Research on Security of Routing Protocols Against Wormhole Attack in the Ad hoc Networks

Huang Wen hua
School of Telecommunications and Information Engineering
Xi'an University of posts and telecommunications
Xi'an, 710061
China
Email: hwh_xa@126.com

Abstract: - Ad hoc networks are made of a group of portable terminals with wireless transmitter as multi-hops provisional autonomy system. Ad hoc networks are very easy to be attacked by various kinds of network attacks, as the limited resources, dynamic topology and open communication channel and so on. Wormhole attack is an internal attack means against routing protocols in the Ad hoc networks，The research on security of routing protocols against wormhole attack in the Ad hoc networks is performed. The security routing mechanism against wormhole attack in the Ad hoc networks is put forward, on the basis of deeply research on wormhole attack principles and models. The modeling and simulations are presented in detailed.

Key-Words: - Ad hoc networks; routing protocols; wormhole attack; security routing mechanism; modeling and simulation

1 Introduction

Ad hoc network is the core technology of the Internet [1], it can be used as the routing information and exchange platform and it can provide a variety of wireless access to comprehensive information, which can realize the seamless integration of all kinds of wireless communication. Namely that the Ad hoc technology in the Internet is becoming a real combat multiplier, it will bring the fundamental impact to the future network. At the same time, Ad hoc network in an open, cooperative environment, any suitable hardware, network topology and network of terminals can be accessed to the network, which make the potential attacker can perform eavesdropping or conversion into network information. Compared with the traditional network, some exposure physical nodes or network are more vulnerable to be interfered. Another characteristic of Ad hoc networks is highly dependent on intermediate nodes. Due to the limited dynamic connection between individual nodes, Although the jump communication is not a new concept, because it has been widely used in the structure of the Internet, but in Ad hoc network nodes usually are mobile, and at any time within the scope of a node or from may disappear in the entire network, some of the data transmission paths may become invalid, so the role of the intermediate node is more important than the fixed node in the network, and also are more vulnerable to be attacked [2]. At the same time, in the application environment, the existence of rival network node, Omni-directional radiation interference, trust risk node forwards the packet, recovery degree of hidden nodes, design of routing and redundancy, QoS control, etc, are the problems need to be solved. Therefore, the security research of key technology of Ad hoc network, and the improvement of existing routing mechanism are of great significance in constructing the system of communication.

Facing vast application prospect of the Ad hoc network in the future, more and more the scholars are concerned on the related research, in recent years, it has become a research focus in the wireless network, although many useful research results have been obtained in the Ad hoc network [3-14], but there still exists many problems, e.g., Ad hoc network security problems restricts the network in the practical application directly, especially in communication applications. So in the paper we choose "worm hole" attack security problems as main research topic in the Ad hoc network routing protocol, and carry out the research of "worm hole" in the Ad hoc network attacks and the corresponding security routing mechanism, all the works will have certain contribution on security of network. Due to the importance of Ad hoc network in the future communications, so the research of technology especially the security technology of network will play a important role in the future.

As known that "worm hole" attack is aim at the routing protocol in Ad hoc network ,it belongs to the internal attack, so it is very difficult to be detected, because information path it adopts is usually not a part of the actual network, it can be used in the damaging without knowing the information of the agreement or network, through the wormhole ,it can launch at least two kinds of attacks, so damage of the wormhole attack is especially big. Many researchers according to network attack mentioned above, put forward the corresponding solutions, they are shown as follows:

1. Based on the geographical location
2. Based on synchronous clock
3. The use of encryption algorithm
4. The use of the RF frequency watermark
5. SECTOR
6. Based on the directional antenna
7. DelPHI

In the paper, we make research of Ad hoc network routing protocols running mechanism, and select the typical Ad hoc routing protocols. we focus on the specific Ad hoc network routing protocols of the "wormhole" attack, and make the analysis of "wormhole" attack principle, according to the Ad hoc network attack model of the "wormhole" ,we design related algorithm. We prove the Ad hoc network security routing mechanism and its related algorithm in OPNET network simulation platform, through the simulation ,comparison and analysis, the validation of "wormhole" attack damage and the effectiveness of the security routing mechanism is obtained.

2 Protocol of Ad hoc Network Routing

According to the Ad hoc network routing protocols and based on the security of the Ad hoc network structure and OSI model, we make the comparative analysis of the existing types of Ad hoc network routing protocols. It provides the theoretical support in the Wormhole attacks and the routing mechanism design of the Ad hoc network.

