Uma Proposta de Plataforma de Simulação para Avaliação de Criptografia Pós-Quântica em Redes IoT

David Tavares[1], **Diego Abreu**[1], **Antônio Abelém**[1]

[1]Instituto de Ciências Exatas e Naturais – Universidade Federal do Pará (UFPA)
Rua Augusto Corrêa, 01 – Guamá
Caixa Postal 479 – 66.075-110 – Belém – PA – Brazil

{david.tavares}@icen.ufpa.br, diego.abreu@itec.ufpa.br, abelem@ufpa.br

Abstract. *Post-quantum cryptography is a promising alternative for protecting IoT systems against future quantum threats, although it may introduce communication and performance overhead. This work presents a proposal for a simulation platform to evaluate post-quantum cryptography in IoT networks. Based on Mininet and Mininet-WiFi, the platform is intended to support the future comparison of classical, hybrid, and post-quantum configurations under different topologies, protocols, and metrics. As a contribution, the article outlines the planned architecture and the evaluation methodology.*

Resumo. *A criptografia pós-quântica é uma alternativa promissora para proteger sistemas IoT diante de futuras ameaças quânticas, embora possa introduzir sobrecarga de comunicação e desempenho. Este trabalho apresenta a proposta de uma plataforma de simulação para avaliar criptografia pós-quântica em redes IoT. Baseada em Mininet e Mininet-WiFi, a plataforma foi concebida para apoiar a futura comparação entre configurações clássicas, híbridas e pós-quânticas sob diferentes topologias, protocolos e métricas. Como contribuição, o artigo descreve a arquitetura planejada e a metodologia de avaliação.*

1. Introdução

A Internet das Coisas (IoT) vem sendo aplicada em diferentes domínios que exigem coleta, transmissão e processamento contínuo de dados. Nesses cenários, a segurança das comunicações é essencial, sobretudo em dispositivos com restrições de energia, processamento, memória e largura de banda. Entretanto, parte da infraestrutura criptográfica atual ainda depende de algoritmos assimétricos clássicos, como RSA e ECC, cuja segurança pode ser comprometida pelo avanço da computação quântica [Shor 1997, Bernstein and Lange 2017].

Nesse contexto, a criptografia pós-quântica (*Post-Quantum Cryptography* – PQC) surge como alternativa para preservar confidencialidade, integridade e autenticidade [Bernstein and Lange 2017]. No entanto, sua adoção em redes IoT não é direta, pois muitos mecanismos pós-quânticos aumentam o tamanho de chaves, assinaturas e mensagens, além de impactarem latência, vazão, processamento e consumo energético [Sikeridis et al. 2020, Scott 2023].

A transição para a era pós-quântica tende a ocorrer de forma gradual. Por isso, abordagens híbridas, que combinam mecanismos clássicos e pós-quânticos, têm sido consideradas como estratégia intermediária [Stebila and Mosca 2017, Bindel et al. 2019,

Girón et al. 2023]. Ainda assim, essas abordagens também acrescentam *overhead*, reforçando a necessidade de ambientes que permitam avaliar seus impactos de forma controlada.

Diante desse cenário, este trabalho apresenta uma proposta de plataforma de simulação para avaliação de criptografia pós-quântica em redes IoT. A proposta é baseada em Mininet e Mininet-WiFi e busca permitir, em etapas futuras, a comparação entre cenários clássicos, híbridos e pós-quânticos. Como contribuição, o artigo descreve a arquitetura planejada, define uma metodologia de avaliação e delimita uma prova de conceito inicial. Por estar em fase de desenvolvimento, o trabalho é apresentado como uma proposta de plataforma em andamento.

2. Fundamentação Teórica e Trabalhos Relacionados

A segurança em IoT depende do uso combinado de criptografia simétrica, troca de chaves e autenticação. Embora algoritmos simétricos possam permanecer viáveis com ajustes de parâmetros, mecanismos assimétricos tradicionais são diretamente afetados por algoritmos quânticos, como o algoritmo de Shor [Shor 1997]. Esse cenário motiva a substituição ou complementação dessas primitivas por alternativas resistentes a ataques quânticos [Bernstein and Lange 2017].

