Security Requirements and Mechanisms in Vehicular ADHOC Networks (VANET)

M.Newlin Rajkumar[1], M.Nithya[2], M.Krithika[3]

[1]*Assistant Professor, Department of Computer Science, Anna University Regional Office, Coimbatore,Tamilnadu,*
[2]*PG Scholar, Department of CSE, Anna University Regional Office, Coimbatore, Tamilnadu, India.*
[3]*PG Scholar, Department of CSE, Anna University Regional Office, Coimbatore, Tamilnadu, India.*
E-mail: newlin_rajkumar@yahoo.co.in,krithikalilly2@gmail.com,nithisri92@gmail.com.

Abstract: **In recent years, Vehicles are becomes the more intellectual system which is operated with the help of radio communications. Thus the vehicles are formed the network for communications called as Vehicular Adhoc Network(VANET) which depends on Mobile Adhoc Network(MANET).However in Vehicular Adhoc Networks (VANET),the security will make an big issue, due to communication development, because of dynamically changing protocols, high mobility of vehicles and also high partitioned network. In this paper we address the security requirements of vehicles and needed mechanisms to avoid the threats and attacks in VANET.**

Keywords: **VANET, NDM, ARAN, SEAD, ARIADNE**

I. INTRODUCTION

VANET communication is takes place in three ways, Vehicle-to-Vehicle communications, Infrastructure-to-Vehicle communication, Vehicle-to-Infrastructure communication,. VANET will developed for wide variety of non-safety applications and safety applications, which permit for value added examination includes location-based service, automated toll payment, traffic management, vehicle safety, enhanced navigation, that should be used for predict the following applications such as access to the internet(infotainment applications), closest fuel station, finding the restaurant or travel lodge.

The vehicles are operated with one type of radio interface called OnBoard Unit (OBU), which is used for transforming the information between the vehicles and the Road Side Unit (RSU) that forms the small ad hoc wireless networks. The supreme goal of VANET is to offer the road safety information in the vehicles, thus the continuous exchange of data in the network specifies the function of security. Thus any attack in the network will make loss of information in VANET, which leads to accidents and all.

A.TYPES OF ATTACKER

1) ACTIVE vs PASSIVE ATTACKER

The active attacker will generate the packets or any signals and send to the destination node, while the passive attacker will just gain the information which is passing between the sender and receiver.

2) LOCAL vs EXTENDED

The attacker makes control of various base stations or any vehicles to a local network is said to be an Local attacker, whereas the extended attacker makes control of a variety of base stations or vehicles which is scattered among the network. Example of this attacks are warm hole attack and privacy-violating attack.

3) INSIDER vs OUTSIDER

The attacker act as a authenticated member and communicate with the other member of the network is called as inside attacker, whereas the outsider is the network member who act as an intruder and makes misuse the network.

4) MALICIOUS vs RATIONAL

The attacker who didn't get any benefit in the attack, but to injure the functionality or any member of the network is said to be an malicious attacker, whereas the rational attacker get personal gain in the network.

II.SECURITY REQUIREMENTS AND SECURITY MECHANISMS

The security trouble is not same as the common communication network, the implementation of VANET is different from various network, because of mobility, size of network, geographic relevancy etc. Design of VANET security protocols,

cryptographic algorithms, VANET architecture makes more security challenges. VANET should be suitable for some cryptographic related security requirements, before they are deployed in the network. Thus this paper explains about the security requirements with related attacks happened in the cryptographic based classification moreover their corresponding security mechanisms and protocols used.

A.AVAILABILITY

To send and receive the message, the network should be available at any time, and it also makes sure that the network is serviceable and convenient information should available in any functioning time.

The threats which are likely present in this availability techniques is:

1) Denial of Service

The network insiders and outsider makes the network unavailable for the users who are actually authenticated by jamming and flooding with high volumes of messages. Thus the Road Side Unit (RSU) and On Board Unit (OBU) cannot be control this large volume of received information.

