SURVEY OF FLOODING ATTACK IN MOBILE ADHOC NETWORK

Guide –Mr.neeraj shukla*

Mansi kharya*

Abstract—

Mobile ad hoc networks will appear in environments where the nodes of the networks are absent and have little or no physical protection against tampering. The wireless nodes of MANET are thus susceptible to compromise and are particularly vulnerable to denial of service (DoS) attacks launched by malicious nodes or intruders. Flooding attack is one such type of DoS attack, in which a compromised node floods the entire network by sending a large number of fake RREQs to nonexistent nodes in the network, thus resulting in network congestion. In this paper, the security of MANET AODV routing protocol is investigated by identifying the impact of flooding attack on it. A simulation study of the effects of flooding attack on the performance of the AODV routing protocolis presented using random waypoint mobility model The simulation environment is implemented by using the NS-3 network simulator. It is observed that due to the presence of such malicious nodes, average percentage of packet loss in the network, average routing overhead and average bandwidth requirement− all increases, thus degrading the performance of MANET significantly.

Keywords-AODV; flooding attack; malicious nodes; MANET; NS-3 simulation; packet loss; wireless security

* Gyan ganga college of technology

I. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a group of wireless mobile hosts, which has no stationary infrastructure or base station for communication. Each individual node communicates beyond their direct wireless transmission range by cooperating with each other and forwarding packets through multi-hop links. The nodes act as routers for forwarding and receiving packets to/from other nodes. Ad hoc networking are extensively use for military purposes, disaster relief, mine site operation, etc. For such applications, a secure and reliable communication is necessary. Routing in ad hoc networks [2] [3] [4] has been a challenging task ever since wireless networks came into existence. Due to the high mobility of nodes, interference, multipath propagation and path loss, there is no fixed topology in MANET. Hence a dynamic routing protocol is needed for these networks to function properly.

Dynamic routing protocols can be classified as proactive and reactive routing protocols, as follows:

The *proactive (table-driven)* routing protocols like DSDV [5], etc. maintain the routing information to every other node in the network, even before it is needed.

The *reactive (on-demand)* routing protocols like AODV [6], DSR [7] etc., do not maintain the routing informations to other nodes in the network, until and unless required. This type of protocols finds a route on demand by flooding the network with Route Request packets.

In many situations, the on-demand (reactive) routing protocols have proved to perform better with significantly lower overheads than the periodic (proactive) routing protocols. This is because the on-demand protocols can react quickly to the dynamically changing topology, while reducing the routing overhead in those areas of the network, where changes are less frequent. In this paper, the focus is mainly on the reactive routing protocols (namely AODV) for MANET.

All available nodes in ad hoc networks participate in routing and forwarding, in order to maximize the total network throughput. Hence, successful operation of MANET is possible if and only if all the participating nodes fully cooperate in communication. Due to the lack of a

fixed base station, the ad hoc nodes are forced to rely on each other to maintain network stability and functionality. However, misbehaving nodes [8] [9] [10] are capable of causing significant problems. A node may misbehave when it is overloaded, broken, selfish, or malicious.

A malicious node [11], also called compromised node, can sabotage the other nodes or even the whole network, by launching a denial of service attack, by either dropping packets or by flooding the network with a large number of RREQs to invalid destinations in the network, thus jamming the routes of communication. Flooding attack is one such type of DoS attack, in which a compromised node floods the entire network by sending a large number of fake RREQs to nonexistent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network. This results in network congestion, thus leading to a Denial of Service.

In this paper, a simulation study of impact of flooding attack in AODV [6] performance, using the NS-3 network simulator is given.

The rest of the paper is organized as follows. In section II, an overview of the AODV routing protocol is presented, followed by a briefing about the NS-3 network simulator in section III. The impact of flooding attack in MANET is discussed in section IV. In section V, the simulation parameters used are given, followed by the simulation results in section VI and concluding remarks in section VII.

II. OVERVIEW OF THE AODV PROTOCOL

The Ad hoc On-demand Distance Vector (AODV) [6] routing protocol is a simple and efficient on-demand routing protocol, based on the distance vector approach. It is designed specifically for use in multi-hop wireless MANET scenario. The protocol is composed of the two main mechanisms − "Route Discovery" and "Route Maintenance".

Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of routing table entries. *Route Request* (RREQ) message is broadcasted by a node requiring a route to another node and *Route Reply*

(RREP) message is unicasted back to the source of RREQ. Sequence numbers are used for each routing table entry to determine whether the routing information is up-to-date. This prevents routing loops.

AODV includes the *route maintenance* mechanism to handle the dynamic network topology. Routes are maintained by using *Route Error* (RERR) message, which is sent to notify other nodes about a link failure. HELLO messages are sent in periodic beacons for detecting and monitoring the links to the neighbors.

If a node S wants to send data packets to a destination D that is not in its routing table, it will buffer the data packets and broadcast a *Route Request* (RREQ) for D into the network. The RREQ packet will be forwarded by other intermediate AODV nodes to the intended destination node D. On receiving the RREQ, D will send a *Route Reply* (RREP) on the reverse route back to S. S includes the known sequence number of the destination in the RREQ packet. The intermediate nodes, on receiving an RREQ packet check its routing table entries. If it possesses a fresh route toward D, i.e. a route with greater sequence number than that in the RREQ packet, it unicast an RREP packet back to its neighbor from which it has received the RREQ packet. Otherwise, it sets up the reverse path and then rebroadcasts the RREQ packet. Duplicate RREQ packets received by one node are silently dropped. As the RREP packet is propagated along the reverse path to the source, the intermediate nodes update their routing tables and set up the forward path.

III. THE NS-3 SIMULATOR

For simulation analysis, NS-3 [12] [13] was used for implementing the network simulation environment. NS-3 is an open source discrete event network simulator targeted primarily for networking research and educational purpose. Previously, NS-2 [14] was the tool for academic networking research. But it had several disadvantages. It required the involvement of both oTcl and C++. For new modules and features, it required a lot of manual recoding and compilations.

NS-3 is a new simulator. It is not an extension of NS-2. It does not support the NS-2 APIs. It

is written entirely in C++, with optional Python bindings. Hence, simulation scripts can be written either in C++ or in Python. The oTcl scripts are no longer needed for controlling the simulation, thus abandoning the problems which were introduced by the combination of C++ and oTcl in NS-2. Thus, NS-3 is a more readily extensible platform and much easier to use.

NS-3 has sophisticated simulation features, which include extensive parameterization system and configurable embedded tracing system, with standard outputs to text logs or PCAP (tcpdump). It is very object oriented for rapid coding and extension. It has an automatic memory management capability as well as an efficient object aggregation/query for new behaviors & states, like adding mobility models to nodes. Moreover, NS-3 has new capabilities, such as handling multiple interfaces on nodes correctly, efficient use of IP addressing and more alignment with Internet protocols and designs and more detailed 802.11 models, etc. NS-3 integrates the architectural concepts and code from GTNetS [15], which is a simulator with good scalability characteristics. The Simulation Network Architecture looks just like IP architecture stack. The nodes in NS-3 may or may not have mobility. The nodes have "network devices", which transfer packets over channel and incorporates Layer 1 (Physical Layer) & Layer 2 (Data Link layer). The network devices acts as an interface with Layer 3 (Network Layer: IP, ARP). The Layer 3 supports the Layer 4 (Transport Layer: UDP, TCP), which is used by the Layer 5 (Application Layer) objects.

IV. IMPACT OF FLOODING ATTACK

A malicious (compromised) node generally aims to launch a denial of service in the whole network. Flooding attack [11] [16] [17] [18] is a denial of service attack, in which a compromised node floods the network by sending large number of fake RREQs to nonexistent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network.

Flooding attack can be classified into two types [17]: RREQ Flooding Attack and Data Flooding Attack.

A. RREQ Flooding Attack

The RREQ Flooding Attack is a denial-of-service attack in which malicious nodes take advantage of the route discovery process of the reactive routing protocols (e.g. AODV, DSR) in MANET. In this attack, a compromised node aims to flood the network with a large number of RREQs to non-existent destinations in the network. It generates a large number of RREQs and broadcast them to invalid destinations. Since a node with such invalid destination node-id does not exist in the network, a reply packet cannot be generated by any node in the network and they keep on flooding the RREQ packet. When such fake RREQ packets are broadcasted into the network in high numbers, the network gets saturated with RREQs and is unable to transmit data packets. Thus, it leads to congestion in the network. The RREQ Flooding Attack also results in overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a denial- of-service attack. Moreover, unnecessarily forwarding these fake route request packets cause wastage of precious node resources such as energy and bandwidth.

