A Survey on Message Authentication for Secure Data Dissemination in VANET

[1]Pooja Patel, [2]Krunal Panchal

[1] *Student ,Information Technology, L.J.I.E.T, Gujarat, India*
[2] *Assistant Professor, Computer engineering, L.J.I.E.T, Gujarat, India*

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) have been researched with regard to enhance driver's safety and comfort in revolutionizing the vehicular communication industry. VANETs facilitate vehicles to share safety and non-safety information through messages. Safety information includes road accidents, natural hazards, roadblocks etc. Non-safety information includes falling information ,traveller information etc. The main goal behind sharing this information is to reduce road accidents by alerting the driver about the unexpected hazard. In these paper use advance cryptography mechanism between V2V,V2I,V2R for message authentication using ECC.

Keyword : *VANET,Authentication*

1. INTRODUCTION

1.1 VANET

Vehicles connected to each others through an ad hoc formation form a wireless network called "vehicular Ad hoc Network". "A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in as decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars, this is called vehicular ad hoc network"[1].VANET is subgroup of MANET. Vehicular ad hoc networks (VANETs) are expected in improving road safety and traffic conditions, in which security is essential[2]. Vehicles communicate with each other via vehicle-to-vehicle (V2V) communication and with an infrastructure called Road Side Unit (RSU) via Vehicle-to-Infrastructure (V2I) communication. Each Vehicle is equipped with an On Board Unit (OBU) with communication and processing capabilities. Vehicles communicate with each other and with the infrastructure through a Dedicated Short-Range Communication (DSRC) standard[3].

1.2 VANET ARCHITECTURE

There are three ways for data dissemination in VANET.

Vehicle to Vehicle

This is vehicle to vehicle architecture where vehicles act as both consumers and producers as vehicles receive information from other vehicles in the network and distribute that information to other vehicles in the network. So, both collection and distribution of data are done within the network for faster delivery of messages[4].

Vehicle to Infrastructure

This is vehicle to infrastructure wireless architecture in which infrastructure is used to collect information from vehicles and provide that information to other vehicles when necessary[4].

Hybrid

This is the combination of both V2V and V2I. Every node i.e., a vehicle or RSU communicates with other nodes in single hop or multi hop. VANETs are designed with the goals of enhancing driving safety and providing passenger comfort[4].

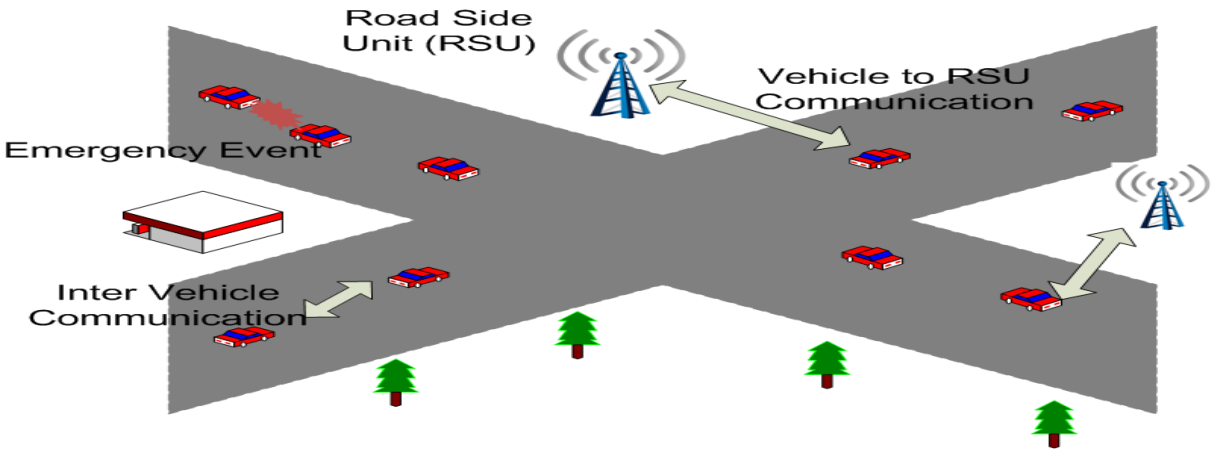

Fig -1: VANET Architecture[3]

In VANETs, the types of communication are the following:

- Vehicle-to-Vehicular (V-V) or Inter-Vehicular Communication.
- Vehicle-to-Infrastructure (V-I) or Vehicle-to- Roadside Communication.
- Inter Roadside Communication[4].

