Distributed Authentication in Decentralized VANETS

Sujash Naskar, PhD student, Mid Sweden University, Sundsvall, Sweden.

Vehicular Ad-Hoc Networks (VANETs) offer enhanced road safety, efficient traffic management, and improved vehicle connectivity while dealing with privacy and security challenges in public communication. In these networks, authentication mechanisms are mandatory to establish trust among communicating entities, such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), without losing identity and location-based privacy. The prevailing conventional authentication mechanisms frequently depend on a centralized trust authority (CA) to ensure the mutual verifiability of transmitted messages. Nevertheless, in scenarios where the density of vehicles within the network is notably high, an overwhelming influx of authentication requests may result in a communication bottleneck at the CA, leading to a single point of failure. This paper proposes a novel distributed authentication scheme in a decentralized VANET with multiple independent CAs connected to multiple local inspectors to eliminate a single point of failure.

Furthermore, prior solutions lack the capability to immediately revoke a disputed vehicle that is transmitting malicious messages in the network. In this regard, the proposed scheme also facilitates an immediate revocation of a disputed sender to prevent other vehicles from further receiving malicious messages. As vehicles share time-sensitive data for driving assistance, our scheme minimizes the computation and communication costs for V2I key sharing and direct V2V authenticated message sharing significantly compared to previously proposed schemes. Using comparatively lightweight elliptic curve cryptography and eliminating the direct involvement of CAs in the authentication process, we have reduced the overall delays and achieved a maximum of 3.9 times faster V2I authenticated key sharing, and a maximum of 7.5 times faster V2V message sharing compared to state-of-the-art bilinear pairing-based protocols.

A comprehensive efficiency analysis validates our scheme's ability to outperform time-sensitive responses, such as sending and receiving an alert within nearly 4 milliseconds.

Supervisors: Prof. Mikael Gidlund, Prof. Tingting Zhang, Prof. Gerhard Hancke