International Journal of Innovative Computing, Information and Control
Volume **11**, Number **1**, February **2015**

ICIC International ©2015 ISSN 1349-4198
pp. 203–211

BLACK HOLE ATTACK MODEL AND SIMULATION FOR MOBILE AD HOC NETWORK

Yuanming Ding[1,2], Hao Qu[1,2,3] and Guang Li[1,2,3]

[1]University Key Laboratory of Communication and Signal Processing
[2]Key Laboratory of Communication Networks and Information Processing
[3]College of Information Engineering
Dalian University
No. 10, Xuefu Street, Jinzhou Xinqu, Dalian 116622, P. R. China
dingyuanming@dlu.edu.cn

Received September 2013; revised June 2014

Abstract. *With the widespread applications of mobile Ad Hoc network (MANET), the network security is getting more and more attention. In order to achieve the simulation studies of black hole attacking the network, first, the black hole attack principles using protocol vulnerabilities are analyzed based on AODV protocol. Then, an attack model containing different types of black hole nodes is established based on NS2 network simulation platform. Finally, the impact of black hole attack on network performance is analyzed by simulation in different types and attack intensity. The simulation results show that the model can simulate the impact of black hole attack on network performance actually, which can provide reference and corresponding simulation environment for the research of Ad Hoc network security and tactical Internet information combat technology.*

Keywords: Black hole attack, Network security, MANET, NS2 simulation

1. Introduction.

Mobile Ad Hoc network (MANET) is a kind of multi-hop mobile network which is highly autonomous and each node has a wireless transceiver device. It can rapidly build a network in arbitrary network topology structure, achieving real-time data transmission between nodes without any infrastructure. It is widely used in military operations command, disaster emergency communications, temporary major events, business meetings and other occasions [1]. As Ad Hoc network technology originated in battlefield network communications, it is mainly applied in tactical application occasions, such as military operational command, tactical battlefield communications network.

Due to its openness and flexibility, Ad Hoc network is widely used and developed. However, it is precisely because of these characteristics that determine it vulnerable to cyber attacks, especially attacks to the network layer routing protocol [2-4]. Most existing design of Ad Hoc network routing protocol do not fully take the network security issues into account and do not take effective detection and processing means to resist route attack. Currently, literature [5] divided the commonly black hole attack modes in Ad Hoc on demand vector (AODV) protocol into ordinary black holes, passive black holes and active black holes. In addition, some literatures made studies in black hole nodes attack, but these studies tended to stay in the theoretical analysis phase and the simulations were relatively simple [6,7], lacking a more complete attack platforms for testing. And the present study on the black hole attack model only has been involved in [6], but it introduced mainly targeted at OPNET simulation platform and only researched on active black hole attack, so the study has certain limitations. For the present more commonly used NS2 network simulator, by analyzing the protocol codes in NS2 network simulator, this paper establishes the NS2-based black hole attack model, makes simulation testing and analyzes the effects of different black hole to network performance. The establishment of the black hole attack model can provide a reliable simulation testing environment for network black hole attack. At the same time, it can provide reference for the research of the information counter technology in tactical Internet.

2. **Analysis of AODV Protocol.**

AODV routing protocol is an on-demand distance vector routing protocol, and it is also one of the few RFC standards published by MANET working group of IETF. Its essential is the integration of DSR (Dynamic Source Routing) protocol and DSDV (Destination -Sequenced Distance-Vector) protocol [8,9]. It combines the mechanism of route discovery and route maintain of DSR protocol based on the mechanism of hop-route and sequence number of DSDV protocol. AODV protocol run mainly consists two parts, namely route discovery and route maintenance.

2.1. **Route discovery.**

When the source node needs to communicate with the destination node, it will first check its routing table whether there exits a valid route to the destination node. If exists, it will send data through this route. If not, the source node will broadcast RREQ (route request packet) to create a route to the destination node. The RREQ packet send by the source node contains two serial numbers, namely the source node serial number and the most recent serial number of the destination node that source node knows. The former is used to maintain a reverse route to the source node and the later shows the newness degree of the route reaching to destination node. Node will choose the item with a larger serial number to create a route.

