Novel Secure Routing Protocol for Detecting and Preventing Sybil Attack

Mr. Shankar M. Sawant [1*], Mr. Vikas T. Ligade [2]

[1] Department of Computer Engineering, Shivaji Polytechnic College Sangola.

[2] Department of Computer Engineering Shivaji Polytechnic College Sangola.

*Corresponding author

doi: https://doi.org/10.21467/proceedings.118.55

ABSTRACT

Secure communication network is the demand of today's transportation due to excess number of vehicles and limitation to the existing communication protocol. This Paper discusses the secure communication protocol between the vehicles and the detection and prevention of the Sybil attack. Fake node request, multiple routing entries these are the common example of Sybil attack which can be detected and prevented using existing proposed method. Virtual nodes are created and messages are sent to nodes. The proposed method detects the identity of received message and number of fake entries of that particular massage in the routing buffer. If messages are validated then communication is possible otherwise request is terminated. Results showed that the existing proposed method is able to detect and prevent Sybil attack by maintaining single node identity.

Keywords*:* VANET, ad hoc network, sran, sybil attack.

1 Introduction

Vehicular Ad-hoc Network is the technology [4] which can form a secure network between vehicles, i.e., Vehicles communicate to every alternative and transfer information to another vehicle. VANET provides safety to driver of vehicles by exchanging messages between vehicles. VANET is not secure because many types of attacks can be appeared in it so it can leads to insecurity of drivers of vehicles. Vehicular Ad Hoc Network (VANET) is an emerging area for research. Vehicular Ad-Hoc Network is a challenging topic because of its mobility and link disruption. Many researchers [3] have been working on specific issues of VANET like routing, broadcasting, Quality of Service, security, architectures, applications, protocols, etc. Security is a main issue in VANET because malicious drivers in the network disrupt the system performance. Sybil attack creates multiple identities which lead to subvert the computer System.

Novel secure routing protocol detects and prevents the Sybil attack particular on Vehicular ad- hoc network. The proposed Secure routing protocol is based on ad-hoc on demand (AODV) distance vector secure routing (DVSR) for Mobile ad-hoc network (MANET) or other wireless ad-hoc network (WAN). This protocol maintains routing information and route discovery that detects and prevents Sevier Sybil attack and each node have unique identity and entry in route table. Inter vehicle communication is passing and receiving the information to increase traffic efficiency, detection of road conditions, avoid collisions, detect emergency situations and overall increase of the efficiency of network.

In a MANET or VANET, mobile or vehicular nodes are making huge impact on the performance of routing protocols because of its varying mobility characteristics. So many of the scholars and researchers [2] developed Ad hoc On-demand (AODV), Dynamic Source Routing (DSR), Destination Sequence Distance Vector (DSDV) routing protocols for MANET but they cannot directly used in VANET. Because of it's apparently, widely varying mobility characteristics of mobile or vehicular nodes are expected to have a significant impact on the performance of routing protocols. Therefore, even though researchers [2] have developed routing protocols like Ad hoc On-demand Vector (AODV), Dynamic Source Routing (DSR),

Proceedings DOI: 10.21467/proceedings.118; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-6-4

Destination Sequence Distance Vector (DSDV) etc. for MANET, these protocols cannot be directly adopted in VANETs, efficiently, because of the rapid variation in link connectivity, high speed and extremely varied density of vehicular nodes in VANET. Researchers have developed special routing protocols for VANET [1], and these are aimed to adapt rapidly. However, these recent protocols are not fully secure and able to prevent attacks on VANET. These attacks are fraud information, denial of service, black hole, alternative attack and Sybil attack.

Sybil attacks become a serious threat which 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/create multiple identities known as Sybil nodes or fake nodes. Sybil attack has been found in mostly peer-to-peer network where a node in the network can operate as multiple identities at the same time it can gains the authority and power in reputed systems. The main purpose behind this attack is to gain the majority of influence in the network actions in the system. In a Sybil attack a single entity that is computer has the capability to create and operate multiple identities such as user accounts or IP address based accounts. For the other observers these multiple attacks look like a real unique identity.

2 Formal Model of Sybil Attack

Sybil attack model consists of following parts:

E entities = c (correct) entities + f (faulty) entities

i) Correct – entities that follow the protocols and rules setup in the network honestly (whose honesty is verified).

ii) Faulty – entities whose behavior are arbitrary and can't be predicted. They don't honestly follow the protocols and rules in the network.

iii) A communication cloud: A very general cloud through which messages between different entities travel.

iv.) Pipe: to connect an entity with the communication cloud.