2) Broadcast Tampering

The inside attacker choose one route and infuse bogus messages into the network, that makes the network to cause any damage such as accidents by hiding the traffic warnings or creating traffic flow in that route.

3) Malware

When the On Board Unit (OBU) and Road Unit Side (RSU) update their software and firmware, the inside attacker may inject the viruses and worms to make continuous disruption in the network.

4) Spamming

The transmission latency will be increased, due to the presence of spamming message. It is very difficult to control this type of attack due to the infrastructure and centralized administration absence.

Black Hole attack

If a node decline to contribute the network or the node comes out from the network, then the message should drop down and not reached to all the nodes in the network. This type of process is called as black hole attack.

6) SECURITY MECHANISMS FOR AVAILABILITY

Data Correlation

It is very difficult to identify the false safety message attack. The data correlation method is used to avoid this type of attack by collecting the information which is gained from various sources and makes decision based on the credibility, relevance, and consistency of the information.

Secure Positioning

To secure the position of the vehicle, thus other vehicles should also know the position of all vehicles in the partitioned network. The Global Positioning System (GPS) are the main solution for this securing position of the vehicle, but it also has some security leaks.

7) SECURE PROTOCOL FOR AVAILABILITY

SEAD (Secure and Efficient Ad hoc Distance Vector)

It is a new secure routing protocol which avoids the incorrect routing in the traffic. This protocol depends on Destination Sequenced Distance Vector (DSDV). If the attacker makes DOS attacks, it just controls it, if the node has the limited CPU. It uses the one way hash function, by choosing the random value in the node.

ARIADNE

This type of protocol can prevent the DOS attack and routes of uncompromised attack. DSR is basic for this type of protocol. Symmetric cryptographic method is used in ARIADNE protocol. The transmitter transmit the message through the K_{SR} key with timestamp, while the receivers receives and resend the message through the K_{RS} key and also MAC calculation also done in the receiver side.

B) AUTHENTICATION

If the vehicle wants to access the available services in the network, it should be authenticated before access the service. During authentication process, if any violation takes places it leads to significant consequence in the network. Authentication is making sure to avoid the falsified identity which is provided by the outside or inside attacker.

The following some attacks available in this category is:

1) Sybil Attack

An attacker can state multiple identities in once. This type of attack is very dangerous attack in VANET, which provides terrible consequences in the network.

2) GPS Spoofing

The node in the network makes the neighbor node as false location information. These types of attack are very serious in VANET. The attack is occurred in the transmitter side which generates signals stronger then the signals generated by the receiver side.

3) Node Impersonation Attack

The vehicles in the network are different by others through the network ID. But in this attack, the attacker gained the ID moreover act as the genuine vehicle and gained information, even when the vehicle absent in the network.

4) SECURITY MECHANISMS FOR AUTHENTICATION

Tamper Proof Hardware

The VPKI private or public keys, ELPs are the cryptographic items which is stored in the tamper proof hardware, in which each vehicle will have this type of hardware. It keeps the substance safe from the intruders and reduces the information leakage from the vehicle.

Novel Position Detection Scheme

The vehicle will continuously broadcast the information about its position and it also catches this type of information from the neighbor. Once the vehicle receive the position information from the neighbor, it just check whether the line of sight is blocked or not, the transmitter again send the message if it is blocked again. It mainly uses two main types of resources; they are Eye device and Ear device.

5) SECURE PROTOCOL FOR AUTHENTICATION

ARAN (Authenticated Routing for Ad hoc network)

It is based on the AODV protocol, which prevents the authentication attacks including spoofing. A certificate server which uses public key cryptography method. Each node in the network have the record of its neighbor ,where they receive the message from the source which broadcast the route discovery packet(RDP),then the neighbor again broadcast the packet to all its neighbor. Once the receiver receives the packet, it just directly communicates with the source node. Thus the destination uses the Reply in Request (REP) packet to send the packet to transmitter. It requires each node must need routing table.