2.1 Overview of the Ad hoc network

Ad hoc is a word derived from Latin. [15], its English meaning is"the Purpose only", which means “without advance preparation and meaning of the temporary”. Ad hoc network is usually referred to as no fixed facilities network or self-organizing network [16,17] . Ad hoc network is a special kind of wireless mobile network, all nodes in the network of have equal status, without setting any center control node. In Ad hoc network, each mobile terminal has both routers and hosts two functions, when it is looked as the host, it needs to run the user oriented application; when it is looked as the router, it needs to run the corresponding routing protocol, according to the routing policy, the routing between nodes usually consists of multiple segments, because of scope limitation of wireless transmission, it will be unable to communicate directly between the end nodes, and the communication may be realized through multiple intermediate nodes. Therefore, it is also known as jumping wireless networks, self-organizing networks, unfixed infrastructure network or peer-to-peer networks. Ad hoc network has the characteristics both mobile communication network and computer network, it can be seen as a special type of mobile computer communication network.

2.1.1 Ad hoc network structure

Ad hoc network can be divided into two different types of network structure generally [18.19]. The classification (Hierarchical) and peace (Flat) structure, they each have advantages and disadvantages, and they are suitable for different needs.

1. The flat structure of Ad hoc network

Flat structure Ad hoc network is the distributed structure as whole, there are multiple paths between source node and destination node, which can realize the load balance, also can choose the appropriate path for different type of business; All the nodes in the network are equal in status and function, there is no bottleneck problem and it has a certain robustness; coverage of each node is small, probability of listening or intercept is small, its structure as shown as Fig.1.

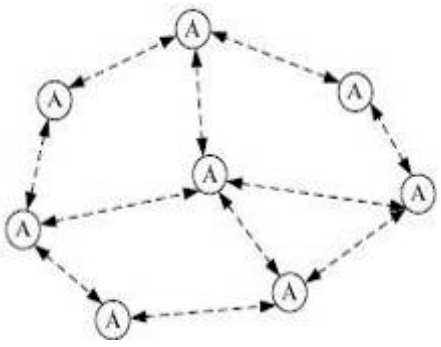


Fig.1 Flat Ad hoc networks

2. The hierarchical structure of Ad hoc network

In the hierarchical structure, network structure can be divided according to the cluster. Each cluster consists of a cluster head and multiple cluster members. Clusters formed a high level of the network, and at the high level of the network, It can

form a cluster, then forms the higher level of network and until to the highest. In the hierarchical structure, cluster head node is responsible for forwarding data between clusters, it can be specified in advance, and it can also be elected by nodes using related algorithm. Its structure as shown in Fig.2

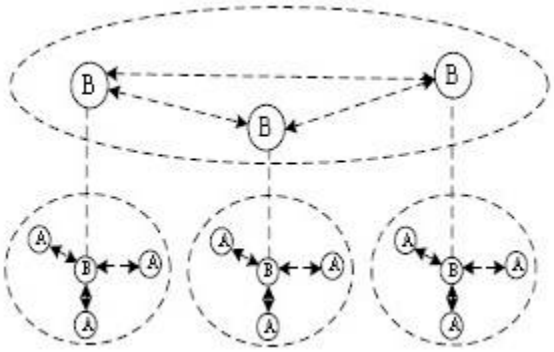


Fig.2 Hierarchical Ad hoc networks

2.1.2 Ad hoc network layered OSI model

Compared with wired networks, there are many differences in Ad hoc network environment, so the selected technology is also different. They ate mainly reflected in the bottom of the three layers of the network, namely that, physical layer, link layer and network layer, the biggest differences exists the network layer. According to the characteristics of Ad hoc network, and 7 layers OSI model, we make the analysis of the technical features of Ad hoc network, the protocol stack structure as shown in Fig.3.

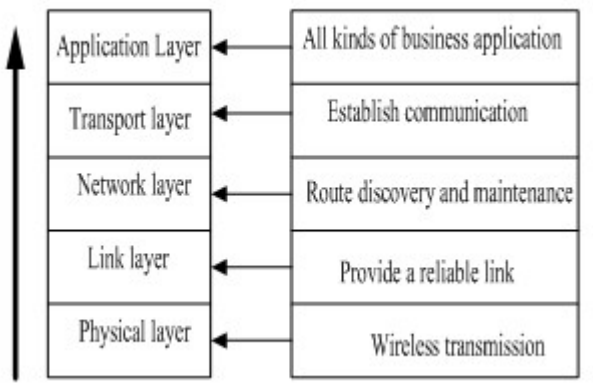


Fig.3 Protocol structure of the Ad hoc networks

Bottom is a set of equipments low power, high capacity, can work in the movement of physical transmission, providing wireless transmission capacity, complete the wireless signal encoding decoding, sending and receiving, etc, in order to support mobile networking. Link layer to control access to Shared wireless channel and the logical link control, provide reliable wireless communications, access to support effective medium. Network layer is the focus of the Ad hoc technology, also is the main difference between it and other existing network, the support network layer transport protocol, mobile network algorithm and dynamic routing protocol. Transport layer is mainly the establishment of a complete end-to-end communication, general is currently on the wired network in the TCP/UDP, adapt the wireless environment; Ad hoc network executives including based on Ad hoc wireless applications and mobile core network access to the various business.

