International Journal of Computer Applications Technology and Research
Volume 4– Issue 7, 535 - 539, 2015, ISSN:- 2319–8656

VANET Security against Sybil Attack by Using New SRAN Routing Protocol

Omkar Shete
Department of Computer Engineering
Sinhgad Academy of Engineering,
Pune University,
Maharashtra India

Sachin Godse
Department of Computer Engineering
Sinhgad Academy of Engineering,
Pune University,
Maharashtra India

Abstract: A VANET facilitates communicate between vehicles and between vehicles and infrastructure. Vehicular Ad-Hoc Network is a sub type of Mobile Ad-Hoc Network i.e. MANET. Now days, road traffic activities are one of the most important daily routines worldwide. VANET provides you most of information that are required for better safety and driving such as an accurate weather description or early warnings of upcoming dangers. To successfully deploy VANET, security is one of the major challenges such as protection from selfish vehicles that may block or mess traffic, bogus notifications etc. that may harm and losses lives, that must be addressed. Sybil attacks have become 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 create multiple identities known as Sybil nodes or fake nodes. This project detects and prevents the Sybil attack using "Secure Routing for Ad Hoc Network" (SRAN) routing protocol. SRAN is based on AODV protocol. In our proposed work, we have developed SRAN protocol to maintain routing information and route discovery in such manner that will detect as well as prevent Sybil Attack. Each node will have a unique identity and their entry in route table. SRAN Protocol easily detects such route that is not valid anymore for communication. It deletes all the related entries from the routing table for those invalid routes.

Keywords: VANET, ITS, V2V, V2I/V2R, Sybil attack, Routing Protocols.

1. INTRODUCTION

The vehicular ad hoc network (VANET) is a special communication pattern to provide communication information within the roadside-to-vehicles and inter-vehicle with the aid of wireless network and information technology. Road traffic activities are one of the most daily routines of common men. The increasing road accidents and traffic congestion are becoming major problems. VANET, a sub type of Mobile Ad hoc Networks is developed to solve these problems which provides scalable and cost-effective solutions for applications such as safety messaging, dynamic routing. VANETs are used in many safeties, critical applications; one of the applications considered in this paper is secure safety routing which is meant for cooperative driving and avoidance of accidents. Sybil attack is more dangerous than any other threat. It injects malicious vehicles on the road.

2. VANET

VANET is considered as a subgroup of Mobile Ad-hoc Networks (MANETs) in which all nodes are vehicles that move at various speeds. The main objective of VANET is to enable communication between vehicle to vehicle and in between vehicle to infrastructure. Transportation system's safety, security and efficiency are improved by using Intelligent Transportation Systems (ITS). ITS consist of various technologies like communications, information processing and control. The integration of ITS technologies with VANET systems is intended to save time, money and lives. There are two types of VANET, used for communication. First, Inter-vehicular communication refers to the kind of communication in which vehicles communicate with each other via wireless technology, also referred to as Vehicle-to-Vehicle communication (V2V) as shown in Fig. 1. It shows when a vehicle breaks down, immediately, the vehicle begins the information dissemination process using the broadcast communication mode. The vehicles that are near to the vehicle, which has broken down, re-transmit the message. In this way vehicles are notified and can take alternative routes, avoiding a possible problem of traffic congestion. In second type vehicles and fixed infrastructure exchange information. This communication mode is referred to as Vehicle-to-Infrastructure (V2I) or Vehicle to Roadside (V2R) communication. V2R 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 Fig. 2 [1].

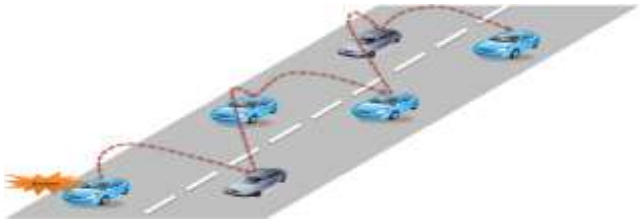

Figure 1: V2V [1]

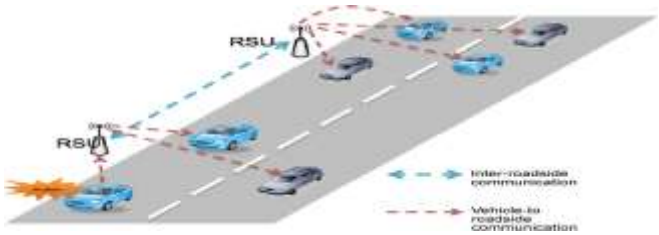

Figure 2: V2R/V2I [1]

