Impact of Security Attacks on Routing Protocols in MANETs

[1]Priyanka Chandragiri, [2]Dr Muzzammil Hussain
[1]Dept. of CSE, Christu jyothi Institute of Technology and Science, Jangaon, Telangana, India
[2]Dept. of CSE, Central University of Rajasthan, India

Abstract
Most of the routing protocols, applications and services in mobile ad-hoc networks assume a cooperative and friendly network environment and therefore do not accommodate security. The routing protocols in mobile ad-hoc networks are more vulnerable to these security attacks. Malicious nodes attack by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information due to which the network will not be able to provide service properly. Attacks like reducing the amount of routing information available to other nodes, failing to advertise certain routes or discarding routing packets or parts of routing packets are due to selfish behavior of a node. In this paper we discuss various security attacks like Worm hole, Rushing attack, and Sybil attack on routing protocols in MANETs and also study the impact of those attacks on the performance of the routing protocols.

Keywords
Malicious Nodes, MANETs, Worm Hole, Rushing Attack, Sybil

I. Introduction

Routing is an important function in any network, be it wired or wireless. The protocols designed for routing in these two types of networks, however, have completely different characteristics. Routing protocols for wired networks typically do not need to handle mobility of nodes with the system. These protocols also do not have to be designed so as to minimize the communication overhead, since wired networks typically have high bandwidths. Very importantly, the routing protocols in wired networks can be assumed to execute on trusted entities, namely the routers. These characteristics change completely when considering ad hoc wireless networks. Mobility is a basic feature in such networks. Ad hoc networks also do not have trusted entities such as routers, since every node in the network is expected to participate in the routing function. Therefore, routing protocols need to be specifically designed for wireless ad hoc networks. Most of the routing protocols, applications and services in mobile ad-hoc networks assume a cooperative and friendly networks environment and therefore do not accommodate security. The routing protocols in mobile ad-hoc networks are more vulnerable to these security attacks [1]. Malicious nodes attack by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information of that the network is not able to provide service properly. Attacks like reducing the amount of routing information available to other nodes, failing to advertise certain routes or discarding routing packets or parts of routing packets are due to selfish behavior of a node

II. Attacks

The attacks on routing protocols can be of three types [2]:

- Wormhole attack
- Rushing attack
- Sybil attack

A. Wormhole Attack

A wormhole attack [3-4, 6-7] typically requires the presence of at least two colluding nodes in an ad hoc network. The malicious nodes need to be geographically separated in order for the attack to be effective. In this attack, a malicious node captures packets from one location and "tunnels" these packets to the other malicious node, which is assumed to be located at some distance. The second malicious node is then expected to replay the "tunneled" packets locally. There are several ways in which this tunnel can be established. We consider two possible methods.

In the first method for establishing the tunnel shown in fig. 1, a malicious node denoted X in the figure, encapsulates a packet received from its neighboring node A. Node X then sends the encapsulated packet to the colluding malicious node Y. Node Y then replays the packet in its neighborhood after decapsulating the packet. Thus, the original packet transmitted by node A in its neighborhood is replayed by node Y in its neighborhood, which includes node B. For example, if the original packet transmitted by bode A (and tunneled by node X) was a hello packet, then node B on receiving this packet would assume that node A is its neighbor, which is not true. As another example, if node A transmits a route request packet for node B, then node X can "tunnel" such a packet to node Y by encapsulating the packet. As a result, this route request packet will arrive at the destination node B with a lower hop count than the other Route Request packet going through the other route. This happens in spite of using any secure routing protocol such as the ones given earlier. Note that nodes between X and Y that relay the packet cannot interpret the packet as it is encapsulated. Therefore, they cannot increment the hop count.