When node along the route receives RREQ, it will first establish a reverse route to the source node according to the information in RREQ. Then it will transmit the RREQ message to its neighbors until to the destination node or an intermediate node with the route to destination node. The destination node or intermediate node will reply a RREP (routing reply packet) to source node along the reverse route. Node receiving RREQ message will establish a forward route to the destination node according to the RREP information. AODV does establish a valid route to the destination node through RREQ and RREP controlling the messages sending and receiving.

2.2. **Route maintain.**

Since Ad Hoc network nodes keep moving constantly, any node in the network is likely to move out the effective communication range of its neighbor nodes, and this will cause part link interrupted. So rout maintenance process is necessary in AODV.

When a valid route is established, nodes on the route will periodically broadcast HELLO packets to check the link state of each section on the route. HELLO packet is essentially a special RREP packet, whose TTL is 1. Since TTL is equal to 1, HELLO packet can only propagate one hop distance. When it reaches its neighbors, it will be discarded as its TTL becomes 0 [10]. By broadcasting HELLO packets, a node tells its neighbors that it is effective. The neighbor node receiving this HELLO packet considers that the rout between them is complete and available. If after a period of time, a node dose not receive HELLO packet from one of its neighbors or any other grouping, it considers that the route between it and the node has failed.

3. **Black Hole Attack in AODV.**

3.1. **Black hole attack summarizes.**

Because AODV protocol does not consider security mechanisms, the network performance is vulnerable to attack once the malicious node joins in network. It is this weakness that the black hole node uses to attack the network.

Black hole attack is the most common attack type in MANET. It is a denial service attack, as the name suggests, when the black hole attacker receives a packet it will not forward or handle it with the provisions of the routing protocols but discard it directly. The attacker incepts but does not transmit packets it received, which is like a black hole in the universe [11,12].

3.2. **Black hole attack classification.** In the process of establishing attack model in the AODV, the black hole attacks is divided into three categories for modeling according to the different levels of damage to the network: the ordinary black hole node, the passive black hole node and the active black hole node. In the network topology shown in Figure 1, the attack characteristics of different types of black hole nodes are as follows:

(1) **Common black hole.** Supposing that node 3 is a common black hole node in the network. When node 3 starts black hole attack, it will discard the data packets received from its neighbors whether they are control packets or data packets. This prevents its neighbor nodes establishing a route through node 3, which will increase the delay to build a normal route in network and increase the network load. Therefore, the network performance is affected to some extent. However, the affect is limited and it will have a great damage to the network only when the number of black hole nodes is large enough.

(2) **Passive black hole node.** Compared with common node, the passive black hole node transmits control packets normally, so it does not prevent its neighbor nodes establishing route through it. However, it discards the data packets through it. Taking Node 3 as an example all the same, when source node S establishes an effective route (S-1-2-3-D) to destination node D through node 3 and deploy data transmission, communication from S to D will be interrupted. When node S discovers the link interrupted, it will repair it. If it failed, S will restart the route discovery mechanism. At this time, as node 3 can transmit control packets normally, it may appear on the new route and drop all data packets via it again, resulting in the new route interrupted. It is by this manner that the passive black hole nodes affect the normal data transmission and destroy the network performance. Compared with common black holes, the passive black hole nodes can transact RREQ, so it has a relatively larger impact on the network.

(3) **Active black hole node.** From the analysis of Sections 3.1 and 3.2, we can see that the destructiveness of passive black hole is larger than that of common black hole. However, the destructiveness of passive black hole nodes will decrease in the two following cases [13]:

① There are two routes from source node S to destination node D in the network, namely S-1-2-3-D and S-1-4-5-6-D. Because passive black hole node is regarded as a normal node in the process of route discovery, the source node may choose S-1-4-5-6-D to establish a route, which avoids the damage to network made by node 3.

② When node S needs to send packets to destination node D1, it will select the route S-1-2-7-D1, which avoids damage from node 3.