To reduce congestion in a network, the AODV protocol adopts some methods. RREQ_RATELIMIT [19] is the maximum allowable number of RREQs that a node can sent per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may again try to discover a route by broadcasting another RREQ, until the numbers of retries reach the maximum TTL value. The default value for the RREQ_RATELIMIT is
10 as proposed by RFC 3561. However, a malicious node can
override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node can do so because of its self-control over its parameters. This allows it to flood the network with fake route requests, leading to a kind of DoS attack due to the network-load imposed by the fake RREQs.

B. Data Flooding Attack

Once an attacker node has set up the paths to all the nodes in the networks, it may cause DATA Flooding Attack by streaming large volumes of useless DATA packets to them along these paths. The excessive DATA packets in network clog the network and reduce the available network bandwidth for communication among the other nodes in the network. The

destination node gets busy on receiving the excessive packets from the attacker and cannot work normally. The available network bandwidth for communication also gets exhausted, so that the other nodes cannot communicate with each other due to the congestion in the network. Moreover, the process of receiving the attack packets consumes a lot of resource in all the intermediate nodes.

If an attacker combines both types of flooding attacks, it will result in the whole network crashing.

Due to flooding attack, a non-malicious genuine node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs and useless data packets. This leads to several problems, as follows:

- Wastage of bandwidth
- Wastage of nodes' processing time, thus increasing the overhead
- Overflow of the routing table entries, causing exhaustion of an important network resource like memory
- Exhaustion of the nodes' battery power
- Degraded throughput

Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication.

V. SIMULATION SETUP

The simulation was done using the NS-3 simulator [12], which provides a scalable simulation environment for wireless networks. In order to measure the impact of flooding attack in MANET performances, the AODV routing protocol was modified to simulate a flooding attack scenario.

The simulated network consists of 16 nodes placed randomly in 500x500 areas. For different scenarios of simulation, Constant position mobility and Random-walk 2D mobility model are used. Each node moves at a speed of 20 m/s.

The *Ping* application was used in the application layer. To simulate flooding attack, some malicious nodes were introduced to flood the network. These flooding nodes generated fake RREQ packets with invalid destination addresses and broadcasted them in the network at the rate of 8 packets per sec. By default, RREQ_RATELIMIT [19] of each node is 10, as proposed by RFC 3561. This RREQ_RATELIMIT was changed to 50.

The simulation parameters along with their values are listed down in Table I.

TABLE I. SIMULATION PARAMETERS

Parameters	Valu
routing protocol	AODV
simulation time	60s
number of mobile	95
transmission area	1000 x1000
mobility model	Random-walk 2d
traffic type	UDP
data packet size	1024Bytes
rate	2Kbps
speed of node	20m/s
RREQ_RATELIMIT	50

VI. SIMULATION RESULTS

After simulating the flooding attack in AODV, some graphs were plotted and they were used to see the simulation results when the network gets flooded by fake RREQs to invalid destinations.

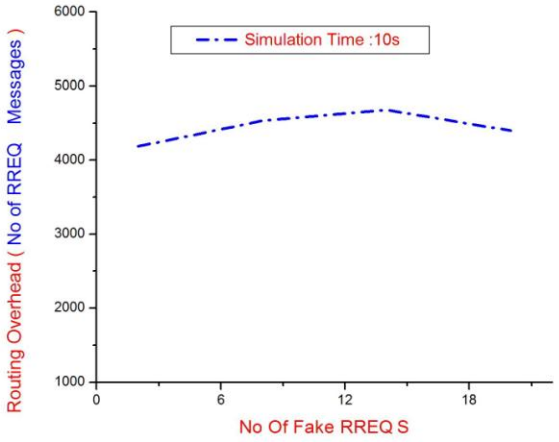

Figure 1. Number of Fake RREQs vs. Routing Overhead

For the simulation in Fig. 1, fake RREQ packets were generated and the total number of original RREQs that arrived at each node was calculated. *Routing Overhead* denotes the total number of RREQ messages (original, as well as fake) broadcasted in the network. The graph in Fig. 1 depicts that the average Routing Overhead increases with the number of fake RREQs. Because of these fake RREQ messages, routing table of each node needs to maintain more entries, thus creating an extra overhead.

