Comunicação Segura com a Combinação de Algoritmos Criptográficos Simétricos e Assimétricos para a Rede Wi-Fi do Instituto Superior Técnico Militar.

Por Capitão (Inf.) EXE Jorge Pina Nacoca Evaristo

Luanda,
2024

Resumo

A segurança das comunicações tornou-se uma prioridade estratégica em ambientes militares. Este artigo analisa a eficácia da combinação de algoritmos criptográficos simétricos e assimétricos na protecção da rede Wi-Fi do Instituto Superior Técnico Militar (ISTM). Ao aliar a velocidade dos algoritmos simétricos com a robustez dos assimétricos, propõe-se um modelo de comunicação segura que resguarda a integridade, confidencialidade e autenticidade dos dados. A abordagem híbrida é analisada à luz das mais recentes ameaças cibernéticas e tecnologias emergentes, como blockchain e inteligência artificial.

Palavras-chave: criptografia híbrida, segurança cibernética, redes Wi-Fi militares, algoritmos simétricos, algoritmos assimétricos.

1. Introdução

A segurança da informação é uma preocupação crítica em organizações militares, onde a integridade e confidencialidade das comunicações são indispensáveis. No contexto do Instituto Superior Técnico Militar (ISTM), a adopção de medidas tecnológicas para garantir a protecção da rede Wi-Fi é urgente, dada a crescente sofisticação dos ataques cibernéticos.

A combinação de criptografia simétrica (como AES) com assimétrica (como RSA ou ECC) representa uma solução eficaz para enfrentar os desafios de segurança digital, ao permitir a troca segura de dados e autenticação confiável dos usuários. Essa abordagem é especialmente relevante em contextos africanos, onde há uma transição crescente para a digitalização das instituições militares (Nwaobi, 2019; Kasanga, 2020).

2. A Importância da Comunicação Segura em Ambientes Militares

A comunicação segura garante a confidencialidade, integridade e disponibilidade das informações em operações militares. A violação desses princípios pode comprometer toda a estrutura de defesa e estratégia operacional. O uso combinado de algoritmos criptográficos fortalece os sistemas contra interceptações e ataques man-in-the-middle.

Autores como Vella (2017) discutem a necessidade de revisar continuamente conceitos de uso dual e segurança cibernética. Ademais, abordagens baseadas na teoria dos jogos vêm sendo exploradas para modelar comportamentos adversariais em redes SCADA e ambientes militares (Kovach, 2016).

3. Compreensão dos Algoritmos Criptográficos

A criptografia simétrica utiliza uma única chave compartilhada para cifrar e decifrar dados. É rápida e eficiente, ideal para volumes grandes de informação. Já a criptografia assimétrica utiliza um par de chaves (pública e privada), proporcionando um canal seguro para a troca inicial de chaves e autenticação.

Essa combinação híbrida permite construir sistemas mais seguros e resilientes, optimizando o desempenho sem sacrificar a segurança (Alanhdi & Toka, 2024). No contexto do ISTM, a aplicação de ambos os métodos pode reduzir significativamente a superfície de ataque e mitigar riscos de acesso indevido.

3.1. Papéis Complementares dos Algoritmos Criptográficos

A criptografia simétrica oferece velocidade no tratamento de dados, sendo adequada para a protecção contínua da comunicação. A assimétrica, por sua vez, protege a fase inicial de negociação, assegurando que as chaves sejam trocadas com segurança. Essa sinergia garante tanto desempenho quanto segurança, princípios fundamentais para comunicações militares sensíveis (Calafate et al., 2024).

4. Implementação em Redes Wi-Fi Militares

A implementação da criptografia híbrida na rede Wi-Fi do ISTM não apenas reforça a segurança da informação, mas também se alinha a tendências modernas de protecção de redes sem fio. A integração com tecnologias emergentes, como blockchain e computação de borda, pode amplificar ainda mais os níveis de segurança e auditabilidade (Alanhdi & Toka, 2024).

Sistemas de identificação baseados em identidade (IBC – Identity-Based Cryptography) também vêm sendo explorados como alternativas promissoras para redes militares, reduzindo a complexidade na gestão de certificados e chaves (Zhao, 2012).

4.1. Benefícios da Abordagem Híbrida

A aplicação conjunta de algoritmos simétricos e assimétricos resulta em:

- **Maior desempenho** na criptografia de grandes volumes de dados.

- **Troca segura de chaves**, reduzindo a possibilidade de ataques de interceptação.
- **Autenticação confiável**, essencial para ambientes com múltiplos usuários.
- **Escalabilidade** e **resiliência**, atendendo à crescente complexidade das operações militares modernas.

5. Conclusão

A segurança da comunicação nas redes militares requer soluções que combinem robustez, eficiência e adaptabilidade. A integração de algoritmos criptográficos simétricos e assimétricos mostra-se como uma abordagem viável e eficaz para garantir a segurança da rede Wi-Fi do ISTM.

Além dos benefícios técnicos, tal estratégia fortalece a confiança institucional e prepara a infraestrutura tecnológica militar para os desafios futuros, especialmente diante da rápida evolução de tecnologias emergentes. A ética e a responsabilidade coletiva no tratamento de dados sensíveis devem ser pilares fundamentais na construção de uma cultura sólida de segurança cibernética (Miller & Bossomaier, 2024).

Referências Bibliográficas (Atualizadas)

- Alanhdi, A., & Toka, L. (2024). *A Survey on Integrating Edge Computing With AI and Blockchain in Maritime Domain, Aerial Systems, IoT, and Industry 4.0*. IEEE Access. https://doi.org/10.1109/access.2024.3367118
- Calafate, C. T., Cano, J. C., Curtò y Díaz, J. de, & Zarzà, et al. (2024). *Enhancing communication security in drones using QRNG in frequency hopping spread spectrum*. CORE. https://core.ac.uk/download/624406818.pdf
- Kasanga, G. (2020). *Passenger and luggage tracking system using sensor networks for public transport*. University of Zambia. https://core.ac.uk/download/618066592.pdf
- Kovach, N. S. (2016). *A Temporal Framework for Hypergame Analysis of Cyber Physical Systems in Contested Environments*. AFIT Scholar. https://core.ac.uk/download/277531444.pdf
- Miller, S., & Bossomaier, T. (2024). *Cybersecurity, Ethics, and Collective Responsibility*. Oxford University Press. https://doi.org/10.1093/oso/9780190058135.001.0001
- Nwaobi, G. (2019). *Emerging African Economies: Digital Structures, Disruptive Responses and Demographic Implications*. CORE. https://core.ac.uk/download/231920090.pdf
- Vella, V. (2017). *Is There a Common Understanding of Dual-Use?: The Case of Cryptography*. STRI. https://orbi.uliege.be/bitstream/2268/259287
- Zhao, S. (2012). *Issues and Solutions of Applying Identity-Based Cryptography to Mobile Ad-Hoc Networks*. University of Windsor. https://core.ac.uk/download/72791191.pdf