2.2 Ad hoc network routing protocol classification

Conventional network routing protocol can be divided into distance based vector routing protocols just as RIP and link based state routing protocols just as OSPF. These two types of routing protocol are mainly suitable for fixed network, fixed network topology structure. But, in Ad hoc networks due to mobility of the node, which will leads the topology dynamic, random, rapid change, it is fatal for conventional routing protocols. The agreement will remain the state of convergence. In addition, adopting the regular Ad hoc network routing protocol has the following several factors, different sizes and power of transmission equipment in Ad hoc wireless network, and existence if interference lead the existence of one-way channel; Wireless channel broadcast the conventional routing protocol routing which were cause the large number of redundant link; in the conventional routing protocol routing updates group and some complex routing algorithm will cause an infinite terminal and thus affect the normal function. Therefore, Ad hoc network routing protocol design is the key if the network.

3. Analysis of “wormhole”Attack

As we known that Ad hoc network is in an open, cooperative and highly random environment, any appropriate hardware, network topology and network of terminals can be able to access the network, which cause the potential attacker can perform eavesdropping or infiltration of network information. Compared with the traditional network, functions of Ad hoc network are more susceptible to interference. Ad hoc network is another characteristic is that the intermediate node is highly dependent on communications. Due to the limited dynamic connection between individual nodes, the information can be passed through intermediate nodes. Although the jump communication is not a

new concept, as in the Internet it has also been widely used. As in the Ad hoc network, the nodes usually are mobile, and it may go out from the scope of a node or disappear from the whole network at any time, some paths of the data transmission may become invalid, so the intermediate nodes of communication is more important than in the fixed network, which also make the interfere more easy in Ad hoc network than the traditional network. Essentially Ad hoc network vulnerability determines its facing more complex and diverse way of attack.

According to the root causes of the attackers, they can be divided into internal and external attackers. External attack is launched by external illegal node. In comparison, the internal attacks are from internal network and are launched by internal node, which can produce very big threat to the whole performance of the network, and belong to compromise among the network node can actually protected by network defense mechanism, so they can disable defense mechanism. So internal attack is more effective than external attack, and it is uneasy to be stopped. "Worm hole" attack is a kind of internal special attack according to Ad hoc network routing protocols specifically, most of the existing Ad hoc network routing protocol is the lack of effective defense to this kind of attack. It mainly aim at Ad hoc network routing protocols, "wormhole" attack means, between two or more than two malicious nodes, it establishes a private channel, the attacker in a certain position of the network collects records or information, through this private channels, it can steal the information passed to another location in the network. Because the private channel distance is greater than the single hop wireless transmission range, so transfer of the information through private channels is earlier than normal jump route packets in arriving at the target node.

If the “worm hole” intentional attack node only transfer part of the packet, such as message routing control packets or tamper with the packet content, which will lead to packet loss or damage. In addition, the length of the tunnel must be greater than coverage radius of the ordinary jump distance of the node, but on the routing ,it presents a jump distance, thus when choosing routing nodes, the system certainly tend to choose the path which is formed by the wormhole, therefore this attack does great harm to routing protocol. “Worm hole” attacks are very difficult to detect, because pass information path it used is often not a part of the actual network, and it is particularly dangerous, because they can damage without knowing the network protocols and services provided under certain situation.

4. Design of Ad hoc Network Security Routing

The Ad hoc network routing protocols running mechanism and the principle of "wormhole" attack, attack algorithm, combined with typical routing protocols are analyzed. On this basis, we will design Ad hoc network security routing mechanism according to “worm hole” attack .

4.1 Comparison of “wormhole” attack prevention methods

4.4.1 Prevention methods of “wormhole” attack

“Worm hole” attack on Ad hoc network routing protocols can caused great destruction, but at present most of the routing protocols have no effective protection method according to “wormhole” attack yet, how to detect and prevent "wormhole" attack effectively has become hot spot of the research, now the related detection method is mainly as below:

1. Location-based routing protocols: GEAR.
2. Based on the synchronous clock "packet" (packet leashes).
3. The security strategy based on the encryption algorithm, such as SAODV, SEAD, SAR.
4. Method based on using of RF frequency watermark.
5. Method based on using of special hardware transceiver SECTOR [18].
6. Method based on using a directional antenna, SeRloc agreement is proposed [19].
7. Method based on statistical average jump each path [20].
8. Method based on the monitoring of adjacent nodes, according to the data packet transmission method of trust value [21].
9. Method based on the cycle method of trip time (RTT) [22].
10. Based on statistical analysis, the method of statistical link SAM agreement and neighbor number is put forward [23,24].
11. A method based on node positioning, which can determine the relative position of all nodes, they mainly adopt technologies such as GPS, GLONASS positioning function adjacent node list and its transmission radius are stored in each node, through comparing the distance between the node and node transmission radius and it can detect the “worm hole” node [25].