For Fig. 2 simulation, the total number of data packets that were dropped due to the RREQ flooding was calculated. The graph depicts that the average percentage of data packet loss increases with the increase of fake RREQs in the network.

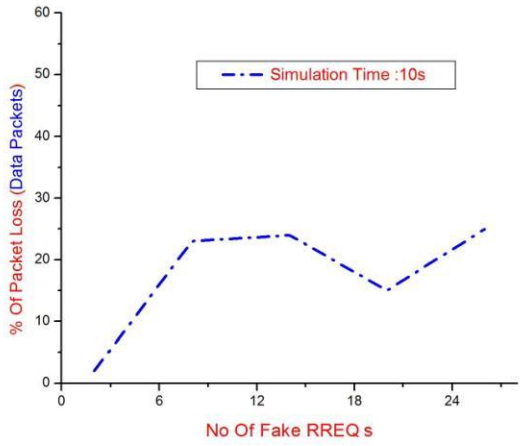

Figure 2. Number of Fake RREQs vs. Percentage of Data Packet Loss

Next, some flooding nodes were introduced, which generate eight RREQs per second. The graph in Fig. 3 depicts that with the increase in the number of flooding nodes, Routing Overhead, (i.e. total number of original and fake RREQ packets in the network) increased drastically.

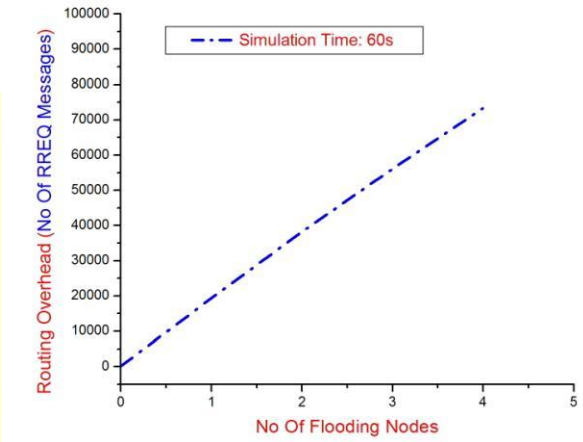

Figure 3. Number of Flooding Nodes vs. Routing Overhead

The bandwidth usage in the network was calculated, as follows:

Bandwidth usage =

(Total num of packets received/Simulation Time)*(8/1000) Bandwidth usage of a network is inversely proportional to the throughput of the network.

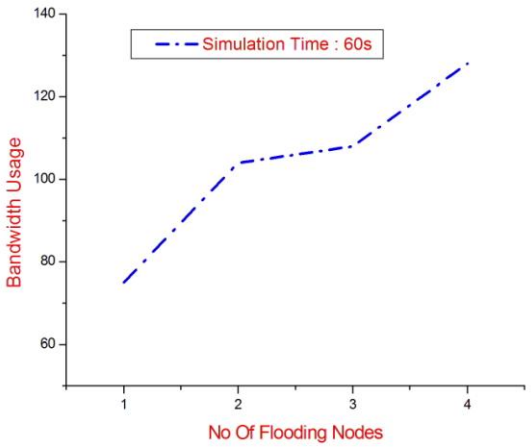

Figure 4. Number of Flooding Nodes vs. Bandwidth Usage

The graph in Fig. 4 depicts that the average bandwidth usage of the network increases as more flooding nodes join the network. Because of this flooding attack, average bandwidth usage of the network increases considerably, thus decreasing the network throughput.

Fig. 5 shows the average percentage of data packet loss due to the presence of flooding nodes in the network. The graph depicts that the average percentage of data packet loss in the network increases with the number of flooding nodes.