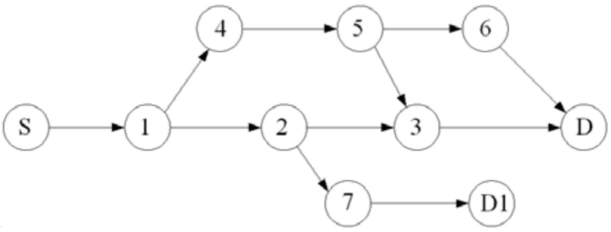

FIGURE 1. The network topology

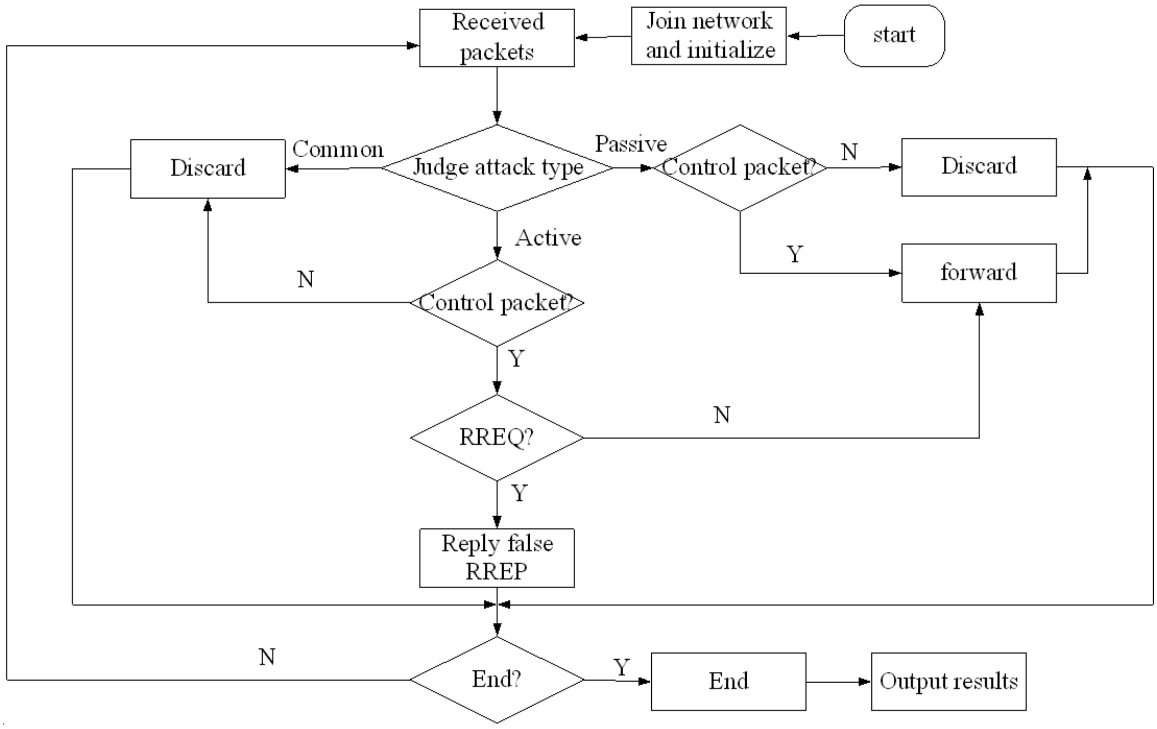

FIGURE 2. The flow chart of black hole attack

Because of these limitations of passive black hole attack, there appears active black hole attack. The destruct of the active black hole attack is the largest. The active black hole node will reply RREP packets to the source node actively, in which it will declare its next hop is the destination node or it has a large enough destination sequence number. By this, it can attract source node to establish a normal route making more data sent to it. Active black hole node not only disrupts the normal communication, but also destroys the routing information acquisition of entire network, increasing the network load. For example, in Figure 1, no matter with whom source node S wants to communicate, it needs to broadcast RREQ packets. When node 3 receives the RREQ, it will reply a RREP immediately declaring that its next hop is the destination node or it has a large enough destination sequence number. In this case, node S will not consider the route replies by other nodes resulting in a large number of packets transmitted to black hole 3. Therefore, node 3 destroys the network performance.

According to the previous discussion, we can see that the basic attack methods of black hole node mainly contain:

① Attack node does not send any routing request, and does not forward packets;

② Attack node receives any request packets and will reply response message;

③ Attack node discards all data packet through it.

Therefore, the attack process of black hole node is shown in Figure 2. In Figure 2, after the black hole joins the network and initializes, it will take appropriate action according to the attack type and the data packet type to complete network attacks.

3.3. **Black hole attack model.** According to the attack process of black hole node, the black hole model can be established as Figure 3.

