International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

Security Analysis in VANETs: A Survey

Mrs.Kadam Megha V
M.E(Computer Engg.) GHRCEM, Pune

I. ABSTRACT

VANET means mobile ad hoc network is nothing but the group of independent mobile nodes which are moving throughout the mobile network freely. Such kind of networks are temporary as they mobile nodes and their positions are not fixed and hence the all the routing paths which are established in order to make the communication in between the source and destination are on demand and depends on the nodes movement into the network. The architecture is not at all needed for such kind of networks. Role of routing protocols is most important for the VANET which is used to route the data from source to destination, but they are also vulnerable to the many of the security attacks in the VANET. Due to the unprotected nature of the VANET networks routing protocols, such networks also unprotected from the malicious mobile nodes in the network itself. Hence the primary objective of vehicular ad hoc networks (VANETs), i.e., secure communication of the time critical information, is possible only if a robust infrastructure provides this security at all times. In this paper we presenting the survey over security framework for vehicular ad hoc networks and performance of mechanisms used to provide security.

Index Terms: *VANET, MANET, ACID, ACM, WAVE, IEEE 1609.*

II. INTRODUCTION

VANET network is network with collection of the mobile nodes which are independent on the other mobile nodes in the network and moving arbitrarily throughout the network. Such networks build the temporary networks without using any infrastructure for the same or the centralized administration for it. Mobile nodes in the network are depends on the multihop routing protocols in order to forward packets from the source mobile node to the destination mobile node [1]. Each node in the network like VANET acts as the host node as well as router node in order to perform the forwarding operation. For the building of the routes and in order to build the network, the mechanism of routing protocols in the VANET networks introduced. The main functionality of routing protocols is to build the dynamic routes in the network in between any source and destination nodes in the network. Network topology for the VANET networks is not fixed because of the frequent nodes movement in the network. According to the movements of the nodes is resulted into the frequent topology changes. There are mainly three types of routing protocols proposed for the VANET routing such as proactive, reactive and hybrid routing protocols and their simulation study with different network scenarios and traffic patterns [2] [3]. DSDV and OLSR are the examples of the proactive protocols, AODV and DSR are the well known reactive routing protocols and ZRP is one of the hybrids routing VANET protocol.

Building of dynamic communication a route in the entire network is done among the source node to destination node for communication purpose on demand way and hence this is the core functionality of VANET routing protocols. The mobile ad hoc networks are not having the fixed network topology due to the reason that mobile nodes are frequently changing their positions and movement. Network topology for the VANET networks is not fixed because of the frequent nodes movement in the network. Mobile ad hoc networks having different types of routing protocols like reactive, hybrid, and proactive protocols type of routing protocols. We can use these protocols with different network scenarios and mobility patterns. The reactive protocols such as DSR (Dynamic Source Routing) protocol and AODV (Ad hoc on demand Distance Vector Routing) protocol are frequently used VANET protocols. Apart from this, DSDV (Destination Sequenced Destination Vectoring) as well as OLSR (Optimized Link State Routing) are examples of reactive protocols. Zone Routing Protocol (ZRP) is one kind of hybrid protocol for the mobile ad hoc networks [5].

As we know that a mobile ad hoc network (MANET) is a kind of an ad hoc network of mobile nodes connected by wireless links. The nodes are free to move randomly and organize themselves arbitrarily. A Vehicular ad hoc network (VANET) is a special kind of MANET in which the mobile nodes are vehicles. The main difference between VANETs and MANETs is that in VANETs the nodes move in a random but predictable manner, but at much

higher speeds compared to traditional MANETs. The advantage of VANETs over traditional ad hoc networks is that nodes (vehicles) possess substantial power resources. VANETs enable vehicles to communicate with each other (V2V) and road side infrastructure (V2I) to increase the awareness of their surroundings thereby in- creasing safety and possibly optimizing traffic. Following are different applications of VANET:

• Safety related applications - e.g. Early Warning messages.

• Best Effort Applications - e.g. Infotainment, traffic optimization.

• Secure Transactions - e.g. Toll collection.

Most of the critical messages in VANETs are broadcast oriented safety messages that should have a deep penetration and should be delivered in a short time. Additionally these messages must be secure and must not leak personal, identifying, or linkable information to unauthorized parties, as the owners of the vehicles involved in the communication have a right to privacy.

In this paper we will present the survey over the VANET security analysis. In section III we will discuss the important parameters considered for VANET security, in section IV, we will discuss the present scenarios of VANET security. In section VI we will discuss the algorithm used for accepting and dropping the messages, further more in section VII we will discuss how to design security framework for VANET.

III. VANET SECURITY PARAMETERS

Following are points those are important while designing the VANET security methods.

