza do protocolo, as vantagens da utilização da modulação CHIRP incluem: Alta imunidade a interferência, operação com sinais de baixo *SNR* (relação sinal-ruído), de baixa probabilidade detecção, flexibilidade na configuração de parâmetros de largura de banda, fator de espalhamento e taxas de dados com distâncias de comunicação ponto a ponto superior a 15 km com uso de baixas potências (2W), ideal para dispositivos portáteis. Entretanto, existe restrições no volume de transmissão em alguns países devido a regulação local.

C. Segurança

A segurança do protocolo *LoRa* apoia-se em criptografia AES-128 aplicada ponta a ponta e na autenticação mútua entre dispositivo, *Network Server* (NS) e *Join Server* (JS). Cada sessão gera duas chaves derivadas: NwkSKey (integridade) e AppSKey (confidencialidade da aplicação). Esse modelo separa responsabilidades entre rede e aplicação, introduz contadores de quadro de 32 bits, DevNonce crescente e um JoinNonce de 3 bytes gerado pelo NS. Além disso, com o Frame MIC (Message Integrity Code) e a obrigatoriedade de TLS entre componentes de *backend*, cria-se uma cadeia de confiança que permanece válida mesmo quando os *gateways* são considerados não confiáveis [3].

Apesar desses mecanismos, pesquisas recentes mostram que ameaças práticas persistem, tais como: captura física de nós com possibilidade de expor chaves e ataques de *jamming*. Estudos de 2024-2025 evidenciam que a maioria dos incidentes reportados envolveu falhas de configuração como por exemplo, reuso de AppKey, DevNonce não sequencial ou desativação do *frame counter check*. A

literatura aponta ainda soluções de *machine learning* para prever *jamming* e protocolos de *Zero Touch Provisioning* que elevam o nível de segurança sem impactar o consumo energético [4].

III. APLICAÇÕES MILITARES

A adoção da tecnologia *LoRa* em ambientes militares se justifica por sua capacidade de operar com eficiência energética, baixo perfil de detecção, resiliência a interferências e custo acessível.

Suas características a tornam ideal para diversos cenários táticos e logísticos, especialmente onde outras soluções são inviáveis ou vulneráveis.

A. Comunicações de Contingência em Campo Hostil

Em operações militares ou missões humanitárias, em regiões sem cobertura de infraestrutura convencional, a comunicação entre unidades é vital, mesmo que intermitente. O *LoRa* permite o envio de mensagens curtas, criptografadas e discretas (como localização ou alertas) entre dispositivos portáteis, tablets ou rádios táticos, operando em topologias ponto a ponto ou em malha. O baixo *duty cycle* reduz a probabilidade de detecção e o consumo de energia, tornando-o adequado para cenários onde discrição e autonomia são essenciais [5].

Em ambientes com densa cobertura vegetal, como regiões de mata fechada, os sinais em VHF sofrem significativa atenuação devido à absorção e espalhamento pelas folhas, galhos e umidade. Nesses cenários, a tecnologia *LoRa* pode ser empregada como solução contingencial de comunicação, aproveitando sua capacidade de operar com sinais de baixo nível (baixo SNR) e sua maior robustez à propagação em condições não ideais.

B. Comando e controle de tropas e ativos

O rastreamento contínuo de tropas, veículos e equipamentos é essencial para o planejamento tático e a segurança operacional. Dispositivos vestíveis ou embarcados, equipados com GPS e módulos *LoRa*, permitem a transmissão periódica de coordenadas à base de comando, mesmo em ambientes sem linha de visão direta. A utilização de topologias em malha viabiliza o encaminhamento dos dados por múltiplos nós, garantindo cobertura em áreas sem infraestrutura convencional, com consumo energético reduzido e alta confiabilidade.

Em missões de infiltração, que demandam discrição extrema e minimização do perfil eletromagnético, o uso do *LoRa* se mostra particularmente vantajoso. Patrulhas e unidades destacadas podem empregar dispositivos portáteis para comunicações bidirecionais discretas, utilizando transmissões curtas e espaçadas para manter o comando informado — seja por telemetria passiva ou envio ativo de alertas. Operações anfíbias exemplificam bem esse cenário, exigindo conectividade resiliente em áreas remotas ou hostis, onde a exposição a sistemas de guerra eletrônica representa um risco constante.

