International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

VANET: A Survey on Secure Routing

Omkar Shete[1], Sachin Godse[2]

[1]Sinhgad Academy of Engineering, Computer Engineering Department, Pune University, Maharashtra, India

[2]Professor, Sinhgad Academy of Engineering, Computer Engineering Department, Pune University, Maharashtra, India

Abstract: ***Vehicular Ad-Hoc Network is a sub branch of Mobile Ad-Hoc Network i.e. MANET. A VANET provides communication between vehicle to vehicles and vehicles to infrastructure. Now, road traffic activities are one of the most important daily routines. VANET provide us information that is required for better safety and driving. Security is major challenge in VANET. One of the major threats is Sybil attack, is a serious threat as they can affect the functionality of VANETs for the benefit of the attacker. The Sybil attack is the case where a single faulty entity, called a malicious node, can present or create multiple identities known as Sybil nodes or fake nodes. This paper detects and prevents the Sybil attack using new secure routing protocol. It is based on AODV protocol. Also it proven that multiple identities of fake node can create confusion in the VANET network or collapse entire network.***

Keywords: VANET, MANET, ITS, Sybil attack, Routing protocols.

1. Introduction

"Vehicular Ad hoc Network" is a wireless network that formed by vehicles. VANET communications obtain in between vehicles to vehicles (V2V) and in between vehicle to roadside equipments or infrastructure (V2R/V2I). For improving the transportation systems security, safety and efficiency to required novel vehicular applications. Applications of transportation systems are generally referred as Intelligent Transportation Systems (ITS) (2013) [1]. VANET is one way to implement Intelligent Transportation System (ITS).It is a technique to give similar information and communication technology to transport infrastructure and vehicles. A VANET is a decentralized network in that every node performs the functions of both host and router. The main benefit of VANET communication is transferring secure information between vehicles.

This paper is organized as follows. Section 2 deals with VANET, Section 3 on Challenges on VANET, Section 4 on Routing protocols in VANET, Section 5 gives a comparison of the various secure routing protocols, Section 6 gives Future scope and Section 7 concludes the paper.

2. VANET

2.1 VANET's and MANET's

Now a day's VANET's and MANET's are new emerging technologies. VANETs and MANETs provide us common features such as the movement, self organization and self-management of information in a distributed fashion. Although VANETs share common characteristics with MANETs, VANETs have distinctive features that impact the design of communication systems, protocols, and applications. Their analysis is presented in Table 1 (2013) [1].

Table 1: Comparison of VANET and MANET

Parameter	*MANET*	*VANET*
Cost of production	Cheap	Expensive
Change in topology	Slow	Very fast
Mobility	Low	High
Node density	Sparse	Dense and frequently variable
Bandwidth	100 kbps	1000 kbps
Range	Up to 100 m	Up to 500 m
Node lifetime	Depends on power resource	Depends on the lifetime of vehicle
Multihop routing	Available	Weakly available
Moving pattern of nodes	Random	Regular
Position acquisition	Using ultrasonic	Using GPS, Radar, etc.

2.2 Communication in VANET

VANET communication can be categorized into inter-vehicular communication and vehicle to infrastructure communication (2013) [1]. The first mode refers communication in which vehicles communicate with each other via wireless technology, also referred to as Vehicle-to-Vehicle communication (V2V) as shown in Figure 1. As Figure 1 shows when a vehicle breaks down, immediately, the vehicle begins the information distribution process using the broadcast communication mode. In V2V, re-transmit the message from near vehicle when communication broken down. In this way vehicles are notified and can take alternative routes, avoiding a possible problem of traffic congestion. The second mode refers to communication between Vehicle-to -Infrastructure (V2I) or Vehicle to Roadside (V2R). V2I is the direct wireless exchange of relevant information between vehicles and the communication units placed on the side of roads and avenues as shown in Figure 2. In V2I, re-transmit the message from nearest fixed infrastructure when communication broken down to identify the problem. The base station notifies the vehicles that are within its coverage area about the problem identified. At the same time, the base station could begin the inter-roadside communication process to extend the area of coverage. In this way vehicles further away are notified and

can take alternative routes, avoiding a potential problem of traffic congestion.