12. In the paper [26] neighbor trust evaluation method is proposed. Due to the evaluation results is lagging behind “wormhole” form in time, so the method to detect “wormhole” has a big delay in time.

4.1.2 Analysis of the “wormhole” attack protection method

From the table above, we can find that there exist two methods which can't position the malicious nodes, if we cannot locate malicious nodes, it will not be able to isolate the malicious nodes in time; so it's probably that the system will suffer “worm hole” attack again, in later the operation of the network. So there exist the hidden dangers in the two methods. In addition, as the Ad hoc network terminal node energy and storage space are limited, which requires reduce the network expense as far as possible. From the table.1, we can find that there are six kinds of methods need large calculation; so it is a challenge for Ad hoc network in the mobile terminal. In the table the last indicators reflect the cost of some kind of protection method, if you need any additional hardware support, also means that network deployment cost is high, and Price performance ratio is low,this method will block its practical application.

From the research above, it can be concluded that in the solutions of “worm hole” attack in Ad hoc network, efficiency is an important factor, which is decided by the characteristics of Ad hoc network. Based on concrete analysis of three typical Ad hoc network routing protocols OLSR, DSR, AODV "wormhole" attack, it can be found that "worm hole" can isolate the malicious nodes in time, it's probably suffer another “worm hole” attack in the operation of the network, so there exists of hidden dangers in the two methods of network security maintenance. In addition, as the Ad hoc network terminal node energy and storage space are limited, which requires reduce the expense of network as far as possible.

From the above research, based on the analysis of typical Ad hoc network routing protocols “wormhole” attack, it can be seen that the dangers of “worm hole” attack on the Ad hoc network are huge. Therefore, the designing of high efficient and practical security routing mechanism in protecting “Hole” to attack is necessary and imperative.

4.2 Principles security routing mechanism design

The protective security routing mechanism of “wormhole” attack, it should be effective in detecting "wormhole" attack as basic index function, it does not use the digital signature technology, public/private key encryption system or hash function in general, as the prices of them are quite high. Also, it should also take characteristics of Ad hoc network into account, so, in the designing of security routing mechanism, the algorithm should be simple, easy to operate, in order to reduce the consumption of node energy. In addition, strict clock synchronization mechanism should be avoided.

And it should avoid using the high sensitivity of network equipment, especially for some flexible small network. From what has been discussed above, the design for "wormhole" attack security routing mechanism should adopt the following principles:

1. The algorithm is simple, and it is easy to implement.
2. It does not need to use complex algorithm such as the digital signature technology,

public/private key encryption system or hash function.

3. It does not need to use special high sensitivity, expensive equipment.
4. The routing information of node storage requirements is not high.
5. The routing operation of node energy consumption demand is not high.

5.Simulation and analysis"wormhole" attack

5.1 the simulation purpose

Through basic steps of OPNET simulation, we build process model, node model and network topology model. We validate “wormhole” attack damage and the effectiveness of the security routing mechanism according to the attacks of “wormhole”, and the improved routing protocol simulation. The purpose of the research is to find out the change of performance after suffering the “wormhole” the attack when the Ad hoc network running OLSR, DSR and AODV routing protocol, and then verify dangers of “worm hole”.

5.2 the simulation implementation

As mentioned above, OPNET simulation can be divided into the three levels, network model, model of node, the process model. As to the functions, behavior of each node is simulated through the process model, its specific logical operation is realized by the standard C language code, and the core of the process provided by OPNET.

5.2.1. Model of “worm hole” node

Node model is set in OPNET, and as the basic model of network equipment can adopt directly through simple configuration. But in the basic model libraries, there is no “worm hole” in the node model, which requires the development of new model of network equipment. In the the experiments, we will make modifications (the Node Model) manet_station_adv according to the principle of “wormhole” attack model, establish “wormhole” manet_station_adv as worm node model, and then perform simulation experiment, as shown in Fig.4. Among them, the modified part are mainly concentrated on the ip_encap, IP, manet_rte_mgr_Worm module.