C. Monitoramento de Perímetros com Redes de Sensores

A vigilância de áreas sensíveis, como bases operacionais ou zonas temporárias de ocupação, requer sistemas de detecção que sejam ao mesmo tempo, discretos, eficientes e de rápida implantação. Sensores autônomos — como magnetômetros, microfones ou detectores de movimento — podem ser integrados a módulos *LoRa* e operados com baterias de longa duração. Esses dispositivos formam redes distribuídas, sem necessidade de cabeamento ou infraestrutura fixa, o que facilita sua instalação em ambientes remotos ou de difícil acesso.

Devido à baixa potência de operação do *LoRa*, esses sensores podem ser alimentados por painéis solares compactos, possibilitando funcionamento contínuo com mínima intervenção humana. Essa autonomia energética reduz a necessidade de manutenção periódica e aumenta a viabilidade do sistema em missões prolongadas ou áreas com acesso restrito [6].

D. Controle de Drones e Robôs Autônomos em Missões Táticas

Drones aéreos e veículos terrestres não tripulados (UGVs) têm sido amplamente empregados em missões de reconhecimento, vigilância e transporte em ambientes de alto risco. Seu uso tem se intensificado em operações militares e de segurança, especialmente em cenários hostis onde a presença humana é limitada ou indesejável. A tecnologia *LoRa* pode ser integrada a esses sistemas para comunicação de comandos essenciais — como partida, parada, retorno ao ponto de origem e envio de rotas — além da transmissão de dados de telemetria, incluindo nível de bateria, integridade do sistema e status da missão [7].

Veículos de Superfície Não Tripulados (VSNTs) têm ganhado destaque em operações militares, de vigilância costeira e patrulhamento fluvial, oferecendo uma plataforma robusta e versátil para atuação em ambientes aquáticos hostis. Equipados com sensores de navegação, câmeras, sonares e cargas úteis específicas, os VSNTs podem operar de forma autônoma ou semiautônoma em missões como reconhecimento de litoral, monitoramento ambiental, varredura de minas navais e logística de curto alcance.

IV. ESTRATÉGIAS DE RESILIÊNCIA E SEGURANÇA

Em aplicações críticas, como operações militares, missões humanitárias ou sistemas de infraestrutura sensível, a comunicação precisa ser confiável, segura e resiliente a interferências deliberadas ou acidentais. Cabe assim, descrever as principais estratégias adotadas para reforçar a segurança e a continuidade operacional em redes baseadas em *LoRa* como criptografia ponta a ponta e autenticação forte. A proteção dos dados transmitidos, por exemplo, é assegurada por criptografia ponta a ponta (E2E), garantindo que somente os dispositivos autorizados possam interpretar o conteúdo da comunicação. Já o *LoRa*WAN, incorpora camadas de segurança com chaves AES de 128 bits tanto para a rede quanto para a aplicação, mas soluções militares e críticas podem empregar protocolos criptográficos adicionais ou personalizados. Além disso, são utilizadas autenticações mútua e por desafio resposta, impedindo que dispositivos falsos se infiltrem na rede ou executem comandos não autorizados [8].

Para evitar a detecção e localização por sistemas de guerra eletrônica ou por agentes maliciosos, as transmissões são projetadas para serem breves, espaçadas e imprevisíveis. Ao limitar o tempo de transmissão e variar o intervalo entre os envios, reduz-se significativamente a probabilidade de que o sinal seja interceptado, analisado ou triangulado. Essa abordagem também contribui para economia de energia, aumentando a autonomia de dispositivos alimentados por bateria [9].

A resiliência é ampliada com a utilização de múltiplas tecnologias de comunicação em paralelo ou de forma redundante. Sistemas que combinam *LoRa* com links de satélite, redes LTE militares, rádio HF ou Wi-Fi tático podem alternar entre canais conforme a disponibilidade, qualidade do sinal ou nível de ameaça (ex: *jamming*) [10]. Essa arquitetura multimodal assegura continuidade de operação mesmo diante da falha ou comprometimento de uma das camadas de comunicação.

V. PROPOSTA DE ARQUITETURA

Para exp*LoRa*r todo o potencial da tecnologia *LoRa* em aplicações críticas — civis e militares — propõe-se uma arquitetura descentralizada, interoperável e adaptável, capaz de operar de forma autônoma ou integrada a sistemas maiores, mesmo em ambientes hostis ou com infraestrutura degradada (Fig. 1).

