International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 195-208
http://dx.doi.org/10.14257/ijsia.2015.9.6.19

Comparing the Performance of the Ad Hoc Network under Attacks on Different Routing Protocol

Haiyan Liu[1,*] and Zhanlei Shang[2]

Engineering Training Center, Zhengzhou University of Light Industry, Zhengzhou, 450002, China
[1]2003056@zzuli.edu.cn, [2]shangzl@ zzuli.edu.cn

Abstract

Ad Hoc network is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. [1] Due to lack of infrastructure support, security problem in these networks is a challenging issue. There exist previous work that studied the performance of the network under different types of security attacks. In this paper, complementary research by providing more realistic network scenarios such as various protocol used in the network is made. We consider two common types of attacks, black hole attack and gray hole attack, based on both AODV and DSR protocol respectively. We study the performance of the network in different number of malicious nodes and on different protocol via observing the metrics of a connection such as packet delivery ratio, throughput and end-to-end delay. The simulation result shows that the performance of the network based on both routing protocol is similar. It is should be noticed that the end-to-end delay is different in two routing network. The results enable us to put forward some suggestions to minimize the impacts of the above types of attacks in Ad Hoc network.

Key words: *Ad Hoc network, black hole attack, gray hole attack, AODV, DSR*

1. Introduction

With the rapid increase of the number of the mobile terminal, a kind of convenient wireless network, ad hoc network, is used in more and more situation. A Mobile Ad Hoc Network (MANET) is a group of mobile nodes that can communicate with each other without relying on predefined infrastructure or centralized administration [2], therefore, such network is more available. This network is suitable for applications in military battle field, emergency rescue, vehicular communications, mining operations and so on. Ad Hoc Network is a multi-hop network, which transmits information by nodes cooperating with each other. All the nodes in this network are movable and the topology of the network is changing dynamically. The flexibility of Ad Hoc Network bring the significant challenges in security.

Ad Hoc Network is more vulnerable to security attacks compared to the wired network in which the infrastructure is provided in advance and the stations are fixed. Several common types of attacks which includes Denial of Service (DOS), black hole attack and gray hole attack have been discussed in other papers. These classified attacks have been always investigated on a single routing protocol. [3] In this paper, the performance under attacks on Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector(AODV) protocol is shows respectively by simulating. Then a comparison of the difference has been made based on the simulation.

The rest of this paper is organized as follows: Section 2 briefly presents the related knowledge, the features of Ad Hoc Network, the types of the attacks and the two main known routing protocols. The related work on study of routing security in Ad Hoc

ISSN: 1738-9976 IJSIA

Network is summarized in Section 3. We present a simulation-based study of the effects of different types of attacks on both AODV and DSR protocol respectively in MANETs in Section 4. In the same section, via analyzing the metrics such as packet delivery ratio, throughput, end-to-end delay, and delay jitter in the experiments and the paper suggests some measures to minimize the impacts of the malicious attacks. The paper is concluded in Section 5.

2. Background

2.1. Vulnerabilities of Mobile Ad Hoc Network

Mobile Ad-hoc networks are composed of autonomous wireless nodes. it requires no central node to manage the networks. All the work is done with the mutual agreement and understanding between the nodes. Thus every node will work in both configurations. These nodes have the ability to configure themselves and because of their self–configuration ability. [4] A simple topology of MANET is illustrated in Figure 1.

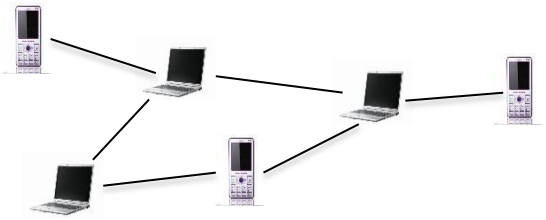

Figure 1. A Simple Topology of MANET

Because Ad Hoc Network is a multi-hop network, it is prone to attack by the malicious nodes. The characteristics of such network are described in details below:

Lack of the Infrastructure: There are some essential infrastructure, consisted of central server, special hardware equipment and so on, in the conventional wired network. However, the infrastructure is absent in the Ad Hoc Network. All the function of the network is fulfilled by each cooperative node. This trait of the MANET disable the conventional security mechanism such as access authentication due to the absence of the AP (access point).