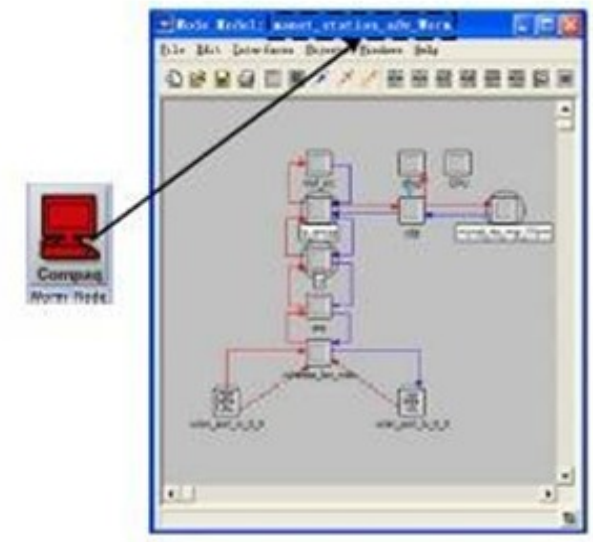


Fig.4 Wormhole node model

5.2.2. The "worm hole" process model

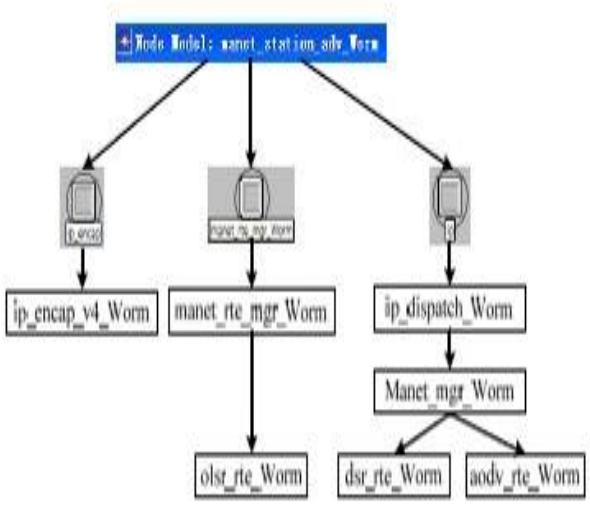


Fig.5 Wormhole process model

On the application of the network in OPNET simulation,they are looked as corresponding network protocol, so “wormhole” attack also can be seen as a kind of agreement. According to the principle, we set up new standard application layer protocol model and its embedded module in OPNET. The inner module ip_encap, IP, manet_rte_mgr in the model manet_station_adv are modified in internal process, and we established a "worm hole" process model. Fig. 5 is diagram of the new connection between process model.

5.2.3. Trajectory define of the node movement

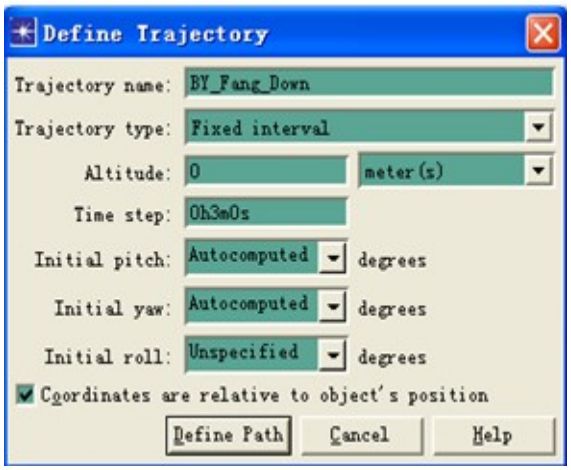


Fig.6 Trajectory BY_Fang_Down definition

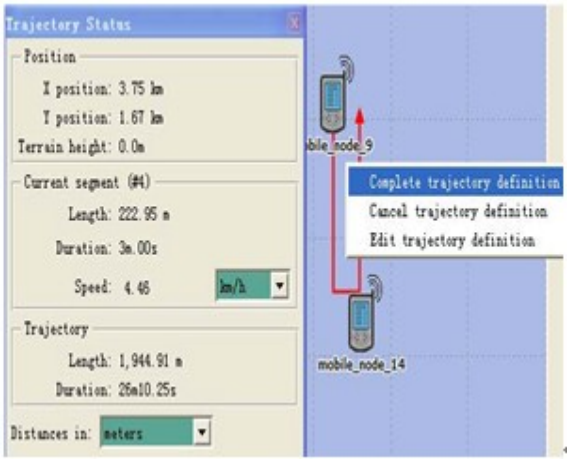


Fig.7Trajectory BY_Fang_Down segment definition

We define node movement track through a series of predefined points in the OPNET, and the method is based on the movement of segment. The moving time between two points can be subdivided into two types, the fixed time interval and the unfixed time interval. Fixed time interval refers to no matter how far distance, running time of each segment is equal. The unfixed time interval is to set

the speed, height and retention time to form the trajectory. This experiment adopts fixed time interval of segmented moving trajectory, the setup steps are shown in Fig.6- 8.

