Analysis Security of Vehicular Ad Hoc Networks (VANET)

Ashish R. Ponkiya
Dept. of Computer science & Engineering
B.H. Gardi College of Engineering & Technology, Rajkot, Gujarat, India

Abstract:
Vehicular Ad Hoc Network (VANET) has mostly gain the attention on today's research and industries due to life saving factor. Whatever the solution is made until now for protect the network form adversary and attack that is not sufficient for securing the VANET. The need of strong VANET is totally dependent on the security and privacy features; those are discus in this paper. Security of vehicular network is most significant concern in VANET deployment because it is mandatory to assure the public and transportation safety. In this paper we review the various type of security problem and challenges of VANET been analysed and discussed; we also provide some taxonomy and critical review of notable security solution- for challenges and problem.

Keyword: VANET, DOS, Security attack, Vehicular - Communication,

I. Introduction

Wireless communication is ubiquitous because of its flexibility to work with different scenarios and topology. Mobile Ad Hoc Network (MANET) is one type of ad hoc network which coined for continually varying topology for handling the mobile device. Vehicular Ad Hoc Network (VANET) is one of its types. Node or vehicle in network can move around freely and speedy in environment [6]. In the world today battle field lies on the road, the estimated number of death is about 1.2 million people yearly worldwide [7], and injured forty times of this number, if not apply any traffic congestion that will make big amount of time and fuel wasting prosier.

Around 1991 the FCC (Federal Communication Commission) allocates a frequency spectrum for V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). DSRC (Dedicated short Range Communication) is used 5.850-5.925 GHz band for safety and private application for the Vehicular Communication [1]. At this allocated band the vehicle and Road side unit in VANET communicate wirelessly with each other while there is no infrastructure, ultimately vehicle become "Computer on Wheels" or "Computer network on Wheels". It is expected that software and automobile will cover 50% of total cost of automobile [8], However today automobile is fully equipped with IT and software technologies, and also VANET system is mainly design for the safety related information , safety of driver, vehicle and also avoid the minimizing the road accidents.

VANET is special type of MANET (Mobile Ad Hoc Network) [5]. Both are characterized by its mobility or movement and self organizing of nodes. But they are different in some way. By Having high mobility and unreliable channel condition VANET have many challenging research issues such as data sharing, security issue. In Addition there are no battery constrains for VANET so it is suitable for long distance for communication through vehicle. Safety application must be protected from intruder because compromising safety application is directly related loss of human life. Ultimately this life critical information must be protected while communicating. Without security, a vehicular Ad hoc network can be affected by many security attacks like DOS (Denial of service attack), message suppression attack and timing attack, Sybil attack, propagation of false message attack etc. That makes may be accident on road.

Our focal point in this paper is trash out the major security issues, basic requirement and challenges to design to fail safe and secure framework, and we will also discuss set of solution presented to solve these challenges and requirements.

a. WORKING OF VANET

Vehicular network consist of large number of vehicle, approximately 750 million in the world today [4]. Each vehicle can communicate with each other with sort rang radio signals DSRC (5.9 GHz) [1], within 1 km area of rang vehicle can communicated with freely movement. Here no wire has been required, the router used called RSU (Road Side Unit), RSU work as router between two node that also provide connection between the other higher authority network, like...PSTN. Each Vehicle has OBU (On Board Unit), this unit connected the vehicle to RSU via DSRC radio, and also other device TPD (Tamper Proof Device), Which holding the secrecy of vehicle, and all information about vehicle like keys, driver, identity, speed, rout…etc see figure-1.

In Section II we will briefly introduce possible attack in VANET. In Section III we proposed what r the requirements of VANET security. In IV Classification of security schema that proposed some of existing solution in VANET, and finally V discuss the overall paper in brief.

