International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

A Survey on Security in VANETS and Applications

Sumanth G M[1] , Prabodh C P[2]

[1]*M-tech Student, siddumatdar@gmail.com*
[2]*Assistant Professor, prabodhcp@gmail.com*

Abstract- *Vehicular Adhoc Networks (VANETs) are significantly exploring field from past few years because of their diverse application. This sense the research analyst to build up their interest and research endeavors over late years to offer an enhanced safety and great travel comforts. yet, security concerns that are either generally seen in Adhoc networks is unique in VANET thus it presents great challenges. This paper is survey on possible variety of attacks and recent progress in the field of research that aim to intensify security of VANETS and variety of application.*

Key Words: Trusted Platform Module, Elliptic Curve Digital Signature Algorithm, Dedicated Short-Range Communications, Elliptic Curve Cryptography

1. INTRODUCTION

Mobile Ad-hoc network (MANET) is a Adhoc network in which network participants are mobile node which are moving randomly over the network and communicating wirelessly. Vehicular Ad-hoc Networks (VANET) are the special instance of MANETS in which the network participants are vehicles which are movable in a pre-defined pattern. It is the fact that the numerous lives lost in motor vehicle crashes every year is prominent among all the list of accidental deaths. Due to the increase in the human populations and roads will get busier by vehicles and other transporting activities. Thus, there is an urgent need to upgrade road safety and cut down traffic congestion. In this modern era technology is used to make life comfortable and convenient. Progressively vehicles are being fitted with sensors, embedded processing system and wireless communication system yielding a myriad of possibilities for influential life style changing applications on safety, efficiency, comfort, public involvement while they are on the road. Vehicles can also be employed to gather, interpret and share knowledge of an Area of Interest (AoI) in applications such as civilian surveillance (snapshot of violence incidents in progress can be sent to public authorities through certain powerful infrastructure),can be helpful for pollution control, roads and traffic planning and enormous others urban-aware applications. A current trend is to provide vehicles and roads with potential to make the travelling infrastructure prominently secure, more efficient, urban aware, and to make passengers' time on the road more entertaining. VANET architecture has hierarchy structure for security management. It has three variant levels in which each level has a different component to participate. The three different components of VANETS are Trusted Third Party (TTP), Road-Side Unit (RSU) and On-Board Unit (OBU) which include three types of communication.

As shown in fig-1 In VANETs, vehicles can talk with each other is named as inter-vehicle communication or Vehicle-to-Vehicle communications (V2V), vehicles can converse with base i.e. road Side Unit is named as vehicle-to-roadside or Vehicle-to- Infrastructure communication (V2I) to get some service. This infrastructure need to build along the roads and infrastructure can talk to each other is called as inter-roadside or infrastructure-to-infrastructure (I2I) communication.

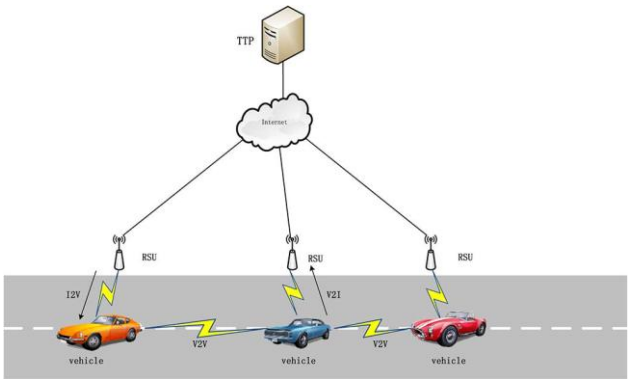


Fig -1: VANET Components and Communication Model

2. CHALLENGES AND THREATS IN VANETS

The vehicles has a sufficient enough source of electricity for computational unit, hence OBU need not to worry about limited battery life like other mobile devices like smart phones and wearable devices. Thus, one can embed all kinds of processors and chips into the OBU to allow the vehicle capability. But along this advantage, such computational effectiveness also leads to attacks that are computationally powerful and are not feasible in normal Adhoc networks. It is necessary to define the possible types of attacks because all attacks cannot be defended by one method. So, Different types of attack may require different technique to avoid their malicious intrusion. The more and more demanding requirements expected by the complicated real life situation serve as one of the driving forces that motivate researchers to come up with new methods.
The U.S. Federal Communications Commission (FCC) has allotted 75 MHz of Dedicated Short-Range Communications