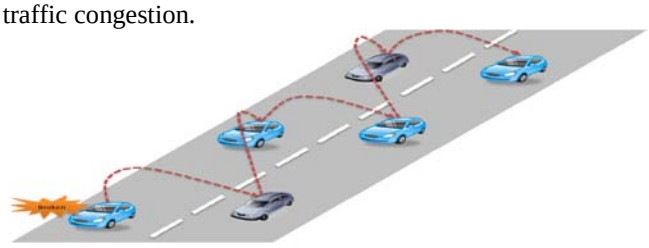

Figure 1: V2V [1]

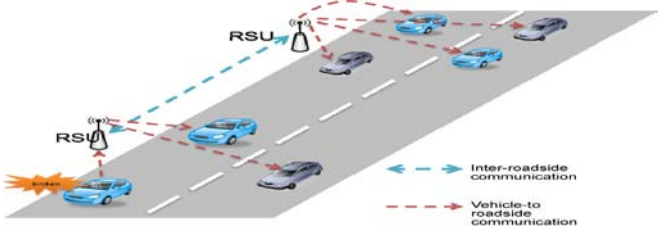

Figure 2: V2R/V2I [1]

3. Challenges in VANET

VANET is working on Wireless network there must require communication between vehicles for providing information like emergency break and other. It is necessary to give security when communication between vehicles and need to detect fake nodes (2011) [3]-(2007) [4]

3.1 Types of Attacks in VANET

Bogus Information: Attackers can send wrong or incorrect information in the network so that it can affect the behavior of other drivers.

Denial of Service (DOS): Here, Attacker wants to bring down the network by sending unnecessary messages on the communication channel. DOS attack can occur by jamming the channel system so that no authentic vehicle can access the channel.

Sybil Attack: In this type of attack, the attacker uses different identities at the same time. These identities can be used to play different type of attack in the system. Also these false identities create an illusion that there are additional vehicles on the road. It provides illusion to other vehicle by sending some wrong messages like traffic jam message.

Black Hole: In this type of attack a node refuses to participate in the network or when an established node drops out to form a black hole. In this whole traffic of the network get redirected towards a specific node which is actually doesn't exists which results in data lost.

Alteration Attack: This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted.

4. Routing protocols in VANET

In VANET highly challenging tasks is to transporting information from one vehicle to another or all vehicles within specified area. There are several routing protocols defined to transporting information (2014) [2], (2012) [5]. In VANET, the routing protocols are classified as:

4.1 Topology Based Routing Protocols

This routing protocol uses links information for sending packets from source to destination. They are further classified as:

a) **Proactive routing protocols:** Here routing information is maintained in the background irrespective of communication requests; like next forwarding hop. There is no route discovery since the destination route is stored in the background. It provides low latency for real time application.
b) **Reactive/Ad hoc based routing:** It opens route only when it is necessary for communication between nodes. Reactive routing consists of route discovery phase in which the query packets are flooded into the network for the path search and this phase completes when route is found.
c) **Hybrid Protocols:** It is combination of proactive and Reactive protocol. It introduced to reduce the control overhead of proactive routing protocols and decrease the initial route discovery delay in reactive routing protocols.

4.2 Position Based Routing Protocols

Position based routing is also called geographic routing. In these protocol each node must knows own current location. Source node sends packet or message to destinations geographic location without using of network address.

4.3 Cluster Based Routing Protocols

Cluster based routing is based on cluster. Cluster is a group of nodes. One of them is designed to cluster head to broadcast the packets into cluster. It provides good scalability for huge networks but it incurred the network delays and overhead when forming cluster.

4.4 Broadcast Based Routing Protocols

In certain applications, the host has to send packets to many or all other hosts. Sending a packet to all destinations at a time is called Broadcasting. This broadcast based routing protocols used in VANET for sharing weather, traffic, emergency and road conditions among all the vehicles.

5. Secure Routing Protocols

In VANET network number of routing protocols as well as number of secure routing protocols available. Secure routing protocols analysis is shown in Table 2.