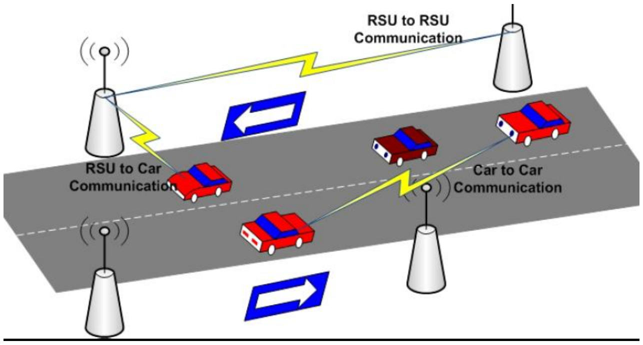

Fig-1 Strcture of VANET

II. POSSIBLE ATTACK IN VANET.

As VANET is also Ad hoc Network so it is suffer from various attacks that discuss in bellow section.

a. *Denial of service (DOS) Attack*

The availability of network is very important in network environment where all users are relying on network. Attacker send dummy message to jam the channel thought the performance and efficiency may reduce inn network [4]. In Fig-2 illustrated that malicious car transmits dummy massage to “Accident ahead” to other user and RSU to create jam on network. DDOS is variance of DOS where attack launch from different location, they may used different time slots for sending massage. The aim of those attacks is to slow down the network.

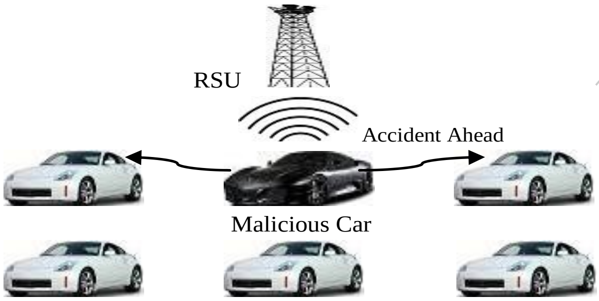

Fig-2 DOS Attack

b. *Bogus Information Attack*

In this type of Attack intruder may transmit the wrong or bogus information in VANET for their own benefit. For instance intruder may transmit the wrong information about the traffic condition on road for easily movement on road. This type of attack relies on authentication security requirement. By using Digital Signature Algorithm like Elliptical Curve Digital Signature Algorithm (ECDSA) [10], we can prevent message secure from this authentication attack.

c. *Black Hole Attack*

Another availability problem is black hole attack. In this type attack the Attacker is advertised its routing advertisement by using its own protocol. In this advertisement he clam that he has shortage path to the destination vehicle, As result one black hole area is created where traffic is redirected, either there is no destination node reside in that particular network. This causes data packet lost.

The one solution of black hole attack is used packet sequence number in header field of packet, so destination can easily identify that which packet is lost from the missing packet sequence. Another solution is design such a protocol that used number of route from source to destination, but this improved overhead of network.

d. *Sybil Attack*

In this type of attack intruder used multiple identify to send multiple massage; so different identity is used at same time. At this way attacker creates illusion that message has been send by different entity. The basic objective of this type attack is to mislead the vehicle [11].

Fig- 3 Sybil Attack

Sybil attack can eliminated using public key cryptography [12] where each vehicle is authenticated using public key. Key revocation is another approach that reduces effect of Sybil attack in Ad Hoc network using predefined propagation model.

e. *Timing Attack*

In this type of attack attacker main objective is to add time slot in original massage and create some delay in to massage. Attackers do not disturb the original massage, only create some delay and this massage received after it time required.

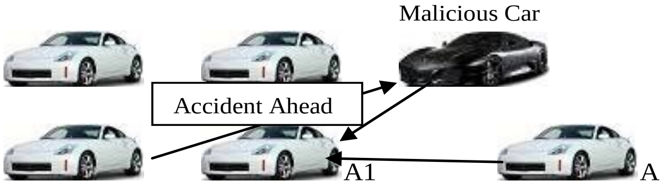

Fig-4 Timing Attack

In fig-6 illustrates that malicious black vehicle receives the “Accident Ahead” message it does not transmit it to other vehicles whenever it is at right position A but transmit it to the message to adding some timeslots so that whenever the vehicle receives the message it is not spot A1 where the accident has happened.

f. *Reply Attack*

In this type of attack hacker can reply a valid massage of a benign user. The attacker reply the transmitted of earlier information at a later time. The purpose of this type of attacks is to confuse authority and to take advantage of situation, in order to propagate the information into the network [12].

g. *Impersonation Attack*

In this type of attack hacker used identity of user-by using the MAC and IP Spoofing. They hide the original identity of user and uses identity of another node for perform the illegal activity in the network. By using the authentication certificate this attack may be protected because it is impossible to forget the certificate.

