Simulation Study and Prevention of AODV against Rushing Attack on Random Topologies in VANETs

Mr. Karthik Pai, Ms. Pratheeksha Hegde N, Mrs. Rashmi Naveen

Abstract— **Vehicular adhoc networks (VANETs) is subordinate class of mobile ad-hoc network (MANET) in which nodes are considered as vehicles. VANET is different from architecture, characteristics and application when compared with MANET. Vehicles are able to communicate through wireless technology by dedicated short range communication. Security is one of the main issues in VANET. VANET contains information which should not modified by attacker likewise the legal responsibility of drivers should be established so that they can inform traffic environment at correct time. This paper explains the effects of Rushing attacks in adhoc on demand distance vector (AODV) protocols on VANETs. The effects of these attacks in VANET have been studied using various performance metrics. NS2.34 is extensively used to simulate these attacks.**

Index Terms— **VANETs, AODV, Rushing attack, MD5, Initial vector**

I. INTRODUCTION

VANET (Vehicular adhoc network) consists of network of moving vehicles at a comparatively speed that communicate among themselves [1]. The main aim is to improve security on road and reduce accidents. VANET is the natural creation of wireless network by applying the principles of MANET for exchange of data to the domain of vehicle. Vehicular communication system (VTS) consists of two types of communication they are vehicle-vehicle (V2V) communication and vehicle- infrastructure (V2I) communication. Communication among these is adhoc in nature. V2V uses multicast technique and communicate about traffic and pathway conditions to one another. V2I has high bandwidth link with vehicle & roadside equipment which broadcast message and communicate between the vehicles. Vehicles communicate about gathered data to the RSU so that it can allocate data faster and more effectively.

VANET consists of some individual components that are On-Board Units (OBU), Roadside Unit (RSU) and Application Unit (AU). OBU is a wireless gateway located inside the vehicles. It can be associated to other RSU and OBU. It also consists of wireless transmitter and receiver. There are sensors, storage and warning devices associated with this unit that are temper proof in nature. It is used to exchange the information by Dedicated Short Range Communication (DSRC) which is used to provide high data transfer rates and minimum latency in communication link. RSU acts as router between the vehicles on road and other network devices. AU is a device equipped in vehicles which communicates with the network through OBU. AU is an in-vehicle entity and executes a set of applications utilizing the communication capabilities of OBU. The main intention of VANET is to look up passenger's security by distributing traffic, control of speed, pathway and weather conditions among nearby vehicles. There are many threats in VANET but they can be avoided using digital signatures.

The rest of the paper is described which is mentioned below: In Section II, the routing protocols in a VANET are explained. In Section III, routing attack against VANET is explained. In section IV deals with literature review. In section V deals with proposed methodology. In Section VI deals with the analysis of simulation and their experimental results and in Section VII we have concluded the paper.

II. ROUTING PROTOCOLS IN VANET

A. Proactive Routing Protocol

In Proactive routing protocol, each node contains route table which has the routing information of other node in the network. OLSR is a proactive routing protocol. Optimization of link reduces the control packets size and its transmission [2]. OLSR is mainly suitable for large networks. By using multipoint relay OLSR reduces traffic overhead. MPR is node's one hop neighbor which forwards data packets from the source. It determines the shortest path to the destination which is the advantage of multipoint relay. All MPR's should have the information of the routes which should be exchanged periodically which is the main requirement for MPR.

B. Reactive Routing Protocol

This routing algorithm finds the route only when it is preferred to send information to the destination and when it requires to communicate with each other. AODV is a reactive routing protocol. Each node maintains with table and the required information about the neighboring node and destination. Till the source node is available the routes in this network are maintained in AODV. The main attraction of AODV is sequence numbers which gives freshness to the routes.

Reactive routing consists of route-discovery and route-maintenance process. In route-discovery process the inquiry packet are broadcasted into the network for the path

Manuscript received May 23, 2016

Karthik Pai received his M.Tech degree in computer science and engineering from NMAM institute of Technology

Pratheeksha Hegde N is a PG Scholar in the Information Science Department, NMAM Institute of Technology. She received her B.E degree in Information science and engineering from NMAM Institute of Technology Nitte. Her research interests are wireless network and adhoc sensor network

Rashmi Naveen received her M.Tech degree in computer science and engineering from NMAM institute of Technology

search and it completes this phase when route is found. This process is carried out by route request (RREQ) packet and Route Reply (RREP) packets. When a source node sends data to destination it floods a RREQ packets to its neighbors and responds with RREP if it is not a destination node or do not have new route to the destination. In RREQ message source and destination sequence number are used to prevent loops and determines the freshness of the route respectively. Hop count is incremented when message is broadcasted by intermediate node and is used to find out the direct path to destination.

In route-maintenance process, a sequence number maintains freshness of the routes. Here nodes examine link perspective of next hops in active routes by using hello messages.

III. ROUTING ATTACK AGAINST VANET

On the basis of layers, several types of attacks are classified [3]. At physical layer and link layer, an attacker disturbs the communication network by overloading it by sending useless message. Some attackers can destroy OBU or RSU. In network layer, attacker can add useless message or overload the system with route information. Some of these attacks are briefly explained later.

A. Rushing Attack

When an attacker is present in the network and if a node sends route request packet to its neighbor node then the attacker will accept the route request packet and send it to its neighbor with high transmission speed by which it reaches the destination node as early as possible when compared with the other nodes [4]. Destination node will accept this route request packet which reached earlier and discards remaining route request packets which have reached later. Receiver will think that this is suitable route and uses this for communication. This way attacker will gain contact in the communication between sender and receiver.