1.3 CHALLENGES IN VANETS

a) Multi-hop data delivery is challenging task as frequent disconnections and high mobility is there in VANETs.
b) Gathering of information like accident, speed limit, obstacle information, and traffic conditions etc. for safety and entertainment convenience purpose.
c) Vehicles should be chosen for data delivery in such a way that packets will be transmitted with minimum delay to destination[4].

1.4 APPLICATION

Accident Alert system:

The Accident alert system alerts the vehicle about the road accidents and the traffic conditions in the roads. According to the traffic conditions the vehicles has to choose the roads. Safety related information will be send to the vehicles through the messages in frequent time intervals. The message will also contain the accident location information which will be more useful for the vehicles[5].

Traffic Congestion alert system:

The Traffic congestion alert system alerts the vehicle drivers about the current traffic situation in a location.The driver of the vehicle is informed about the traffic condition and the nature of the traffic. The alert message will be normally generated from a vehicle which faces the traffic slow down problem. Whenever a vehicle receives these messages it retransmits the message to the centralized system as well as to the surrounding vehicles in its range[5].

Roadside Hotspots:

Nowadays people need internet facilities while on the move. One good solution for this scenario is implementation of roadside hotspots. This system consists of roadside access points and the vehicles on the road are

also act as transmitters. Whenever a vehicle comes in to the range of a roadside access point or a vehicle's range it will get access to the internet[5].

Parking management system:

The Parking management system provides information about the space availability in the parking location. Here the vehicles in the parking as well as the sensors in the parking location send messages frequently; this information will be used by the server and the incoming vehicle to know about the space availability in the parking location[5].

2. RELATED WORK

- ECDH-ECDSA aggregation[6] is a new security schema, by specifying an interaction zone,where a secret shared resulting from ECDH algorithm have been before the authentication step ,simulation proves that even if ECDH-ECDSA aggregation schema takes about 40ms more than ECDSA schema and provides higher level of security but using ECDH-ECDSA aggregation schema average of end to end delay is higher than ECDSA.
- Qr code[7] is used in message encryption and decryption increases the performance of the system, since it provides the facility of high speed encoding and decoding process.
- Secure data dissemination among vehicles in VANET is difficult for sloving that Timestamp defined message authentication code(TDMAC)[8] is used,which performs well in both qualitatively and quantitatively.
- cooperative authentication protocols[9] and group key (GK)[9] distribution protocols were proposed for efficient authentication and revocation. The protocols intake advantage of the fact that each vehicle can cooperate in the message verification processes by selectively verifying its received signatures and by reporting its own verification results to neighboring vehicles, because vehicles in same area possess nearly the same set of messages.
- PBAS[10] propose for reduce the computational overhead of RSUs using the distributing computing.In PBAS proxy vehicles are used to authenticate multiple messages with verification function at the same time[10].

2.1 LITERATURE REVIEW

Amina Bendouma, Boucif Amar Bensaber[6] propose ECDH-ECDSA schema to firstly ensure identification for RSU by an Elliptic Curve Diffie-Hellman(ECDH) algorithm where the vehicle confirms that the two neighbours RSU have the same shared secret, then secondly the vehicle authenticates the message beforehand signing, using Elliptic Curve Digital Signature Algorithm(ECDSA).This model provides higher level of security but average of end-to-end delay is increased.

Anirudh Paranjothi, Mohammad.S.Khan, Mais Nijim, Rajab Challoo[7] in their algorithm social networks are used to create anactive topology from all possible users in sender's profile, who are active at a particular point of time.Message authentication achived by providing profile of user and Quick Response Code(QR code) technique.The proposed architecture is used from the car dashboard.

Atanu Mondal, Sulata Mitra[8] proposed in the present work for secure data dissemination among vehicles in VANET using TDMAC. A timestamp defined MAC (TDMAC) is proposed in the present work as a light weight security solution. Detailed security analysis shows that TDMAC also thwarts passive attack as well as active attack. Its performance outperforms the existing MACs both qualitatively and quantitatively.

Hyo Jin Jo, In Seok Kim, and Dong Hoon Lee[9] proposed An anonymous message authentication protocol based on a cooperative authenticaton method, it is used for the safe transmission of message in VANETs ,but for the efficient authentication the cooperative authentication technique used and using this technique there is no synchronization problem between the non-cooperative and cooperative modes.In addition using this method reduce the overhead of Revocation List(RL) management using two-layer pseudo-identities.

Yiliang Liu, Liangmin Wang, Hsiao-Hwa Chen[10] proposes PBAS, Proxy Based Authentication Scheme makes use of vehicle's computational capacity to reduce the overhead of RSUs and the proxy vehicle can authenticate the multiple messages from the other vehicles and it can negotiate a session key with every other vehicle for confidentiality of sensitive information. Using these scheme reduce the transmission overhead , message delay , message loss ratio.

