ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization

Vol. 5, Special Issue 4, March 2016

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

A Survey on Security Challenges in Cluster Based VANET with an Alert System

Ranjini.B[1], Naslin Sithara.N[2]

M.Tech Student [AECS], Dept. of ECE, NCERC, Pambady, Kerala, India [1]

Assistant Professor, Dept. of ECE, NCERC, Pambady, Kerala, India [2]

ABSTRACT: Vehicular Ad Hoc Networks (VANETs) is intelligent vehicular communication systems consist of a Road Side Unit (RSU) as main propagation module. Modelling of clustered VANET processed separately and propagates some security issues. Development of unusual behaviour is due to the absent of a standard verification scheme. In this paper we are proposing a solution for the general security and privacy issues and attacks. Survey mainly focused on analyzing the issues which emerged with different conditions and proposing an idea to overcome the security challenges in Vehicular Ad Hoc Networks. An integrated model of VANET is our future research.

KEYWORDS: RSU; VANET; Attacks; Verification Scheme

I. INTRODUCTION

Vehicular ad Hoc networks are transpiring as a new encouraging field of wireless technology that aims out a intelligent transportation system for the public safety and road topology. The basic architecture of vehicular networks comprises vehicles or nodes, an active communication network and a base station or Roads Side Unit (RSU). There are mainly four types of communications schemes are widely used in VANETs. Inter vehicular communication, Vehicle to Vehicle Communication (V2V), Vehicle to Infrastructure (V2I) and Vehicle to Broadband cloud (V2B).This schemes are emerging an efficient data exchange platform, share information and offer warning messages for driver assistance. Vehicle to road infrastructure communication scheme enables real time traffic and weather updates. Also provides environmental sensing and continuous monitoring.

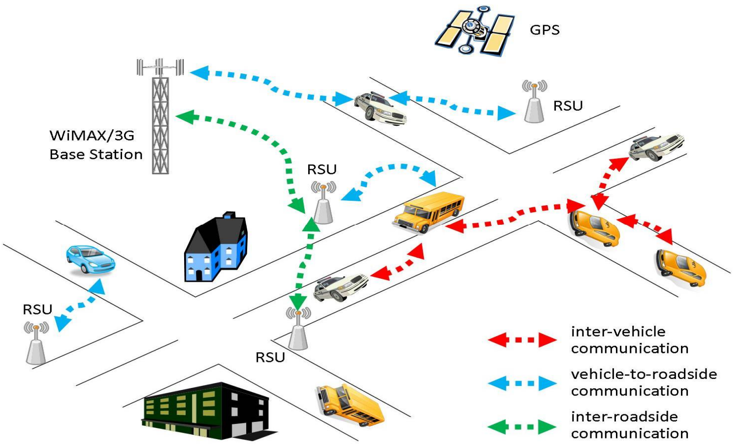
GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig. 1: Communication schemes in VANET

The main procedure in the intelligent VANET is to send traffic information to RSU or to other nodes. When we point out the communication part we have to protect our network from some attacks, fault messages and misuse of private content. To analysing these kind of unusual effects we must concentrated on network management, packet loss and collision control, environmental impact and security. Influentially a standard cryptographic verification scheme can be include to the network to abstain from the all privacy issues. An integrated model that consolidates MAC operations, channel conditions and traffic will expand the overall performance of VANET with increased throughput and manageable packet loss. In This paper the research discusses the security and privacy issues like confidentiality, authenticity, integrity, availability and non repudiation. The related issues are perturbed with protecting driver's personal information such as name, location, plate number etc.

II. SECURITY ISSUES IN VANET

Considering the architecture of VANET system, security got less attention so far. The communication packets comprise decisive information hence it is essential to make sure the packets are not be modified by the other network, attacker or third party. If any issues occurred with the system the information packets not be reached properly or it contains fault codes. A validation scheme with powerful cryptography validates the encrypted data with appropriate hash code and confirms the acceptance. This idea is often useful to detect the faulty messages or attack.

The security issues should be considered during the design of VANET, protocols and encryption/decryption algorithm. While considering the security challenges we have to consider the transmission delay, data consistency liability, error probability, key distribution and high mobility. In VANET the packets should be transmitted with in 100 ms Transmission delay. To achieve that should use a fastest cryptographic algorithm and a message authentication method. To avoid data inconsistency a validation scheme required which validates the messages if true otherwise declined. This scheme avoids malicious activities of nodes. Error probability is another important factor that we have to be considered. The design of routing protocols is depend upon the probability of error. Key generation is made during the encryption the key is only known by the maker. It will decrypt during reception. The two keys namely public key and private key have the main role in the key generation part. In high traffic conditions the packet loss will be high. Mostly the security problems occurred during the heavy traffic conditions.

III. RELATED WORKS

Researches and discussions are processing about the security issues in VANETs. In 2007, Raya and Hubaux proposed a method to hide all real information of users by anonymous certificates. Standard Public Key Infrastructure (PKI) is adopted to achieve authentication and data integrity. Generates large number of public/private key pairs to avoid the movement tracking. But the difficulty is that each vehicle needs large storage capacity to accommodate the key pairs.

In 2007,Lin *et al.* [12] proposed a scheme related to group signature that is only a group public/private key are stored in vehicle. In this scheme the group public key is same for all vehicles in the group but the group private key is different. The receiver validates the information by message authentication. Problem involving this scheme is the size of group signature is larger than the individual. So the overall cost increased.

