Performance Analysis and Prevention Mechanism of AODV against Rushing Attack under Collaborative Environment using MANETs

Mr. Karthik Pai B H, Ms. Akshaya, Dr. Nagesh H R

***Abstract*— MANET stands for "Mobile Adhoc Networks, is a kind of Adhoc network that can modify its locations and organize them self on the fly. As the MANETs are mobile in nature, they use wireless connections to connect to different communicating system. As the number of movable device increases, Adhoc networks are gaining importance with the increasing number of widespread applications. As the MANETs find its applications mainly in military, emergency and disaster situations, security is of prime importance for the basic functionality of the network. To provide secure communication and transmission different types of attacks and their properties must be well understood. Effect of Rushing attack in Adhoc On-Demand Distance Vector (AODV) routing protocol and a cryptographic prevention mechanism is being discussed in this paper. Various performance metrics are considered to study the effect of Rushing attack on AODV in MANETs.**

***Index Terms*— AODV, MANETs, RC4-MD5, Rushing attack, and SHA1.**

I. Introduction

MANETs are the decentralized independent wireless system which has the group of free nodes that communicates on a wireless shared channel. Nodes form a very short-lived network without any preset infrastructure and thus are free to move randomly. The communication between these mobile nodes is carried out without any organized structure and centralized control. In the absence of centralized control in a dynamic atmosphere, it requires collaboration within the nodes [1]. If there are only two nodes positioned very closely to each other and want to exchange a data packets among themselves, then there is no need of routing protocols.

If there are a many portable nodes wish to share information among them, then the routing protocols come into picture [2].

Further this paper has being prearranged as: Section II discusses theoretical background and related works. In Section III, proposed prevention method is being discussed. A section IV deal with the experimental results and analysis and finally this paper is concluded in section 5.

II. THEORETICAL BACKGROUND AND RELATED WORK

A. Overview of AODV

In this protocol [2], the paths to the destination node are only obtained when the originating node has some packets to forward and floods the network with Route Request Packets. The routing involves two stages: the Route finding and Route Maintenance process. Route finding process is carried out by Route Request (RREQ) and Route Reply (RREP) packets. For illustration, when an originating node has some packets to forward, it forwards RREQ packets to all of its neighbors [1] [2]. Every node on receiving the route request packets replies the originator node with the RREP packet along the shortest path. Route maintenance is the second process, where the freshness of the routes is maintained by the sequence number.

B. Rushing Attack

Here, the greedy node transfers earlier RREQ packets to all of its neighbors thus forcing the rebroadcast from the genuine ones. In this attack, the attacker removes the delay that a message suffers at MAC layer and thus the greedy node sends the RREQ packets before the normal nodes send. As in the routing algorithms, the intermediary node reacts only for the first RREQ packet received and discards the photocopied RREQ packets. As the RREQ packets only pass through attacker node, it causes the genuine packets to be forwarded in dysfunctional manner [3].

C. Related Work

In [4] the authors have proposed protection techniques "Secure Neighbor Detection" and "Randomized RREQ forwarding" for Rushing Attack. In "Secure Neighbor Detection" method every node checks whether every other node in its neighborhood is within the specified maximum transmission range. Once the verification message is received by the node a message is sent to all of its neighbors which allows it to forward the RREQ packets, the neighbor node will then confirm that the message sent by the node is inside the permissible range. In second method "Randomized Selection", in order to forward the RREQ packets, duplicate suppression process of the on-demand routing protocol is being replaced. In this procedure the midway nodes collects a number of RREQ packets and randomly select the RREQ packets. This provides most effectual defense against rushing attack, since it ensure that the RREQ packet which has been arrived at the first is not rebroadcasted at all times.

III. PROPOSED METHODOLOGY

Input: A message is plaintext of any length.

Manuscript received May 23, 2016

Mr. Karthik Pai B H, Information Science and Engineering, NMAM Institute of Technology, Karkala, India

Ms. Akshaya, Information Science and Engineering, NMAM Institute of Technology, Karkala, India

Dr. Nagesh H R, Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, India,

Output: In the sender side a message digest of 128 bit for the input message.
In the receiver side Decrypted message.

The algorithm works in the following steps:
Initial Vector (IV) is being shared among all the nodes in the network.

At the sender:

Initially the plain text of any type is being entered. Then the Plain text is being hashed using the SHA1 hashing algorithm [5] [6], and a message digest key is generated. We use RC4-MD5 [5] [6] encryption algorithm for encrypting the input string. Then the plain text is being encrypted along with the key generated by SHA1 hashing algorithm. And thus we obtain the encrypted (cipher text) message. This is then appended with packet and sent to the receiver.