In the model, according to the types of black hole node and received packets, the network node contains six different states:

(1) Ordinary black hole node discards all packets;

(2) Passive black hole node receives an AODV routing packet and normally processes it;

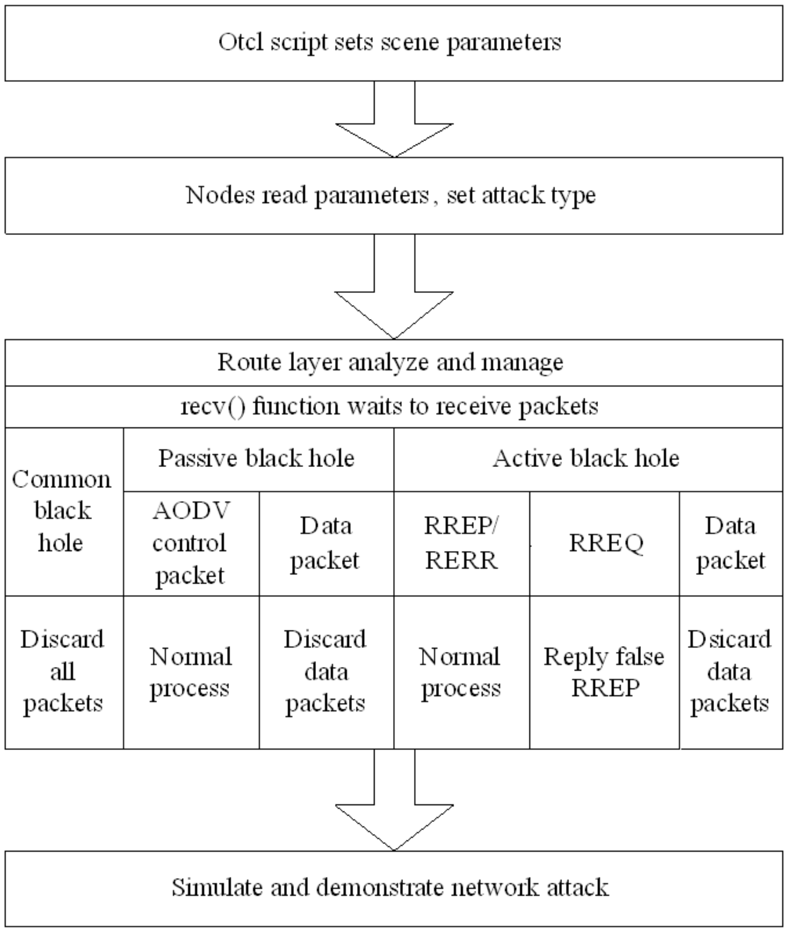

Figure 3. The black hole attack model

(3) Passive black hole node receives a data packet and discards it;
(4) Active black hole node receives RERR or RREP packets and processes them normally;
(5) Active black hole node receives the RREQ packet and returns false RREP packet;
(6) Active black hole node receives a data packet and discards it.

Concrete realization of the model is completed in C++ object of the underlying of NS2 simulator. The recv (), recvAODV (), recvRequest () and sendReply () functions are modified, achieving different states of the nodes based on configuration parameters of user Otcl scripts.

4. **NS2 Simulations and Result Analysis.** Using the most common network simulation tool NS2 (Network Simulator) which is used in the modeling process, black hole attack model in Ad Hoc network is simulated. In simulation experiment, the location and movement of node are collocated using the NS2 setdest random node scenario configuration tool. Other simulation parameters are set in Table 1.

Table 1. The simulation parameters setting

Number of nodes n	50	data operation type	CBR
Maximum node speed $V_{\max}$	20 m/s	Package transition rate	2 packet/s
Minimum node speed $V_{\min}$	0 m/s	Large of data package	64 B/packet
Node movement range	1000 m×300 m	Number of black node	0,1,3,6,7,8,12

In the simulation, packet loss rate, end-average delay, average throughputs are used to evaluate the network performance, which are calculated as follows:

$$packet\ drop\ rate = 1 - \frac{received\ packets\ number}{sent\ packets\ number},$$

$$average\ delay = \frac{\sum(packets\ receiving\ time\text{-}packets\ sending\ time)}{received\ packets\ number}\ [\mathrm{s}],$$

$$average\ throughput = \frac{\sum received\ packets\ number \times packet\ large}{simulation\ time}\ [\mathrm{kbps}].$$

In the simulation process, according to the simulation model above, the effect of different numbers of black hole node to network performance are simulated in three different kinds of black hole attacks. The results are shown in Figure 4 to Figure 6.

