Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 200-207 EISSN 2392-2192

Security Requirements and Mechanisms in Vehicular Ad-Hoc Networks (VANET)

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

Anna University, Regional Center, Coimbatore – 641 046, India

[1-3]E-mail address: newlin_rajkumar@yahoo.co.in , nithisri92@gmail.com , krithikalilly2@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 based on the mobile Ad- hoc network (MANET) which is called as Vehicular Ad-hoc Network (VANET). However security in Vehicular Ad-hoc Networks (VANET) should become great challenges, 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, Ad-hoc Networks, Vehicular Ad-hoc Network, mobile Ad-hoc network

1. INTRODUCTION

VANET communication is takes place in three ways, Vehicle-to-Vehicle communications, Vehicle-to-Infrastructure Communication, Infrastructure-to-Vehicle 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

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

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 on Board 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.

1. 1. TYPES OF ATTACKER

1. 1. 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.

1. 1. 2. LOCAL vs EXTENDED

The attacker makes control of various base stations or any vehicles to a local network is said to be a 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.

1. 1. 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.

1. 1. 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.

2. 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.

2. 1. AVAILABILITY

To send and receive the message, the network should be available at any time, and it also make 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:

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.

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.

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.

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 absence of centralized administration and Infrastructure.

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.

2. 1. 1. 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.

2. 1. 2. 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. This protocol is based on DSR. Symmetric cryptographic method is used in this protocol. The sender sends 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.

2. 2. 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:

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.

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.

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.

2. 2. 1. 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, if is blocked it again

request the sender to resend the information .It mainly uses two main types of resources, they are Eye device and Ear device.

2. 2. 2. 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 source. It needs every node should have the routing table.

ARIADNE
This type of protocol can prevent the DOS attack and routes of uncompromised attack. This protocol is based on DSR. Symmetric cryptographic method is used in this protocol. The sender sends 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.

2. 3. 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:

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.

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.

2. 3. 1. 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.

2. 3. 2. 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.

2. 4. 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:

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

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.

Tampering/Suppression/Fabrication/Alteration
The attacker alters the message during transmission from the sender to receiver or vice versa and then transmits to the target.

2. 4. 1. 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.

2. 4. 2 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 to source. It needs every node should have the routing table.

ARIADNE
This type of protocol can prevent the DOS attack and routes of uncompromised attack. This protocol is based on DSR. Symmetric cryptographic method is used in this protocol. The sender sends 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.

2. 5. 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.

2. 5. 1. 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 to source. It needs every node should have the routing table.

3. 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 measures the needed security mechanisms for those type of attack.

References

[1] R. Bala and C. R. Krishna, Performance analysis of topology based routing in a VANET, *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2014, pp. 2180-2184, doi: 10.1109/ICACCI.2014.6968256

[2] J. Bernsen and D. Manivannan, Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service, *2008 The Fourth International Conference on Wireless and Mobile Communications*, 2008, pp. 1-6, doi: 10.1109/ICWMC.2008.15

[3] Raj Bala, C. Rama Krishna, Scenario Based Performance Analysis of AODV and GPSR Routing Protocols in a VANET, *Computational Intelligence & Communication Technology (CICT) 2015 IEEE International Conference on*, pp. 432-437, 2015

[4] Bhuvan Mehan, Sanjay Batish, Rajesh Bhatia, Amardeep Dhiman, BNSR: Border Node preferred Social Ranking based Routing Protocol for VANETs, *Contemporary Computing (IC3) 2015 Eighth International Conference on*, pp. 555-560, 2015

[5] Hanan Saleet, Rami Langar, Kshirasagar Naik, Raouf Boutaba, Amiya Nayak, Nishith Goel, Intersection-Based Geographical Routing Protocol for VANETs: A Proposal and

Analysis, *Vehicular Technology IEEE Transactions on*, vol. 60, no. 9, pp. 4560-4574, 2011

[6] Bruno G. Mateus, Carina T. de Oliveira, Arthur Callado, Stenio Fernandes, Rossana M. C. Andrade, Impact of Density Load and Mobility on the Performance of Routing Protocols in Vehicular Networks, *Vehicular Technology Conference (VTC Fall) 2012 IEEE*, pp. 1-5, 2012

[7] Arif Sari, Onder Onursal, Murat Akkaya, Review of the Security Issues in Vehicular Ad Hoc Networks (VANET), *International Journal of Communications, Network and System Sciences*, vol. 08, pp. 552, 2015

[8] U. Nagaraj, M. U. Kharat and P. Dhamal, Study of Various Routing Protocols in VANET, *International Journal of Computer Science and Technology*, vol. 2, pp. 45-52, Oct.-Dec. 2011

[9] S. Singh and S. Agrawal, VANET routing protocols: Issues and challenges, *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, 2014, pp. 1-5, doi: 10.1109/RAECS.2014.6799625

[10] Y. Toor, P. Muhlethaler, A. Laouiti and A. D. La Fortelle, Vehicle Ad Hoc networks: applications and related technical issues, in *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74-88, Third Quarter 2008, doi: 10.1109/COMST.2008.4625806

[11] Qiong Yang, Song Xing, Weiwei Xia, Lianfeng Shen, Modelling and performance analysis of dynamic contention window scheme for periodic broadcast in vehicular ad hoc networks, *Communications IET*, vol. 9, no. 11, pp. 1347-1354, 2015

[12] O. Dousse, P. Thiran and M. Hasler, Connectivity in ad-hoc and hybrid networks, *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, 2002, pp. 1079-1088 vol.2, doi: 10.1109/INFCOM.2002.1019356

[13] Ueda, A., Mizui, K. and Ihara, T. (2005), Intervehicle communication and ranging system using code-hopping spread spectrum technique. *Electron. Comm. Jpn.* Pt. III, 88: 50-60. https://doi.org/10.1002/ecjc.20078