At the receiver:

At first we de-capsulate the packet and obtain the cipher text. Then using the Initial Vector we hash the encrypted message and obtain the key. By using RC4-MD5 decryption algorithm, the plain text is being decrypted and the original message is obtained.

Since the Initial Vector is being shared only among the genuine nodes, the attacker nodes may not be able to decrypt the message and thus we can predict the secure transmission of data.

```
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. EXPERIMENTS AND RESULTS

This section includes simulation and assessment of proposed methodology. For this purpose, AODV protocol with and without rushing attack is being compared with the AODV protocol after prevention method. Simulations are been carried out using NS-2.34 and the simulation parameters are listed in Table 1. Packet delivery ratio and throughput are the parameters considered for the evaluation purpose.

Table I: Simulation Parameters

Parameter	Value
Simulator	Ns 2.34
Routing Protocols	AODV
Traffic generated	CBR
Data rate	1Mbps
Mobility Model	Random way point
Number of communicating Nodes	20
Network area	1000m x 1000m
Simulation time	100s

a) Throughput

From the Figure 1 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.

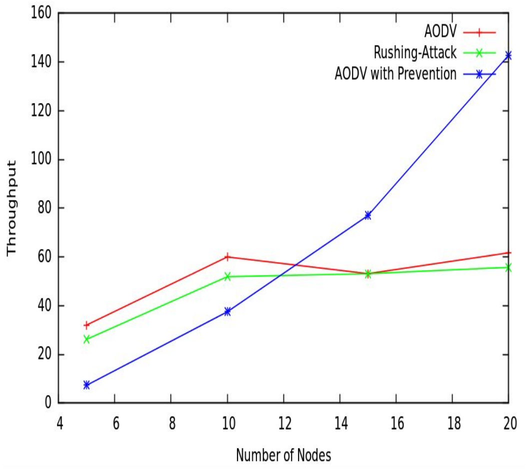

Fig 1: Throughput

b) Control packets

The Figure 2 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.

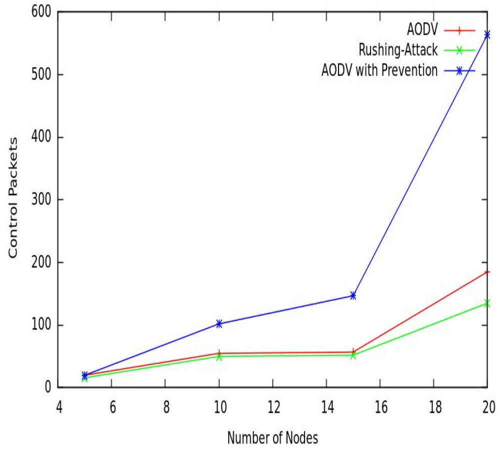

Fig 2: Control packets

CONCLUSION

This paper discusses a complete study of the effect of Rushing attack on AODV routing protocol on randomly generated scenarios. Different parameters like average throughput, control packets are being calculated. The simulation study and analysis indicates that Rushing attack degrades the network performance.

The cryptographic prevention mechanism proposed in this research work can prevent the network from rushing attack. By the analysis study we conclude that the proposed method provides higher throughput and control packets for both AODV with rushing attack. For the future work this proposed mechanism can be implemented on proactive and hybrid routing protocols and on other routing attacks, and examine the performance of network.

REFERENCES

[1] Savita Gandhi, Nirbhay Chaubey, Pathik Shah and Madhvi Sadhwani. “Performance Evaluation of DSR, OLSR and ZRP Protocols in MANETs.” International Conference on Computer Communication and Informatics, IEEE 2012.

[2] Amit Kumar Sanghi, Dharm Singh and Rakesh Poonia. “ Simulation Performance of Manet Routing Protocol Dsr With Different Mobile Nodes” , pp 444-448, IEEE 2011.

[3] 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), pp 220-224, IEEE 2014.

[4] Y.C.Hu, A.Perrig and D.Johnson. “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols.” Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2003.

[5] William Stallings, “Network Security Essentials Applications and Standards”, (chapter 11) Pearson Education, 2000.

[6] Atul Kahate, “Cryptography and Network Security”, (chapter 4) third edition, McGraw Hill Education Private Limited.

Mr. Karthik Pai B H received the M.Tech degree in computer science and engineering from NMAMIT, Nitte. He is actually a Associate Professor of Information Science and Engineering in NMAM Institute of Technolgy, Nitte. He is currently pursuing his Ph.D in the area of computer Networks.

Ms. 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.

Dr. Nagesh H R is Ph. Dr. in Computer Science and Engineering, National Institute Technology Karnataka, Surathkal. He is the Head of CSE department in National Institute of Technology.