Implementação de protocolos de autenticação pós-quânticos para Veículos Aéreos Não Tripulados em 6G

Laura Naves *l242819@dac.unicamp.br*
Marco Amaral Henriques *maah@unicamp.br*

Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (UNICAMP)

Resumo

A próxima geração de redes móveis (6G) exigirá comunicações com latência extremamente baixa e alta taxa de transferência, especialmente em cenários críticos como a comunicação entre Veículos Aéreos Não Tripulados (VANTs). Contudo, a iminente computação quântica torna obsoletas as criptografias assimétricas atuais, forçando a transição para a Criptografia Pós-Quântica (PQC). O principal desafio reside no fato de que os algoritmos PQC atuais são, em geral, computacionalmente pesados, podendo introduzir latência significativa e, consequentemente, prejudicar a comunicação em tempo real essencial para as operações de VANTs em redes 6G. Dessa forma, esta pesquisa foca na avaliação de novos protocolos de autenticação pós-quânticos otimizados que sejam eficientes o suficiente para serem aplicados na comunicação entre VANTs, dentro do ambiente 6G. O objetivo é garantir a segurança criptográfica contra ataques quânticos, mantendo a baixa latência e a autenticidade para a comunicação segura e em tempo real.

Palavras-Chave — Criptografia Pós-Quântica, Otimização de Protocolos, Protocolos de Autenticação, Redes 6G, VANTs.

1. Introdução

A evolução das redes móveis em direção à Sexta Geração (6G) representa um salto nas telecomunicações, prometendo taxas de pico de terabits por segundo e latências na faixa de microssegundos [1]. Este nível de desempenho não apenas aprimora as aplicações móveis existentes, mas também viabiliza cenários, como o de VANTs. A comunicação em tempo real entre drones e suas estações base é essencial para missões autônomas de monitoramento, entrega e resgate, onde qualquer atraso na troca de dados ou comandos pode resultar em falha da missão [2]. Os protocolos de autenticação e acordo de chaves (AKA) são fundamentais para a arquitetura de segurança das redes móveis, permitindo a autenticação mútua entre utilizadores e fornecedores de serviços, ao mesmo tempo que estabelecem chaves criptográficas para proteger a integridade e o sigilo dos dados [3]. No entanto, o desenvolvimento iminente da Computação Quântica representa uma ameaça a essas estruturas, uma vez que o Algoritmo de Peter Shor é capaz de quebrá-los em tempo polinomial. A transição para algoritmos de Criptografia Pós-Quântica (PQC) é, portanto, inevitável e urgente para garantir a segurança da infraestrutura de comunicação futura. Apesar de serem resistentes aos ataques quânticos, a maioria dos algoritmos PQC atualmente padronizados pelo NIST (*National Institute of Standards and Technology*) exige um custo computacional e de largura de banda significativamente maior do que suas contrapartes clássicas. Diante deste cenário, o presente trabalho se propõe a avaliar a eficiência de protocolos de autenticação pós-quânticos na comunicação entre VANTs, para que os requisitos de latência de redes 6G sejam atingidos.

2. Trabalhos Correlatos

No trabalho de Aissaoui et. al [2] é apresentada uma avaliação do impacto da criptografia pós-quântica (PQC) na comunicação de sistemas aéreos não tripulados (UAS). Os autores analisam como o PQC afeta o desempenho das tarefas em tempo real, alertando para o seu potencial impacto crítico em missões de drones. Entretanto, o estudo limita sua análise a cenários de redes existentes, não considerando as rigorosas demandas e os requisitos específicos de latência em 6G. O estudo estudo de Hülsing et. al [4] apresenta uma contribuição ao oferecer autenticação pós-quântica e segurança na troca de chaves validada simbolicamente pelo *Tamarin Prover*, mas a análise possui limitações. A metodologia utiliza apenas provas simbólicas, não oferece garantias de segurança computacional, limitando a confiança que podemos ter no protocolo.

