ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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

Pratheeksha Hegde N, Rashmi Naveen

M.Tech Student, Department of ISE, NMAM Institute of Technology, Karnataka, India

Assistant Professor, Department of ISE, NMAM Institute of Technology, Karnataka, India

ABSTRACT: Vehicular adhoc networks (VANETs) is a rising technology with a special class of MANET. It does not have any fixed infrastructure. Communication among vehicles is between vehicles and roadside infrastructure. So security is a significant area for VANET. For authentication purpose, lowers the performance and bandwidth is high. And availability of network must be obtained when a node sends any essential information to other node. The aim of this paper is to give an overview of VANETs with special effects of Gray Hole attack in Adhoc on demand distance vector Routing (AODV) protocol based on VANETs. We have used different performance metrics for Gray Hole attack in VANETs. To simulate this attack NS-2.34 has been used widely.

Keywords: VANETs, AODV, Gray Hole attack, initial vector, MD5.

I. INTRODUCTION

VANET is not same as MANET in the characteristic of higher mobility, privacy requirements etc [1]. The idea of VANET is to make available communication between vehicles to get better road condition and make driving safer. Every vehicle needs an OBU (On-Board Units) through which vehicles can communicate with each other as well as with RSU (Roadside unit) connected to a network so that it uses services including internet access that is accessible to vehicles. Since VANET maintains essential information, they should pursue with security necessities like privacy, confidentiality, integrity to provide secure communication against attacker node [2]. Attacker node not only affects the driver's privacy but also cooperate safety of traffic. Hence, widespread researches are carried out to provide security in VANETs. During the communication in VANETs the identity of drivers should be uncovered since it utilizes this data to introduce the attack with fake identities and by no means had get caught which is the aim of providing security and privacy in VANETs. Identities of vehicle and driver have to make known to RSU to communicate with them. So security and privacy should be carefully handled so that opponent cannot misuse them.

This paper is structured as follows: In Section II, background and related work are discussed. In Section III, we have brief explanation on proposed methodology and in section IV we have explained experimental results analysis and finally we have concluded the paper in section V.

II. BACKGROUND AND RELATED WORK

A. OVERVIEW OF AODV

When a node needs to send information to destination then only the path is formed [3]. In the network, path is maintained until they are required by the source. AODV handles unicast and multicast routing. Here every node preserves a table and the necessary data about the neighbor and destination nodes. Main attraction of this protocol is sequence numbers which gives freshness to the routes. If the sequence numbers are used frequently then the existing path is more up to date. The path is established by issuing RREQ message. Path is established when RREQ message is received. To get multiple paths then multiple RREQ message should be received. Source updates data of a path if RREP holds data which is more up to date.

B. ROUTING ATTACK AGAINST VANET

Gray Hole Attack

Here an attacker node acts as a normal node which is similar to Black Hole attack [4]. So it is not easy to detect Gray Hole attack, due to this type of behavior since it acts as a normal node. Gray Hole attack is also called node misbehaving attack. Each node preserves routing table that stores the data of neighbor node, which is path to destination. This attack has two dissimilar phases. In first, attacker node performs AODV protocol having valid path to destination. In second, the nodes drop irregular packets with specific opportunity. When packets are not dropped, the Gray Hole attacker act as normal node then it switches to its malicious behavior.

C. RELATED WORK

In [5] author has taken a MANET consisting of related type of nodes. Every node will wander or remain fixed in a location for a random time. A node may connect or go away from network any time. The node carries out peer-to-peer communication over wireless multi hop channel. We assumed that for the use of differentiation, every node contains distinctive nonzero identity and all the association in network are considered to be bi-directional. The proposed mechanism will not consider operation of promiscuous mode of interfaces of nodes. To process the transit packets, promiscuous mode may not put on further computation overhead and energy utilized but it will be insufficient where nodes set with directional antenna. At dissimilar points of time in the network there may be many Gray Hole nodes and these attacker nodes might assist with each other to disturb the communication in network. To identify any attacker in the network, proposed mechanism involves recognition & eradication technique. If attacker node is detected, notification for sending messages to every node excluding attacker, so that it can be inaccessible to make use of any network. Mechanism consists of local irregularity security actions which is call upon consecutively.

III. PROPOSED METHODOLOGY

Description of Proposed Algorithm:

A message digest of 128 bit from the sender is taken as a message input of any length. In sender side, message is being entered and decrypted message is obtained by the receiver. Here Initial Vector is circulated among every node in a network. Message is hashed using SHA1 hashing algorithm to produce a key. Then input string is encrypted using MD5 encryption algorithm. Message is encrypted along with generated key by SHA1 hashing algorithm, to get encrypted message. The encrypted message is attached with packet and sends to the receiver. In receiver side, primarily we decapsulate the packet and get the encrypted message. The original message is obtained when plain text is decrypted using MD5 decryption algorithm.

```
Algorithm: In sender side,
Step 1: Key and node id is concatenated to get initial vector
Step 2: Input string is taken as the message input
Step 3: The Initial Vector and message is hashed to attain message digest key
Step 4: Check this condition
            if (! gray hole attack)
               Message digest key and message is encrypted using encryption algorithm to achieve encrypted message
            else
               attacker_module ( )
Step 5: Achieved encrypted message is appended with packet
Step 6: Then this packet is sent.
In receiver side,
Step 1: Key and node id is concatenated to get initial vector
Step 2: The received packet is decapsulated to obtain encrypted message
Step 3: Initial vector and encrypted message is hashed to attain message digest key
Step 4: Check this condition
            if( ! gray hole attack )
               Message digest key and encrypted message is decrypted using decryption algorithm to achieve original message
            else
              attacker_module ( )
```
Step 5: The original message is displayed
Step 6: end

IV. EXPERIMENTS AND RESULTS

The proposed cryptographic algorithm is implemented with NS 2.34. Performance metrics are calculated from trace file using the AWK script. In this section the simulation results are shown in the form of line graphs. We have selected control packets with respect to number of nodes and buffer size as the simulation parameter to evaluate the performance.

