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

Performance Analysis and Mitigation of Gray Hole Attack against AODV under Collaborative Environment using MANETs

Akshaya, Karthik Pai B H

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

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

ABSTRACT: A mobile Ad Hoc network is a group of portable nodes whose links are broken in an arbitrary way that is in MANET there is no infrastructure, thus each node act as a host and router. They are linked to each other by peer-to-peer network. As the MANETs find its applications mainly in emergency situations, security is of prime importance. In this paper, we have implemented a cryptographic security mechanism in order to secure one of the packets dropping attack say gray hole attack for AODV under collaborative environment using MANETs. The proposed mechanism applies cryptographic primitives on the routing packets. Simulation results shows that this method has a drastically high prevention rate with reasonable network traffic load.

KEYWORDS: AODV, Gray Hole, MANET, RC4-MD5, initial vector

I. INTRODUCTION

MANETs are infrastructure-less networks with the collection of portable nodes, these nodes are either mobile phones, personal computers or MP3 players etc. These nodes willingly forward the data packets to the nodes which are outside its range. As the portable nodes can join or depart from the network freely with no constraints, topology of network changes simultaneously. The nodes communicate using a highly error prone wireless links and these links break frequently due to mobility of nodes. Thus the routing of packets on an optimal path is of most important concern.

Further the paper is prearranged as: Section 2 deals with, theoretical background and relative works. Section 3 discusses the proposed scheme. Section 4 deals with simulation results and finally this paper is concluded in section 5.

II. THEORETICAL BACKGROUND

A. *Overview of AODV*

Ad-hoc On Demand Distance Vector Routing Protocol is a routing algorithm which is designed for routing in mobile Adhoc networks. It is a reactive routing algorithm which means that the routes are formed only when requested by the originating node. And these routes are maintained as long as it is required for the source node [1] [2].

AODV routing has mainly two processes. Route discovery is the first process which is carried out by Route Request (RREQ) and Route Reply (RREP) packets. The route maintenance is the second process where a sequence number is used to maintain the freshness of the routes. When the originating node wants to link with the destination node, it broadcasts the RREQ message. The node receiving the RREQ packets will reply with RREP packets if it contains path to the destination or that itself is the destination node provided the current sequence number is more than or same as the sequence number in the packet. If not then it will rebroadcast the RREQ packets until the route is discovered [1] [2].

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

B. Gray Hole Attack

Gray Hole attacks are the packet drop attack, which is a deviation of black hole attack in which the greedy node performs this attack selectively. In this packet drop attack, the attacker advertises itself as a co-operating node, and thus participates in route request and reply mechanism. After route discovery stage, when originator node transmits information through a fake route, the greedy node will just drop each data packet from the source node [3].

C. Related work

Jian-Ming Chang [4] proposed a methodology called as Cooperative Bait Detection Scheme (CBDS), which aims to detect as well as to prevent greedy nodes initiating collaborative black-hole/ gray-hole attacks in MANET based networks.. In this proposed method, in order to send the RREP packets, the originating node stochastically chooses a neighbouring node so as to use the address of selected node as destination address for the bait. On the way to activate the detection mechanism again, when a considerable packet is dropped in the pdr, a notification alarm is forwarded to the originating node by the destination node. Thus the detection and prevention of greedy nodes from taking part in the routing process are handled.