(DSRC) spectrum at 5.9 GHz to be used for V2V and V2R communications. DSRC is a wireless protocol which allows data transfer and also may enable data to be easily monitored, modified and forged, including sensitive data information regarding the drivers' privacy. Therefore, to secure data shared in VANETs and managing the driver privacy have turn in two big challenges and reasons for lagging in the large scale deployment of VANETs. Researchers have been dedicated to solving these problems and many models have been proposed. Before analyzing the security models of VANETs, one must first identify the threats and challenges, requirements of security.

2.1 VANETS Have Unique Challenges -

Highly dynamic peers/vehicles/nodes-vehicles are mostly mobile and dynamic. At good speeds reacting for an imminent situation is very tough. For peers/vehicles it is crucial to verify/trust incoming information in real-time. Results in vigorous change in topology which leads to communication overhead for sharing new topology information.

Very large scale network-the number of vehicles in can be more. For an instance, in urban areas average number of vehicles active in the network may be in order millions. This may leads to network overload and congestion. To overcome this scalable system is required that can detect and react to these potentially hazardous situations by effectively deciding with which peers to communicate.

Decentralized infrastructure-VANET has a decentralized infrastructure means peers may enter or leave the network at anytime. If a peer is connected to a vehicle now, it is not guaranteed that it will be connected with the same vehicle in the future. And in such an environment, there is very much confusion in deciding trusted one.

Dynamic Environment -road condition are keep on varying briskly in VANET environment, for example road may be busy at one place but after travelling 5min it's free with no vehicles.

High Density Environment –Density of vehicles will not be constant in all the regions; it will be more inside the city and will be less in outskirts. VANET has to deal with highly varying node density.

2.2 Variety of Attacks

Monitoring
Social attack
Timing attack
Application attack
Network attack

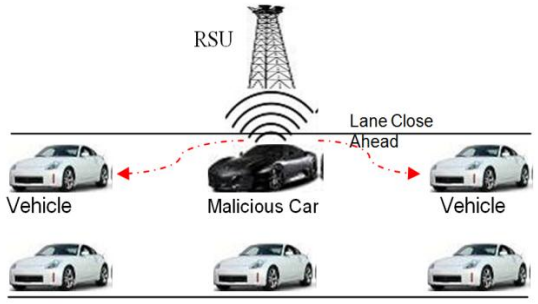
Table -1: Classes of Attacks

Attack classes:
The intention of the attackers is to incur problems in the network and preventing proper functioning of VANET by changing the contents type of messages

First class: Network Attack
This class includes attackers who are desired to directly impact neighbor vehicle and respective infrastructure of network. They have high concern because they impact the whole network. Main goal of the attackers is to do problem for legitimate users participating in the network

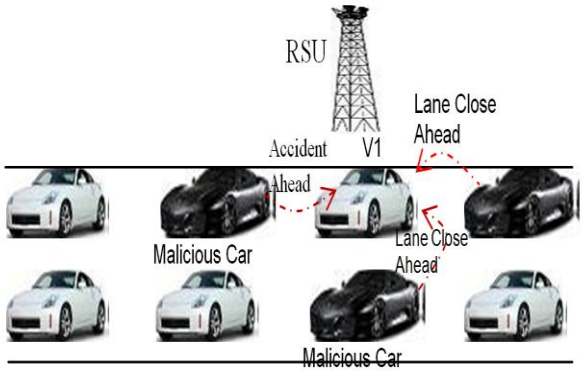
Some of the network attacks are
DOS (Denial of Service) Attack -attacker wants to jam the main communication medium by creating repeated false traffic in network and make network is no more accessible to legitimate users. The main goal of DOS attacker is to block the legitimate users to access the services provided by network. Hence users will not able to communicate with neighbor vehicles and also with infrastructure. Fig -2 illustrates that a malicious black car transmits a message "Lane Close Ahead" to a legitimate car behind it and also to an RSU to create a jam in the network.