In the second method for establishing the tunnel shown in fig. 2, the two malicious nodes X and Y are assumed to have access to an out-of-band high bandwidth channel. This could be achieved for example by having a wired link between the two nodes or by having a long range high bandwidth wireless link operating at a different frequency. Thus, this method requires specialized hardware capability and hence is more difficult than the previous method. In this case also, a hello packet transmitted by node A can be retransmitted in the vicinity of node B. As a result node B infers that node A is its neighbor. Similarly, a route request packet, from node A for node B, can also reach node B (which is the destination for the route request packets) faster and possibly with fewer hops, since a high-bandwidth direct link is being used between the two malicious nodes. As a result, the two endpoints of the tunnel can appear to be very close to each other. To see this, consider Figure 2 Here node B receives three route requests. It is clear that the route request received through the wormhole will have the least hops.

It seems as if the malicious nodes are performing a useful service by tunneling the packets. This would be so if the nodes were performing this service without any malicious intent, but malicious nodes could use this attack to undermine the correct operation of various protocols in ad hoc networks. The most important protocol that is impacted is the routing protocol, as we can see from the examples given earlier. Data aggregations, protocols that depend on location information, data delivery and so on, are some other examples of services that can be impacted. Note that the wormhole

attack can be successful even without access to any cryptographic material on the nodes.

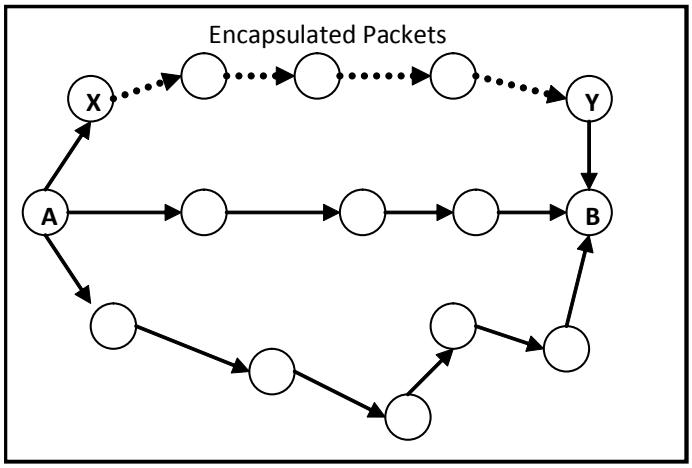

Fig. 1: Encapsulated Packets

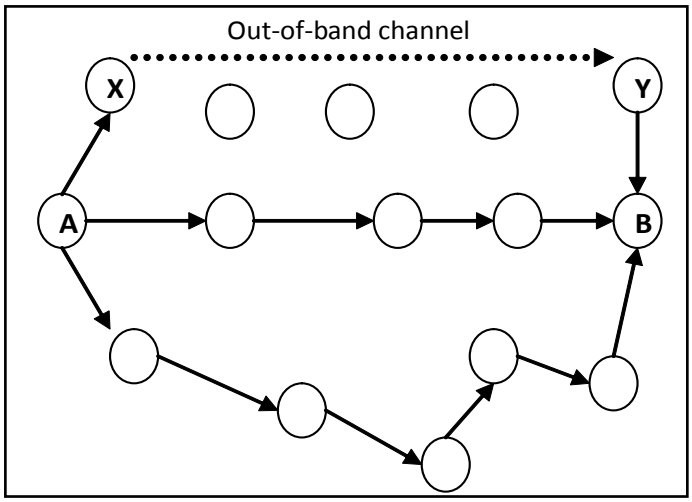

Fig. 2: Out-of-band Channel

B. Rushing Attacks

This attack impacts a reactive routing protocol. Note that, in the case of a reactive routing protocol, a node that needs a path to a destination floods the network with route request packets. Such route request packets are flooded in a controlled fashion in the network, thus, every node only forwards the first route recovery packet that it receives and drops the rest. The adversary can exploit this feature of reactive routing protocols. It does so by "rushing" the route request packets towards the destination. As a result, the nodes that receive this "rushed" request forward it and discard the other route requests that arrive later. The resulting routes would then include the adversary, which places the adversary in an advantageous position.