In 2008, Zhang *et al.* [15] [19] found a Identity Based Batch Verification (IBV) scheme in VANET. They proposed one time identity based signature, which reduced the verification and transmission costs. This verification scheme is faster than the other PKI schemes.

Recently, Lee and Lai described two main problems of IBV scheme. Scheme is susceptible on the replaying attack. An opponent may simulate a fake condition such as traffic jam. Next is the IBV is not satisfy the property of non repudiation. Lee proposed a method to enhance security after research.

IV. SECURITY REQUIREMENTS AND SOLUTIONS

VANET system should satisfy the following requirements.
1. Authentication: Authentication shield message is generated by the genuine user. In vehicular network nodes are reacts based on the information came from the other vehicle hence authentication must satisfied.
2. Availability: Availability requires that the message must be available to the actual users. Attacks can bring down the network and hence the message cannot be public.
3. Non-Repudiation: non repudiation is the assurance that node can't deny the information or message he/she send. It may be critical to describe the correct sequence during reconstruction.
In this paper we discussed about vehicular ad hoc networks and some general security issues. We are proposing two solutions that will become very effective in VANETs. First method we found is the enhanced identity based batch verification scheme (EIBV). This scheme used a one time identity based signature that replaces the group

public/private keys and deduced the verification and transmission costs. Vehicles needs lesser storage capacity because it having one time validation signature. Before messages are sent, vehicles have to sign with their dedicated private keys. Validate the messages before reception by message authentication and validation. Deny if it is false. This scheme protects the network from all attacks. Next scheme related to the modelling of VANET and the performance of the system. Introduce an integrated model to increase the throughput and the packet delivery ratio. Clustering the vehicles is the main part. Clusters are generated by grouping vehicles or nodes moving in the same direction. Modelling of clustered VANET comprise three factors in to one model such as MAC operations in data link layer, channel conditions and mobility or traffic.

V. RESULT AND DISCUSSION

Figure 2 shows Packet delivery ratio Vs number of nodes of VANET with and without integrated modelling and IBV. In the result we can see in the integrated model the packet delivery ratio is increased with increased no of vehicles. So the overall throughput of the system increased.

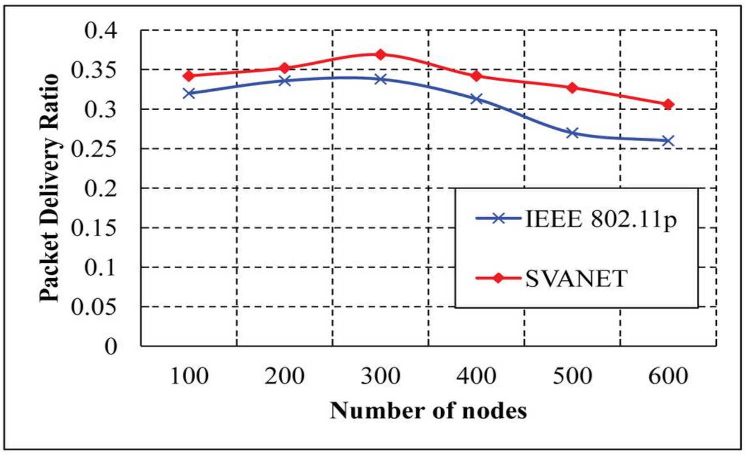

Fig. 2: comparison of conventional VANET and VANET with integrated model

TABLE I: SECURE ROUTING PROTOCOL

Security problem	Security attacks	Technique
Availability	Interruption	Group signature
Authentication	Fabrication	Certificate authority
Integrity	Modification	Digital signature
Confidentiality	Interception	Decryption / Encryption
Non repudiation		digital signature

VI. CONCLUSION

This paper has briefly introduced VANETs and the security issues related to the VANETs. In the final processing of this survey we found two efficient methods for solve the security, privacy issues and to increase the network performance. Identity based batch verification scheme adopted one time validation signature method. It will deduce the validation and transmission costs. Message will be decline if the validation is fail. Otherwise message will be validate.

By considering the performance of the VANET an integrated model is very effective to increase the packet delivery ratio and system throughput. VANET with EIBV and integrated model promise an efficient propagation system in the transportation field. An efficient alert system with EIBV and integrated modelling is our future research.

REFERENCES

[1] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," *B. Proceedings of the 2006 Workshop on Dependability Issues in wireless ad hoc network and sensor network 2006*, pp 1-8

[2] Z. Tong, R. R. Choudhury, N. Peng, and K. Chakrabarty, "P2DAP sybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 3, 2011, pp. 582 - 594.

[3] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," *Mobiquitous*, Aug. 2009

[4] G. Jyoti, S. G. Manoj, and L. Vijay, "A novel defense mechanism against sybil attacks in VANET," in *Proceedings of the 3rd International Conference on Security of Information and Networks (SIN '10). ACM*, New York, NY, USA, pp. 249-255. 2010

[5] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin,and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements,Architectures, Challenges, Standards and Solutions," *IEEE Commun. Surveys* & *Tutorials*, vol. 13,no. 4, pp. 584-616, Fourth quarter2011.

[6] IEEE Std 802.11p TM-2010, Amendment 6: Wireless Access in Vehicular Environment (Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications), IEEE Std, approved 17 June2010.

[7] H. Su and X. Zhang, "Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, no.56, pp. 3309-3323, 2007.