Fig -2: Denial of Service (DOS) Attack



The Distributed DoS (DDoS) is more impactive and harder than the DoS where a huge number of malicious cars attack on a legitimate car in distributed manner from different locations and in different timeslots. Fig -3 illustrate that distributed malicious black cars attack on V1 from different direction and time so that V1 cannot afford all them at a time communicate with other vehicles.

Fig - 3: Distributed Denial of Service (DDos) Attack



Sybil Attack -the attacker floods the multiple messages to other participating vehicles and each message contains different fabricated source identity (ID). It yields delusion to neighbor vehicle by sending some dummy messages like traffic jam message. The objective is to impose other vehicles on the road to leave the road for the favor of the attacker.

Second class: Application attack

The main interest of the attacker is to manipulate application by altering details or contains of it and uses it for their own favors. In safety applications, the attacker manipulates the matter of the actual message and move on wrong or false information to neighbor vehicles which causes accident. Bogus information attack can be an attack example, in which intruder send bogus message to the network and these fake messages impact the behavior of vehicles on the road. E.g. Attacker receives one warning message "road under maintenance" from nearby vehicle. So attacker changes the matter of the message and sends the message as "Road is Clear" to other vehicle which may leads to road crashes. Same can happen in *Parking Availability* application of VANET.

Third class: Timing attack

This is a new and peculiar type of attack in which main objective of attacker is to incur more delay in the network. The attacker adds some time slot into original message and creates delay in original message in turn increases the delay in the network. One good thing is Attackers do not alter the other content of message or message payload, only create more delay between each message transmission and reception in the network.

Fourth class: Social attack

It is a kind of sensitive and social attack. In this attack some kinds of messages indirectly create problem in the network by mentally disturbing participants. Authentic users show abnormal behavior when they receive such kind of messages. E.g. Attacker passes a message "You are irritating" to nearby vehicle. When other user of VANET receives this message and his driving behavior may be affected by increasing the speed of his vehicle. This would indirectly disturb the other user in the network.

Fifth class: Monitoring attack

This includes monitoring and tracking of the vehicles attacks. In monitoring attack, the attacker just monitor the whole network, listens to the interaction between V2V and V2I. If any related information is found, then it is passed to the concerned person. E.g. Police plans to perform some operation against criminal and they communicate each other. Attacker would listen to all communication and informs the criminal about the police operation.

3. VARIOUS SECURITY APPROACHES

The section deals with various attacks and corresponding solutions.

3.1 Security Solution Using Cryptography

The transmission medium used in VANET is wireless and it has flaw that can make the network more vulnerable to security attacks such as jamming, eavesdropping and interference. Along with this, the upper layers of VANET protocol stack implicate the Open System Interconnection network model (OSI). Therefore vulnerabilities of OSI network model are inherited to vehicular networks. Fortunately, existing cryptographic solutions can be used for dealing security attacks.

Table-2: Attacks, Cryptographic solutions, and Respective Proposals.

Attacks	*Targeted Service*	*Proposals*
Eavesdropping	Confidentiality	Encryption on Sensitive Messages
Jamming	Availability	Pseudorandom Frequency Hopping
Traffic Analysis	Confidentiality	Randomizing Traffic Patterns
Dos	Availability	Signature based Authentication and Access Control
Message Modification	Integrity	Integrity Metrics for Content Delivery
Brute Force Attacks	Confidentiality	Public Key Schemes
Impersonation	Authentication	Trusted Hardware Module
Position Faking	Authentication	Active Detection Systems
Illegal Tracking	Privacy	ID based System for User Privacy

On studying [1] and [2] which has a very detailed survey on the classification of intrusions and corresponding countermeasures and cryptographic solutions. Table -2 summarizes the variety of attacks, their targeted services and corresponding cryptographic solutions and proposals. For other major attacks, one of the general cryptographic solutions namely standard public and secret key encryption schemes, public key infrastructure (PKI) and signature based authentication, network access control schemes and so on.