We see that this attack is not very difficult to launch. All it requires is that the adversary be able to forward route request packets faster than can be done by valid nodes. The adversary can do this by forming wormholes. The adversary can also do this by choosing to ignore the delay between the receipt and forwarding of route request packets. Such delays are specified by the routing protocols to avoid collisions of route request packets. The adversary can also choose to ignore delays specified by the protocols to access the wireless channel. Thus, in all these cases the route request packet can be rushed by the adversary.

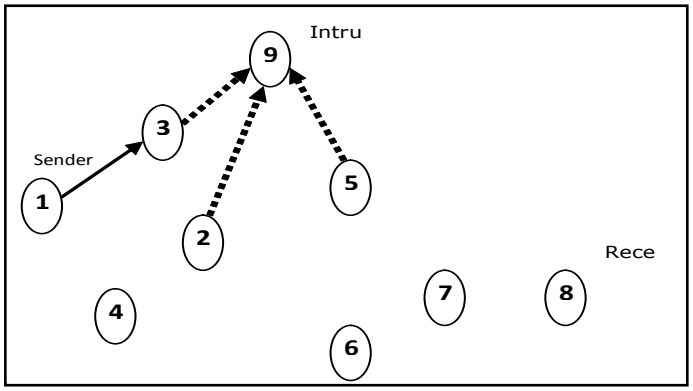

Fig. 3: Rushing Attack Scenario

C. Sybil Attacks

The Sybil attack [4, 6-8] consists of a node assuming several node identities while using only one physical device. The additional identities can be obtained either by impersonating other nodes or by making use of false identities. These identities can all be used simultaneously or over a period of time. This attack can impact several services in ad hoc networks. For example it can impact multi path routing, where a set of supposedly disjoint paths can all be passing through the same malicious node which is using several Sybil identities. This attack can also impact data aggregation where the same node can contribute multiple readings each using a different identity. Fair resource allocation mechanisms will also be affected since a node can claim more than its fair share by using the various Sybil identities. Mechanisms based on trust, voting, and so on, are also affected by this attack.

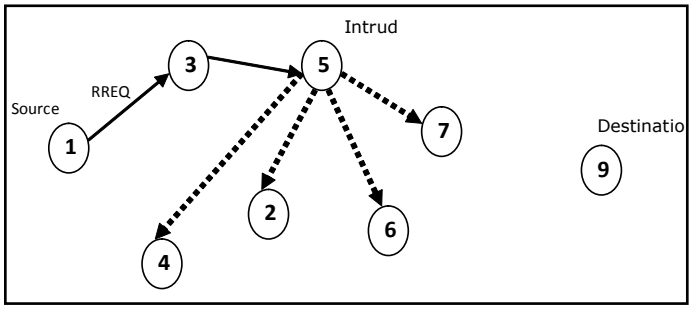

Fig. 4: Sybil Attack Scenario

III. Simulation and Results

The security attacks under study were implemented in NS-2 simulator [6, 9]. The attacks were simulated using My-Aodv [7] agent in NS-2 simulators. My-Aodv agent is used to introduce attacks in network topology. The intruder node in the network was identified and located. The results of simulation are:

Table 1: Packet Drop in Worm-hole Attack

Number of Packets Received in Normal Mode	Number of Packets Received in Worm-hole attack Mode	Number of Packets Dropped
213	23	190
283	28	255
314	27	287
367	31	336
418	17	401
437	18	419
372	12	360
293	17	276

Table 2: Packet Drop in Rushing Attack

Number of Packets Received in Normal Mode	Number of Packets Received in Rushing attack Mode	Number of Packets Dropped
381	38	343
363	42	321
415	56	359
437	57	380
511	71	440
314	36	278
371	31	340
237	27	210

Table 3: Packet Drop in Sybil Attack

Number of Packets Received in Normal Mode	Number of Packets Received in Sybil attack Mode	Number of Packets Dropped
237	56	181
264	64	200
310	69	241
337	76	261
383	81	302
413	78	335
418	85	333
307	52	255