- Authentication - There can be malicious and genuine sources for messages in VANETs. Authentication is the ability to distinguish between these sources.
- Anonymity - The physical identity of the originator of a message should not be easily identifiable from the message.
- Data Integrity - The data received are exactly as sent by the authorized entity without any modification.
- Low Overhead - The messages being time critical, the security overheads should retain the usefulness of the message.

IV. LITERATURE REVIEW OF CURRENT METHODS

Before discussing the VANET literature review, we will present the commonly used abbreviations in current methods of VANET security.

- DSRC - is a short to medium range communications service that supports both public safety and private operations in roadside to vehicle and vehicle to vehicle communication environments.
- ACID - An application class identifier is a code (number) that identifies a class of applications.
- ACM - An application context mark is a code that identifies a specific instance of an application within a class.
- OBU - A WAVE device that can operate when in motion and supports information exchange with roadside units (RSUs) and other OBUs.
- RSU - A wireless access in vehicular environments (WAVE) device that operates only when stationary and supports in- formation exchange with on board units (OBUs).
- WAVE - Wireless Access in Vehicular Environments (WAVE), a new name for DSRC [2].

Now we will discuss the current scenarios of VANET. The IEEE 1609 Family of Standards [1] defines architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. The layers of the protocol stack are as follows in figure 1:

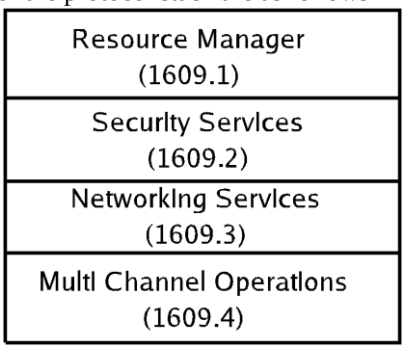

Figure1: Layered Protocol Stack

- IEEE P1609.1- Resource Manager- describes the key components of the WAVE system architecture and defines data flows and resources at all points. It also defines command message formats and data storage formats that must be used by applications to communicate between architecture components, and specifies the types of devices that may be supported by the OBU resident on the vehicle or mobile platform.
- IEEE P1609.2 - Security Services for Applications and Management Messages - defines secure message formats and processing. It also defines the circumstances for using secure message exchanges and how those messages should be processed based upon the purpose of the exchange.
- IEEE P1609.3 - Networking Services - defines network and transport layer services in support of secure WAVE data exchange. It also defines Wave Short Messages (WSM), providing an efficient

WAVE-specific alternative to IPv6 (Internet Protocol version 6) that can be directly supported by applications.

- IEEE P1609.4 - Multi-Channel Operations - provides enhancements to the IEEE 802.11 MAC to support WAVE operations. It provides mechanisms for prioritized access to the physical channel.

The IEEE P1609.2 standard defines secure message formats and the processing of those se- cure messages within the WAVE system using the Public Key Infrastructure (PKI). It covers methods for securing WAVE management messages and application messages with the exception of vehicle originating safety messages, and also describes administrative functions necessary to support core security functions. For obtaining anonymity each vehicle is issued a set of certificates, as periodically sent beacons with position and time information enable external eavesdroppers to create movement pro- files [4].

But for the robustness of the security, timely access to revocation information is important. However real time availability and penetration of the revocation information is a particularly hard problem in vehicular networks. Some proposals for certificate revocation in vehicular networks have been made [8], which include temporary revocation of the attacker till the connection to the CA is established.

Security requirement and time constraints for applications based on criticality of the information have been proposed and the security characteristics of these applications along with general characteristics like degree human involvement on events have been enumerated in [7]. The end to end delays based on the criticality of the applications are as follows.

- Up to 0.5 seconds - message is highly critical, e.g. break down warning.
- 0.5 seconds to 1 second - time is critical, e.g. Emergency vehicle approaching warning.
- 1 to 5 seconds - delays up to 5 seconds are acceptable, e.g. glare reduction.
- Other delays - time is not critical, e.g. intelligent traffic flow control.

V. OVERIVE OF BLACKHOLE ATTACK IN VANET

The In Blackhole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe. So the specific node is named as a Blackhole. A Blackhole has two properties in order to detect. First, the node exploits the ad hoc routing protocol, such as DSR, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets [7] [8].

Blackhole attacks in AODV protocol routing level can be classified into two categories: RREQ Blackhole attack and RREP Blackhole attack.

