Resumo do artigo: MiTM Attack Detection Scheme Using Monitoring Information in V2X Communication

Ana Fernanda S Cancado, Arthur de Sá B de Matos, Gabriel Praes B Nunes, Guilherme O de Oliveira, Júlia P Roque, Vitória S Araújo

April 29, 2025

1 Motivação

Com o avanço dos veículos autônomos e das cidades inteligentes, a comunicação *vehicle-to-everything* (V2X) tornou-se essencial para garantir a segurança e eficiência no tráfego. No entanto, essa comunicação é vulnerável a ataques do tipo Man-in-the-Middle (MiTM), que podem modificar ou descartar mensagens críticas, levando a acidentes e congestionamentos. Métodos existentes de autenticação e modelos de confiança não são suficientes para detectar ataques em todos os contextos.

2 Objetivos

O artigo propõe um novo esquema de detecção de ataques MiTM em ambientes V2X, utilizando informações de monitoramento do comportamento de veículos em tempo real, com o objetivo de superar limitações das abordagens existentes e melhorar a segurança dos sistemas de transporte inteligente.

3 Modelo

O esquema proposto baseia-se na estrutura BM-DEVS (Behavior Monitor - Discrete Event System Specification), que permite modelar comportamentos esperados dos veículos por meio de regras em lógica temporal. Ao detectar desvios nesses comportamentos, é possível identificar ataques. O modelo analisa trajetórias e eventos, validando a autenticidade das mensagens recebidas com base em monitoramento do ambiente e regras definidas.

4 Resultados

Simulações foram realizadas com cinco veículos autônomos em um ambiente de sistemas de transporte inteligente (ITS). O esquema proposto detectou ataques de modificação de mensagens com 9,84% mais eficácia e ataques de descarte com 10,45% mais eficácia em comparação com métodos baseados apenas em confiança. Em média, houve uma melhoria de 10,16% na taxa de detecção de ataques MiTM.

5 Conclusão e trabalhos futuros

O modelo demonstrou eficácia superior na detecção de ataques MiTM ao combinar verificação de mensagens com monitoramento comportamental. Como trabalho futuro, os autores pretendem explorar a detecção simultânea de múltiplos tipos de ataques e aprimorar o modelo para diferentes cenários de tráfego.