PROBLEMAS DE SEGURANÇA EM REDES IOT

Luis Enrique Cardozo Ramirez

Adrian Alejandro Chavez Alanes

Segurança em IoT Agrícola: Ataque de Falsificação de Dados em Redes LoRa

10/10/2024

—

T546- IoT

—

Prof. Samuel Baraldi

ÍNDICE

1. Introdução

A Internet das Coisas (IoT) tem revolucionado a agricultura moderna, permitindo o monitoramento em tempo real de variáveis cruciais como umidade do solo, temperatura e níveis de nutrientes. Esses sistemas frequentemente dependem de redes de longo alcance e baixo consumo, como LoRa, para transmitir dados de sensores dispersos por grandes áreas agrícolas [1]. No entanto, a natureza sem fio dessas comunicações as torna vulneráveis a ataques cibernéticos, que podem comprometer a integridade dos dados e levar a decisões agrícolas prejudiciais.

2. Descrição do Problema de Segurança

Este estudo foca na vulnerabilidade de falsificação de dados em redes LoRa utilizadas na agricultura. LoRa é um protocolo de rede popular para IoT devido ao seu longo alcance e eficiência energética [2]. Contudo, certas implementações podem ser suscetíveis a ataques que permitem a injeção de dados falsos, comprometendo a confiabilidade das informações coletadas.

Figura 1: Comparação

Fonte: Elaboração Própria, 2024

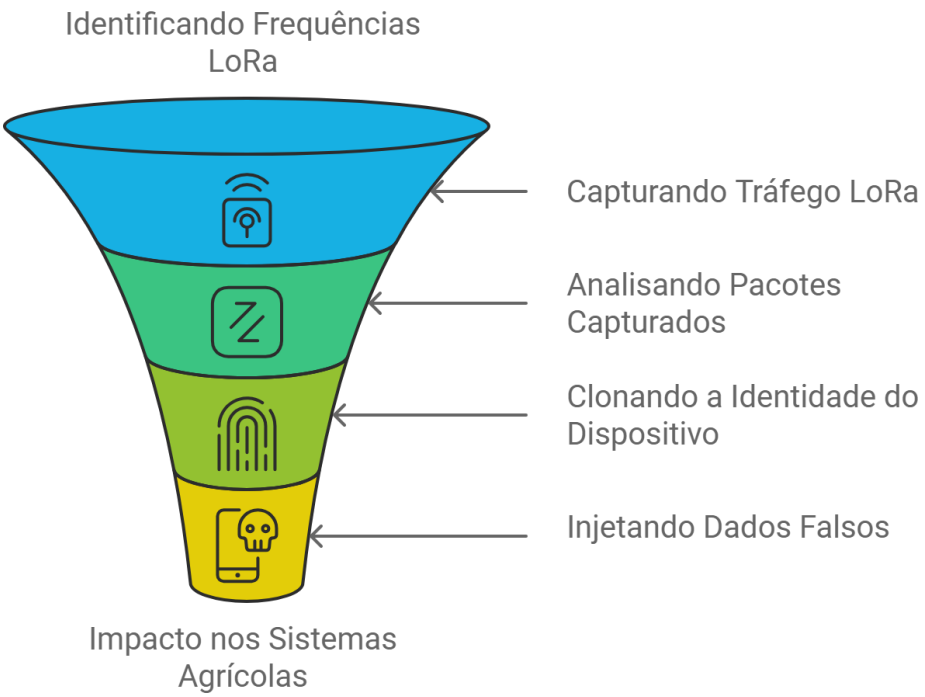
3. Descrição Detalhada do Ataque

O ataque de falsificação de dados em uma rede LoRa agrícola pode ser realizado seguindo estes passos:

- Reconhecimento: O atacante utiliza um analisador de espectro para identificar as frequências LoRa utilizadas na fazenda.

- Captura de Pacotes: Emprega-se um receptor SDR (Software-Defined Radio) para capturar o tráfego LoRa [3].
- Análise de Pacotes: Os pacotes capturados são analisados para entender o formato dos dados e identificar dispositivos alvo.
- Clonagem de Dispositivo: O atacante cria um dispositivo falso que imita a identidade de um sensor legítimo.
- Injeção de Dados: Utilizando o dispositivo clonado, o atacante injeta dados falsos na rede, por exemplo, indicando níveis errôneos de umidade do solo.
- Impacto: Os sistemas de irrigação automatizados respondem aos dados falsos, potencialmente causando danos às culturas por excesso ou falta de água.