Multi-hop: Ad Hoc Network is a peer-to-peer architecture. For the lack of the centralized router, each node in the Ad Hoc Network acts as both station and router. When the destination node is beyond the coverage of the source node, a node which is equivalent with a router in function is essential. This intermediate node is also an ordinary node in the network. Due to the nodes itself and even nodes which act as router are not trusted, it is inevitable that the serious security problem exist in the network.

Mobility of the Nodes: The nodes in the network can be mobile thus topology of the network gets changed over the period of time and makes the ad-hoc network to be a non– infrastructure network. Any malicious node attempt to join into the network is easier compared the conventional network which has a relative perfect security infrastructure and security mechanism. Thus MANET structure is very prone to the attack by malicious node.

Dynamic Topology: Due to the position of the nodes in the MANET is possibly changed at all times, the topology of the network is subsequently changed. The former correct routing path is possibly unavailable either because the intermediate node moved out of the coverage of the network or because of the move of destination node. Thus it is difficult to distinguish the false routing path caused by the move of the nodes or by the fake routing information. What's more, the

distinguished malicious node in a certain position can join the network again after moving to a new position and altering the identity.

Security Mechanism: In the conventional public key cryptogram mechanism, the user realizes the security service including confidentiality, integrity and non-repudiation by encryption, digital signature and message authentication code and so on. However, there is no such trusted authentication center in the MANET. Even if one certain node is assigned the authentication center, it is difficult to realize for the limited bandwidth in the MANET, in which each node attempting to join the network is needed to communicate with the authentication center node, the network will be congested by the authentication packets. Thus some research proposed the distributed authentication mechanism. This security mechanism will enhance the attacked robability.

2.2. Routing Protocol Analysis

With the evolution of the MANET, many routing protocols have been proposed and some of them have been realized in the real communication, among which DSDV (Destination Sequenced Distance Vector), AODV (Ad Hoc On-demand Distance Vector), DSR (Dynamic Source Routing), LAR (Location-Aided Routing), ZAP (Zone Routing Protocol), GPSR (Greedy Perimeter Stateless Routing) and DART (Dynamic Address Routing) are known. In this paper, the two most popular protocol adopted in MANET are discussed, AODV and DSR. They are described in detail as follows.

AODV analysis

The AODV routing protocol is designed for mobile ad hoc networks with populations of tens to thousands of mobile nodes. AODV can handle low, moderate, and relatively high mobility rates, as well as a variety of data traffic levels. AODV is designed for use in networks where the nodes can all trust each other, either by use of preconfigured keys, or because it is known that there are no malicious intruder nodes. AODV has been designed to reduce the dissemination of control traffic and eliminate overhead on data traffic, in order to improve scalability and performance.

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program.

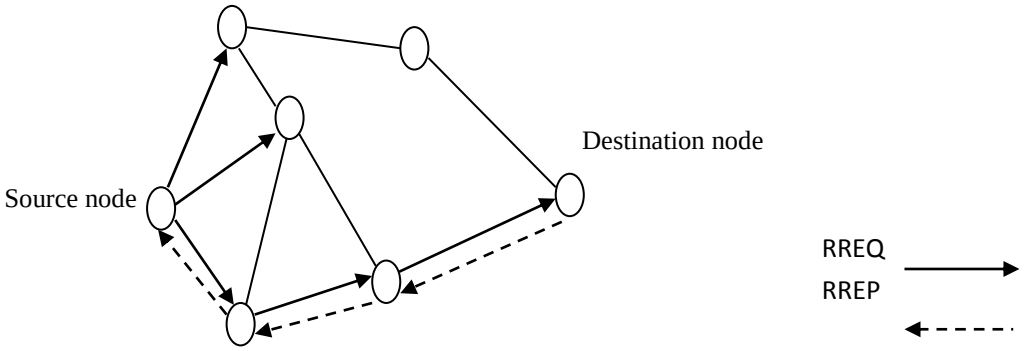

Figure 2. Establishing a New Route based on RREQ and RREP

Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.

Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations (possibly subnets) which are no longer reachable by way of the broken link. [5] The route maintenance is shown in Figure 3. When intermediate node B is lost for such reasons as broken and moving beyond the coverage of node A, node A will send a RERR message to source node and node C to notify them the unavailability of node B. Of Course, node C won't make further process because it isn't included the route and then discard the RERR.