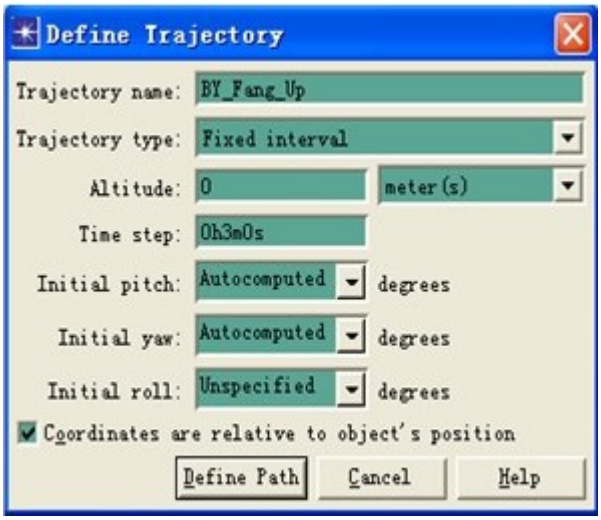
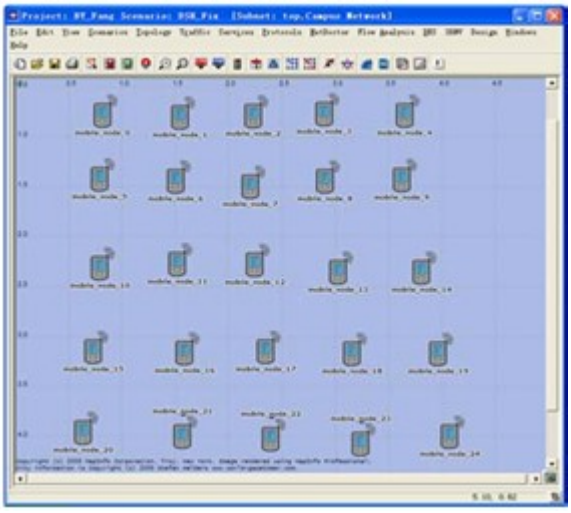


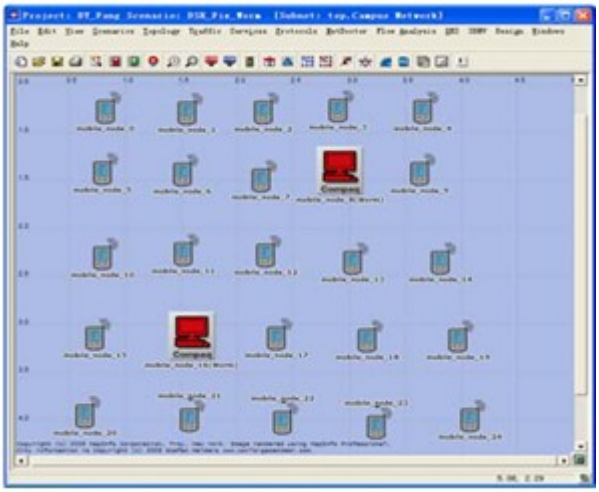
Fig.8 Trajectory BY_Fang_Up definition

5.2.4. Model of "wormhole" attack network simulation

"Worm hole" attack network model is the certain network topology combined with new "wormhole" node and ordinary node in Ad hoc network, and the corresponding relationships are established between all nodes, and thus the system are entire mapped as the OPNET network simulation system model. Fig.9 (a),(b) are fixed basic model, the Ad hoc network on (a)of the Fig.9 is 25 common nodes, (b)of the Fig.9 is 23 common nodes and with 2 "worm hole" nodes.



(a)



(b)

Fig.9 Fix Ad hoc networks model

The Fig. 9 is the basic model of mobile Ad hoc network, which is similar to fixed Ad hoc network basic model, and the difference is that all the nodes in the mobile Ad hoc network model are defined in the trajectory.

5.2.5. Main parameters in the simulation

Table 2 Simulation parameters setting

Simulation area	5×5 km2	node number	25
Carrier transmission model	two-way	"wormhole " node number	2
Business type	CBR	MAC protocol	802.11
Destination node	Random	start time	100 seconds
Package size	100 bits	exponential interval	exponential(1)
simulation time	9 minutes		
Simulation of routing protoco	OLSR、DSR、AODV protocol		

The parameters in the simulation is shown as table.2

5.3 simulation results and analysis

5.3.1. In view of the OLSR protocol "wormhole" attack simulation analysis

Fig.10 is the simulation result according to OLSR protocol “Wormhole” attack, and it put network capacity as statistical variable, As can be seen from the simulation results, in the fixed network throughput in Ad hoc network has fallen by about 12%, “wormhole”attack effect is obviously, and the performance of network is declined

