A secure anonymous on-demand routing protocol to defend wormhole attack in Vehicular Adhoc Network

Er. Gurjot Singh

(1) K.M.V., (GNDU), Jalandhar, Punjab, India, Email: dr.gurjotsingh@yahoo.com

Abstract: Vehicular Ad-Hoc Network is a sub class of MANETs (Mobile Ad-Hoc Networks). It’s a technology that provide secure driving environment by wireless communication between the vehicles. The technique of self-driving vehicle is more significant in today’s world. VANET converts each participating vehicle into wireless sensor nodes that allow vehicles to communicate among themselves. It creates a network of wide range. Due to non-centralized infrastructure, self-driving and Ad-Hoc nature of VANETs it’s vulnerable to various critical attacks that breach the security. One of the critical attacks is wormhole attack which mainly occur least two or more malicious nodes. It enables an attacker to capture packets at one location and tunnels them to another location forming a wormhole link in-between the legitimate nodes of the network. In this paper, secure routing protocol ANODR is implemented to prevent the wormhole attack in VANETs. The ANODR prevents strong adversaries from tracing a data packet flow back to its originator and for location privacy problem; ANODR ensures that adversaries/attackers cannot discover the real identities of authenticated transmitters. The performance of ANODR is evaluated on the basis of metrics like throughput, end-to-end delay, total packet received and jitters.

Key words: VANETs, wormhole attack, ANODR, RSU, MANETs

1. Introduction

Vehicular Network (VANET) is a form of Mobile ad-hoc network, to provide communications among vehicles and nearby fixed equipment known as roadside equipment (RSU). By enabling vehicles to communicate with each other through Inter-Vehicle Communication (IVC) and with roadside base stations via Roadside-to-Vehicle Communication (RVC), vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and authorised authorities. The interesting research area of Vehicular Networks is where ad hoc networks can be brought to their full potential.

Both modern high-speed motorways and vehicles that drive upon them are becoming increasingly intelligent. In particular, communication devices through which the communication between the vehicles and RSU are done are installed in cars and roadside infrastructure components (RSU). In the not-too-distant future, travelling Vehicles will be able to communicate in rapidly changing ad hoc networks. At the same time, they will have direct access to a fixed roadside network infrastructure with information flowing in both directions. This environment of network motivates the need for an infrastructure that will provide drivers with access to a variety of vital vehicular and roadside information. This results in improving the highway
A Secure Anonymous On-demand Routing Protocol to Defend Wormhole attack in Vehicular Adhoc Network

safety. The main goal of VANET is providing safety and comfort for peoples. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the people [2].

Every vehicle is equipped with VANET special electronic device that will be a node in the Ad-Hoc network and can receive, relay messages through the wireless link. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way [2].

In vehicular adhoc networks, radio [VHF], micro waves and infrared waves have been used in Vehicle-to-Vehicle systems. Infrared and millimetre waves allow communication only in VHF and the microwaves allow broadcast communications. The VHF can provide long links but at low speed. In the PHY/MAC layer for a VANET network, the problem of robust communication between vehicles and an efficient sharing of the radio medium is solved. The other problem comes from the fact that there is large variation in the density of nodes i.e. vehicles in a VANET network. For instance, in traffic jams or just after an accident, the density of nodes may increase considerably. Another problem of ensuring quality of service (QoS) is difficult in a VANET environment [1,2].

VANET caused significant problems in wireless ad hoc and sensor network research. The issue of VANET security become more challenging due to the unique features, such as high-speed mobility of network nodes i.e. vehicle and extremely large amount of network entities. It’s basic necessary to make sure that the “life-critical safety” information cannot be deleted, inserted or modified by an attacker or adversaries; likewise, the system should be able to help establishing the liability of drivers; but at the same time, it should protect the privacy of the drivers and passengers. The malicious behaviour of users such as a modification and replay attack with respect to the disseminated messages could be fatal/ dangerous to other users. In the past few years research, efficient effort has been done on VANET networking protocols to make it secure against critical attacks. The VANET security should satisfy the following requirements i.e. Message authentication and integrity, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification [3, 4].