Table 2: Analysis of the various secure routing protocols

Protocol Attack & Parameters affected	*Strength*	*Weakness*	*Future Scope*
SEAD. 2008.[6] DoS. Scalability, mobility or capability of Packets Delivery Ratio, End-to end Delay, Control Overhead.	1. Lightweight secure routing protocol. 2. They avoid asymmetric cryptography to protect against DoS attack and to overcome limited CPU processing capability. 3. Used efficient one-way Hash functions to provide authentication for both the sequence number and metric field in each routing entry.	1. It does not prevent an attacker from tampering other fields or from using the learned metric and sequence number to send new routing updates.	1. Propose a secure routing protocol with the least time cost.
SRP. 2002.[7] DoS and Black hole. Packets Delivery Ratio, End-to end Delay.	1. Low overhead. 2.Capable of operating without the existence of an on-line certification authority or the complete knowledge of keys of all network nodes. 3. The protocol introduces a set of features, such as the requirement that the query verifiably arrives at the destination, the explicit binding of network and routing layer functionality, the consequent verifiable return of the query response over the reverse of the query propagation route, the acceptance of route error messages only when generated by nodes on the actual route, the query/reply identification by a dual identifier, the replay protection of the source and destination nodes and the regulation of the query propagation.	1. Not handle Wormhole attacks. However, it can nevertheless prevent them.	1. It would be interesting to investigate whether the use of soft state at intermediate nodes would further contribute to the protocol efficiency in a non-benign environment.
Ariadne. 2005.[8] DoS. Packet Delivery Ratio, Packet Overhead, Byte Overhead, Mean Latency, Path Optimality	1. Ariadne provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the pair of communicating nodes.	1. It is very much immune to Worm Hole attacks through clock synchronization between nodes, but not in all.	-
ARAN. 2010.[9] Packets Delivery Ratio, End-to end Delay.	1. It introduces authentication, message integrity and non-repudiation to an ad hoc environment as a part of a minimal security policy. 2. The route maintenance is done through special error messages. 3. It prevents impersonation attacks by providing end-to-end and hop-to-hop authentication of route discovery & reply messages.	1. Does not have any mechanism that deals with black hole attack, wormhole attack, Denial of service attack. 2.ARAN does not guarantee a shortest path, but offers a quickest path	1. Areas in secure ad hoc network routing that have been explored are trust establishment, key generation, nodes that maliciously do not forward packets, and security requirements for forwarding nodes.
SAODV. 2009.[10] DoS and Wormhole. The impact of delayed verification, Adaptive reply decision.	1. It uses a central key management in its routing topology. 2. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. 3. Includes cryptographic operations that can have a significant impact on performance.	1.It requires heavyweight asymmetric cryptographic operations 2.This gets worse when the double signature mechanism is used	1. Evaluate the behavior of SAODV and of the proposed optimizations under attack.

6. Future Scope

We studied different existing routing protocols in VANET. Most of the routing protocols not consider security in message forwarding or in communication. Few of secure routing protocols are exist but it having some limitations or drawbacks. There are different types of attack can be easily occurred. One of the major threats is Sybil attack. Sybil attack can easily occurred into that protocols and these attack can launch another different types of attacks. Now we are considering, designing and implementation of new routing protocol as a future scope from this study. In this new protocol, each node in VANET must have unique identity in the route table to identify the node is original node or fake node. This protocol can easily detect and prevent Sybil attack in VANET. This new protocol can help to improve performance of VANET.

7. Conclusion

Secure data forwarding is one of the important challenges in VANET. If message forwarding is not secure it can cause fake messages delivery by malicious nodes, misguiding nodes in the network. This may cause accidents or traffic on road. After studying different routing protocols in VANET we found that most of the routing protocols are not providing security for data transmission. Instead of providing separate technique for attack detection and prevention we can provide in routing protocols itself it improve performance of VANET. This new routing protocol will be considered for designing for Sybil attack. This new routing protocol which will provide unique identity to each node in its route table. Then this new secure routing protocol can easily identify fake node or original node. Also it detects and prevents Sybil attack and gives high performance than other.

References

[1] J.A. Guerrero-Ibáñez, C. Flores-Cortés, and Sherali Zeadally, "Vehicular Ad-hoc Networks (VANETs): Architecture, Protocols and Applications", Computer Communications and Networks © Springer-Verlag London 2013.
[2] Hemlata Chaudhary, "A Review of Topology based Routing Protocols for Vehicular Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, Volume 4, Issue 2, February 2014,Page 142-147.
[3] Mina Rahbari and Mohammad Ali Jabreil Jamali , "Efficient Detection Of Sybil Attack Based On Cryptography In Vanet", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, PP 185- 195.
[4] M. Raya and JP. Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security 15 (2007), PP 39–68.
[5] Mushtak Y. Gadkari and Nitin B. Sambre, "VANET : Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38.
[6] Wei-Shen Lai, Chu-Hsing Lin, Jung-Chun Liu, Yen-Lin Huang, Mei-Chun Chou, "I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks", International Journal of Multimedia Ubiquitous Engineering, Vol. 3, No. 4, October, 2008,PP 45-54.
[7] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[8] yih-chun hu and adrian perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc", Wireless Networks 11, 21–38, 2005,@2005 Springer Science + Business Media, Inc. Manufactured in The Netherlands, PP 21-38.
[9] Seema Mehla, Seema Mehla and Preeti Nagrath, "Analyzing security of Authenticated Routing Protocol (ARAN)", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 664-668,PP 664-668.
[10] Alekha Kumar Mishra and Bibhu Dutta Sahoo, "A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet", International Journal Of Computer Applications In Engineering, Technology And Sciences (Ij-Ca-Ets), ISSN: 0974-3596 | April '09 – September '09 | Volume 1: Issue 2, PP 443-447.