Figura 2: Etapas do Ataque de Falsificação de Dados em Redes LoRa



Fonte: Elaboração Própria, 2024

Este tipo de ataque pode passar despercebido por longos períodos, causando danos significativos à produção agrícola e resultando em perdas econômicas substanciais.

4. Medidas deMitigação

Para prevenir e mitigar ataques de falsificação de dados em redes LoRa agrícolas, recomenda-se uma abordagem multicamada:

. Implementação de Criptografia Robusta:

- Utilizar AES-128 para criptografia de ponta a ponta, conforme recomendado pela especificação LoRa1.1 [4].

- Implementar criptografia em nível de aplicação além da criptografia LoRa padrão para uma camada adicional de segurança.

- Considerar o uso de algoritmos pós-quânticos para proteção futura contra-ataques baseados em computação quântica [9].

. Rotação Regular de Chaves:

- Estabelecer um processo para atualização periódica das chaves de sessão, idealmente a cada 24 horas ou após um número específico de mensagens [5].

- Implementar um sistema automatizado de gerenciamento de chaves para facilitar a rotação regular.

- Utilizar técnicas de derivação de chaves para gerar novas chaves de sessão sem transmitir material de chave sensível pela rede.

. Autenticação Mútua:

- Implementar autenticação bidirecional entre dispositivos e gateways usando o protocolo de junção OTAA (Over-The-Air Activation) do LoRa [6].

- Considerar a implementação de autenticação baseada em certificados X.509 para dispositivos críticos.

- Utilizar tokens de autenticação com prazo de validade curto para reduzir o risco de reutilização de credenciais comprometidas.

. Monitoramento de Integridade:

- Utilizar códigos de autenticação de mensagens (MACs) para verificar a integridade dos dados recebidos [7].

- Implementar verificações de consistência de dados, comparando leituras de múltiplos sensores em uma área para detectar anomalias.

- Desenvolver um sistema de log seguro e imutável para registrar todas as transmissões de dados, facilitando auditorias de segurança e forenses digitais.

. Análise Comportamental:

- Implementar sistemas de detecção de anomalias baseados em machine learning para identificar padrões incomuns nos dados dos sensores [8].

- Utilizar técnicas de análise de séries temporais para detectar desvios sutis nos padrões de dados que possam indicar manipulação.

- Estabelecer linhas de base para o comportamento normal dos sensores e configurar alertas para desvios significativos.

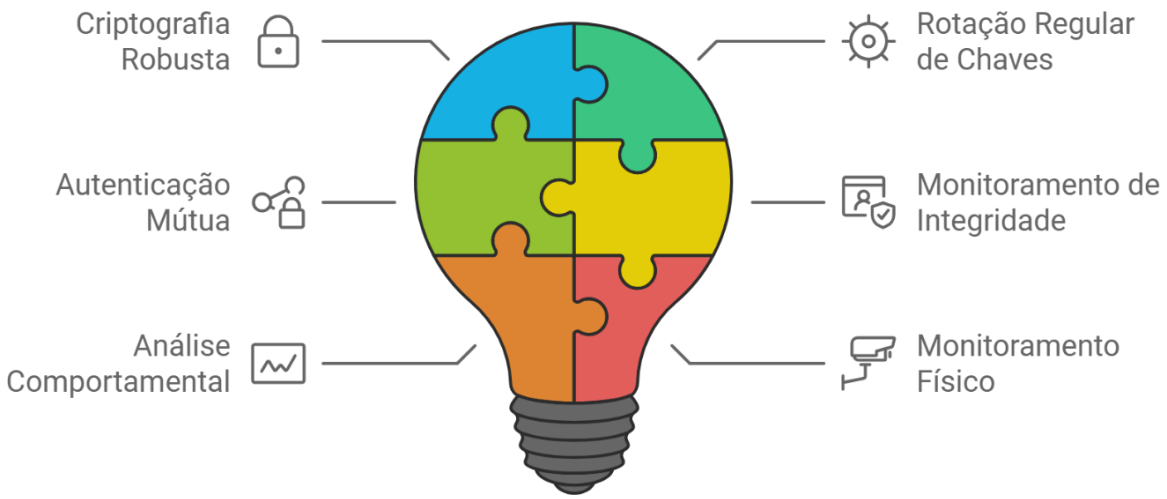
. Monitoramento Físico:

- Implementar medidas de segurança física para proteger sensores e gateways contra adulteração.