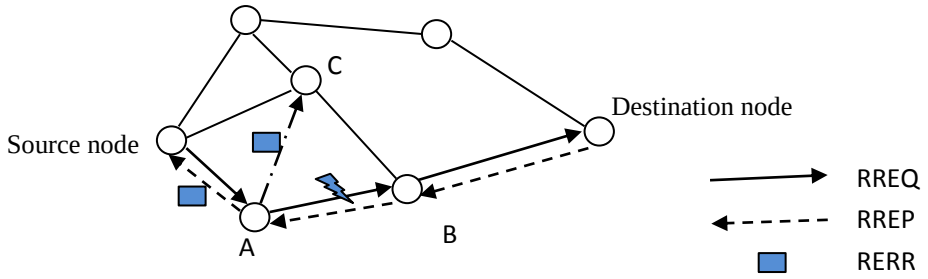

Figure 3. Route Maintenance based on RERR

DSR Analysis

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its

packets, for example, for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well even with very high rates of mobility. In DSR, Route Discovery and Route Maintenance each operate entirely "on demand". In particular, unlike other protocols, DSR requires no periodic packets of any kind at any layer within the network [6].

2.3. Typical Types of the Attacks in the MANET

There are many ways to classify various attacks in the MANET. The attacks in MANETs are divided into two categories in most research: passive attacks and active attacks according to the criterion that whether attackers disrupt the operation of a routing protocol or not. In a passive attack, the malicious nodes do not disrupt the operation of a routing protocol but only attempts to discover valuable information or drop the sending packets. In an active attack, however, malicious nodes disable the network by advertising the faked routing message or modifing the message formats and then forwards or sending a faked message, resulting in all the packets or most of the packets do not arrive the expected destination because of choosing the fake path or destination nodes receiving the faked message. In this paper, we focused on the two representative attacks, black hole attacks and gray hole attacks.

black hole attack:

Both passive black hole attack and the active black hole attack are studied in our research. A malicious node just forwards routing messages but discards all data packets which are expectedly sent to the destination node going by the malicious node in the passive black hole attack network , so that it can deceive other nodes. In this kind of attack, the invader only cause the loss of packets but does not inject any additional packets into the network, thus the damage of the passive black hole is limited comparatively. However the malicious node tries to attract the data from all neighboring nodes to it in an active black hole attack by means of replies to them blindly RREQ as if it is the shortest route to the destination. Compared with traditional selfish behavior known as passive black hole, active black hole can attract a wider range of its neighboring nodes and have severe influence on the success rate of data communication [7].

How the Active Black Hole Attack Works

In AODV, when the source node wishes to communicate with the destination node, illustrated in Figure 4, if there is no route available, it will initiate the routing discovery process in which the source node will flooding RREQ. When the other nodes receives a RREQ during the route discovery phase it replies to the source node with RREP. Of course, the source node will receive more than one RREP. Eventually the source node will judge which one will be the best route for sending the data to the destination. During this process, a malicious node sends a forged RREP packet to a source node by which the malicious node advertises that it is the destination or the shortest route. Subsequently, the data traffic will flow toward the attacker and source and destination nodes became unable to communicate with each other. Even more seriously, the malicious node will drop the packets. At last, the function of entire network can’t work normally [4].

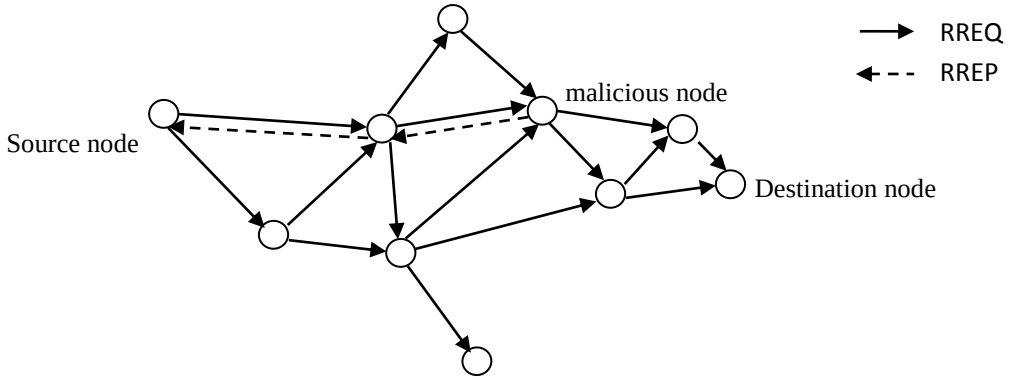

Figure 4. The Process of the Black Hole Attack

Gray hole attack analysis:

Gray hole attack, sometimes it is called selective black hole attack, is a special kind of black hole attack in fact, which can be easily launched on reactive routing protocols like DSR or AODV. Performances of the gray hole nodes are classified into three: (i) The malicious node may drop packets from certain nodes while forwards all other packets. (ii) A node may behave maliciously for certain time only, later it behaves as a normal node. (iii) Is the combination of both attacks. The process of the gray hole attack is illustrated as Figure 5. We can observe that the number of the data packets after passing by the malicious node obvious less than the number of the data packets sent from the source node. Of course, both the number are probably equal sometimes according to the principle of the gray hole attack. Even if the received number of the packets by the destination is less than the sending number, this case is also exit in normal network accused by other reasons such as congestion in the network. As because only partial data packets are dropped, gray hole attack is even harder to detect than black hole attack. A gray hole attack can disturb route discovery process and degrade network's performance [8].

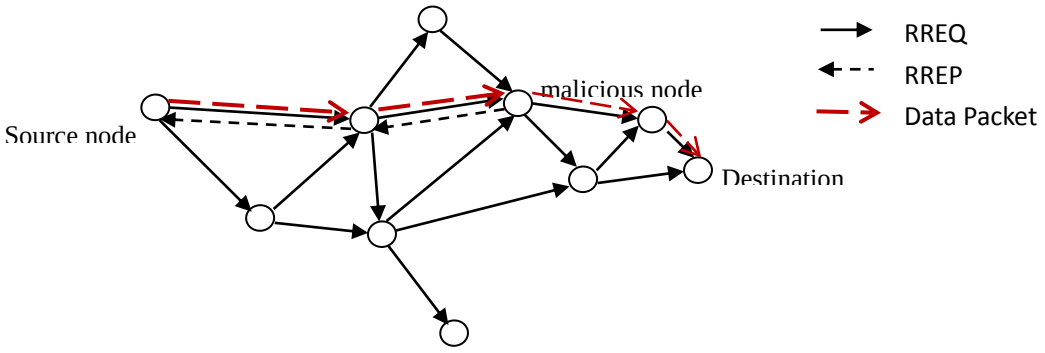

Figure 5. The Process of the Gray Hole

3. Related Work

Black hole attacks and gray hole attacks have serious impact on reactive routing protocols such as AODV or DSR. It had drawn significant attention in recent research activities and a great amount of research result have been made. In [4], Ms.Nidhi Sha and rma Mr.Alok Sharma analyze black hole attack in MANET and present two possible solutions .Then they compares the presented solutions to the original AODV depending on the pause time at a minimum cost of the delay in the

networks. [7] focuses on mobile ad hoc network's routing vulnerability and compares network performance under several attacks. They put forward an enhanced type of black hole and then implement this attack on DSR protocol, using Network Simulator 2, and another two attack patterns--passive black hole and RREQ flooding attack for comparison. Finally, the authors evaluate these attack patterns' impact and draw the conclusion that flooding attack is more dangerous than black hole attacks and active black hole bring about larger damage. In [9], the author firstly analyse the vulnerability of the Ad hoc network, emphasizing that black hole attack is one of the crucial attacks in the network. Based on the above analysis, they give some crucial attacks in the Ad hoc network and then evaluate the performance of the network in two different scenarios under black hole attack. M. Mohanapriya and Ilango Krishnamurthi stated that Selective black hole attack is a special kind of black hole attack where malicious nodes drop the data packets selectively. Aiming at the above attack,they present a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack.

4. Simulation and Analysis

The simulator we used to conduct our designed experiment is the network simulator (ns-2.35). The ns2 is an authoritative network simulator, therefore it is used extensively by the research of the network. [10] The proposed scheme is implemented for the purpose of comparing two kinds of attacks discussed above on AODV-based network and DSR-based network respectively. Based on the experimental result, we analyze the impact of two attacks on MANT.

4.1. Implementation of Black hole and Gray Hole

The experiment scheme is carried out in NS2. However the NS2 doesn’t contain the Black hole attack model. Thus we must implement the black hole attack in the MANET by modifying the routing protocol.