Table I: Comparison of Security attack with their type and security requirements.

Attack	Type of Attack	Security Requirements
Denial of Service	Insider, malicious, network attack.	Availability
Bogus Information	Insider	Integrity, Authentication
Black hole	Passive, outsider	Availability
Sybil	Network , Insider	Authentication
Timing	Insider, malicious	Integrity
Replay	Insider	Authentication
Impersonation	Network, Insider	Authentication

III. Requirements of VANET SECURITY SOLUTION

a. *Authentication*

For the trustworthy transformation the authentication is necessary in network. By authenticating the vehicle tit is sure that message has been sent from allege source and not from malicious vehicle. Otherwise Sybil attack, Reply Attack may possible in network. For authentication each vehicle assign every message with private key along with certificate, at receiver side , the receiver will receive message and check for the key and certified once this is done, the receiver will verifies the message [4]. For signing the message overhead is cause, for reducing this overhead we can used ECC (Elliptical curve cryptography), the efficient public key cryptography, or we can sigh key for just special message.

b. *Privacy*

Keeping the information of the driver away from unauthorised intruder, this information like real identity, trip path, speed, etc...

Privacy could be achieved by using the temporary key, these key should be changed continually. After using once the key will be expired after used [4], all the will be stored in to the TPD, and will be reloaded against next time that the vehicle makes an official check-up.

c. *Availability*

VANET specially designed for safety and security related information. For such information the life the network should be available must all the time (24/7) because life critical information has been transmitted between the sender and receiver [4].

By attempting to meet the real time demand make the system vulnerable to the DOS attack. Some time small delay in message is make it meaningless, and problem is become much bigger.

d. *Non-repudiation*

Any illegal activity of illegitimate user can equally harm people’s life. Non repudiation wills facilitate the ability to identify the attacker even after the attack will happen. These prevent the intruder from denying their crimes.

e. *Location Accuracy*

An adversary may report false information about its location and misguide others; so it is critical to determine whether the sending vehicle is at a given location or is on logical place. Therefore, to get accurate location of sending node is very important in VANETs.

f. *Real time Constrains*

As vehicle move fast on road, so this will response real time constrain to follow in some situations [6].

IV. CLASSIFICATION OF SECURITY SCHEMAS

Number of existing schema may classify in following category.

a. *Identity -Based Cryptosystem*

Sun et al. [9] presented a cryptosystem for VANETs which is identity based. This scheme uses pseudonym to provide privacy and traceability. This system avoids the use of certificates and in this way reduces overheads. The pseudonym may be generated by node itself or by the fixed RSUs. This system uses identity based cryptography that allows public key to be derived from user’s public identity like name or email address. This cryptosystem uses a defense scheme in which threshold signature and threshold authentication are to be considered for achieving non frame ability and privacy preservation against misbehaving nodes. This system uses proof of knowledge technique for authentication based defense scheme. This non frame ability scheme is basically designed for law enforcement authorities. It is desirable that there should be two or more authorities for identity retrieval process. This scheme has some issues like there is no simulation or experimentations so it is not clear that how id based cryptosystem will operate in vehicular ad hoc networks.

b. *Public key Cryptography Approach*

In this approaches,, each vehicle has a pair of secret key and public key. So public key must be efficiently handle by using key management approach for providing security. This system used whenever vehicle has two extra hardware one is TPD (Tamper proof device) and other is Event data recorder for the recording the event.

In VANET many security solution has been proposed, and many paper has been purposed for management of securing it.

The author of [4] suggested the used of virtual private key infrastructure (VPKI) where each vehicle have a public/private key pair, the public key is known to each node and private key is vehicles identity. When vehicle send safety massage to other vehicle at that time it sigh the message with it private key and add certificate to it as follows.

V → r: M, SigPrKV [M|T], Certv [4].

Where V is sending vehicle, M is message, T is timestamp, r is receiver of message. The receiver will get the public key by using the certificate, and verify the V's Signature using the certificate public key. For doing this receiver must have public key of it. This method has used the certificated based cryptography, this have some limitation one is that each time certificate have to verification, registration, revocation processes. These causes overhead in message transmit.