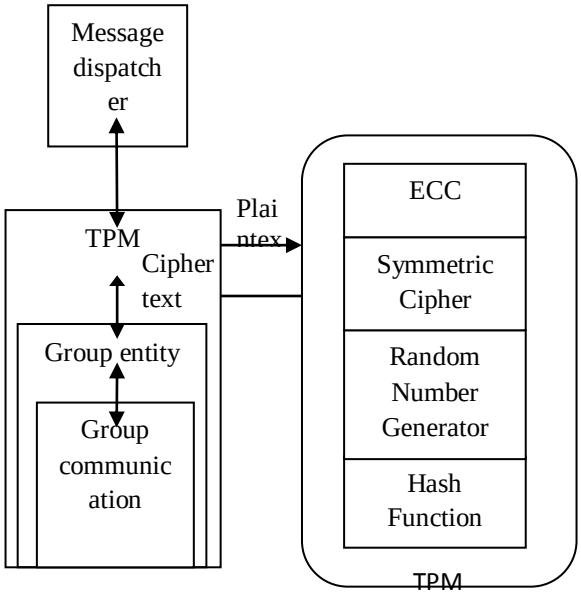
3.2 Framework For trust Grouping

In VANET, major security concern is exchange of safety messages that allow neighboring vehicles aware about the conditions and situations of the road. These safety messages are periodic and event driven. As the name says periodic messages are exchanged periodically many times

per second with surrounding messages. In the same way, event driven messages are exchanged only when an event occurs. Event may be the hazardous situations like accidents emergency within propinquity. Event messages must be delivered to concerned vehicles as faster as possible. Message encryption as well as decryption can cause delay which may lead to bad results like death. Hence here always be a tradeoff between interaction speed and security.

Asymmetric Public Key Infrastructure (PKI) a security system which uses Elliptic Curve Digital Signature Algorithm (ECDSA) is proposed as default security system for VANET in IEEE 1609.2.But this ECDSA algorithm has complexity in getting the results which leads to long delays of safety messages. Thus security concerns are diverting towards any other method that adopt symmetric cryptographic schemes. In order to tradeoff between security and speed of transmission, developers come up with a hybrid method [3] that make use of both asymmetric and symmetric cryptographic schemes. The method involves integration of both asymmetric and symmetric cryptography modules using hardware module for safety messaging. For nearby vehicles in vicinity trust grouping strategies are developed.

Fig -4: Trust Grouping Framework and TPM architecture.



This framework involves four major components as shown in the fig -4 [3]. Namely, message dispatcher, Trusted Platform Module (TPM), group entity and group communication. All these components form the desired trusted group through interactions that is shown in fig -4.

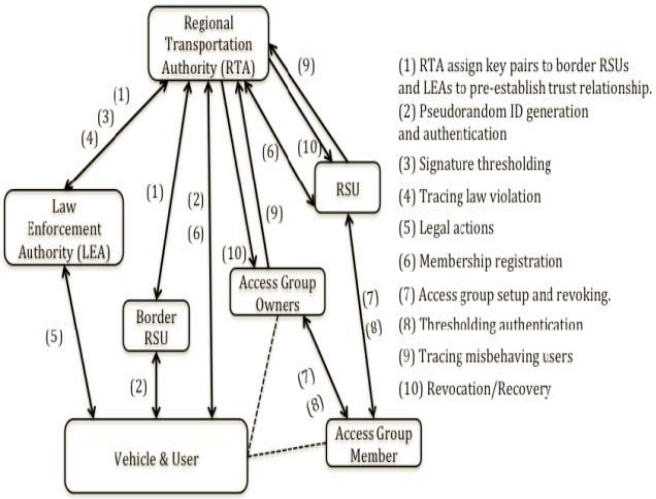
The TPM module includes the cryptographic capabilities involving asymmetric-Elliptic Curve Cryptography (ECC) and symmetric encryption, random number generation and hash function. Message dispatcher gives input message to TPM, TPM takes the messages and encrypts it, and send back the message to message dispatcher with desired security strength and speed. The ECC module along with hash function computes signatures for messages. Group entity contains group leader - an RSU, and group members - vehicular units in vicinity. The RSU computes onetime secret session keys and distributes among vehicular units by using the asymmetric ECC scheme. The vehicles form trusted groups in the network that use symmetric scheme for message security while preserving the security strength of asymmetric schemes.

