abtechchennai@gmail.com
www.abtechnologies.in
9840511458

ALMS: ASYMMETRIC LIGHTWEIGHT CENTRALIZED GROUP KEY MANAGEMENT PROTOCOL FOR VANETS

ABSTRACT

Vehicular ad hoc networks (VANETs) were initially designed to assist in traffic management and delivery of safety messages. Due to the significant evolution in modern vehicles, the features offered by VANETs have expanded to include comfort and entertainment relevant services. This expansion has further increased the need to secure them. The security of VANETs is mainly dependent on sharing a cryptographic group key confidentially. Due to the frequent change in group membership, there is a need to update the group key repeatedly, which is difficult in highly dynamic networks like VANETs. Therefore, designing a secure, scalable, and efficient group key management protocol is challenging. Existing group key management protocols introduce a variety of limitations, including high computational cost for both group key computation and retrieval, additional computational and communication overhead when the membership in the group changes, and collusion among receiving vehicles. To overcome these limitations, this project introduces a novel group key management protocol, ALMS. Performance analysis reveals that, compared to existing protocols, ALMS is more scalable since it introduces a low computational overhead for both the Trusted Authority (TA) and the receiving vehicles. Also, it does not suffer from the key distribution limitation as symmetric key management protocols do. Moreover, ALMS introduces only a light overhead on the TA for group membership change. This is achieved by decoupling the initialization from group key computation and performing it offline without affecting the size of the encrypted group key.