3. Algoritmos Criptográficos Pós-Quânticos

Os algoritmos pós-quânticos são métodos criptográficos desenvolvidos para resistir a ataques de computadores quânticos. Allgyer et al. [5] descreve em seu trabalho a divisão dos algoritmos em principais famílias: baseados em reticulados (como Kyber e Dilithium), códigos (HQC, Classic McEliece), funções *hash* (SPHINCS+), isogenias (SIKE) e sistemas multivariados (Rainbow). O NIST (*National Institute of Standards and Technology*) tem liderado o processo de padronização, já aprovando Kyber e HQC para encapsulamento de chaves, e Dilithium, SPHINCS+ e Falcon para assinaturas digitais.

4. Comunicação de VANTs

A comunicação em Sistemas Aéreos Não Tripulados (UAS) envolve múltiplas comunicações. A primeira é entre o drone (VANT) e a Estação de Controle de Solo (GCS), um link que transmite comandos, telemetria e dados de vídeo. O segundo é entre o UAS e o sistema UTM (Gerenciamento de Tráfego de UAS), no qual o UAS envia telemetria para monitoramento de tráfego e recebe informações de segurança. Adicionalmente, pode haver comunicação direta entre os drones (UAVs), permitindo a troca de dados ambientais ou informações de roteamento para a GCS ou o UTM. A Figura 1 a seguir apresenta o cenário de comunicação.

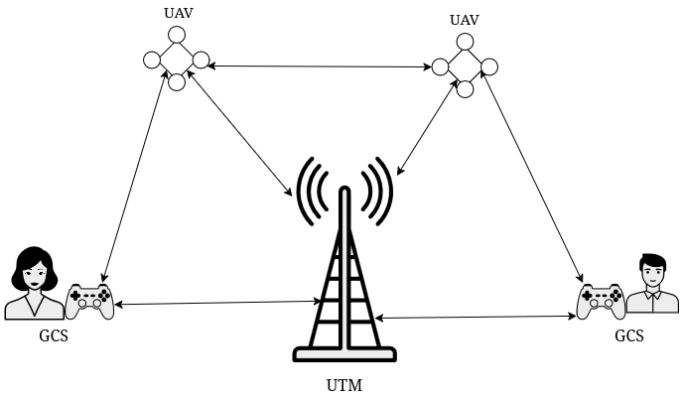

Figura 1: Tipos de comunicação em Sistemas Aéreos Não Tripulados (UAS).

É fundamental que todas essas comunicações garantam Autenticação e Integridade para assegurar a operação.

5. Métodos

Esta seção apresenta o processo metodológico que será adotado para a avaliação de um protocolo de autenticação pós-quântico para o cenário de comunicação de VANTs em redes 6G.

5.1. Execução Experimental

A abordagem de pesquisa será estruturada em cinco fases principais: inicia-se com a implementação de um protocolo de autenticação otimizado que incorpore a Criptografia Pós-Quântica (PQC). Em seguida, a segurança e a correção lógica do protocolo modificado são avaliadas por meio de um software de verificação formal, como o *Tamarin Prover*. Na sequência, é feito a instalação de um Sistema Operacional em Tempo Real (RTOS) em *containers*, os quais irão representar drones. Nesta próxima fase, será usado o emulador Mininet-WiFi para criar um canal de comunicação que executará o protocolo de autenticação com criptografia Pós-Quântica. Por fim, será usado um *sniffer*, como o Wireshark por exemplo, para fazer a análise do tráfego da rede e assim avaliar o desempenho da latência.

5.2. Diagrama do Experimento

Esta subseção apresenta o diagrama de implementação do experimento proposto desta pesquisa.

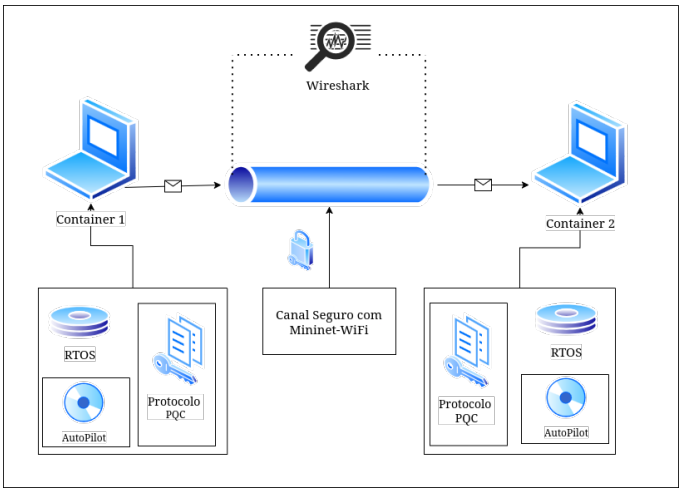

Figura 2: Diagrama de implementação.