Control packets:

It is total number of route request and route reply packets consumed by a protocol.

a) Simulation parameters:

The following parameters from Table 1 are used for network simulation.

TABLE 1: SIMULATION PARAMETERS

Parameters	Values
Simulator	NS 2.34
Routing Protocol	AODV
Traffic produced	CBR
Number of Nodes	20
Simulation time	100s
Network area	1000m x 1000m

b) Control packets versus number of nodes:

TABLE 2: CONTROL PACKETS VERSUS NUMBER OF NODES ON AODV

Number of nodes	AODV	Gray Hole attack	AODV with prevention
5	220	151	449
10	255	175	525
15	255	175	525
20	255	175	525

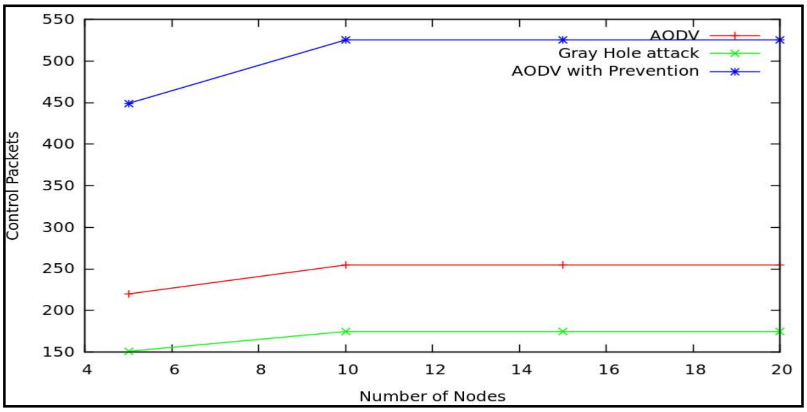

Fig 1: Control packets versus number of nodes

From the Fig 1, it 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 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.

c) Control packets versus buffer size:

TABLE 3: CONTROL PACKETS VERSUS BUFFER SIZE ON AODV

Buffer size	AODV	Gray Hole attack	AODV with prevention
50	459	376	696
100	459	376	696
150	459	376	696
200	459	376	696

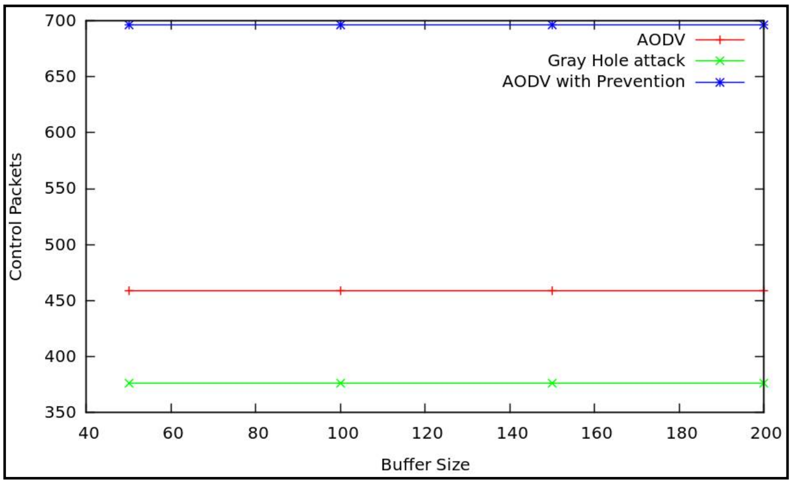

Fig 2: Control packets versus buffer size

DOI: 10.15680/IJIRCCE.2016. 0405025

From the Fig 2, it 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.

V. CONCLUSION

In this paper, performance analysis of Gray Hole attack using routing protocol on randomly generated scenarios is studied. The parameters like control packets with regard to number of nodes and buffer size are used for analysis. The simulation study and analysis of Gray Hole attack in control packets indicates that it degrades the network performance to very large extent in the presence of attacker using AODV. Here first we have focused on the detection of Gray Hole attack and then RC4-MD5 prevention mechanism is implemented. In future we can add few more attacks and performance of network can be compared with and without attacker. And also try to implement prevention mechanism for those attacks.

VI. REFERENCES

1. M.A. Razzaque, Ahmad Salehi S., and Seyed M. Cheraghi, “Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead”, Springer-Verlag Berlin Heidelberg, Vol No 2, Issue No 4, pp.107-132, 2013.
2. Mohammed Saeed Al-kahtani, “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)”, pp 1-9, 2012.
3. 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, Vol No 4, Issue No 3, pp 467-470, 2015.
4. Shani Makwana, Krunal Vaghela , “Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET”, International Journal of Computer Applications, Vol No 125, Issue No 4, pp 1-6, 2015.
5. Onkar V. Chandure, Prof. V. T. Gaikwad, “A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol No 2, Issue No 6, pp 2607- 2611, 2011.

BIOGRAPHY

1) 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.

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