Abstract

Vehicular ad hoc networks (VANETs) ensure improvement in road safety and traffic management by allowing the vehicles and infrastructure that are connected to them to exchange safety messages. Due to the open wireless communication channels, security and privacy issues are a major concern in VANETs. A typical attack consists of a malicious third party intercepting, modifying and retransmitting messages. Heterogeneous vehicular communication in VANETs occurs when vehicles (only) or vehicles and other infrastructure communicate using different cryptographic techniques. To address the security and privacy issues in heterogeneous vehicular communication, some heterogeneous signcryption schemes have been proposed. These schemes simultaneously satisfy the confidentiality, authentication, integrity and non-repudiation security requirements. They however fail to properly address the efficiency with respect to the computational cost involved in unsigncrypting ciphertexts, which is often affected by the speeds at which vehicles travel in VANETs. In this paper, we propose an efficient conditional privacy-preserving hybrid signcryption (CPP-HSC) scheme that uses bilinear pairing to satisfy the security requirements of heterogeneous vehicular communication in a single logical step. Our scheme ensures the transmission of a message from a vehicle with a background of an identity-based cryptosystem (IBC) to a receiver with a background of a public-key infrastructure (PKI). Furthermore, it supports a batch unsigncryption method, which allows the receiver to speed up the process by processing multiple messages simultaneously. The security of our CPP-HSC scheme ensures the indistinguishability against adaptive chosen ciphertext attack (IND-CCA2) under the intractability assumption of q-bilinear Diffie-Hellman inversion (q-BDHI) problem and the existential unforgeability against adaptive chosen message attack (EUF-CMA) under the intractability assumption of q-strong Diffie-Hellman (q-SDH) problem in the random oracle model (ROM). The performance analysis indicates that our scheme has an improvement over the existing related schemes with respect to the computational cost without an increase in the communication cost.