Figure 4 shows the relationship of network packet loss rate and the number of black holes in different types of black holes. As can be seen from the figure, in general trend, packet loss rates of three types of attack will increase with the increase of the number of black holes, which finally becomes more balanced. In the same number of black holes, active black hole attack is the best attack mode, followed by passive black hole and the general black hole.

Figure 5 shows the relationship of average network delay and the number of black holes. Notably, the average delay displays an upward trend in early simulation stage but shows a downward trend in late stage. It is because with the increase of the number of black hole nodes, many network areas become unreachable. In fact, the network is divided into no communicating small areas and the packet can only be transmitted within short distances in this small area. Therefore, when transmission distance reduces, delay will decrease to some extent.

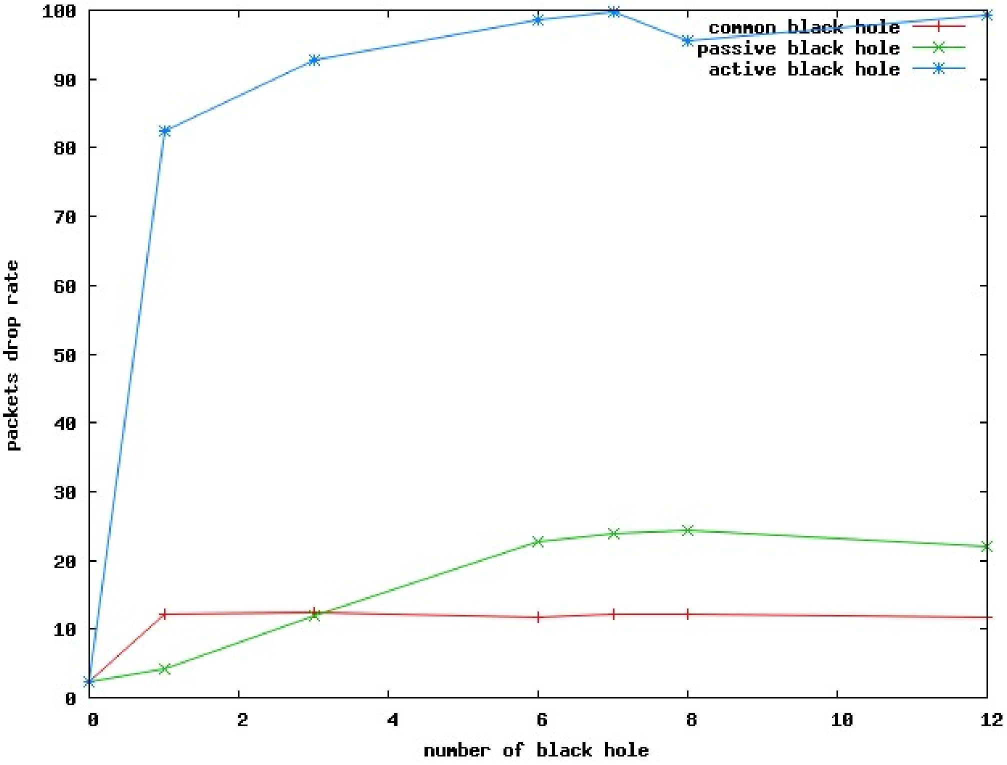

Figure 4. Relationship of drop rate and the number of black holes

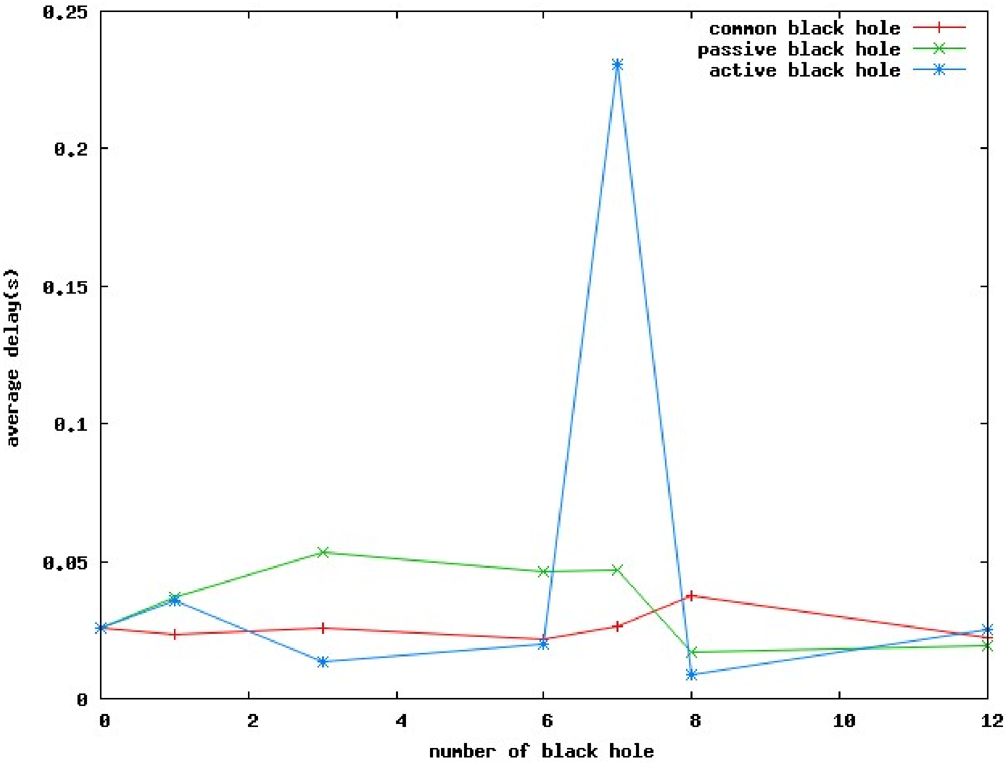

FIGURE 5. Relationship of delay and the number of black holes

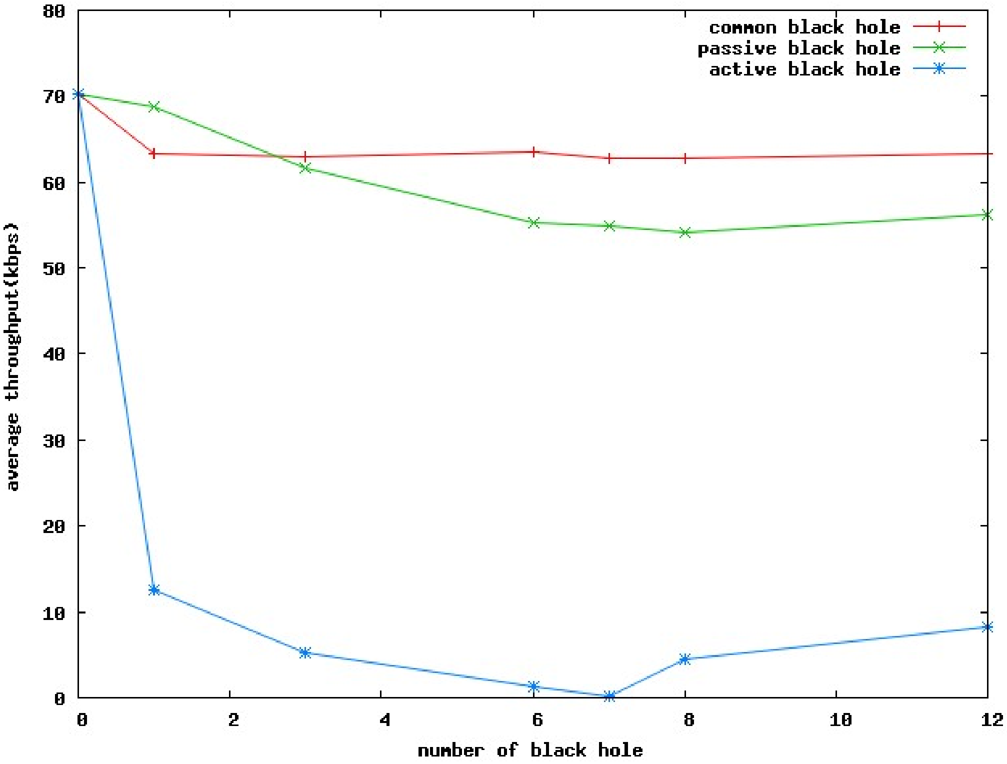

FIGURE 6. Relationship of throughputs and the number of black holes

It can be analyzed from the simulation results in Figures 4 and 5, network packet loss rate and network delay are not two independent parameters and just the change of one parameter cannot be used to evaluate the quality of network performance. In addition, when there is an active black hole node, the delay curve twitters significantly larger which means that the network is extremely unstable compared with other two cases. So network effects caused by active black node are more severe.