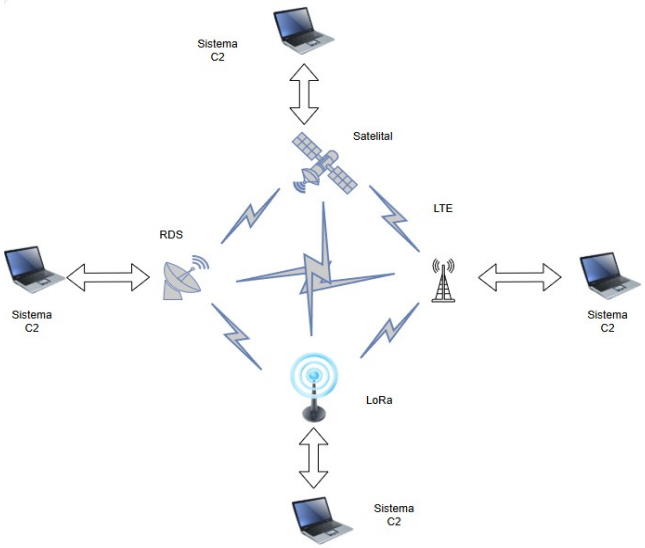

Fig. 1 – Arquitetura proposta

A arquitetura se baseia nos seguintes pilares:

A. Integração de redes LoRa com camadas IP por meio de gateways inteligentes

Gateways funcionam como pontes entre dispositivos *LoRa* (comunicação em nível físico e de enlace) e redes IP (camadas superiores). A proposta inclui o uso de *gateways* inteligentes, capazes de encapsular mensagens *LoRa* em protocolos IP (UDP/TCP/MQTT/NATS, por exemplo), permitindo a interoperabilidade com redes locais, sistemas de comando e controle, ou servidores remotos via internet ou intranets militares. Esses *gateways* também devem oferecer suporte à autenticação, encriptação, compressão e priorização de pacotes.

B. Redes mesh e ad hoc com roteamento dinâmico

Em situações onde não há infraestrutura fixa ou cobertura contínua, a comunicação entre nós deve se organizar de forma autônoma e distribuída. A proposta prevê o uso de redes *mesh* (malha) ou *ad hoc*, nas quais cada nó pode atuar como retransmissor e roteador de mensagens. Algoritmos de roteamento dinâmicos baseados em métricas como qualidade do link, energia residual ou prioridade da mensagem asseguram que os dados encontrem o caminho mais eficiente até o destino, mesmo diante de falhas, bloqueios ou mobilidade dos nós.

C. Estrutura híbrida (LTE, satélite, rádio HF)

Para permitir a conexão entre redes locais e centros de comando distantes, é necessário uma infraestrutura capaz de operar sob diversas condições. A arquitetura prevê o uso de links híbridos, combinando redes LTE, satélite de baixa órbita (LEO) ou rádio HF, selecionados automaticamente de acordo com a disponibilidade, latência, segurança e custo energético. Em cenários militares, essa redundância é essencial para manter a comunicação mesmo sob bloqueio seletivo de frequências ou sabotagem da infraestrutura local.

D. Gateways com funções de cache, retransmissão e roteamento de missão

Os *gateways* da arquitetura proposta não são meros pontos de passagem, mas nós ativos de processamento e decisão. Devem ser capazes de armazenar temporariamente mensagens em cache para retransmissão posterior em caso de falha de enlace, agrupar ou segmentar pacotes de acordo com a prioridade, e até mesmo executar regras de roteamento orientadas à missão, por exemplo: redirecionar automaticamente alertas críticos para múltiplos destinos ou operar em modo offline com sincronização posterior. Essa capacidade é especialmente útil em missões móveis, veículos táticos ou áreas sem cobertura constante.

VI. RESULTADOS

Os experimentos realizados com os protótipos (Fig. 2) do sistema de comunicação tática distribuída demonstraram a viabilidade prática do modelo proposto sob diversas condições adversas e dinâmicas, validando aspectos fundamentais da arquitetura distribuída sem dependência de infraestrutura centralizada. O protocolo de acesso múltiplo TDMA com sincronização implícita mostrou-se operacionalmente estável mesmo em cenários com deriva de clock natural dos dispositivos, entrada e saída aleatória de nós e geração estocástica de tráfego pelos usuários.