3. SECURITY IN VANET

As VANET is becoming more popular, a serious challenge in this environment is security. As we mentioned previously, VANET is sub branch of MANET. Consequently, VANETs inherit all the security issues associated with MANETs. The malicious behavior of users, such as the modification of the messages, could be fatal to the other vehicular users, etc. Security and privacy in vehicular networks are important for their acceptance. VANETs' architectures and communication schemes provide developers an environment for the deployment of a wide variety of applications. However, major concerns of such environments are privacy and security. Strong security mechanisms are required to protect both applications and users from possible attacks. Therefore, powerful schemes are required to protect users' private information.

VANETs' security is of great importance because any vulnerability could lead to disastrous accidents where people's integrity may be put at risk. Security mechanisms and schemes guarantee the protection of personal data transmitted through VANET but not to identity, location, and destination, among others. In VANET, multiple threats or attacks are possible. One of them is Sybil attack which is considered as major threat.

The Sybil attack is a well-known harmful attack. In this attack malicious vehicles are injected into same network. This attack is very dangerous since a malicious vehicle can present in different positions at the same time, thereby creating massive security risks in the network. The Sybil attack harms the network topologies and connections as well as network lives. In Fig.3, an attacker 'A' sends multiple messages with different identities to the other vehicles. Thus, other vehicles understand that there is heavy traffic. In ad hoc networks, there are three common types of security against sybil attacks which are registration, radio resource testing, and position verification. Registration itself is not sufficient to prevent Sybil attacks, because a fake node has possibility to entry with multiple identities by non-technical means such as stealing. However, a strict registration may lead to serious privacy problem. Radio resource testing is based on the assumption that all physical entities are limited in resources. In position verification the position of nodes will be verified. The goal is to make sure that each physical or original node refers to one and only one identity [2].

Figure 3: Traffic Congestion [2]

4. EXISTING SYSTEMS

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:

In VANET, the routing protocols are classified into four categories. These protocols are characterized on the basis of area where they are most suitable [3], [4].

4.1 Topology Based Routing Protocols

These routing protocols use association information that exists in the network to perform packet forwarding. This protocol further divided into three types.

4.1.1. Proactive routing protocols: Proactive routing protocols continuously try to maintain up-to-date routing information on every node in the network.

Advantage: Routing information is already available when the first packet is sent so connection times are fast.

Disadvantage: When there is no traffic, continuously use resources to communicate routing information.

Types: DSDV, OLSR, CGSR.

4.1.2. Reactive/Ad hoc based routing: Reactive routing opens the route only when it is necessary for a node to communicate with other nodes. Reactive routing consists of route discovery phase so that the query packets are flooded into the network for the path search and this phase completes when route is found.

Types: AODV, PGB, DSR, TORA, and JARR.

4.1.3 Hybrid Protocols: It is combination of proactive and reactive routing protocols. The hybrid protocols are used to reduce the control overhead of proactive routing protocols and decrease the initial route discovery delay in reactive routing protocols.

Types: ZRP, HARP.

4.2 Geographical Routing Protocols

Some routing protocols make use of geographical information, such as GPS coordinates. Typically, nodes communicate their location through the network, so that other nodes can determine shortest path. Select shortest path by using this geographical information.

Disadvantage: Each node need to know its location.

4.3 Cluster Based Routing Protocols

Cluster based routing is like in clusters. Cluster consists of the group of nodes that identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Good scalability is essential characteristic that can be provided for large networks but network delays and overhead are occurred when forming clusters in highly mobile VANET.

Types: COIN, LORA-CBF, TIBCRPH, and CBDRP.

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.

Types: BROADCOMM, UMB, V-TRADE, and DV-CAST.

Also, there are several secure routing protocols are available and there comparison is shown in Table I [5].

Table 1: Analysis of Secure Routing Protocol

Protocol Attack & Parameters affected	Strength	Weakness	Future Scope
SEAD. 2008. DoS. Scalability, mobility or capability of Packets Delivery Ratio, End-to end Delay, Control Overhead, End-to-end Delay.	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.
Ariadne. 2005. 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.	-
SRP. 2002. DoS and Blackhole. 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.
ARAN. 2010. 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. 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

5. PROPOSED WORK

In VANET, Security is most important factor for secure communication. Sybil attack is one of the major threats in the network. It injects multiple malicious vehicle nodes in the network and that harms the networks or loosing life. We are proposing new secure routing protocol named as Secure Routing for Ad hoc Network (SRAN) routing protocol. This SRAN protocol detects as well as prevents Sybil attack. SRAN is based on AODV. This SRAN protocol does not allow Sybil node into Route discovery, hence Sybil node is eliminated from the route. Also using RSU we can remove this Sybil node from the Network. In SRAN protocol we consider the following factors.

