ABSTRACT

The Vehicular ad hoc networks (VANET), a subclass of Mobile ad hoc networks (MANET) is an important technology used for improvement of Intelligent transportation system (ITS). VANET facilitates communication and coordination between vehicle drivers which helps to prevent road accidents, traffic congestion etc. In addition, VANET also provides other luxuries like internet access, weather information, mobile e-commerce and multimedia applications.

VANET’s architecture hosts three units: Road side unit (RSU), On board unit (OBU) and a suitable infrastructure which in combination enables communication and coordination between users and connectivity to the Internet. Specifically, VANET allows communication between road-vehicle, in-transit and inter-vehicle focusing on road safety and security. However, VANET is associated with security concerns related to confidentiality, integrity and possibility of unauthorised data elimination. Security and privacy issues are the foremost concerns amongst the VANET communications. This needs a high degree of liability from its participating vehicles (nodes) in the network.

Therefore, the prime objective of this research is to (1) provide authentication of VANET safety messages in vehicle-to-vehicle and vehicle-
to-infrastructure communications, (2) solve the security and privacy issues of VANET and (3) eliminate the use of conventional certificate based authentication methods.

In order to integrate security and confidentiality in VANET, different signature systems introduced by various researchers have been investigated. These signatures include Elliptic curve Pinstov Vanstone signature (ECPVS), proxy signature, blind signature and Public key cryptosystems (PKC).

Compared to Elliptic curve digital signature algorithm (ECDSA), ECPVS signature provides more confidentiality and compresses signature size up to 10 fold compared to Rivest Shamir Adleman (RSA) signatures. In addition, implementation of the ECPVS scheme is straightforward.

Proxy signature is a variation of the ordinary digital signature method, wherein the original signatory is assigned a secondary secret key derived from a primary secret key. The system is designed so that it is not possible to retrieve the primary secret with the knowledge of secondary secret. It involves three parties: original signer, a proxy signer and a verifier. The user who receives the messages can verify the identity of the original signer. It has been observed that the scheme proposed in this research showed improved performance compared to ECDSA. In addition, the inference from
simulation results shows that the packet delivery ratio is higher than the traditional signature algorithm.

On the other hand, blind signature does not reveal any information about the message. The hallmarks of blind signature scheme are untraceability and unlinkability, of messages received by the signer. Proxy blind signature in VANET is the first study in this research perspective. Moreover, the message delivered using the proxy blind signature maintains anonymity of the OBUs. This accomplishes the privacy requirement of the OBU and hence the user’s.

Another scheme called Identity based cryptosystem (IBC) is combined with PKC, where signer’s public keys are predetermined by information that uniquely identifies them, such as vehicle registration numbers or license plate numbers.

This study aims to test the proposed digital signature based authentication scheme using Network simulator (ns-2.34) to obtain results in controlled user environment. The ns2 is an open-source simulation tool that runs on Linux. The throughput of the system is enhanced by using the ECPVS algorithm while attaining the authenticity of the messages.