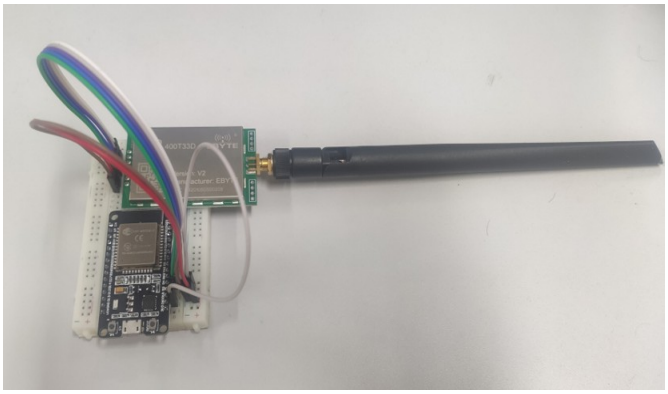

Fig. 2 – Protótipo *LoRa*

As operações experimentais, realizadas com enlaces de até 5 km de distância e monitoramento contínuo por software de rádio definido por software (SDR) Fig. 3, confirmaram a robustez da camada de transporte customizada na gestão do fluxo de dados, retransmissões seletivas e manutenção da integridade lógica das sessões de comunicação. A utilização de criptografia ponta a ponta com AES-128, implementada diretamente no hardware do microcontrolador ESP32, assegurou o sigilo operacional das comunicações, mesmo sob inspeção passiva do espectro.

Do ponto de vista de engenharia de sistemas, destaca-se a tolerância nativa a falhas transitórias de nós e enlaces, essencial em cenários militares, humanitários e de resposta a desastres e a capacidade de operar com dispositivos de baixo custo, reduzido consumo energético e alta mobilidade, com potencial de operação em ambientes austeros. Além disso, a eficiência espectral alcançada por meio da combinação do TDMA com sincronização adaptativa e mecanismos de controle de fluxo assíncronos, foi outro aspecto positivo.

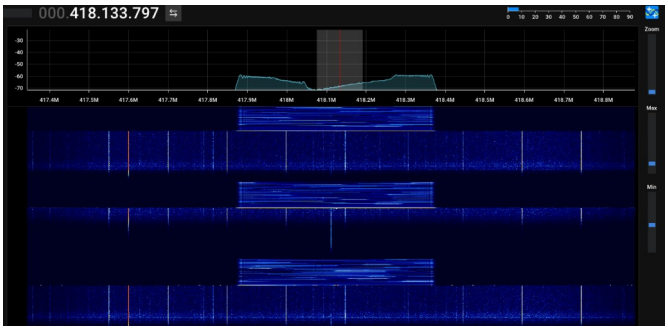

Fig. 3 – Monitoramento da transmissão

As observações experimentais permitem identificar oportunidades concretas de continuidade e aprimoramento desta linha de pesquisa, tais como: O desenvolvimento de técnicas preditivas baseadas em estimativa de deriva e algoritmos de controle adaptativo, algoritmos de roteamento resiliente para reduzir a degradação da malha em face de múltiplos nós intermitentemente indisponíveis, assegurando maior qualidade de serviço e implementação de defesa ativa contra a ataques à rede (ciberdefesa embarcada) visando aplicações militares e de segurança crítica.

A continuidade dos trabalhos permitirá consolidar um arcabouço tecnológico aplicável a diversos cenários operacionais, unindo eficiência espectral, segurança criptográfica, resiliência topológica e defesa ativa integrada.

VI. CONCLUSÃO E TRABALHOS FUTUROS

A tecnologia *LoRa* representa uma solução estratégica e versátil para comunicações digitais de longo alcance, especialmente em ambientes adversos ou com infraestrutura limitada. Sua operação em bandas não licenciadas, o baixo consumo energético, a facilidade de implantação e a resiliência a interferências a tornam particularmente adequada para aplicações que exigem discrição, autonomia e confiabilidade — como monitoramento ambiental, agricultura de precisão, cidades inteligentes e, com especial destaque, operações militares e contingenciais.

No campo militar, *LoRa* oferece uma plataforma robusta para comunicações táticas, rastreamento de ativos, redes de sensores perimetrais e controle de sistemas autônomos, tudo com um perfil de exposição minimizado e suporte a redes descentralizadas e dinâmicas. Combinada a técnicas de segurança como criptografia ponta a ponta, roteamento adaptativo, frequência variável e diversificação de backhaul.

Entretanto, o verdadeiro potencial de *LoRa* só é plenamente realizado quando integrada a uma arquitetura híbrida e interoperável, capaz de combinar diferentes camadas e tecnologias de comunicação — como IP, LTE, rádio HF ou satélites — por meio de *gateways* inteligentes com funções de cache, retransmissão e tomada de decisão local. Essas arquiteturas, descentralizadas e flexíveis, são fundamentais para garantir a continuidade operacional em cenários críticos, onde falhas pontuais ou ataques coordenados podem comprometer toda uma missão ou sistema de resposta.

Olhando para o futuro, a tendência é de expansão acelerada da tecnologia *LoRa* em setores estratégicos, tanto no domínio civil quanto militar. Esse avanço virá acompanhado de um esforço por soberania tecnológica, com o desenvolvimento local de hardware, firmware e protocolos abertos, reduzindo a dependência de soluções estrangeiras e aumentando o controle sobre aspectos de segurança e interoperabilidade.