Algorithm 1: Blackhole attack caused by RREQ

An attacker can send fake RREQ messages to form Blackhole attack. In RREQ Blackhole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Blackhole attack by faked RREQ message as follows:

• Set the type field to RREQ (1);

• Set the originator IP address to the originating node's IP address;

• Set the destination IP address to the destination node's IP address;

• Set the source IP address (in the IP header) to a non-existent IP address (Blackhole);

• Increase the source sequence number by at least one, or decrease the hop count to 1.

The attacker forms a Blackhole attack between the source node and the destination node by faked RREQ message as it is shown in Fig. 2.

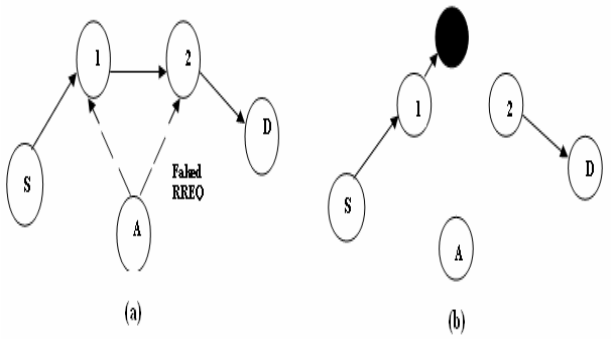

Fig.2: Blackhole is formed by Faked RREQ.

Algorithm 2: Blackhole attack caused by RREP

The attacker may generate a RREP message to form Blackhole as follows:

• Set the type field to RREP (2);

• Set the hop count field to 1;

• Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route;

• Increase the destination sequence number by at least one;

• Set the source IP address (in the IP header) to a non-existent IP address (Blackhole).

The attacker unicasts the faked RREP message to the originating node. When originating node receives the

faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Blackhole is formed as it is shown in Fig. 3

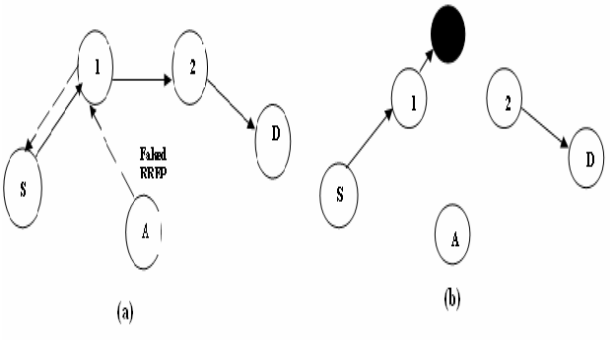

Fig. 3 Blackhole is formed by Faked RREP.

VI. MECHANISM OF MESSAGES ACCEPTANCE AND DROPPING IN VANET

In this section we will present survey over algorithm used to accept and drop the messages in VANET. The trivial algorithm for accepting/dropping a message relies on local information that is residing at the receiving OBU in terms of the CRLs. The mechanism proposes dropping a received message if the sender happens to be in the CRLs. However, it is not very clear what step should be taken if the sending entity is not listed in the CRLs available at the receiving OBU. Clearly, absence of the sender in the CRLs available at the receiver does not guarantee that the sender's certificate has not been revoked by the authority (CA) that issued certificate to the sender.

Thus, the receiver faces the dilemma of whether to accept the message or simply drop it. In order to improve the performance of the message flow in V2V communications, an most important point to be addressed is to have an algorithm (criteria) to accept/drop a message received by an OBU. In short the packet can be accepted/dropped based on the Confidence on the Security infrastructure (CoS). The Security Infrastructure represents the Public Key Infrastructure along with the mechanism for issue and distribution of certificates and CRLs issued by the CAs. Hence the CoS is the probability of accepting the packet when the certificate is not present in the CRLs available in the OBU and the packet satisfies all other criteria mentioned in the standard for accepting the packets. This CoS is dependent on following points:

- This freshness of the certificate specifies how fresh the current certificate is. The more recent/fresh the less probable is its revocation. This freshness complements the honest majority concept of vehicular networks that assumes most of the nodes in the V2V are honest, but the cost of obtaining this freshness needs to be analyzed for various Security Infrastructure designs.
- The freshness of the CRLs. The freshness of CRLs in the OBU is the penetration capacity of the CRLs, which in turn is completely dependent on the mechanism used for distributing the CRLs.

The concept of freshness of certificates is not new but a similar concept was mentioned in [9] and can be obtained if security infrastructure considers the following points.

- The signer should provide all the evidence (if possible) the acceptor needs, including the recency/freshness information. Fresh certificates are the best evidence.
- The acceptor of the messages should set the recency/freshness requirements of the certificate and not the CA.

Thus if the performance is measured as the fraction of packets dropped due to failure in authenticating a genuine sender, to the total number of packets transmitted, then the mechanism used for implementing the security infrastructure determines the performance of the system.