Entre as abordagens de PQC, os *Key Encapsulation Mechanisms* (KEMs) são relevantes para o estabelecimento de chaves de sessão, enquanto assinaturas digitais pós-quânticas são importantes para autenticação e integridade. Neste trabalho, considera-se inicialmente a análise de mecanismos clássicos, como ECDH e ECDSA, mecanismos pós-quânticos, como ML-KEM e ML-DSA, e combinações híbridas entre essas primitivas [Bindel et al. 2019, Girón et al. 2023].

Apesar dos ganhos de segurança, esquemas pós-quânticos costumam apresentar objetos criptográficos maiores que os equivalentes clássicos. Em redes IoT, esse aumento pode elevar o número de pacotes transmitidos, o tempo de processamento, o uso de memória e o consumo de energia [Sikeridis et al. 2020, Scott 2023]. Esse impacto pode variar conforme o protocolo utilizado, como MQTT, CoAP ou HTTP, a topologia da rede e o número de saltos entre origem e destino.

Ferramentas como Cooja/Contiki-NG são comuns em estudos de IoT de baixo nível. Neste trabalho, opta-se por Mininet e Mininet-WiFi porque o foco inicial está na avaliação em nível de rede e aplicação, com variação de topologias e execução de aplicações em ambiente emulado. Assim, a proposta não substitui testes em hardware real, mas oferece uma base controlada para comparar diferentes configurações criptográficas.

3. Proposta da Plataforma e Metodologia

A plataforma proposta tem como objetivo oferecer um ambiente modular e reprodutível para avaliação de mecanismos criptográficos em redes IoT. Sua concepção baseia-se no uso de Mininet e Mininet-WiFi, permitindo emular redes cabeadas e sem fio com diferentes topologias. Sobre essa infraestrutura, planeja-se representar nós IoT, *gateways* e servidores de aplicação.

O principal diferencial da proposta é uma camada criptográfica intercambiável. Com isso, uma mesma aplicação poderá ser analisada em três modalidades: clássica, híbrida e pós-quântica. No cenário clássico, seriam utilizados mecanismos como ECDH

e ECDSA. No cenário híbrido, seriam combinadas primitivas clássicas e pós-quânticas, como ECDH com ML-KEM e ECDSA com ML-DSA. No cenário pós-quântico, mecanismos críticos seriam substituídos por alternativas resistentes a ataques quânticos, como ML-KEM e ML-DSA [Bindel et al. 2019, Girón et al. 2023].

A implementação futura considera o uso de bibliotecas como *Open Quantum Safe* e *liboqs*, voltadas à experimentação com PQC. Na plataforma proposta, essa camada será posicionada entre a aplicação IoT e os mecanismos de comunicação, permitindo alterar a configuração criptográfica sem modificar a lógica principal da aplicação.

A Figura 1 apresenta a arquitetura conceitual da plataforma proposta.

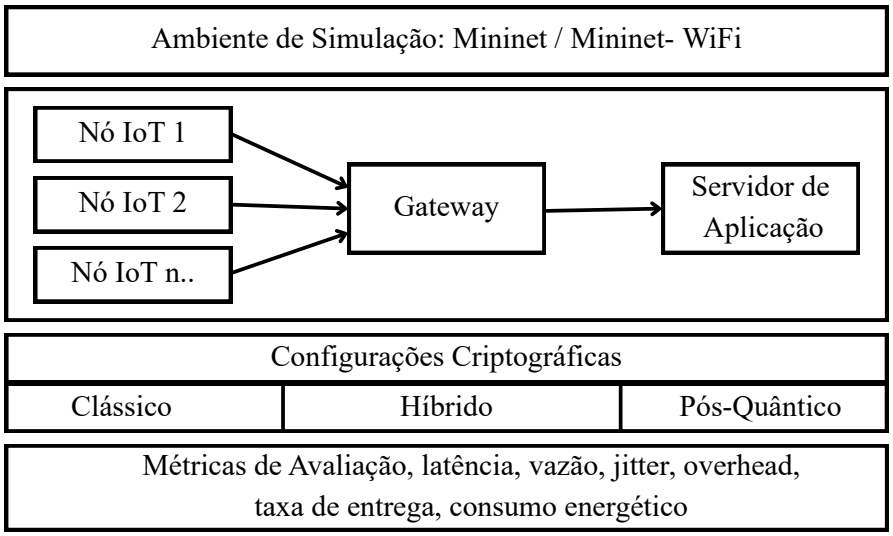

Figura 1. Arquitetura conceitual da plataforma proposta.