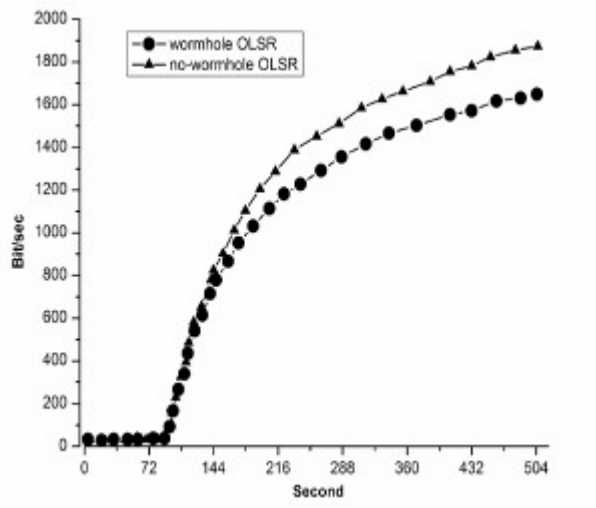


Fig10 Simulation results of wormhole attack against OLSR protocol

5.3.2 Simulation analysis of DSR protocol “wormhole” attack

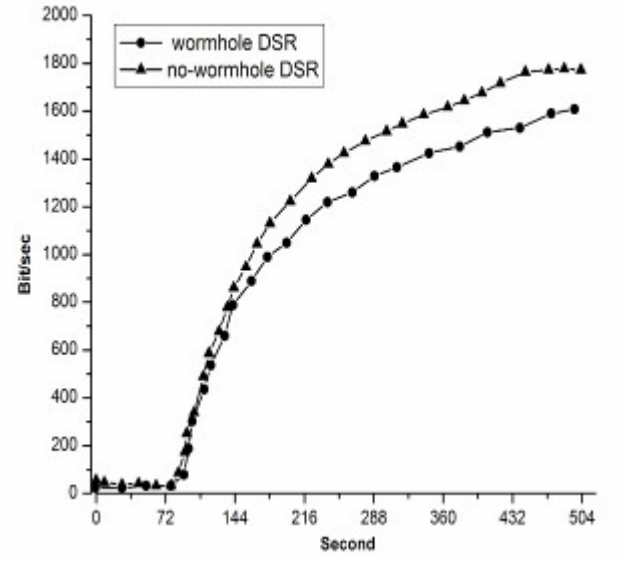


Fig11 Simulation results of wormhole attack against DSR protocol

Fig11 is the simulation result of the DSR protocol “wormhole” , network capacity is looked as statistical variables, As can be seen from the simulation results, in the fixed network throughput in Ad hoc network has fallen by about 9%, “wormhole” attack effect is common .

5.3,3. In view of the "worm hole" attack analysis of AODV protocol

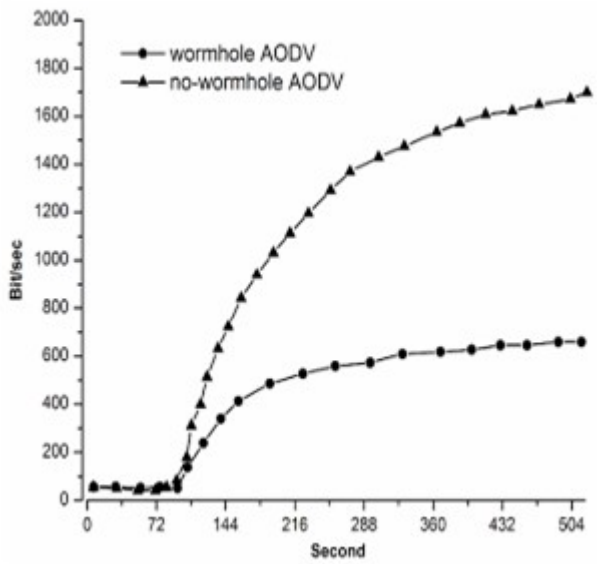


Fig12 Simulation results of wormhole attack against AODV protocol

Fig.12 is the simulation result of AODV protocol “wormhole” attack, take the network capacity as statistical variables, it can be seen from the simulation results, in the fixed network throughput in Ad hoc network has fallen by about 62%, “wormhole” attack effect is very obvious, the network performance is greatly reduced .

6.Conclusion

In the paper, we introduce the concept of wormhole and characteristics of the wormhole attack. We also establish the process model, node model and network model of “worm hole” in the Ad hoc network according to the OPNET simulation process, network capacity is chosen as the evaluation parameters in the simulation, and the simulation results are analyzed in detail.

Through analyzing the simulation results, the following conclusions can be obtained. first, the “worm hole” attacks to different Ad hoc network routing , its attack effect is not the same, but it is real exists, the attack effect is also obvious. The Ad

hoc network security routing mechanism we proposed has good protection effect, it can perform effective protection with the attacks of “worm hole” in the Ad hoc network.

Acknowledgements

The Authors would like to thank Professor Karlof for critically evaluating the manuscript and the control group members of Information Engineering room for their kind help at various stages of the research.