- Utilizar sensores de tamper-evidence para detectar tentativas de manipulação física dos dispositivos.

- Realizar inspeções regulares dos dispositivos em campo para identificar sinais de interferência ou dispositivos não autorizados.

Figura 3: Medidas de Segurança em Camadas para Redes LoRa



Fonte: Elaboração Própria, 2024

A implementação dessas medidas deve ser parte de uma estratégia de segurança abrangente e em constante evolução, adaptando-se às mudanças no cenário de ameaças e às necessidades específicas da operação agrícola.

5. Conclusão

A revolução da IoT na agricultura é inegável, trazendo ganhos impressionantes em eficiência e produtividade. Mas, como toda moeda tem duas faces, essa tecnologia também traz consigo riscos de segurança que não podemos ignorar. Nosso estudo mostrou como ataques de falsificação de dados em redes LoRa podem causar um estrago danado, desde o desperdício de recursos até a perda de safras inteiras.

É por isso que a segurança cibernética no campo precisa ser encarada como uma maratona, não uma corrida de cem metros. As fazendas e empresas agrícolas precisam ficar de olho vivo, sempre atentas às novas ameaças e prontas para se adaptar. Não dá para baixar a guarda.

Para enfrentar esse desafio, todo mundo precisa botar a mão na massa: agricultores, fornecedores de tecnologia, pesquisadores e até o pessoal do governo. Só assim vamos conseguir criar padrões de segurança que realmente funcionem. É unindo forças que o setor agrícola vai poder aproveitar tudo de bom que a IoT oferece, sem comprometer a segurança da nossa produção de alimentos.

E olha, o negócio não para por aí. A tecnologia está sempre evoluindo, e a gente precisa ficar ligado. Imagina só o impacto que a computação quântica pode ter na segurança das nossas redes no futuro? Por isso, a pesquisa nessa área precisa ser constante, pensando não só nos pepinos de hoje, mas também nos que podem aparecer amanhã. No fim das contas, é isso: a IoT na agricultura é uma mão na roda, mas a segurança tem que ser prioridade número um. Com as medidas certas e todo mundo alerta, a gente consegue usar essa tecnologia pra revolucionar a agricultura de um jeito seguro e sustentável. É assim que vamos garantir que o campo continue inovando e produzindo cada vez mais, sem deixar brecha pra ataques cibernéticos atrapalharem a festa.

6. Referências

[1] Jawad, H. M., Nordin, R., Gharghan, S. K., Jawad, A. M., & Ismail, M. (2017). Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review. Sensors, 17(8), 1781. https://doi.org/10.3390/s17081781

[2] Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the Limits of LoRa. IEEE Communications Magazine, 55(9), 34-40. https://doi.org/10.1109/MCOM.2017.1600613

[3] Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017). Exploring the Security Vulnerabilities of LoRa. 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), 1-6. https://doi.org/10.1109/CYBConf.2017.7985777

[4] LoRa Alliance. (2020). LoRa® Specification v1.1. https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1

[5] Eldefrawy, M., Pereira, N., & Gidlund, M. (2019). Key Distribution Protocol for Industrial Internet of Things Without Implicit Certificates. IEEE Internet of Things Journal, 6(1), 906-917. https://doi.org/10.1109/JIOT.2018.2843169

[6] Tomasin, S., Zulian, S., & Vangelista, L. (2017). Security Analysis of LoRa Join Procedure for Internet of Things Networks. 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 1-6. https://doi.org/10.1109/WCNCW.2017.7919091

[7] Butun, I., Pereira, N., & Gidlund, M. (2019). Security Risk Analysis of LoRa and Future Directions. Future Internet, 11(1), 3. https://doi.org/10.3390/fi11010003

[8] Mohamed, A.; Wang, F.; Butun, I.; Qadir, J.; Lagerström, R.; Gastaldo, P.; Caviglia, D.D. Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks. *Sensors* **2022**, *22*, 3498. https://doi.org/10.3390/s22093498

[9] Casola, V., De Benedictis, A., Rak, M. and Villano, U. (2019) Toward the Automation of Threat Modeling and Risk Assessment in IoT Systems. Internet of Things, 7, Article No. 100056. https://doi.org/10.1016/j.iot.2019.100056