Privacy and Security in VANETs

Mahdi Akil & Sujash Naskar

Abstract:

The Vehicular Ad-hoc Network (VANET) is specially designed for private, authenticated and secure communication between vehicles (V2V) and infrastructures (V2I) such as sharing positioning, warnings and other traffic-related data. This communication is public, therefore the potential security vulnerabilities and privacy theft are serious challenges. In our research, we develop solutions to privacy-preserving anonymous authentication and message transfer with the most efficient cryptographic primitives to support time-critical message transfer in VANET.

In VANET every vehicle is registered with a dedicated owner and if a valid driver borrowing the vehicle gets involved in a dispute, the owner will be accountable instead of the current driver. This causes losing privacy of the current driver as the driver might not want the incident to be known by the owner. A direct accountability of the current driver who can either be the owner or any registered driver is missing in the current literature which we have addressed to solve in our research work. In our approach, we have suggested a renting scheme that facilitates an owner to securely rent out the vehicle to a valid driver with an expiration time and an inspection protocol that can take the driver directly into account if a dispute is reported.

In our approach, we have completely removed any third-party involvement in authenticated message transfer between vehicles using secure zero-knowledge proof of knowledge techniques such as CL signatures. We aim to keep the total time needed for an authenticated message transfer within 10 msec, which is proven efficient enough for a vehicle to broadcast precrash warnings in real-time considering the network delays. The results of our research outcome can support vehicles to broadcast warning and traffic messages in real-time even while using comparatively fewer hardware resources compared to the literature. However, in the future, we have also aimed to design a more improved version of the protocol by putting zero trust in the vehicles while generating any authentication message.