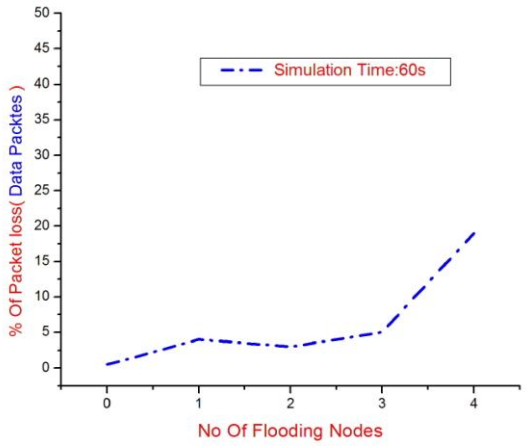

Figure 5. Number of Flooding Nodes vs. Percentage of Data Packet Loss

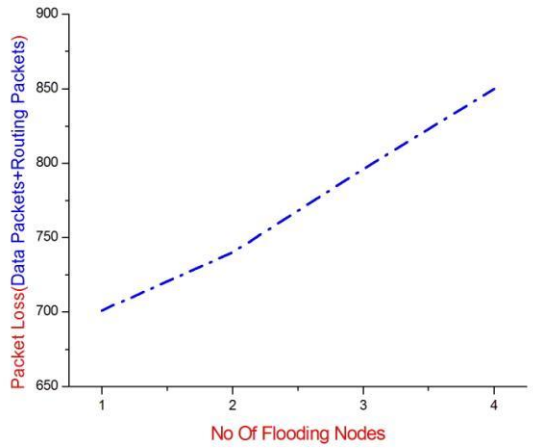

Figure 6. Number of Flooding Nodes vs. Percentage of Overall Packet Loss (Data and Routing Packets)

Due to the flooding attack, the network gets congested, resulting in a loss of RREQ packets as well. The graph in Fig. 6 depicts that as the number of flooding nodes in the network increases, the average packet loss (both data and routing packets) also increases in the network.

VII. CONCLUSION

In this paper, the security of AODV routing protocol in MANET was investigated by identifying the impact of flooding attack on it. The flooding attack in AODV protocol was simulated using the NS-3 network simulator. However, similar results can also be found when using the DSR [7] routing protocol. It was noticed that the presence of malicious flooding nodes in MANET can affect the performance of the overall wireless network and can act as one of the major security threats. From the simulation, it can be concluded that due to the extensive flooding in the network, average percentage of packet loss, average routing overhead and average bandwidth requirement– all increases, thus decreasing the overall network throughput.

A strong monitoring mechanism must be implemented in the mobile nodes of MANET for the identification and isolation of the compromised flooding nodes from the network. Some sort of incentive mechanism may also be incorporated in the network to enforce cooperation among all the nodes in MANET to improve the overall network performance.

In future work, a reputation based trust mechanism is proposed, which helps to resist misbehavior in the network by motivating the nodes to enhance cooperation and thus improve the network performance.

REFERENCES

[1] S Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". Internet Request for comment RFC 2501, Jan 1999.

[2] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks". Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

[3] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, "Routing security in ad hoc wireless networks", Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[4] Krishna Gorantala, "Routing Protocols in Mobile Ad-hoc Networks". June 15, 2006, Master's Thesis in Computing Science, 10 credits; Supervisor at CS-UmU: Thomas Nilsson; Examiner: Per Lindstrom.

[5] C. Perkins and P Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers". In ACM SIGCOMM'94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234-244.

[6] C.E. Perkins, E. Belding Royer, and S.R. Das, "Ad hoc On demand distance vector (AODV) routing", IETF RFC 3561, July 2003.

[7] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[8] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks". International Conference on Mobile Computing and Networking, Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, Boston, Massachusetts, United States, pgs. 255 – 265.

[9] A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols". IETF RFC4593. Status Informational, October, 2006.

[10] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer, 2008.

[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing

attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[12] "The NS-3 Network Simulator", http://www.nsnam.org/

[13] Elias Weingartner, Hendrik vom Lehn, Klaus Wehrle, "A performance comparison of recent network simulators". In Proceedings of the IEEE International Conference on Communications 2009 (ICC 2009), Dresden, Germany, 2009.

[14] "The NS-2 Network Simulator", http://www.isi.edu/nsnam/ns

[15] G. Riley, "Large scale network simulations with GTNetS", in Proceedings of the 2003 Winter Simulation Conference, 2003.

[16] S. Sanyal, A. Abraham, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N. Mody, "Security scheme for distributed DoS in mobile ad hoc networks", 6th International Workshop on Distributed Computing (IWDC'04), vol. 3326, LNCS, Springer, 2004, pp. 541.

[17] P. Yi, Z. Dai, Y. Zhong, S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), April 2005, pp. 657-662.

[18] Z. Eu and W. Seah, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan, January 2006.

[19] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF- MANETterms-00.txt, November 1997.