A Figura 2 ilustra o diagrama de implementação desenvolvido para a etapa de testes. Para simular uma comunicação unicast entre dois Drones, será necessário o uso de dois *containers*. O núcleo do sistema é um Sistema Operacional em Tempo Real (RTOS), imple-

mentado no container. Dentro deste ambiente RTOS, o Mininet-WiFi é instalado para simular e criar o canal de comunicação sem fio. O protocolo de autenticação pós-quântica (PQC) e o sistema de controle automatizado AutoPilot (que gerencia a operação do drone) serão executados neste RTOS. Por fim, o tráfego do canal de comunicação será monitorado e analisado utilizando o sniffer Wireshark para a identificação mais precisa e resolução de problemas de comunicação, congestionamento e latência na rede.

6. Impactos da Pesquisa

A pesquisa objetiva garantir a autenticidade das comunicações em um contexto onde computadores quânticos, capazes de quebrar chaves privadas de criptografias assimétricas já estejam disponíveis. Qualquer otimização de protocolo de comunicação segura deverá buscar um equilíbrio entre segurança e desempenho. Ou seja, para atingir a baixa latência da 6G, um protocolo otimizado para desempenho poderá ter que aceitar um nível de segurança inferior ao ideal, resultando em uma possível vulnerabilidade.

7. Resultados e Discussão

Nesta fase inicial da pesquisa, os esforços concentraram-se na análise de viabilidade e na seleção das ferramentas metodológicas adequadas para a validação empírica. Atualmente, a investigação foca primariamente no estudo aprofundado do Mininet-WiFi, avaliando seu potencial e funcionamento para criar um canal de comunicação controlado. Além disso, está sendo feito um levantamento de protocolos de autenticação clássicos já adotados na literatura para serem adaptados a PQC e, posteriormente, avaliados quanto à segurança e desempenho.

8. Conclusão

Este trabalho abordou a fase inicial de uma pesquisa no cenário de VANTs, focada na implementação e avaliação de protocolos de autenticação pós-quânticos. A motivação central, validada pela revisão de literatura, reside na necessidade urgente de migrar dos algoritmos tradicionais para soluções pós-quânticas que garantam a segurança contra ameaças computacionais quânticas, especialmente considerando as restrições de *hardware* e latência. As próximas etapas se concentração no estudo do Mininet-WiFi para o desenvolvimento do canal de comunicação seguro e a implementação do protocolo de autenticação, a ser definido nos próximos estudos.

Agradecimentos

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio financeiro concedido por meio da bolsa de mestrado, essencial para esta pesquisa.

Referências

[1] M. Noor-A-Rahim *et al.*, "6g for vehicle-to-everything (v2x) communications: Enabling technologies, challenges, and opportunities," *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

[2] R. Aissaoui, J.-C. Deneuville, C. Guerber, and A. Pirovano, "Evaluating post-quantum key exchange mechanisms for uav communication security," in *2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*. IEEE, 2024, pp. 1–10.

[3] 3rd Generation Partnership Project (3GPP), "Technical specification (ts) 33.501: Security architecture and procedures for 5g system," [Online], o URL na solicitação original estava incompleto. Para uma citação completa, adicione os campos 'year', 'month' e 'version' (ex: V17.5.0) específicos que você consultou. [Online]. Available: https://www.3gpp.org/dynareport/33501.htm

[4] A. Hülsing, K.-C. Ning, P. Schwabe, F. J. Weber, and P. R. Zimmermann, "Post-quantum wireguard," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 304–321.

[5] W. Allgyer, T. White, and T. A. Youssef, "Securing the future: A comprehensive review of post-quantum cryptography and emerging algorithms," *SoutheastCon 2024*, pp. 1282–1287, 2024.