2. Related Work

In [2] Er. Jagjit Singh, Er. Neha Sharma had discussed the intrusion detection system to detect wormhole attack by evaluating the decision packet at destination node. VANET is no centralized infrastructure due to which it is vulnerable to various security attacks. The use of self-driving vehicles is becoming more and more significant in last few years. The fact that the vehicles are self-driving can lead to greater difficulties in identifying failure and anomalous states, since the operator cannot rely on its own body perceptions to identify failures.

In [14] Harbir Kaur, Sanjay Batish & Arvind Kakaria had proposed a method in which we use decision packets to detect the wormhole nodes in the network and for maintaining the integrity of the packets we compute hash value of each packet. The source node broadcasts the decision packet to all the nodes after receiving the route reply message from the destination node which contains the list of the route forming nodes. The decision packets from the nodes are then evaluated by the destination node based on the hop count value. If the hop count exceeds the threshold value, it means a wormhole is formed between the nodes.

In [15] Mrs.Kadam Megha V. had presented the survey over security framework for vehicular ad hoc networks and performance of mechanisms used to provide security. VANET is 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. 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.

![Diagram of wormhole attack](image)

Figure. 1. Two or more malicious nodes combine to form malicious short link between each other

3. Wormhole attack in VANETS

Wormholes are one of the most severe attacks on VANET routing.

Two or more malicious nodes can collaborate in setting up a shortcut lower latency link between each other Figure 1 and via this, they forward packets to other side and it replays the packets locally [10]. The adversaries convince the neighbor nodes of these two end points that the two distant points at either end of the tunnel are actually very close to each other [7]. An adversary that placed close to a base station is able to completely disrupt routing by convincing nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole [6]. In such a scenario, the attack is similar to the sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station [5]. Wormhole and sinkhole attacks are particularly difficult to defend against, especially when the two are combined. Wormholes are hard to detect because they use a private and out-of-band channel which is invisible to the network [6]. Packets are forwarded between the malicious nodes by encapsulation and use of additional hardware such as a wired link or a directional antenna [9]. Wormhole attacks are more likely be used in combination with selective forwarding or eavesdropping [6]. The wormhole attack is especially difficult to detect in VANETs.

A wormhole attack is launched in two different modes: hidden-mode and participation mode. Defending against a hidden-mode attack is particularly difficult because it can be launched even if all routing messages are authenticated and encrypted [8]. This is because the malicious node does not need to read or modify the packets, just forward them. Although participation mode wormhole attacks are more difficult to launch (they require modification of routing packets), once launched, they are extremely difficult to detect since the malicious nodes can efficiently ignore the security mechanisms of the routing protocol [9, 11].

4. Secure Routing Protocol

Wireless networks are different from other contemporary communication and wireless ad hoc networks routing is a very challenging task in VANETs. For Security perspectives, a secure routing protocol (ANODR) is used for routing in VANET.

**ANODR (Anonymous on-demand Routing (ANODR) Protocol):** It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network. Anonymous On-demand Routing Protocol is designed to provide an anonymous and untraceable routing scheme for wireless ad-hoc networks. It is based on table-driven AODV routing protocol. As in other routing protocols network routes are open to all i.e. packets sent in wireless manner then any adversaries can trace the network route and infer the pattern of the packets that are being communicate between communicating parties. This may pose a serious threat to network and
also a challenging constraint for routing and data forwarding. The ANODR protocol allows you to protect the wireless communication from being traced and without removing your device’s battery. The adversaries should not trace the data packets that are sent by ANODR secure routing protocol. It provides untraceable path for data communication. Thus reduce the threats of eavesdropping by intruders [13]. ANODR provides the following security services:

1. **Negligibility** - based on anti-tracing such that signal interceptors cannot trace signal transmitters mobility pattern via wireless signal tracing (with non-negligible probability defined on the victim network’s size).
2. **Confidentiality and anonymity** - The path follows by the packets should not be traced by any adversaries.
3. **Traffic flow confidentiality** - Conceals the message content through encryption.
4. **Identity-free routing** - The identity cannot be stole by other.
5. One-time packet contents such that any two wireless transmissions are indistinguishable with each other in regard to a cryptanalyst.

