VANET SECURITY FRAMEWORK FOR LOW LATENCY SAFETY APPLICATIONS

by

ASIF ALI WAGAN

A Thesis

Submitted to the Postgraduate Studies Programme

as a Requirement for the Degree of

MASTER OF SCIENCE

INFORMATION TECHNOLOGY

UNIVERSITI TEKNOLOGI PETRONAS

BANDAR SERI ISKANDAR,

PERAK, MALAYSIA

FEBRUARY 2012

ABSTRACT

Vehicular Ad hoc Network (VANET) is a communication network for vehicles on the road. The concept of VANET is to create communication between vehicles, such as one vehicle is able to inform another vehicle about the road conditions. Communication is possible by vehicle to vehicle (V2V) and vehicle to road side unit (V2R). Presently, VANET technology is surrounded with security challenges and it is essentially important for VANET to successfully implement a security measure according to the safety applications requirements. Many researchers have proposed a number of solutions to counter security attacks and also to improve certain aspects of security i.e. authentication, privacy, and non-repudiation. The current most suitable security scheme for VANET is an Elliptic Curve Digital Signature Algorithm (ECDSA) asymmetric security mechanism. ECDSA is small in key size but it provides the same level of security as the large key sized scheme. However ECDSA is associated with high computational cost, thus lacking applicability in life-critical safety messaging. Due to that reason, alternative security schemes have been proposed, such as symmetric methods which provide faster communication, but at the expense of reduced security. Hence, hybrid and hardware based solutions have been proposed by researchers to mitigate the issue. However, these solutions still do not satisfy the existing safety applications standard or have larger message size due to increased message drop ratio.

In this thesis, a security framework is presented; one that uses both standard asymmetric PKI and symmetric cryptography for faster and secured safety message exchange. The proposed framework is expected to improve the security mechanism in VANET by developing trust relationship among the neighboring nodes, hence forming trusted groups. The trust is established via Trusted Platform Module (TPM) and group communication.

In this study, the proposed framework methods are simulated using two propagation models, i.e. two ray ground model and Nakagami model for VANET environment (802.11p). In this simulation, two traffic scenarios such as highway and urban are established. The outcome of both simulation scenarios is analyzed to identify the performance of the proposed methods in terms of latency (End-to-End Delay and Processing Delay). Also, the proposed V2V protocol for a framework is validated using a software in order to establish trust among vehicles.