5.1 Route Request Packet format:

In SRAN routing protocol, if source wants to send message to destination then it first broadcasts the route request (RREQ) to its neighbors. Neighboring node receives RREQ, if receiving node is not destination and does not have route to the destination then it rebroadcast the RREQ and same time backward route is created to the source. If the receiving node is destination node or it has current route to the destination then Route Reply (RREP) is generated.

1) *RREQ ID:* A sequence number uniquely identifying the particular RREQ when taken in association with the source node's IP address.
2) *Source IP Address:* The IP address of the Source.
3) *Source Sequence Number:* The Sequence number of Source.
4) *Source Unique ID:* The Unique Identification of Source.
5) *Destination IP Address:* The IP address of the destination for which a route is selected.
6) *Destination Sequence Number:*The latest sequence number received in the past by the source for any route towards the destination.
7) *Destination Unique ID:* The Unique Identification of Destination.
8) *Hop Count:* Number of hops needed to reach destination.

5.2 Route Reply Packet format:

RREP is unicast and it is hop by hop fashion to source. In RREP each intermediate node creates the route to the destination. When source node receives RREP then it records the forward route to the destination and starts sending message. If multiple RREP's is received by source then depending upon hop count shortest path is selected.

1) *Destination IP Address:* The IP address of the destination for which a route is given.
2) *Destination Sequence Number:* The Destination sequence number associated to the route.
3) *Destination Unique ID:* The Unique Identification of Destination.
4) *Source IP Address:* The IP address of the Source.
5) *Source Unique ID:* The Unique Identification of Source.
6) *Lifetime:* Time to reach to the next Destination.
7) *Hop Count:* Number of Hops needed to reach the Destination.

5.3 Route Error Packet format

When link break down is detected, RERR is generated and send to the source node in hop by hop fashion. When each intermediate node invalidates route to an unreachable destinations or Sybil node is detected then RERR is sent towards source node. When source node receives RERR then it starts reinitiates route discovery.

1) *Unreachable Destination IP Address:* The IP address of the destination that has become unreachable due to a link break.
2) *Unreachable Destination Sequence Number:* The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.
3) Sybil Node: The information about sybil node which detected.

5.4 Route Maintenance

Once route is defined then route maintenance is also required. It is to provide information about link of the route as well as route to be modified due to movement of one or more nodes in the route. Every time route is used to send packet then its expiry time is updated by adding current time and Active Route Timeout (ART). ART is a constant value that defines how long new route is kept into routing table of node after last transmission done. ART defines both source and intermediate node. If route is not used in the predefined period then node can't be sure that route is still valid or not and then this route is removed from routing table. It ensures that no any unnecessary packet loss.

5.5 MATHEMATICAL MODEL

In our SRAN routing protocol we provide Unique Identity (UID) field in routing table of each node. When source node broadcasts then all nodes in the network will be verified original node or Sybil node by using UID. From Eq. 1 we can identify the original node and get unique identity of node.

A = {x | x=1 then it is original node}

B = {x | x=2 then it is malicious node}

Where, x = Unique Identity of node.

If 'A' condition is true then original route is follow and if 'B' condition is true then route is automatically eliminated.

5.6 Flow chart of Sybil attack Algorithm

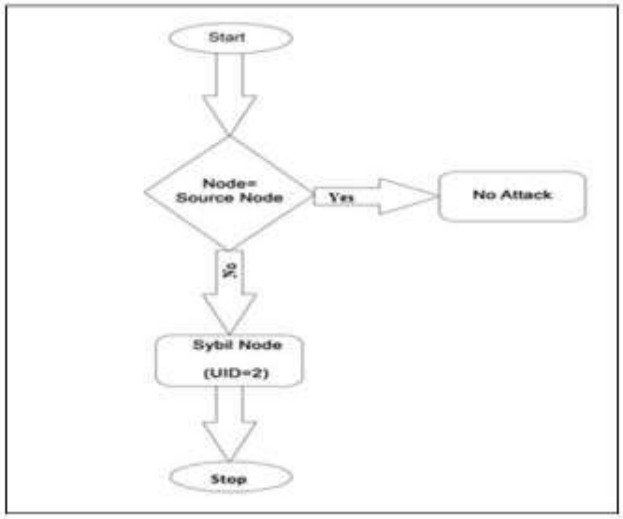

Figure 4: Flow of Sybil attack algorithm.