3.3 Security System for User Privacy

Among the fundamental security requirements of VANET confidentiality is one of major parameter. Every user is concerned about their privacy in network which may be their identity and location history. Thus, it should be preserved by illegal tracking. Otherwise it will lead to cause uneasy for users to use the VANET network in spite of inviting the conveniences provided by it. Unauthorized misbehavers can easily denied by accessing services of VANET but its more complex and difficult to prevent the misbehave of legitimate user as they can pass over the authentication process.

Authenticating using anonymous credentials make it even harder to detect misbehavior of among legitimate users. An identity based [5] security system is proposed for VANET that can effectively deal with problems between privacy and tractability. It involves two separate methods for each of them. A pseudonym based method is used by this IDbased security system preserve user privacy. While, it adopts a threshold signature based scheme to solve the tractability for law enforcements. Both methods integrate to form the privacy preserving defense scheme that influences the authentication threshold.

Fig -5: Interactions of the IDbased Security System. [5]



Authentication beyond the threshold will implies misbehavior and which leads to revocation of the user credentials. Along with, this method adopts a dynamic

accumulator for thresholding that implies more restrictions beyond the threshold on communicating user. This is particularly attractive to service providers since they can achieve better efficiency of their services. Fig -5 shows the entities and their interactions that are in the IDbase system. The direction of flow is indicated by arrows. Message interaction on each arrow are numbered and detailed on the right side with respective numbers. The IDbased cryptosystem provide further design of an efficient communication and storage schemes. The system satisfies the security objectives which includes preserving user privacy, through the security and efficiency analysis.

4. APPLICATIONS OF VANETS

The VANETs applications are categorized as safety application and comfort application and its future application

4.1 Applications in Safety Measures

These application are mainly focused on the safety of the user and to avoid life losses caused by vehicular accidents. The main criteria of these application is to deliver the safety message to the intended user at right time to give the caution about any bad happenings. Intended user is the one who is approaching the danger area on road or in vicinity. Therefore VANET plays important in the ITS-Intelligent Transportation System. Safety applications may incorporate *Assistance Messages (AMs)* like route, collision avoidance (CA), and lane changing; *Information Messages (IMs)* like accident zone or working zone data; and *Warning Messages (WMs)* like post accident, snag or street condition notices. The fundamental objective of CCA application is to anticipate crash impacts. This sort of security applications will be activated consequently when there is a probability of impacts between vehicles. Vehicles, after recognizing a conceivable impact circumstance, send cautioning messages to alarm the drivers drawing closer the crash range. The drivers can take the best possible activities or the vehicle itself can stop or decline the pace naturally. The WMs are begin sending when vehicles identify a mishap to caution vehicles that are near the mischance zone. Another illustration is when vehicles sense risky street conditions they send WMs to different vehicles in a specific region, and these vehicles spread the WMs to the new vehicles entering that territory.

4.2 Applications in Comfort aspect

The fundamental point of comfort applications is to enhance traveler solace and activity effectiveness. These applications incorporated into Value-Added Services (VASs), which can be given through a VANET. Travelers in vehicles who spend a long stretch in travel may be occupied with certain application space for vehicular systems comprising in the procurement of various sorts of data [6].

Some of these applications are:

Atomized toll collection: Using this administration, the drivers don't have to stop and make the pay; rather the pay is done electronically through the system.