A proposta prevê integração com protocolos comuns em IoT, como MQTT, CoAP e HTTP. Também serão consideradas topologias em estrela, árvore e malha, pois o impacto dos mecanismos criptográficos pode variar conforme o número de nós, saltos, sessões estabelecidas e mensagens protegidas.

Como prova de conceito inicial, propõe-se um cenário mínimo composto por dois nós IoT, um *gateway* e um servidor de aplicação. Nesse cenário, os dispositivos enviarão mensagens periódicas ao servidor utilizando MQTT ou CoAP. A mesma aplicação será executada nas três configurações criptográficas, permitindo observar impactos iniciais sobre latência, tamanho das mensagens, tempo de estabelecimento de sessão e uso de recursos.

A metodologia de avaliação foi organizada em quatro etapas: levantamento do estado da arte, modelagem dos cenários, implementação dos módulos e análise dos resultados. As métricas previstas incluem latência, vazão, *jitter*, taxa de entrega, perda de pacotes, *overhead*, uso de CPU, uso de memória e consumo energético estimado. O *overhead* será calculado pela diferença entre o tamanho das mensagens protegidas e o tamanho das mensagens originais da aplicação. O consumo energético será estimado a partir do tempo de processamento, uso de CPU e volume de dados transmitidos.

Como limitação, Mininet e Mininet-WiFi não reproduzem integralmente restrições físicas de dispositivos IoT reais, como consumo medido em hardware, limitações de

microcontroladores e interferências reais de rádio. Portanto, os resultados futuros devem ser interpretados como estimativas em ambiente controlado. Em etapas posteriores, a proposta poderá ser complementada por experimentos em Cooja/Contiki-NG ou testbeds físicos.

4. Considerações Finais

Este trabalho apresentou uma proposta de plataforma de simulação para avaliação de criptografia pós-quântica em redes IoT. A motivação central está na necessidade de preparar sistemas conectados para a transição criptográfica exigida pelo avanço da computação quântica [Shor 1997, Bernstein and Lange 2017], sem ignorar as restrições de desempenho, energia, memória e largura de banda típicas desse domínio [Scott 2023, Sikeridis et al. 2020].

Como contribuição, o artigo descreveu uma arquitetura planejada, baseada em Mininet e Mininet-WiFi, voltada à comparação entre cenários clássicos, híbridos e pós-quânticos. Também foram definidos mecanismos inicialmente considerados, como ECDH, ECDSA, ML-KEM e ML-DSA, além da possibilidade de integração com bibliotecas como *Open Quantum Safe* e *liboqs*.

Por estar em fase de estudo e planejamento, o trabalho ainda não apresenta uma avaliação experimental completa. Essa limitação foi assumida de forma explícita, pois a contribuição principal desta versão está na estruturação da plataforma e da metodologia de avaliação. Como trabalhos futuros, pretende-se implementar os módulos criptográficos previstos, executar a prova de conceito inicial, ampliar os cenários experimentais e refinar os modelos de consumo energético.

Referências

Bernstein, D. J. and Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671):188–194.

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., and Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In Ding, J. and Steinwandt, R., editors, *Post-Quantum Cryptography*, pages 206–226. Springer, Cham.

Girón, A. A., Custódio, R. F., and Rodríguez-Henríquez, F. (2023). Hybrid key exchange in post-quantum cryptography: A systematic mapping study. *Journal of Cryptographic Engineering*, 13:71–88.

Scott, M. (2023). On TLS for the internet of things, in a post quantum world. Cryptology ePrint Archive, Paper 2023/095.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Sikeridis, D., Kampanakis, P., and Devetsikiotis, M. (2020). Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH. In *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, pages 149–156.

Stebila, D. and Mosca, M. (2017). Post-quantum key exchange for the internet and the Open Quantum Safe project. In Adams, C. and Camenisch, J., editors, *Selected Areas in Cryptography – SAC 2016*, pages 14–37. Springer, Cham.