IV. LITERATURE REVIEW

In [5] the authors have proposed "secure route delegation" as a protection technique against rushing attack. In this method, each node will verify whether all the Secure Neighbor Detection procedures are done between any neighboring nodes. Thus, Secure Route Delegation method uses Secure Border Gateway Protocol (S-BGP). In this scenario initially a node N1 receives current RREQ packet. Now N1 performs the secure neighboring detection to find its neighbor node N2. In this method, N1 hand over the RREQ to N2. Here N1 does not hand over whole message, because N2 can rebuild all the fields of the message and verifies its signature. The route delegation message can be filled with the last message of Secure Neighbor Detection. If N2 assumes that N1 is a neighbor, the protocol is continued when the route delegation is accepted. Therefore, signs another route delegation for the next neighbor.

V. PROPOSED METHODOLOGY

A message of any length is taken as input containing a message digest of 128 bit from the sender side. In the receiver side the decrypted message is obtained. Here the Initial Vector is distributed among all the nodes in a network.

In Sender side:

Initially the message of any length is being entered. Key is generated when the message is hashed using SHA1 hashing algorithm. Then input string is encrypted using MD5 encryption algorithm. Message is encrypted along with the key generated by SHA1 hashing algorithm to get encrypted message. Then encrypted message is appended with packet and sends to the receiver.

In Receiver side:

Initially we decapsulate the packet and get the encrypted message. Key is obtained by using Initial Vector as we hash the encrypted message. The plain text is decrypted by using MD5 decryption algorithm and the original message is obtained.

Algorithm:

```
Sender ()
{
    Initial Vector = 'key + node_id'
   message1 = input_string
    MD_key = hash (Initial Vector, message1)
    If ( ! rushing attack)
          encr_msg = encr_algo (MD_key, message1)
    else
          attacker_module ()
          packet_append (encr_msg)
          send (packet)
}
Receiver ()
{
Initial Vector = 'key + node_id'
encr_msg = packet_decapsulate (packet)
MD_key = hash (Initial Vector, encr_msg )
If( ! rushing attack )
          message1 = decr_algo (MD_key, encr_msg)
else
          attacker_module ()
          display (message1)
}
```

VI. EXPERIMENTS AND RESULTS

The simulation parameters are listed in Table 1. A control packet is the parameter considered for the estimation purpose. After prevention method with and without rushing attack for AODV is compared. In this section the simulation results are done in the form of line graphs.

TABLE 1: SIMULATION PARAMETERS

Parameter	Value
Simulator used	NS 2.34
Routing Protocol	AODV
Data rate	1Mbps
Traffic generated	CBR
Number of communicating Nodes	20
Network area	1000m x 1000m
Simulation time	100s

A. Control Packets

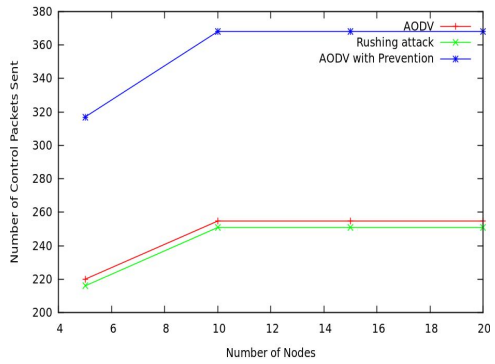

Figure 1: Control packets versus number of nodes

It is clear from Fig 1 that control packets in the presence of attacker nodes with and without prevention mechanism on AODV protocol. It is evident that AODV after using the proposed scheme has a higher value of control packets with respect to number of nodes. It can be observed from the graph that using proposed approach increases control packet by reducing the packet drops in the network.

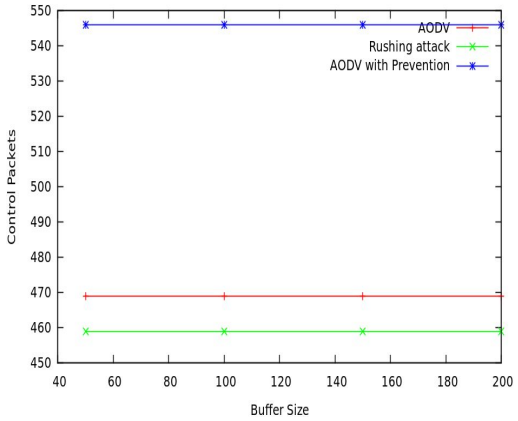

Figure 2: Control packets versus buffer size

Fig 2 shows that control packets in the presence of attacker nodes with and without prevention mechanism on AODV protocol. It is evident that AODV after using the proposed scheme has a higher value of control packets with respect to buffer size. It can be observed from the graph that using proposed approach increases control packet by reducing the packet drops in the network.

CONCLUSION

In this paper we discussed about the complete study of effects of some of the DoS attack against VANETs like rushing attack and we have used different performance metrics for rushing attack. This gives us a clear picture of the effects of rushing attack on VANET in AODV. The parameter like control packets are being calculated. The simulation study and analysis indicates that Rushing attack degrades the network performance to very large extent. By the analysis study we conclude that the proposed method provides higher control packets for AODV and rushing attack. For the future work we can implement on proactive routing protocols with other routing attacks and inspect the performance of network.

BIBLIOGRAPHY

[1] Swapnil G. Deshpande, "Classification of Security attack in Vehicular Adhoc network: A survey", International journal of emerging trends and technology in computer science.

[2] V.Jigisha, Ch.Sudersan Raju, Dr.Ch.Balaswamy "The comparison between OLSR and AODV routing protocols for Vehicular Adhoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, March 2015.

[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), November 2011.

[4] Satyam shrivastava, "Rushing attack and its prevention techniques", International journal of application or innovation in engineering & management (IJAIEM), April 2013**.**

[5] Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari, "Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Networks", International Symposium on Biometrics and Security Technologies (ISBAST), 2014.