



ID da Contribuição: 30

Tipos: Trabalho em estágio inicial

Implementação de protocolos de autenticação pós-quânticos para VANTs em 6G

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.

Autor: NAVES, Laura (FEEC)

Co-autor: AMARAL HENRIQUES, Marco (DCA/FEEC)

Apresentador: NAVES, Laura (FEEC)

Classificação da Sessão: Sessões orais