First of all, the nodes in the network act as different roles, normal nodes and malicious nodes. When the nodes receive the packets passing by, they must decide forwarding or discarding with the accordance to the role which the node acts as. For this reason, we modify the corresponding part of the routing protocol. The nodes are classified into further three types, normal node, passive black hole node and active black hole node, in order to satisfy the experiment. In the modified protocol, we call it black hole protocol, the node can execute the different program according to the node type itself. In summary, we can implement the passive black attack, active black hole attack by the described scheme above. In the implementation of the experiment, we will carry out the three different case respectively, which including normal network, passive black hole attack network and active black hole attack network. Based on the experiment result, we make the further anaylsis. The gray hole attack is realized making use of the similar method.

Of course, our experiment should be simulated not only based on AODV but also based on DSR as stated above. The similar process will be made in AODV-based network and DSR-based network. Therefore, we accomplish the passive black hole attack network, active black hole attack network and gray hole attack network on AODV routing protocol and DSR routing protocol respectively.

4.2. The Experiment Scheme Overview

In the hypothetical network, 50 wireless mobile nodes move randomly in a square area with the size of 1000 meter. Nodes’ movement and position accord with the random waypoint model. The related simulation parameters shown in Table 1. Some simulation parameters described below.

Table I. Parameters in Simulation

Parameters	Values
Channel Type	Channed/Wireless channel
Antenna Type	Antenna/OminiAntenna
Simulation area	1000*1000
Radio propagation model	Propagation/Two Ray Ground
Link Layer type	LL
Mac type	Mac/802_11
Protocols studied	AODV/DSR
Simulation time	100 sec
Maximum speed	20m/s
Maximum Pause time	5 sec
Traffic type	CBR(UDP)
CBR rate	50 Kbps
Number of nodes	50
Number of Malicious Nodes	1 to 10
Interface Queue type	Drop Tail/PriQueue

Mobility Model

In our experiment, the nodes in the hypothetical network should be moving instead of still. Movement of nodes is depends on the speed, direction and rate of change. The movement of the nodes implies the change of the network topology, meanwhile the velocity and pause time of the nodes' movement equal to the changing frequency of the network topology. Thus the choice of mobility models is very important to checking the behavior of the network and the simulation result. Mobility models usually used in research are Random Waypoint Model, Gauss-Markov Model, Reference Point Group Mobility (RPGM) model, and Manhattan Mobility Model. Here we used Random Waypoint Model which first used by Jhonson and Maltz in evaluation of DSR routing protocol. This is a random based mobility model used in mobile management scheme. Mobile node moves randomly in simulated area. This area is in the rectangular.[11] A waypoint model is described with three parameters: minimum velocity, maximum velocity and maximum pause time. The speed of mobile nodes is uniformly distributed between the minimum speeds to the maximum speed. Pause time is defined as the time in which the nodes are stationary. According to this model, Every node chooses a random destination and moves towards it at a random speed. When it reaches the destination, the node waits for a random time before moving again.

Radio Propagation Model

The radio propagation model is used to predict the received signal power of each packet in MANET. There is receiving threshold at the physical layer of each mobile node. A single line-of-sight path between two mobile nodes is propagation. The two ray ground propagation model considers both direct path and ground reflection path. This model gives accurate prediction at a long distance.

Traffic Type

In the simulation, the traffic type is Random traffic connections of Constant Bit Rate (CBR). We used UDP protocol over CBR traffic. UDP is a transporting protocol in the network which is not oriented to connection contrary to the TCP. In case of TCP, the source node will finish the connection if the return acknowledgement is not received. On the contrary, the source node keeps on sending

the packets even if the packets are being dropped. [12]Based on this principle, we can count the sent packets and the received packets separately to measure the performance of the network.

Number of Malicious Nodes

To observe performance of the network under different density of the malicious nodes, the number of the malicious nodes is gradually increasing from 1 to 10.

4.3. Experimental Results and Analysis

Each simulation is repeated for 10 times and calculated the average of the results to reflect the general performance of the network. In NS2, the entire process of the simulation is traced by the simulator and detailed data is written into a output file. After simulation, we program the awk scripts to analyze output files in the previous procedure and measure the network's packet loss rate, average end-to-end delay and throughput.

To evaluate the performance of the network under the different attack, we observe the three metrics as follows.

- **Throughput:**

It is defined as the amount of data transferred or received per second the throughput is denoted by T,

Throughput= received node/simulation time

$$T=\frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \times 100\% \quad \text{....(1)}$$

Where, N_i^r = average receiving node for the i[th] application, N_i^s = average sending node for the i[th] application, and n = number of applications.