Considering analysis of secure routing protocols use different techniques to detect as well as prevent attacks. Sybil attack gets all the properties of original node. When Sybil attack is performed into this network then it first identifies the node as source node, if yes then no attack is performed on that node. If node is not source node then perform Sybil attack on that node. In this attack one or more Sybil nodes are injected into the network. This Sybil node can get all the properties of original node but automatically increase the value of Unique Identity as shown in Fig. 4. So when performing route discovery each node can check UID value when it is one then this node become a part of route. When UID value is not one then this node is Sybil node that means it detects the Sybil node and not gets into the route. So this Sybil node is automatically prevented from the route.

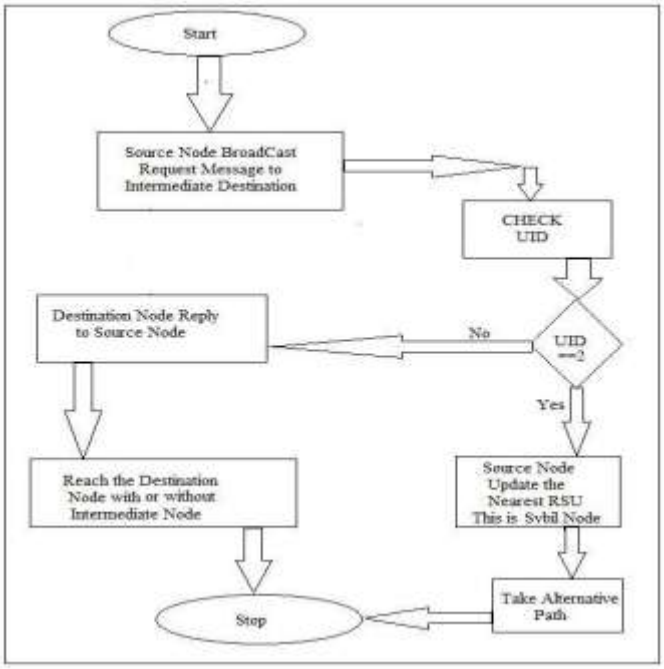

Figure 5: Execution of SRAN Protocol

6. EXPECTED RESULTS

In SRAN protocol separate mechanisms are not used to detect as well as to prevent sybil attack. So it improves the performance of all route activities. It prevents those Sybil nodes to come into that route. It shows total number of packets have been successfully received from source to destination and it also increases the throughputs. In Table II shows RREQ in which UID field consider to identify original node and fake node. Also it has very less delay because of on demand route selection.

Table 2: RREQ

Source ID	Dest. ID	Source IP	Dest. IP	UID
2	4	168.192.10.10	168.192.10.16	1
4	3	168.192.10.16	121.11.10.15	2
4	1	168.192.10.16	121.11.10.17	1

7. CONCLUSIONS

Secure communication is one of the important challenges in VANET. If communication is not secure then it can cause fake messages delivery by malicious nodes, misguiding nodes in the network. This may cause accidents or traffic jam on road. Most of the routing protocols are not providing security for data transmission. Instead of providing separate techniques for attack detection and prevention we can provide in routing protocols. It improves performance of VANET. This SRAN protocol is designed for Sybil attack. SRAN routing protocol provides unique identity to each node in its route table. Then this SRAN routing protocol can easily identify fake node and original node. Also it detects and prevents Sybil attack and gives high performance.

8. REFERENCES

[1] J.A. Guerrero-Ibáñez, C. Flores-Cortés, and SheraliZeadally, "Vehicular Ad-hoc Networks (VANETs): Architecture, Protocols and Applications", Computer Communications and Networks © Springer-Verlag London 2013.

[2] VinhHoa LA, Ana CAVALLI, "Securityattacks and solutions in vehicular ad hoc networks: A survey", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[3] Mushtak Y. Gadkari, 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.

[4] M. Raya and JP. Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security 15 (2007), PP 39–68.

[5] Omkar Shete ,SachinGodse "VANET: A Survey on Secure Routing" ,International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Paper ID: SUB1565, PP 123.

[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-chunhu and adrianperrig, "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, SeemaMehla and PreetiNagrath, "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 BibhuDuttaSahoo, "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.