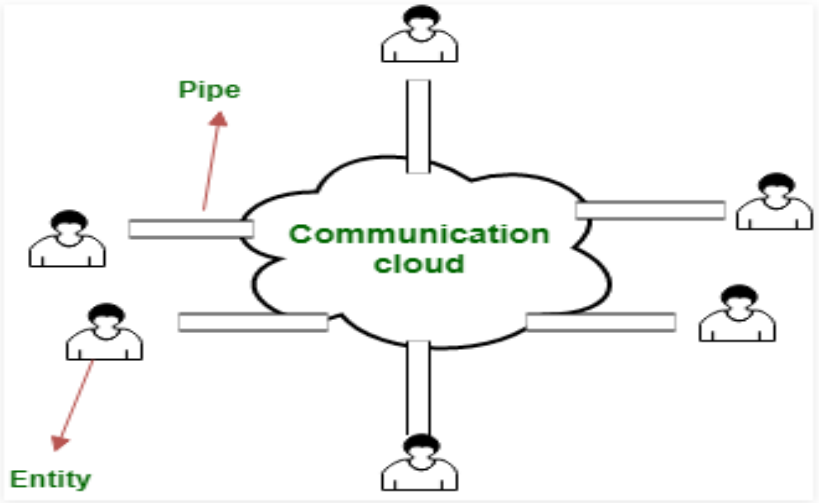

Fig. 1. Formal model of sybil attack.

3 Methodology

The proposed novel Secure Routing protocol for Ad hoc Network (SRAN) is a routing protocol for detecting and preventing Sybil attack. It is based on AODV and does not allow Sybil node into Route discovery by eliminating the node from the route table. Important views of SRAN protocol are route request packet format (RREQ), route reply packet format (RREP) and route error packet format (RERR)

Proceedings DOI: 10.21467/proceedings.118
ISBN: 978-81-947843-6-4

Series: AIJR Proceedings
ISSN: 2582-3922

3.1 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 route request packet format, if receiving node is not destination and does not have route to the destination then it rebroadcast the route request packet format 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.

3.2 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.

3.3 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: -** This information about Sybil node which detected.

3.4 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.

4 Result

Secure Routing protocol (SRAN) can improve the performance of routing in secure communication. It means that this protocol will detect and prevent Sybil attack. In SRAN total numbers of packets sent by source are received successfully at destination. Following table shows the result.

Table. 1. Performance of SRAN protocol with source id and destination id.

Source ID	Destination ID	Source IP	Destination IP	UID
2	4	192.168.10.10	192.168.10.16	1
4	3	192.168.10.16	192.168.10.15	2
4	1	192.168.10.16	192.168.10.17	1

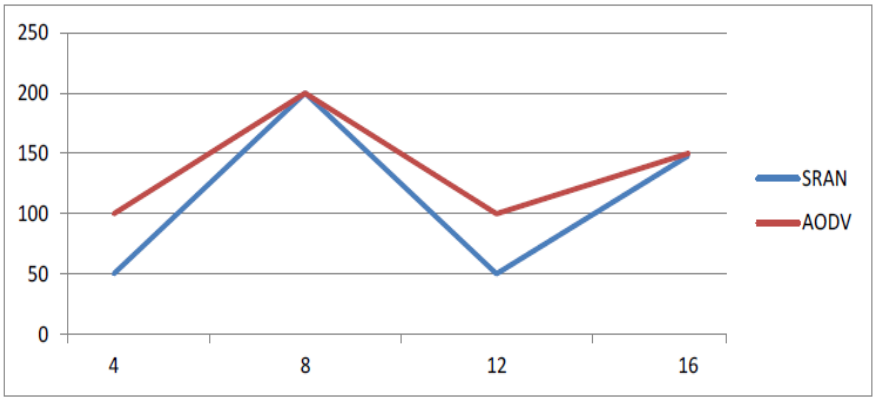

Fig. 2. Difference of performance of AODV protocol and SRAN protocol.

5 Conclusion

Security is the important challenges in VANET. SRAN directly rejects fraud messages introduced by the malicious nodes, misguiding nodes in the network. This avoids accidents and traffic jam on the road and saves vital life and time. SRAN routing protocols are providing security for data transmission. On the road and saves vital life and time. SRAN routing protocols are providing security for data transmission. It provides techniques for attack detection and prevention in routing well before it become malicious, suspicious and harmful. SRAN is better than VANET especially in the performance that successfully detects and prevents Sybil attack. SRAN routing protocol maintains unique identity of the node in order to establish higher secure communication between vehicles to vehicle. SRAN routing protocol is the best solution for the secure communication.

References

[1] E. Fonseca, A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS", NEC network laboratories, 28 pages, Version 1.1, March- 2006, pp. 1-28.

[2] R. Bai, M. Singhal, "DOA: DSR over AODV routing for mobile ad hoc networks", IEEE.

[3] Mushtak Y. Gadkari, Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE)

[4] Md Mahbubul Haque, Jelena Misic, Vojislav Misic, *et al.* Vehicular Network Security, Encyclopedia of Wireless and Mobile Communications, second edition, 2013.