- **Average end-to-end Delay (average E2E delay):**

It represents the time required to move the packet from the source node to the destination node. E-2-E delay [packet_ id] = received time [packet_ id] – sent time [packet_ id].

The average end-to-end delay can be calculated by summing the times taken by all received packets divided by its total numbers

$$D=\frac{\sum_{i=1}^{n} d_i}{n} \quad \text{....(2)}$$

Where, d_i= average end to end delay of node of i[th] application and n=number of application

- **Packet loss rate:**

It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets. Whereas in this simulation, the packets are dropped by the malicious nodes.

Packet loss rate =(sent packets– received packets)/ sent packets.

$$\text{Packet loss rate} =\frac{\sum_{i=1}^{n}(N_i^s-N_i^r)}{\sum_{i=1}^{n} N_i^s}\times 100\% \quad \text{....(3)}$$

where $N_i^s$and $N_i^r$are the number of application data node sent by the sender and the number of application data node received by the receiver, respectively for the i[th] application, and n is the number of applications [13].

The result of the simulation carried out in normal network, black hole attack network and gray hole attack network respectively is plotted graphs as follows.

Throughput and Analysis

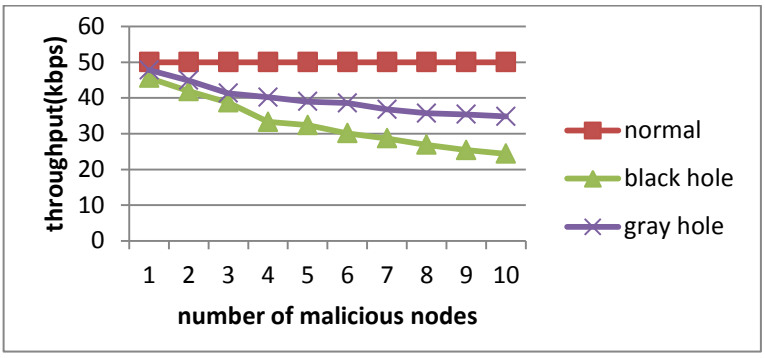

Figure 6. Throughput based on AODV

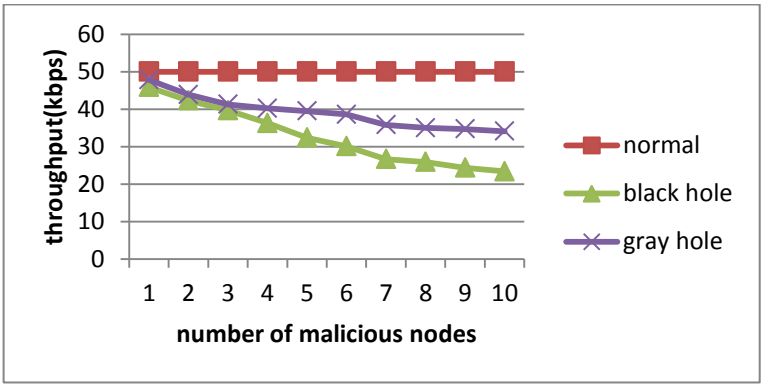

Figure 7. Throughput based on DSR

The graph shows that the throughput in the network both AODV-based network (Figure 6) and DSR-based network (Figure 7). We have simulated the network in three different cases: network without any attack; network with active black hole attack and network with gray hole attack. With the number of malicious nodes increasing, the throughput in the network declining rapidly, the throughput under the ten black hole nodes attacking is about half of the value without malicious nodes. Due to the gray hole nodes don't discard all the data packets, the throughput under gray hole attack is obviously more than the value under balck hole attack. The overall result is very similar between black hole attack and gray hole attack.