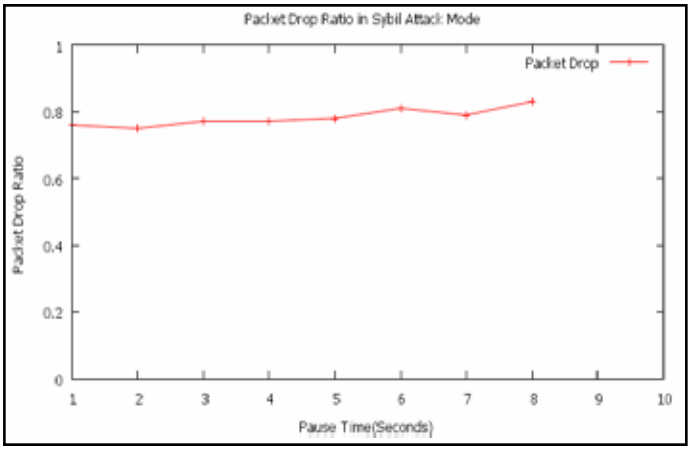

Fig. 5: Packet Drop Ratio in Sybil Attack Mode

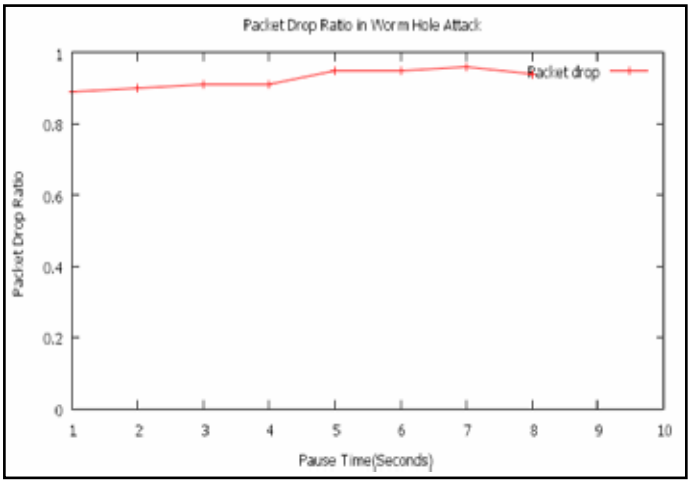

Fig. 6: Packet Drop Ratio in Worm-Hole Attack

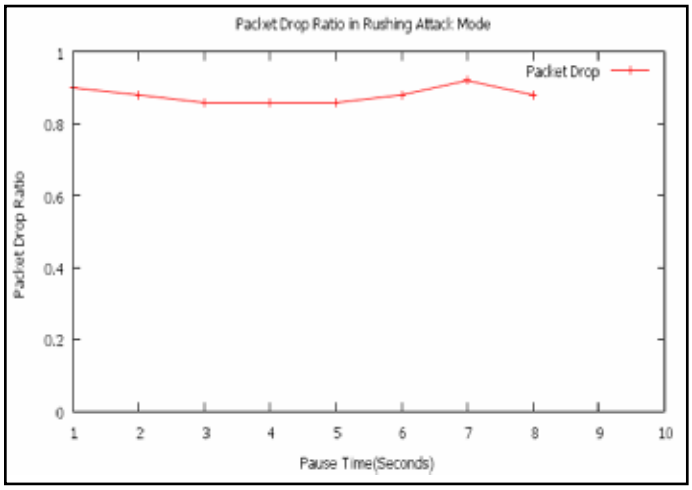

Fig. 7 : Packet Drop Ratio in Rushing Attack Mode

4. Analysis

The performance of the network is measured in terms of Packet Drop Ratio. The packet drop ratio is the ratio of number of packets dropped to the number of packets sent. The packet drop ratio under worm hole attack mode is found to be more than that of rushing and Sybil attack modes. The least and highest packet drop ratio under worm hole attack mode are 0.89 and 0.96 respectively. That is on average 93% of sent packets are dropped due to worm hole attack. The least and highest packet drop ratio under rushing attack mode are 0.86 and 0.92 respectively. That is on average 89% of sent packets are dropped due to rushing attack. The least and highest packet drop ratio under Sybil attack mode are 0.75 and 0.83 respectively. That is on average 79% of sent packets are dropped due to Sybil attack.