III. PROPOSED MECHANISM

Gray Hole attacks are packet drop attacks in which the malicious node performs this attack selectively. In this paper we have developed a cryptographic prevention method for preventing the effect of gray hole attack. In this method plain text of any length is taken as input for the SHA1. SHA1 is a hashing algorithm which hashes the plain text and produces a message digest key. Then with the encryption algorithm say RC4-MD5 the plain text is encrypted and forwarded to the receiver side. At the receiver same procedure takes place. At the receiver side using the initial vector we hash the cipher text and obtain the key. By using this key and applying RC4-MD5 decryption algorithm the plain text is obtained. By this method most of the data packets are securely transmitted to the destination [5] [6]. The algorithm for proposed mechanism is given below.

```
Sender ( )
{
IV = ‘key1+ node-id’
msg = input string
MD5_Key = hash (IV, msg)
encrp_msg = encrp_algm (MD5_Key, msg)
packet_append (encrp_msg)
send (packet)
}
Receiver ( )
{
 IV = ‘key + node-id
encrp_msg = packet_decapsulate (packet)
MD5_Key =hash (IV, encrp_msg)
msg = decrp_algm (MD5_Key, encrp_msg)
display (msg)
}
```

IV. EXPERIMENTAL RESULTS

This section includes simulation and evaluation of well known protocol known as AODV with and without DDoS attack is being compared. Simulations are been carried out using NS-2.34.

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

TABLE 1
SIMULATION PARAMETERS

Simulator	Ns 2.34
Routing Protocol	AODV
Traffic generated	CBR
Mobility Model	Random way point
Number of communicating nodes	25
Network area	1000m x 1000m
Simulation time	100s

a) CONTROL PACKETS

The Figure 1 shows the total number of control packets used, with and without prevention mechanism on AODV protocol. From the graph it's clear that the total number of control packets with the proposed scheme increases for all the scenarios, which indicates that the effect due to malicious attacker is reduced.

TABLE 2
TOTAL NUMBER OF CONTROL PACKETS

Number Of Nodes	AODV	Gray hole Attack	AODV with Prevention
5.0	36	16	107
10.0	95	50	418
15.0	130	52	729
20.0	226	185	1469
25.0	256	137	2530

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

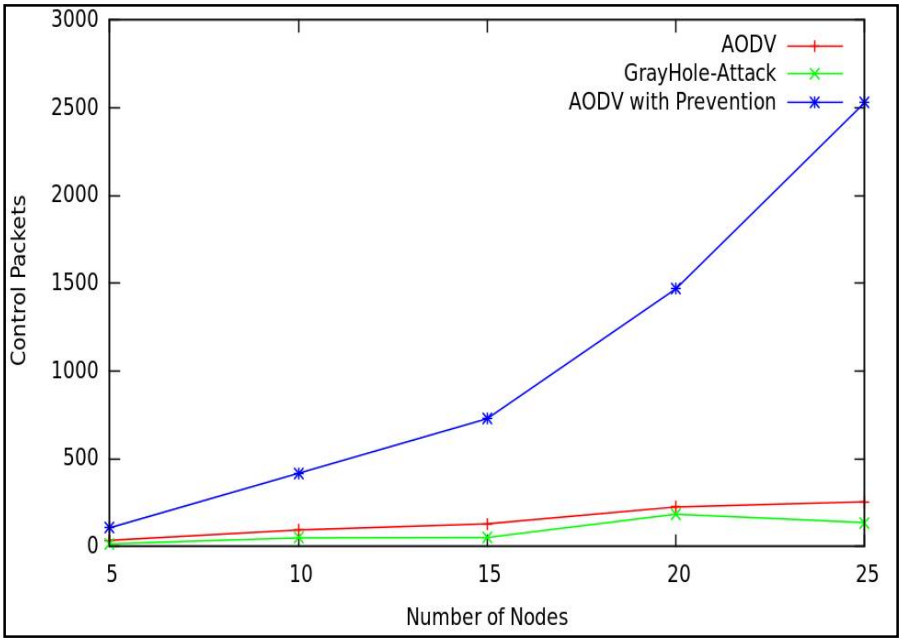

Fig 1: Control packet versus number of nodes

b) THROUGHPUT

From the Figure 2 it is clear that AODV after using the proposed scheme has a higher value of throughput. Even though throughput was below the average at the beginning, later on it increased for more number of communicating nodes.