Results of Packet Loss Rate and Analysis

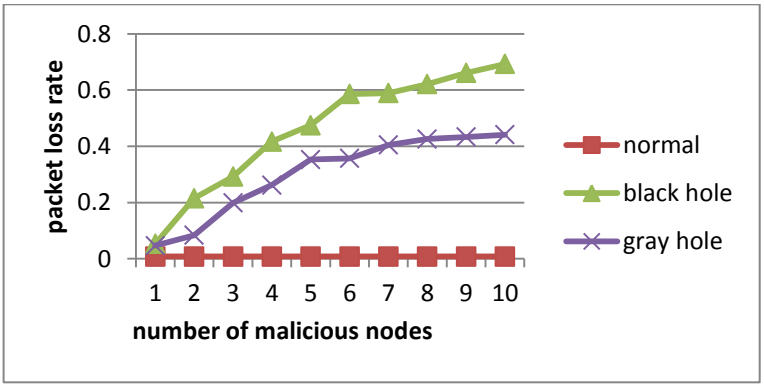

Figure 8. Packet Loss Rate based on AODV

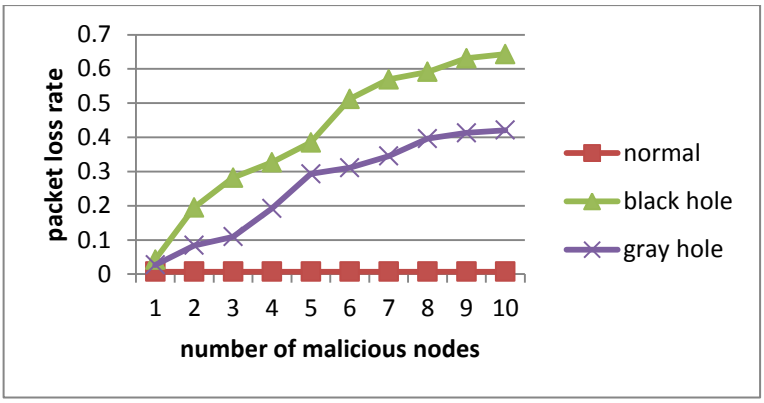

Figure 9. Packet Loss Rate based on DSR

We simulate the experiment based on AODV and DSR respectively. The results that are the average of the simulation repeated 10 times under each environment is shown Figure 6 and Figure 8.

The Figures shown that the trend in percentage of data packets dropped based on AODV in presence of black hole and gray hole are similar. The packet loss rate is increasing with the number of malicious nodes increased. When the number of malicious nodes up to ten, the packet loss rate is over 60 percentage under black hole attack based on AODV, and the result is similar based on DSR as showed in Figure 9. The packet loss rate is always less in the corresponding situation under gray hole attack. Meanwhile a slight trend we should noticed is that the growth rate is reducing with ratio of number of malicious nodes to normal nodes increased, moreover such trend is more obvious under gray hole attack. We think that the result probably caused by the trait of the gray hole attack which drop the data packets selectively. The trait of malicious nodes we set is similar, so they will select the similar data packets to drop. There is a phenomenon we should noticed that the packet loss rate without any attack under AODV routing protocol is around 7%, similar under DSR, which is possibly due to the congestion in the network. The overall trend is similar based on DSR.