Applications in Entertainment aspect: Multimedia documents (music, motion pictures, news, eBooks, etc) can be transferred to vehicles. This information can likewise be exchanged starting with one vehicle then onto the next. Data about neighborhood eateries, inns, shopping centers, service stations can be transferred to the vehicles and can likewise be traded among vehicles utilizing the vehicular systems to encourage travelling.

Routing: Route and outing arranging can be put forth in defense of street blockings.

Internet Avalability: Passengers can surf the web and send/receive messages. The greater part of these applications will be downloaded from different systems (like web). Be that as it may, vehicles utilize the between vehicle systems to convey these data to lessen the expense connected with the establishment of the framework along the streets.

Parking providence: Notifications with respect to the accessibility of parking availability in the metropolitan urban cities finds the accessibility of openings in parking areas in a specific geological zone.

4.3 Future applications

As mobiles are well known and utilized by us as a part of our everyday life, comparatively the fate of VANETs is without a doubt se-cure. It has turned into the part of the government ventures. In India, National Highways Authority of India (NHAI) [6] is wanting to supplant manual toll accumulations at plazas with electronic toll collections (ETC) frameworks the over nation. The ETC framework will be founded on radio frequency identification (RFID), which will be supplemented by a remote on-board unit (OBU) on a vehicle, and in addition a stationery roadside unit (RSU) at the toll court.

Australian police in New South Wales (NSW) and Victoria are thinking about the presentation of new sort of laser velocity camera, which can get drivers utilizing cell telephones, and in addition speeding drivers from a large portion of a mile away [7]. The cameras, known as Concept II, have been made by Tele-Traffic UK and are now being used by UK's Dorset police as the most recent apparatus in their zero resistance battle against driving offenses. Likewise, different ventures are running in different nations to utilize VANETs in activity wellbeing and effectiveness. Similarly, various projects are running in various countries to employ VANETs in traffic safety and efficiency.

5. CONCLUSION

VANET is a rising exploration area with promising future and in addition incredible difficulties particularly in its security. It offers general adhoc system security concerns and confronts assaults, for example, spying, activity investigation and eavesdropping. The unique way of VANET moreover raises new security issues, for example, position discovery, illegal tracing and jamming. Conventional cryptographic methodologies that apply in VANET incorporate public key schemes to circulate onetime symmetric session keys for message encryption, certificate schemes for validation and randomizing activity designs against traffic analysis. The trust grouping framework takes a half and half approach of symmetric and symmetric cryptographic plans to accomplish both attractive handling rate and security quality. The pseudo IDbased framework is then secured and it utilizes threshold strategies for authentication and message signing so as to strike a harmony between the need to safeguard client protection and the necessity for traceability for law implementation powers. VANETS application is classified into safety and comfort and future use.

REFERENCES

[1] Isaac, J.T.; Zeadally, S.; Camara, J.S., "Security attacks and solutions for vehicular ad hoc networks," Communications, IET , vol.4, no.7, pp.894,903, April 30 2010. doi: 10.1049/ietcom.2009.0191 URL:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5454258

[2] Mohamed Nidhal Mejri, Jalel BenOthman, Mohamed Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Vehicular Communications, Volume 1, Issue 2, April 2014, Pages 5366, ISSN 22142096, URL: http://dx.doi.org/10.1016/j.vehcom.2014.05.001

[3] Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, AA; Mughal, B.M.;Hasbullah, H., "VANET Security Framework for Trusted Grouping Using TPM Hardware," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, vol., no., pp.309, 312, 2628 Feb. 2010. doi: 10.1109/ICCSN.2010.115 URL:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5437680

[4] Irshad Ahmed Sumra, Halabi Hasbullah, Jamalul-lail, Masood-ur- Rehman, "Trust and Trusted Computing in VANET", Computer Science Journal, volume 1, issue 1, April, 2011.

[5] Jinyuan Sun; Chi Zhang; Yanchao Zhang; Yuguang Fang, "An IdentityBased Security System for User privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol.21, no.9, pp.1227,1239,Sept.2010.doi:10.1109/ TPDS.2010.14URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5383352

[6] http://www.nhai.org/

[7] www.roadtraffic-technology.com