TABLE 3
THROUGHPUT

Number Of Nodes	AODV	Gray hole Attack	AODV with Prevention
05.0	32.0645	20.3185	6.24
10.0	60.0104	47.1139	33.44
15.0	53.1745	38.2421	58.24
20.0	61.7321	53.1653	117.04
25.0	51.9439	46.0711	202.64

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

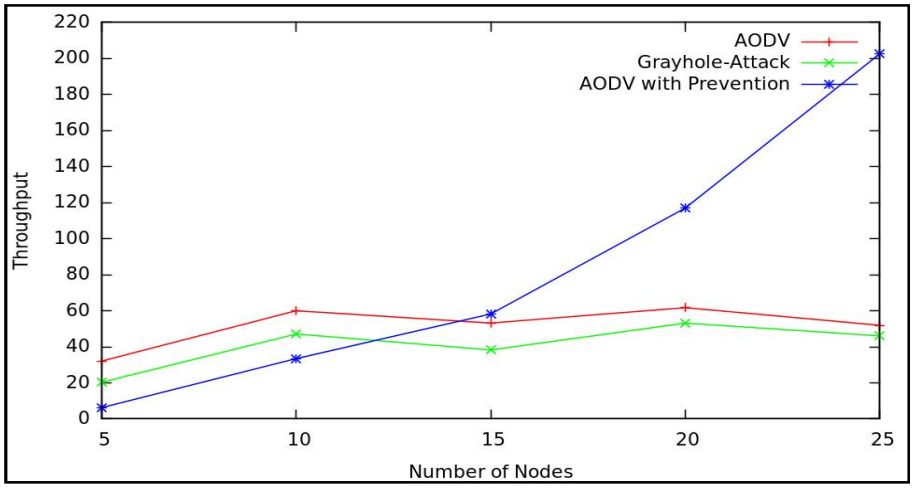

Fig 2: Throughput versus number of nodes

V. CONCLUSION

This paper discusses a complete study of the effects of some of the most destructive attacks say Gray hole under AODV. As the MANETs find its applications mainly in military, emergency and disaster conditions, lots of analysis works are to be done in the region of development of secure routing protocols for MANETs that can resist these DoS attacks.

To conclude with this analysis, the simulation study of gray hole attack on AODV indicates that the packet drop attack on MANETs degrades the network performance in the presence of single and collaborative attackers. Packets destined to a node will always be dropped denying the service to the authorized node. Our proposed mechanism provides better throughput and reduces the packet drop, thus providing the better performance. Further we can use this mitigation method for proactive routing protocol.

REFERENCES

1. Ashok M. Kanthe, Dina Simunic and Ramjee Prasad, "The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-Hoc Network", International Journal of Recent Technology and Engineering (IJRTE), Vol. 2, Issue 2, pp. 245-251, 2012.
2. Jiri Hosek, "Performance Analysis of MANET Routing Protocols OLSR and AODV", Vol. 2, Issue. 3, pp. 22-27, 2011.
3. Ms. Trupti Patel, Ms. Ch.Shyamala Rani, Mrs. Hina Patel, "Performance evaluation of DSR Protocol under DoS attack", International Journal of Electronics and Computer Science Engineering (IJECSE), Vol. 1, Issue. 2, pp. 239-242, 2008.
4. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", Ieee Systems Journal, Vol. 9, Issue. 1, pp. 65-75, 2015.
5. Chaitya B. Shah, Drashti R. Panchal, "secured hash algorithm-1: review paper", International journal for advance research in engineering and technology, Vol. 2, Issue X, pp. 26-30, 2014.
6. Piyush Gupta, Sandeep Kumar, "Comparative Analysis of SHA and MD5 Algorithm", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5(3), pp. 4492-4495, 2014.

BIOGRAPHY

Akshaya 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. Her research interests are sensor network and wireless network.

Karthik Pai B H received the M.Tech degree in computer science and engineering from NMAMIT, Nitte. He is currently pursuing his Ph.D in the area of computer Networks.