Average end-to-end Delay and Analysis

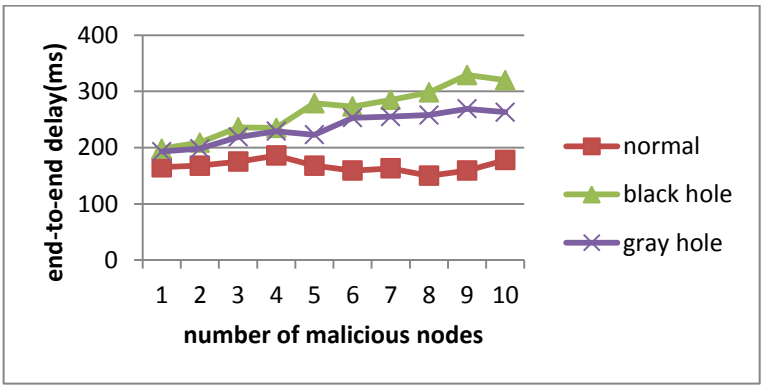

Figure 10. end-to-end Delay based on AODV

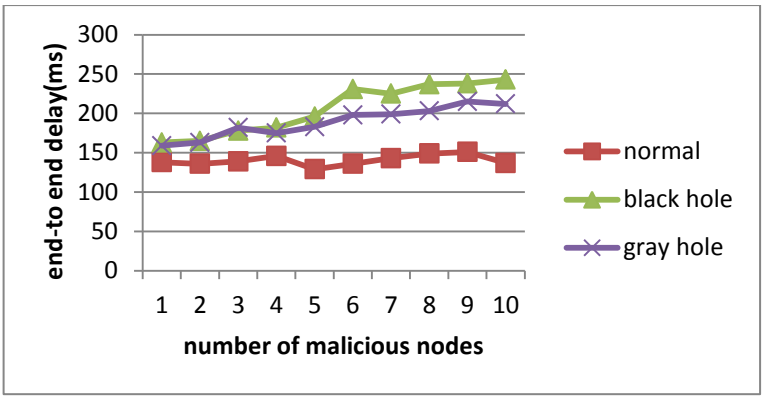

Figure 11. end-to-end Delay based on DSR

With the number of the malicious nodes increasing, the end-to-end delay is increasing too. When the number of the malicious nodes is less than five, the delay is increasing rapidly. However the delay increases slowly in the scenario of more than six malicious nodes. The supposed explanation is given as below. The average end-to-end delay is mostly determined by the number of the hops. When the density of the malicious nodes achieves certain value, the number of the hops through which the packets are transmitted will decrease. The impact of the black hole attack to the network is more obvious than of the gray hole attack based on AODV. The overall trend is similar based on DSR. Nevertheless there is somewhat different between both of them. The average delay based on AODV is higher than on DSR, which possibly due to the DSR protocol is designed more suitable for less nodes and more frequently changed network topology compared AODV.

5. Conclusion

The Mobile Ad hoc Network consists of cooperative mobile nodes which is more vulnerable to security attacks. In this paper, we focused on the performance of MANT in the presence of the black hole attack and gray hole attack. Especially we have evaluated the performance of the network based on AODV and DSR routing protocol respectively by simulating in NS2. The result shows that the most performance including packet loss rate and throughput under routing attack based on AODV and DSR is similar. However the end-to-end delay based on DSR is less than that based on AODV. In both network on different routing protocol, the black hole attack damage more to the network compared to the gray hole attack.

Reference

[1] X. Wang, T. liang Lin and J. Wong, “Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network”, Technical Report, Computer Science, Iowa State University, **(2005)**.
[2] H. Nakayama, Y. Nemoto and N. Kato, “A Survey of Routing Attacks in Mobile Ad Hoc Networks”, IEEE Wireless Communications, **(2007)** October.
[3] H. Lan Nguyen and U. Trang Nguyen, “A Study Of Different Types Of Attacks In Mobile Ad Hoc Networks”, 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), **(2012)**.
[4] N. Sha rma and A. Sharma, “The Black-hole node attack in MANET”, 2012 Second International Conference on Advanced Computing & Communication Technologies, pp. 546-548.
[5] C. E. Perkins and E. M. Belding-Royer, “Ad hoc On-Demand Distance Vector (AODV) Routing”, http://www.ietf.org,RFC3561, **(2003)** July.
[6] D. B. Johnson, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, http://www.ietf.org, RFC4728, **(2007)** February.
[7] J. Cai and P. Yi, “The Simulation and Comparison of Routing Attacks on DSR Protocol”.
[8] N. Shanmugam Bhalaji and A. Anna Univ., Coimbatore, “Association between nodes to combat blackhole attack in DSR based MANET”, Wireless and Optical Communications Networks, **(2009)**.

[9] R. Kumar Sahu and N. S. Chaudhari, "Performance Evaluation of Ad hoc Network Under Black hole Attack", 2012 World Congress on Information and Communication Technologies, pp. 780-788.
[10] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering, vol. 40, **(2014)**, pp. 530–538.
[11] A. M. Kanthe, D. Simunic and R. Prasad, "Effects of Malicious Attacks in Mobile Ad–hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research.
[12] A. Baadache and A. Belmehdi, "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks", Computer Networks, vol. 73, **(2014)**, pp. 173-184.
[13] G. Wahane and S. Lonare, "Technique for Detection of Cooperative Black Hole Attack in MANET", 4th ICCCNT July 4-6, 2013, Tiruchengode, India.

Authors

Haiyan Liu, received her BS in Physical Education from Henan Normal University, Xinxiang, China, in 2000.She got her MS in Subject Teaching Theory from Henan Normal University, Xinxiang, China, in 2003. She is a Lecturer in the Engineer Training Center at Zhengzhou University of Light Industry. Her research interests include computer network and network security.

Zhanlei Shang, received his BS in Computer Software from Zhengzhou University, Zhengzhou, China, in 1996.He got his MS in Computer Technology from Huazhong University of Science and Technology, Wuhan, China, in 2000. He is an Associate Professor in the Engineer Training Center at Zhengzhou University of Light Industry. His research interests include computer network and Database.