2.2 COMPARATIVE TABLE

Table -2: Comparative Table

Sr No.	Paper Title	Method Used	Advantage	Disadvantage
1	RSU authentication by aggregation in VANET using an interaction zone	ECDH, ECDSA	ECDSA has the advantage over RSA in that the signatures are much shorter (256 bits) and achieves the same security levels then RSA.	The average of end-to-end delay of ECDSA+ECDH aggregation schema is higher than ECDSA
2	MAvanet: Message Authentication in VANET using Social Networks	QR Code	Easy to track social interaction of the users through their social tie ups., Using QR code is high-speed encoding, decoding process and large storage space.	input data encrypted using QR is not safe as anyone can access encrypted information using QR reader/decoder.
3	TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET	TDMAC	Its performance outperforms the existing MACs both quantitatively and qualitatively	take maximum 48 vehicles for analysis
4	Reliable Cooperative Authentication for Vehicular Networks	Anonymous message authentication protocol based on Cooperative authentication method	Using these method there is no need to synchronization between non-cooperative and cooperative modes.	If the vehicle density is low these protocol may affect the reliability of authentication
5	Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks	Proxy based authentication	Proxy vehicles to realize efficient verification and PBAS has the lowest message loss ratio even when the speed increases.	Once a proxy vehicle is compromised ,its security performance will be decrease such that the entire verification process in a batch through the compromised proxy vehicles may lose its efficiency.

3. CONCLUSION

Vehicular Ad hoc Networks(VANETs) have been researched with regard to enhance driver's safety and comfort using the different security schema like ECDH-ECDSA,QR code ,proxy based authentication scheme,TDMAC, anonymous message authentication based on cooperative authentication method to get message authentication ,reduce the transmission overhead , reduce message loss, reduce message delay, and reduce the overhead of RL management.

4. REFERENCES

1. https://www.google.co.in/url?sa=t&source=web&rct=j&url=http://shodhganga.inflibnet.ac.in/bitstream/10603/68269/7/07_chapter%25201.pdf&ved=0ahUKEwjUmNO-18_XAhWKOY8KHQLzC3sQFghDMAI&usg=AOvVaw0wuV-rfUX-VAkeJdS3tZ69.
2. Han Yiliang[1,2], Lin Xi[2], Jiang Di[2], Fang Dingyi[1]." Attribute-based Authenticated Protocol for Secure Communication of VANET" 978-1-5090-4657-7/17/$31.00_c 2017 IEEE. pp. 4078-4081.
3. Ubaidullah Rajput[1], (Student Member, IEEE), Fizza Abbas[2], (Member, IEEE), Hasoo Eun[1] (Student Member, IEEE), and Heekuck Oh[1], (Member, IEEE)." A Hybrid Approach for Efficient Privacy Preserving Authentication in VANET" DOI 10.1109/ACCESS.2017.2717999, IEEE Access,vol. 5, pp.12014-12030, 2016.
4. Er. Gaganpreet Kaur, Dr. Sandeep Singh Kang."Technique to control Data Dissemination and to support data accessibility in Meagerly Connected Vehicles in Vehicular Ad-Hoc Networks (VANETS)" 978-93-85670-72-5 © 2016 RTCSIT. pp. 58-64.
5. B.Ayyappan[1], Dr.P.Mohan kumar[2]." Vehicular Ad Hoc Networks (VANET): Architectures, Methodologies And Design Issues" 978-1-5090-1706-5/16/$31.00 ©2016 IEEE. pp. 177-180.
6. Amina Bendouma, Boucif Amar Bensaber." RSU authentication by aggregation in VANET using an interaction zone" 978-1-4673-8999-0/17/$31.00 ©2017 IEEE.
7. Anirudh Paranjothi, Mohammad.S.Khan,Mais Nijim,Rajab Challoo." Mavanet- Message Authentication in VANET using Social Networks" 978-1-5090-1496-5/16/$31.00 © 2016 IEEE. pp. 1-8.
8. Atanu Mondal , Sulata Mitra." TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET" pp. 1-6,IEEE-2016.
9. Hyo Jin Jo, In Seok Kim, and Dong Hoon Lee." Reliable Cooperative Authentication for Vehicular Networks1524-9050 © 2017 IEEE. pp. 1-15.
10. Yiliang Liu, Liangmin Wang, Member, IEEE, and Hsiao-Hwa Chen." Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Network" vol. 64, IEEE Transactions on Vehicular Technology, pp. 3697-3710,IEEE-2015.