ARIADNE

This type of protocol can prevent the DOS attack and routes of uncompromised attack. DSR is basic for this type of protocol. Symmetric cryptographic method is used in ARIADNE protocol. The transmitter transmit the message through the K_{SR} key with timestamp, while the receivers receives and resend the message through the K_{RS} key and also MAC calculation also done in the receiver side. TESLA, MAC, Digital signature are used for the Authentication process.

C) CONFIDENTIALITY

Confidentiality makes sure that the authenticated nodes only should read the data. The attacks in this network are collection of unclear information. The attacker can gain the information through the location of router, vehicle or any user privacy etc. Thus in the absence of confidentiality, the information may gained will affects the individuals privacy and this type of attack should be said as a passive attack which is difficult to detect it. The types of attacks occurred in confidentiality as follows:

1) Eavesdropping Attack

The attacker listen to the media and get the useful information (used for track the location of vehicle), where the packets are transmitted during the network.

2) Traffic analysis attack

It is a passive attack which mainly affects the privacy of the users. After the information collected the attacker analysis the data and get the useful information from the network.

3) *SECURITY MECHANISMS FOR CONFIDENTIALITY*

For eavesdropping attack, the sender and receiver may encrypt the message through any encryption algorithm before they send and receive the message. Then the traffic analysis attack should be reduced by choosing the randomizing traffic pattern.

4) SECURITY PROTOCOL FOR CONFIDENTIALITY

NDM (Non-Disclosure Method)

This type of protocol is mainly used to secure the location information of the vehicle. It takes up the many independent security agents which utilize the private and public key pairs. Thus this protocol method is based on asymmetric cryptography method. The communication for sender and receiver

will takes place through this service agent, where it knows all nodes address. The sender transmits the information to the service agent which encapsulates the information and sends to the receiver, whereas the receiver transmits the message to service agent, from that it will go the sender.

D) DATA INTEGRITY

It makes sure that the data which send between the sender and receiver should not alter during transmission. During transmission the data modification, addition, deletion should be avoided while using this integrity method.
The following attacks may occur:

1) Masquerading attack

In this attack, the attacker uses the identity of the authenticated node and produces the false message in the network.

2) Replay attack

In this attack ,the attacker get the packet which the sender sends and transmit the new packet which is designed by the attacker, but the receiver thought that the packet should from the sender side only.

3) Tampering/Suppression/Fabrication

The attacker alters the message during transmission from the sender to receiver or vice versa and then transmits to the target.

4) SECURITY MECHANISMS FOR INTEGRITY

Integrity Metrics for Content Delivery

VOR4VANET (Voting on Reputation for VANET) is the scheme for data integrity. It is device centric approach which it stores the performance of individual vehicle, which functions on every vehicle locally.

5) SECURITY PROTOCOL FOR INTEGRITY

ARAN (Authenticated Routing for Ad hoc network)

It is based on the AODV protocol, which prevents the authentication attacks including spoofing. A certificate server which uses public key cryptography method. Each node in the network have the record of its neighbor ,where they receive the message from the source which broadcast the route discovery packet(RDP),then the neighbor again broadcast the packet to all its neighbor. Once the receiver receives the packet, it just directly communicates with the source node. Thus the destination uses the Reply in Request (REP) packet to send the packet transmitter. It requires each node must need routing table

ARIADNE

This type of protocol can prevent the DOS attack and routes of uncompromised attack. DSR is basic for this type of protocol. Symmetric cryptographic method is used in ARIADNE protocol. The transmitter transmit the message through the K_{SR} key with timestamp, while the receivers receives and resend the message through the K_{RS} key and also MAC calculation also done in the receiver side. TESLA, MAC, Digital signature are used for the Authentication process.

E) NON-REPUDIATION

It ensure that the data origin confirm that the data has been sent, whereas the data arrival should confirm that the data should be received by the receiver only.

