Abstract

Safety applications are one of the most important applications of Vehicular Ad hoc Networks (VANETs), where safety messages are required to be disseminated in a timely manner to all vehicles within a region of interest. Broadcasting is regarded as the most suitable mechanism to disseminate safety messages, where the focus of routing protocols is on rushing message delivery. However, broadcast routing protocols such as the distributed vehicular broadcast protocol (DV-CAST) and Position-aware reliable broadcasting protocol (POCA) suffer from many types of attack such as forging and modification of safety messages, and repudiation of messages’ sources. To thwart such attacks, this paper proposes to empower DV-CAST with security mechanisms to ensure integrity, authentication, and source non-repudiation of safety messages using digital signature. Further, a position verification mechanism is used to ensure the correctness of node position information. Furthermore, privacy of vehicles is provided using temporary IDs. Simulation showed that the proposed security mechanisms do not affect the effectiveness of DV-CAST protocol.
Security of the Distributed Vehicular Broadcast Protocol DV-CAST

References


Index Terms

Computer Science                Security

Keywords

DV-CAST, VANET, safety application, authentication, non-repudiation, privacy, security mechanisms.