Figure 6 shows the relationship of network average throughput and the number of black holes in different types of black holes. In Figure 6, with the increase of the number of black holes, the average network throughputs will decrease and active black hole has the best performance. Passive hole has certain advantages compared with general black node.

It can be seen from the simulations above, compared with the general black hole and passive node, when the active black hole attack exists in the network, network performance will drastically reduce. Through setting different parameters, simulation experiments can easily get the effect extents of black holes to network performance in different types and intensities, which can provide reliable simulation environment for the research of Ad Hoc network rout security.

5. **Conclusions.** Black hole nodes are relatively common MANET attack nodes, and this paper introduces several different kinds of black hole nodes. A complete simulation model with black hole nodes is presented and corresponding experiments of each attack type in the model are made to validate their different effects to the network performance. Experimental results show that the network performance are various in different attack situations. The model can accurately simulate the impact of black hole attack on the key performance indicators of network which can provide reliable test environment for the research of MANET route security and can also provide reference for the research of the information counter technology in tactical Internet.

Currently, in terms of the prohibit methods to black hole node attack, the easiest and most common one is to prohibit intermediate node responding RREQ message and only allow the destination node to reply RREQ messages. This method, though to a certain extent, can defense black hole attack, but on no doubt that it increases the network burden resulting in the increase of route discovery delay and network routing load and therefore, affect the network performance. In next stage, we will discuss how to prevent the black hole node attack effectively and minimize the consumption of system resources as much as possible.

Acknowledgment. This work was supported by the Scientific Research Project of Liaoning Province Educational Committee (No. L2012440).

REFERENCES

[1] L. Blazevic, L. Buttyan and S. Capkun, Self-organization in mobile Ad Hoc network: The approach of terminodes, *IEEE Communication Magazine*, vol.39, no.6, pp.166-174, 2001.

[2] J. H. Song, F. Hong and X. B. He, Typical network attacks and defenses in mobile Ad Hoc networks, *Micro Computer Applications*, vol.28, no.5, pp.454-458, 2007.

[3] M. Wang and M. Wu, Dominating security threats in MANET and their corresponding solutions, *Journal on Communications*, vol.26, no.5, pp.106-111, 2005.

[4] J. X. Wang, Y. N. Zhang and Z. Xie, Performance analysis of AODV under attacks on routing information, *Journal of Circuits and Systems*, vol.10, no.3, pp.93-98, 2005.

[5] Y. C. Hu and A. Perrig, Ariadne: A secure on-demand routing protocol for Ad Hoc networks, *Wireless Networks*, vol.11, no.1-2, pp.21-38, 2005.

[6] X. Y. Wang, Z. H. Lin and Y. Hu, Simulation of Ad Hoc network under black hole attack, *Journal of Naval University of Engineering*, vol.23, no.2, pp.103-107, 2011.

[7] C. X. Zhao, R. C. Wang, H. P. Huang and Y. M. Ji, Wireless Ad Hoc layered attack simulation mode, *Computer Engineering and Applications*, vol.46, no.24, pp.81-84, 2010.

[8] P. Yi, F. T. Zou, Y. Zou and Z. Y. Wang, Performance analysis of mobile Ad Hoc networks under flooding attacks, *Journal of Systems Engineering and Electronics*, vol.22, no.2, pp.334-339, 2011.

[9] C. E. Perkins and P. Bhagwat, Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computer, *The ACM Sigcomn Computer Communication Review*, vol.24, no.4, pp.234-244, 1994.

[10] S. Madhavi and K. Duraiswamy, Flooding attack aware secure AODV, *Journal of Computer Science*, vol.9, no.1, pp.105-113, 2013.

[11] Q. Y. Liu, P. Yi, X. H. Jiang and J. H. Li, Design and simulation of intrusion detection based on DSR protocol, *Computer Simulation*, vol.25, no.11, pp.146-149, 2008.

[12] F. Ameza, N. Assam and R. Beghdad, Defending AODV routing protocol against the black hole attack, *International Journal of Computer Science and Information Security*, vol.8, no.2, pp.112-116, 2010.

[13] M. Ghonge and S. U. Nimbhorkar, Simulation of AODV under blackhole attack in MANET, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.2, no.2, 2012.