1) SECURITY PROTOCOL FOR NON-REPUDIATION

ARAN (Authenticated Routing for Ad hoc network)

It is based on the AODV protocol, which prevents the authentication attacks including spoofing. A certificate server which uses public key cryptography method. Each node in the network have the record of its neighbor ,where they receive the message from the source which broadcast the route discovery packet(RDP),then the neighbor again broadcast the packet to all its neighbor. Once the receiver receives the packet, it just directly communicates with the source node. Thus the destination uses the Reply in Request (REP) packet to send the packet transmitter. It requires each node must need routing table

III.CONCLUSION

In VANET, Security is the main concern for design and implementing it. It is important to provide the life –critical information to the user without any modification of the information. We have seen the various security requirements with their corresponding attacks and possible mechanisms and protocol for those attacks. Amongst the all security requirements, the authentication is the major problem in the VANET. In future we have taken the particular attack, and measure the needed security mechanisms for that type of attack.

REFERENCES

[1] G. Samara, et al., *"Security issues and challenges of Vehicular Ad Hoc Networks (VANET),"* in 4th International Conference on New Trends in Information Science and Service Science (NISS), 2010, pp. 393-398.
[2] B. K. Chaurasia, et al., *"Attacks on Anonymity in VANET,"* in International Conference on Computational Intelligence and Communication Networks (CICN), 2011, pp. 217-221.

[3] G. Samara, *et al.*, *"Security Analysis of Vehicular Ad Hoc Networks (VANET),"* in Second International Conference on Network Applications Protocols and Services (NETAPPS), 2010, pp. 55-60

[4] M. Burmester, *et al.*, *"Strengthening Privacy Protection in VANETs,"* in IEEE International Conference on Wireless and Mobile Computing Networking and Communications, WIMOB '08., 2008, pp. 508-513.

[5] Chim, TW, Yiu, SM, *"SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs,"* Ad Hoc Networks, Volume 9, Issue 2, March 2011, pp. 189-203.

[6] M. Raya, J.-P. Hubaux, *"Securing vehicular ad hoc networks"*, J. Comput. Secur. 15 (1) (2007) 39–68.

[7] J. Blum, A. Eskandarian, *"The threat of intelligent collisions"*, IT Prof. 6 (1) (2004) 24–29.

[8] O. Trullols, M. Fiore, C. Casetti, C.-F. Chiasserini, J.M. Barcelo Ordinas, *"Planning roadside infrastructure for information dissemination in intelligent transportation systems"*, Comput. Commun. 33 (4) (2010) 432–442.

[9] S. Biswas, J. Misic, V. Misic, *"DDoS attack on wave-enabled VANET through synchronization"*, in: Global Communications Conference (GLOBECOM), 2012 IEEE, IEEE, 2012, pp. 1079–1084.

[10] A. Dhamgaye, N. Chavhan, *"Survey on security challenges in VANET"*, Int. J. Comput. Sci. 2 (2013) 88–96, ISSN 2277-5420.

[11] Kudoh, Y. (2004). *"DSRC standards for multiple applications",* In Proceedings of 11th world congress on ITS, Nagoya, Japan.

[12] Yin, J., Elbatt, T., & Habermas, S. (2004), *"Performance evaluation of safety applications over DSRC vehicular ad hoc networks"*,In Proceedings of VANET'04, Philadelphia, PA, USA, October
2004.

[13] Jiang, D., & Delgrossi, L. (2008). IEEE 802.11p, *"Towards an international standard for wireless access in vehicular environments",*In Proceedings of 67th IEEE vehicular technology conference on vehicular technology (pp. 2036–2040), May 2008.

[14] Festag, A. (2009), *"Global standardization of network and transport protocols for ITS with 5 GHz radio technologie",* In Proceedings of the ETSI TC ITS workshop, Sophia Antipolis, France, February 2009.

[15] IEEE Standard 802.11 (2007). IEEE Std. 802.11-2007, Part 11:*"wireless LAN medium access control (MAC) and physical layer (PHY) specifications"*.