The packet drop ratio of worm-hole attack is highest as the intruder nodes tunnels the packets and the probability of the packets reaching their destinations is the least. In rushing attack the intruder nodes flood the network with routing packets/duplicate packets there by the data packets are dropped due to non availability of channels for delivery of packets. In Sybil attack one node takes the identity of multiple nodes there by the routing packets are sparse and flood the network, here again very few channels are left for data packets.

V. Conclusions

The impact of wormhole attack was found to be high with packet drop ratio of 93, followed by rushing attack with a packet drop ratio of 89 and it is followed by Sybil attack with a packet drop ratio of 79. The packet drop ratio in these security attacks is very high therefore an effective mechanism has to be developed so as to immune Ad hoc networks from these security attacks. Any such designed mechanism should protect the mobile Ad hoc network from intruders by ensuring that only legitimate nodes in the mobile network are equipped to participate in routing and data transfer.

References

[1] IEEE Computer Society LAN MAN Standards Committee,"Wireless LAN Medium Access Protocol (MAC and Physical Layer (PHY) Specification", IEEE Std 802.11-1997, The Institute of Electrical and Electronics Engineers, New York, NY, 1997.

[2] Z.J. Haas, S. Tabrizi,"On Some Challenges and Design Choices in Ad-Hoc Communications", Proceedings of the IEEE Military Communications Conference (MILCOM), Bedford, MA, October 1998, pp. 187-192.

[3] L. Zhou, Z. J. Haas,"Securing ad hoc networks", In IEEE Networks, Vol. 13(6), 1999.
[4] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang,"Providing robust and ubiquitous security support for mobile ad hoc networks", In the Proceedings of the 9th IEEE International Conference on Network Protocols (ICNP'01), 2001.
[5] S. Yi, R. Kravets,"Moca: Mobile certificate authority for wireless ad hoc networks", In the Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.
[6] Kristoffer Clyde Magsino, H Srikanth Kamath, "Simulations of Routing Protocols of Wireless Sensor Networks", World Academy of Science, Engineering and Technology 50, 2009, pp. 211-214.
[7] P Michiardi, R Molva,"Simulation based Analysis of Security Exposures in Mobile ad-hoc Networks", European Wireless 2002 Conference, 2002.
[8] W. Luo, Y. Fang,"A Survey of wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions", Kluwer Academic Publishers, pp. 319-364, 2003.
[9] Muzzammil Hussain, Dr A Vinaya Babu, Dr A Sadanandam,"Time stamp based Routing Protocol for Mobile Ad-Hoc Networks (TSBR)", International Journal of Computer Applications, Foundation of Computer Science, New York, USA January 2012, Vol. 38, No. 8 pp. 40-43.
[10] Priyanka Chandragiri, Muzzammil Hussain,"Performance Evaluation of TSBR with AODV and DSR: A Comparative Study", International Journal of Electronics & Communication Technology, Vol. 4, Issue 4, Dec. 2013, pp. 102–106.

Ms Priyanka Chandragiri received her Bachelor's and Master's degrees in Computer Science & Engineering in the years 2006 and 2011 resp. from Jawaharlal Nehru Technological University, Hyderabad. Currently she is working as Associate Professor in Computer Science & Engineering at Christu Jyothi Institute of Technology & Sciences, Jangaon, Warangal. She has published 5 research papers in various National/ International journals. Her areas of research are wireless and Sensor Networks and Network security.

Dr Muzzammil Hussain, Assistant Professor in CSE, Central University of Rajasthan, India.