Non-interactive & Privacy-preserving authentication scheme in VANETs

Mahdi Akil

Vehicular ad-hoc networks (VANETs) are mobile ad-hoc networks where vehicles communicate with each other by exchanging traffic information. If not secured in a proper way, this communication could allow a passive adversary to eavesdrop, which will give an attacker the ability to reconstruct the vehicles' mobility patterns [1].

Anonymous credential (AC) systems have been proposed in the literature to achieve privacy in VANETs. The primary purpose of AC is to hide the identity of the vehicles while communicating with other vehicles. However, the unconstrained use of anonymous credentials (AC) allows misuse, i.e., an adversary could create multiple credentials at the same time to launch a Sybil attack [2], or the anonymity feature offered by AC could give adversaries the desire to impersonate other vehicles.

In this work, we propose an autonomous anonymous authentication scheme for VANETs based on attribute-based credentials [3]. Our scheme has a decentralized architecture that allows vehicles to issue their own privacy-preserving identifiers without the intervention of a central authority. These identifiers are pseudonyms generated from a token wallet and allow anonymous authentication between vehicles. Our scheme is based on non-interactive zero-knowledge proofs of knowledge (NIZKP) and Camenisch-Lysyanskaya (CL) signatures [4] [5] [6].

References

[1] Pseudonym schemes in vehicular networks: A survey, Petit, Jonathan and Schaub, Florian and Feiri, Michael and Kargl, Frank, IEEE communications surveys & tutorials, 17, 1, 228–255, 2014, IEEE

[2] The sybil attack, Douceur, John R, International workshop on peer-to-peer systems, 251–260, 2002, Springer

[3] Security without identification: Transaction systems to make big brother obsolete, Chaum, David, Communications of the ACM, 28, 10, 1030–1044, 1985, ACM New York, NY, USA

[4] How to prove yourself: Practical solutions to identification and signature problems, Fiat, Amos and Shamir, Adi, Conference on the theory and application of cryptographic techniques, 186–194, 1986, Springer

[5] Efficient signature generation by smart cards, Schnorr, Claus-Peter, Journal of cryptology, 4, 3, 161–174, 1991, Springer

[6] Efficient group signature schemes for large groups, Camenisch, Jan and Stadler, Markus, Annual International Cryptology Conference, 410–424, 1997, Springer