Another solution proposed by author of [13], efficient public key management system for VANETs: the Public Key Registry (PKR) system. Not only does this paper demonstrate that the proposed PKR system can maintain security, but it also asserts that it can improve overall performance and scalability at a lower cost, compared to the certificate-based PKC scheme. It is believed that the proposed PKR system will create a new dimension to the key management and verification services for VANETs.

c. *Certificate Revocation Approaches*

A public key infrastructure (PKI) is widely used to provide security in VANETs which includes certificate revocation (i.e., terminating the membership of a vehicle) [3]. Certificate revocation is performed by CA in two ways: centralized or decentralized. In the centralized approach, a central authority is responsible only for taking the revocation decision whereas in decentralized approach, a group of vehicles which are neighbors of the revoked vehicle take such a decision.

This scheme is centralized and uses pervasive infrastructure and not considered efficient since RSU sends the certificate revocation list (CRL) list to OBU and thus, the deployment cost becomes high. Some modified approaches have been proposed such as Revocation Protocol of Tamper Proof device (RTPD), Distributed Revocation Protocol (DRP), Revocation Protocol using Compressed Revocation Lists (RCCRL). RSU aided Certificate Revocation (RCR) is another newly proposed scheme where a Trusted Third Party (TTP) grants secret keys for each RSU so that it can sign messages in its range. Once a certificate is detected as invalid, certificate authorities (CA) issues messages to the RSU which broadcasts messages to all vehicles to revoke that particular certificate and stop communication with it.

V. DISCUSSION

In near future, it is expected that Vehicular ad hoc networks will deploy in different countries. Security of such networks is very essential because people's lives may be at stake due to it. In this paper we have explained why this problem has such particular requirements. We also describe different types of Attacks that are possible in vehicular ad hoc networks. We also surveyed the literature on several security issues specifically related to VANETs. These security issues make a potential stumbling block to deploy VANETs. From the analysis in survey, we came to know that – up till now – there doesn't exist a comprehensive security protocol or framework that covers all security aspects of VANET

REFERENCES

[1] The FCC DSRC (Dedicated Short Range Communications) web site. http://wireless.fcc.gov/services/its/dsrc/.

[2] Sakib, R., et al.: Security Issues in VANET, Research Thesis (2010)

[3] H. Al. Falasi and E. Barka "Revocatin in vanet: A Servay," *Innovations in Information Technology (IIT),* 2011 *International Conference on*, pp.214-219, 25-27 April 201.1.

[4] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,"Certificate Revocation in Vehicular Networks "Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland, 2006

[5] Gillani, S., et al.: Vehicular Ad hoc Network, Enabling Secure and Efficient Transportation System, Technical Journal, University of Engineering and Technology, Taxila, Pakistan (2008)

[6] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[7]http://www.who.int/features/2004/road_safety/en

[8] Saad, A., Weinmann, U.: Automotive software engineering and concepts. GI Jahrestagung, Frankfurt, Germany, pp. 318–319 (2003)

[9] Sun, J., et al.: An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. IEEE Transactions on Parallel and Distributed Systems 21(9), 1227–1239 (2010)

[10] M. Manvi, M.S. Kakkasageri, and D.G. Adiga,"Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approch",*Future Computer and Communication, ICFCC 2009. International Conference on*, 2009, pp. 16-20.

[11] Gada, D., et al.: A Distributed Security Scheme for Ad Hoc Networks. ACM Crossroads, Special Issue on Computer Security 11(1), 1–10 (2004)

[12] Samara, G., et al.: Security Analysis of Vehicular Ad Hoc Nerworks. In: International Conference on Network Applications Protocols and Services (2010).

[13] Shen, Pei-Yuan, Liu, Vicky, Tang, Maolin, & William, Caelli." An efficient public key management system: an Application in vehicular ad hoc networks" In Pacific Asia Conference on Information System (PACIS), AIS Electronic Library (AISeL), Queensland University of Technology, Brisbane, Qld, p. 175.(2011)

[14] Karagiannis, G., et al.: Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. IEEE Communications Surveys & Tutorials

[15] Xiong, H., Guan, Z., Hu, J., Chen, Z.: Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview (online) (2012)