VII. VANET SECURITY FRAMEWORK DESIGN CONTRAINTS

Many times the security framework design for VANET results into non trivial task due to the high mobility of vehicles and the unavailability of connection with the PKI at all times. The factors that affect the design of the security infrastructure, thus the CoS is:

- The storage capacity of the OBU. As mentioned above the security infrastructure determines the number of certificates and CRLs to be stored, hence the storage capacity limits the maximum number of CRLs that can be stored in the OBU.
- The number of certificates in the certificate chain. The number of links/certificates in the certificate chain to the root determines the number of CAs whose certificates and CRLs need to be stored in the OBU.
- The expected number of certificates revoked and its distribution geographically. The expected number of certificates revoked and the geographical distribution of these revocations determines the number of CRLs required in the OBU.
- The relocation (migration) model of the vehicles. The relocation model describes how the vehicle migrates from one region to the other. If the certificate is to remain the same across geographical domains then the relocation model determines the maximum number of regions whose CRLs need to be stored on the OBU.
- The Mobility Model of the vehicles. The mobility model describes how the vehicle moves from one geographical region to another. This along with the density of the nodes determines the number of other

nodes (RSUs and OBUs) the given node communicates.
- Life time of a certificate. This determines the time for which the certificates need to be stored on the OBU.

VIII. WORK DONE

The implementing approach of the security framework can be divided into the following ways:

1. Only one CA for all vehicles. This has many issues like monopoly and the fact that no organization is universally trusted.

2. Manufacturer Based- The manufacturer is the CA,
- Each vehicle manufacturer is the CA for the vehicles it produces.
- A representative of a group of manufacturers is the CA for vehicles produces by member manufacturers.

However, this model is having following limitations:
- Coordination in installing certificates.
- Coordination for distribution of revocation lists in vehicles running on road.
- It doesn't optimize on localization of information like, probability of communicating with vehicles registered in the same region is high in the region of registration.

3. Geographical Region Based- This can be implemented as vehicle registration authorities becoming the CAs.

- A certificate is issued by a CA of one region and is valid across all geographical regions. The relocation model is such that with a given certificate a vehicle can theoretically relocate to all other geographical regions in the life-time of the certificate.
- A certificate is issued by a CA in one region and it is valid only in the region of issue. On relocation the certificate need to be re-signed or a new certificate needs to be issued by the CA of the current region.
- A certificate is issued by a CA of one region and is valid in a set of regions that are near the region of issue. On relocation new certificates won't be required in nearb y regions.

IX. CONCLUSION

Presence of the attacks in the network or misbehaving nodes in the network one of the major security issues for the VANET which is also affecting the performance of the vehicular ad hoc network. In this paper we discussed the infrastructure design for VANET security. Important parameters of VANET security framework designs along with the constraints of designing the security framework for VANET are discussed here. From this paper we want to clear that for the strong security of VANET communication we not only needs the strong cryptography algorithm but also one need the strong communication framework or strong routing algorithms those can easily detects the malicious vehicles from network and mitigate them. For the future work we will work on framework design based on new algorithm which can detect and mitigate the malicious vehicles from network and reduced the packet drops while maintaining the throughput.

X. REFERENCE

[1] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF: A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005 2005.

[2] Zhou L, Chao H-C: Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 2011, 25(3):29-34. doi: 10.1109/MNET.2011.5772059

[3] Yang H, Lou H, Ye F, Lu S, Zhang L: Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 2004, 11(1):38-47. doi: 10.1109/MWC.2004.1269716

[4] Klaus P., Thomas Nowey, and Christian Mletzko. Towards a security architecture for vehicular ad hoc networks. First Inter- national Conference on Availability, Relia- bility and Security, 2006.

[5] Bryan Parno and Adrian Perrig. Chal- lenges in securing vehicular networks.

[6] Radia Perlman. An overview of pki trust models. IEEE Network, 1999.

[7] A. Kung R. Kroh and F. Kargl. Vanets security requirements version 1.0.

[8] Hu Y-C, Perrig A: Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2004, 2(3):28-39. doi: 10.1109/MSP.2004.1

[9] Raja Mahmood RA, Khan AI: A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks. Paper presented at the International Symposium on High Capacity Optical Networks and Enabling

Technologies, Dubai, United Arab Emirates, 18-20 November 2007 2007.

[10] Saini A, Kumar H: Comparison between Various Black Hole Detection Techniques in VANET. Paper presented at the National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010 2010.

[11] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006 .

[12] H Fussler, S Schnaufer, M Transier , W Effelsberg ,"Vehicular Ad-Hoc Networks: From Vision to Reality and Back", Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[13] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[14] 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 .

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