A Threshold Anonymous Authentication Protocol for VANETs

Vehicular ad hoc networks (VANETs) have recently received significant attention in improving traffic safety and efficiency. However, communication trust and user privacy still present practical concerns to the deployment of VANETs, as many existing authentication protocols for VANETs either suffer from the heavy workload of downloading the latest revocation list from a remote authority or cannot allow drivers on the road to decide the trustworthiness of a message when the authentication on messages is anonymous. In this paper, to cope with these challenging concerns, we propose a new authentication protocol for VANETs in a decentralized group model by using a new group signature scheme. With the assistance of the new group signature scheme, the proposed authentication protocol is featured with threshold authentication, efficient revocation, unforgeability, anonymity, and traceability. In addition, the assisting group signature scheme may also be of independent interest, as it is characterized by efficient traceability and message linkability at the same time. Extensive analyses indicate that our proposed threshold anonymous authentication protocol is secure, and the verification of messages among vehicles can be accelerated by using batch message processing techniques.