The ANODR configuration is based on AODV parameter settings. ANODR parameters use the same terminology as AODV’s parameters, except the name is changed from AODV to ANODR. These services are provided at the Network Layer and Link Layer to protect the IP and link layer protocols [12].

5. Implementation Details

VANET scenario is designed using QUALNET 4.5.1 simulator tool. The scenario is designed using terrain size of 1500*1500. The 9 mobile nodes are placed on canvas will act as vehicle. Clouds are placed on canvas will act as RSU (road Side unit). For mobility of vehicles waypoints are used and the Simulation is run for 150 sec. The simulation design is shown in figure 2. The performance of ANODR protocol to prevent wormhole attack is evaluated on behalf of metrics throughput, end-to-end delay, total packet received and jitter. For simulation the different parameters are set are shown in table 1:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>Qualnet 4.5.1</td>
</tr>
<tr>
<td>Terrain size</td>
<td>1500*1500</td>
</tr>
<tr>
<td>No. of nodes</td>
<td>9</td>
</tr>
<tr>
<td>Radio/Physical layer</td>
<td>802.16e</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random way point</td>
</tr>
<tr>
<td>Security Protocol</td>
<td>ANODR</td>
</tr>
<tr>
<td>Battery Model</td>
<td>Simple Linear</td>
</tr>
<tr>
<td>Antenna Model</td>
<td>Omni Directional</td>
</tr>
<tr>
<td>Simulation time</td>
<td>150 sec</td>
</tr>
<tr>
<td>Data Size</td>
<td>512 bytes</td>
</tr>
</tbody>
</table>

Table 1. Simulation parameters setup for QualNet simulator

![Figure 2. Simulation scenario design](image)
6. Result and Discussion

This section evaluates the performance of ANODR protocol against wormhole attack in VANET network. The performance is evaluated on the basis of metrics like throughput, end-to-end delay, jitter and total packet received.

1. Throughput (bits/sec.)

The above graph shows the value of throughput of VANET. The value of throughput is 3300.75 bits/sec. under wormhole attack and when ANODR secure routing protocol is implied on VANETs to prevent wormhole attack its throughput increases to 3925.5 bits/sec.

2. End-to-end delay (sec.)

The above graph shows the value of end-to-end delay of VANET. The value of end-to-end delay is 0.28036772 sec. under wormhole attack i.e. without ANODR protocol and when ANODR secure routing protocol is implied on VANETs to prevent wormhole attack its end-to-end delay decreases to 0.006694422 sec.

3. Jitter (sec.)

The above graph shows the value of jitter is 0.065651114 sec. under wormhole attack and when ANODR secure routing protocol is implied on VANETs to prevent wormhole attack its jitter decreases to 0.00272448 sec.
4. Total packet received

![Graph showing total packet received]

The above graph shows the value of end-to-end delay of VANETs. The value of total packet send in the network is 48. The packet received value is 14 under wormhole attack and when ANODR secure routing protocol is implied on VANETs to prevent wormhole attack its value increases to 22 packets.

7. Conclusion

In this paper, a secure routing protocol ANODR is implemented in VANETs to prevent it from severe wormhole attack. The performance is evaluated on the basis of metrics throughput, end-to-end delay, jitter and total packet received. The ANODR secure routing protocol avoids the strong adversaries from tracing the data packet flow back to its originator and for location privacy problem; ANODR ensures that adversaries/attackers cannot discover the real identities of authenticated transmitters. It provides untraceable path for data communication. It also provides traffic flow confidentiality and Identity-free routing. The experimental results show that the throughput of the vanet network increases when ANODR routing protocol is implied against wormhole attack. The end-to-end delay and the jitter is probably less under ANODR secure routing protocol and packet receive rate is increasing. Thus, anonymous on-demand secure routing protocol efficiently defends the severe wormhole attack in VANETs.

References


