Chapter 7

Conclusions and Future Scope

7.1 Conclusions

The entire focus of this thesis has been on securing the vehicular communications in vehicular ad hoc networks. After having a thorough review of various approaches adopted for security of vehicular ad hoc networks, it was realized that the public key cryptography, symmetric key cryptography as well as identity based cryptography approaches had few limitations in securing the communications in vehicular entities. One of the available approaches for enhancing the security of vehicular ad hoc networks is certificateless cryptography. Certificateless cryptography has the advantage that it reduces the certificate overhead and certificate revocation problem of public key cryptography. Moreover, it also solves the key escrow problem of identity based cryptography.

A new efficient certificateless aggregate signature scheme is proposed for vehicular communications. The proposed signature scheme is proven existentially unforgeable against the chosen message attack under the assumption that CDH problem is intractable in the random oracle model. The proposed CLAS scheme is adduced specifically for securing vehicular communications in vehicular ad hoc networks by reducing the signature verification time
drastically and helps in verifying more messages in the specific stipulated time, thus increasing the efficiency of the network. The propounded scheme has much less computational cost in terms of verifying signatures when compared with the already proposed works. This scheme will work efficiently in networks which have limited bandwidth such as vehicular ad-hoc networks.

The proposed certificateless aggregate signature scheme is employed for designing a security framework for enhancing the communication process in vehicular ad hoc networks. The proposed security framework achieves the security requirements of authentication, privacy, non-repudiation and confidentiality. The privacy of the scheme is preserved by using the pseudonyms for communication in the network. The proposed certificateless digital signature scheme is employed for inter-vehicular communication allowing the vehicles to anonymously communicate with each other. The message verification process is improved by employing the bloom filters in the scheme. The analysis of the security scheme is done with various parameters and proposed scheme of bloom filters have major performance improvements compared to the simple aggregate verification scheme thus, assuring the accuracy of the proposed security system.

A new fuzzy based trust prediction model has been designed for vehicular ad hoc networks by employing the concept of choosing the relay nodes for the selection of data transmission path. The trust levels are computed for each of the relay nodes chosen for the selection of best possible data transmission path. The effectiveness of the proposed model has been shown by integrating it with the routing protocols and testing it with the help of various evaluation parameters indicating that DSDV-F performs much effectively compared to AODV-F and DSR-F.

The two XML based modules have been designed for vehicular ad hoc networks which are:
Chapter 7 Conclusions and Future Scope

i) The decision inference system for the detection of misbehaving nodes which are transmitting the false information in the network.

ii) The V-health system is proposed by employing the XML dependency tree for the secure transmission of patient specific data to the nearest healthcare centres for the medical emergency.

The major contributions of the thesis are:

i) A privacy preserving authentication based security framework is designed for securing vehicular communications in vehicular ad hoc networks. The framework can be divided into two steps.

   a. A new certificateless aggregate signature scheme is proposed specifically for vehicular ad hoc networks and its security proof has been given in random oracle model.
   
   b. The security framework employs the use of pseudonyms for anonymity and proposed certificateless signature scheme for authentication purposes. It uses the bloom filters to enhance the signature verification process in vehicular communications.

ii) The proposed signature scheme has been implemented using Miracl library and the proposed security framework is implemented on a simulated environment with major performance improvements compared to other schemes.

iii) The trust prediction model has also been designed to secure vehicular communications along with two XML based modules for the secure VANETs.

7.2 Future Scope

In future, work can be extended on fully decentralized VANET authentication schemes while maintaining the applicable efficiency. The lightweight and efficient authentication scheme
can be designed based on decentralized regional transportation authorities in a particular region to further increase the communication reliability. The efficient position based schemes can also be explored to improve the proposed security framework. The impact of the velocity changes of the vehicles on simulation results can also be studied in the future.

The security framework can be further enhanced to incorporate the defense mechanism against various other attacks applicable in VANETs. An intrusion detection mechanism can be developed against various attacks applicable in VANETs to enhance the network security. The solution to inside attacks in the vehicular ad hoc network can also be given. Further, the proposed framework can also be implemented on real vehicles to obtain real time analysis of the results.