Por fim, vislumbra-se o uso crescente de inteligência artificial embarcada, capaz de processar informações localmente, tomar decisões autônomas e filtrar dados críticos para comunicação, reduzindo latência, tráfego e vulnerabilidades. Essa convergência entre IoT, IA e redes resilientes marca uma nova fronteira na forma como comunicamos, monitoramos e respondemos a eventos em campo — seja na defesa, na segurança pública, na gestão ambiental ou na proteção civil.

Assim, *LoRa* não é apenas uma tecnologia de comunicação: é um elemento estratégico de infraestrutura, com potencial de impactar profundamente a autonomia, eficiência e segurança de sistemas que operam nos limites da conectividade.

Como trabalhos futuros, sugere-se exp*LoRa*r a aplicação no ambiente marítimo, avaliando a implementação em embarcações de pequeno porte, comboios ou unidades de vigilância costeira, assegurando conectividade mesmo quando há baixa linha de visada. Em operações terrestres, especialmente com blindados ou unidades mecanizadas que atuam em terrenos de visada parcial e alta hostilidade à infraestrutura convencional. Nas comunicações individuais, pois seu peso reduzido, baixo consumo energético e robustez

permitem a incorporação direta ao equipamento do soldado, mantendo consciência situacional e coordenação tática em missões de infiltração. Também em operações aerotransportadas, incluindo drones de reconhecimento ou retransmissores móveis e, por fim, a interoperabilidade é viabilizada por *gateways* que interconectam redes IP, rádio digital ou satélite, possibilitando a formação de redes híbridas de alta resiliência.

Marcelo Silva de Souza, marcelo-silva.souza@marinha.mil.br; Gabriel Sousa Silva, gabriel.sousa.silva@marinha.mil.br; Iury Justo de Barros, iury.justo@marinha.mil.br.

REFERÊNCIAS

[1] PAGANO, Antonino; CROCE, Daniele; TINNIRELLO, Ilenia; VITALE, Gianpaolo. A Survey on *LoRa* for Smart Agriculture: Current Trends and Future Perspectives. *IEEE Internet of Things Journal*, v. 10, n. 4, p. 3664–3689, fev. 2023. DOI: 10.1109/JIOT.2022.3230505.

[2] *LoRa* Alliance. *LoRa Alliance 2024 End-of-Year Report*. Fremont, CA, fev. 2025.

[3] *LoRa* Alliance. *LoRa*WAN Specification v1.1. Fremont, CA, 2024

[4] Huang, X. et al. "*LoRa*WAN Security: An Evolvable Survey on Vulnerabilities, Attacks, and Countermeasures." ACM Computing Surveys, vol. 57, n.º 2, 2025.

[5] ALAIAN, B.; GREGORY, T.; SURI, N.; RUSSELL, S.; *et al.* Evaluating *LoRa*WAN-based IoT Devices for the Tactical Military Environment. In: *Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT).* Singapore: IEEE, 2018. DOI: 10.1109/WF-IoT.2018.8355225.

[6] MEJIA-HERRERA, M.; BOTERO-VALENCIA, J.; ORTEGA, J.; HERNÁNDEZ-GARCÍA, R. Development of a Solar-Powered Edge Processing Perimeter Alert System with AI and *LoRa*/*LoRa*WAN Integration for Drone Detection and Enhanced Security. *Drones*, v. 9, n. 1, p. 43, 2025. DOI: 10.3390/drones9010043.

[7] ARROYO, Patricia; HERRERO, José Luis; LOZANO, Jesús; MONTERO, Pablo. *Integrating LoRa-Based Communications into Unmanned Aerial Vehicles for Data Acquisition from Terrestrial Beacons.* Electronics, v. 11, n. 12, art. 1865, 2022. DOI: 10.3390/electronics11121865.

[8] *LoRa* Alliance; Gemalto; Actility; Semtech. *LoRa*WAN™ Security – A White Paper. *LoRa* Alliance, fevereiro 2017.

[9] THALES Group. "Staying Hidden on a Digital Battlefield: The Need for Low-Probability-of-Detection Communications." 7 mar. 2025. Acesso em: 26 jun. 2025.

[10] ANGLIN, J.; WALKER, A. Multiple Paths Lead to Network Resiliency. *Army AL&T Magazine*, U.S. Army PEO C3T, 9 dez. 2024. Disponível em: https://www.army.mil/article/281863. Acesso em: 26 jun. 2025.