This project is supported by research program of China.

1、Research on the method for dynamic risk security assessment of IP network, Special Scientific Research plan of the department of education Shaanxi Province , 11JK0920. 2011.7

2、The evaluation for dynamic risk of network security, Natural science fund of Shaanxi Province , 2009MJ8002-3 ,2009.7

Reference

[1] Jacquet P, Clausen T. Optimized link state routing protocol for ad hoc networks[J]. *IEEE Networking*, 2001, 11(28), pp.62-68.

[2] Z. Zhou, Z. Haas. Secuting Ad Hoc networks[J]. *IEEE Networks*, 1999, 13(6),pp.24-30.

[3] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure on-demand routing protocol for wireless Ad hoc networks[J]. *ACM Mobile Computing and Networking*, 2002, 9, pp.12-23.

[4] Lichun Bao, J.J. Garcia-Luna-Aceves. Link-State Routing in Networks with UnidirectionalLinks[C]. *Proceedings of the IEEE International Conference on Computer Communicationsand Networks (ICCCN)*, October 1999,pp. 358–363.

[5] J. Newsome, E. Shi, D. Song, A. Perrig. The sybil attack in sensor networks: analysis & defenses[C]. *Proceedings of the third international symposium on Information processing in sensor networks*, ACM, 2004, pp.259-268.

[6] J. Kahn, R. Katz, K. Pister. Next century challenges : Mobile networking for smart dust [C]. In 5th ACM/ I*EEE Annual International Conference on Mobile Computing (MOBICOM 1999)*, 1999, pp.271-278.

[7] C. Karlof, D. Wagner. Secure routing in sensor networks: attacks and countermeasures[J]. *Ad Hoc Networks*, 2003, 1, pp.293–315.

[8] Zygmunt J. Haas, Marc R. Pearlman. The performance of query control schemes for the zone routing protocol[C]. *Proceedings of the ACM SIGCOMM’98 conference on Applications, technologies, architectures, and protocols for computer communication*, August 1998, pp.167-177.

[9] P. Krishna, N. H. Vaidya, M. Chatterjee, D. K. Pradhan. A cluster-based approach for routing in dynamic networks[J]. *ACM SIGCOMM Computer Communication Review*, 1997, 27, pp.49-65.

[10] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao, Rishav Khemka. A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attack in MobileAd hoc Networks[J]. *International Journal of Recent Trends in Engineering*,2009, 1(2), pp.220-222.

[11] Ravi Prakash. A Routing Algorithm for Wireless Ad Hoc Networks with Unidirectional Links[J]. *ACM/Baltzer Wireless Networks Journal*, November 2001,7(6), pp.617–626.

[12] Jorjeta G. Jetcheva, David B. Johnson. Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks[C]. *Proceedings of the 2001 ACM International Symposiumon Mobile Ad Hoc Networking and Computing*, October 2001,pp.33-44.

[13] M.R. Pearlman, Z.J. Haas, B.P. Manvell. Using Multi-Hop Acknowledgements to Discover and Reliably Communicate over Unidirectional Links in Ad Hoc Networks[C]. *IEEE Wireless Communications and Networking Conference(WCNC)*, September 2000, pp.532-537.

[14] Yih-Chun Hu,David B. Johnson, Adrian Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks[J]. *Ad Hoc Networks* 2003,pp.1175-192.

[15] Y.Yu, R.Govindan, D.Estrir. Geographical and energy aware routing A recursive data dissemination protocol for wireless sensor networks[R]. *University of California at LosAngeles Computer Science Department Tech.Rep*. May 2001.

[16] Xia Wang, Johnny Wong. An end-to-end detection of wormhole attack in wireless ad-hoc networks[C]. *3lst Annual IEEE International Computer Software and Applications Conference*, July 2007,pp342-350.

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Packet Leashes: A Defense

againstWormhole Attacks in Wireless Networks[J]. *IEEE Computer and Communications,*2003, 3(30), pp.1976-1986.

[18] Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks[C]. *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks,*2003,pp.21-32.

[19] L. Lazos, R. Poovendran. Serloc: Secure Range-independent Localization for Wireless Sensor Networks[C]. *Proceedings of the ACM Workshop on Wireless Security,* 2004, pp.21-30.

[20] Hon Sun Chiu, King-Shan Lui. DelPHI Wormhole Detection Mechanism for Ad Hoc Wireless Networks[C]. *2006 1st International Symposium on Wireless Pervasive Computing.*2006,pp.306-311.

[21] Asad Amir Pirzada, Chris McDonald. Circumventing Sinkholes and Wormholes inWireless Sensor Networks[C]. *International Conference on Wireless Ad Hoc Networks* (W WAN), 2005, pp.778-782.

[22] Jane Zhen, Sampalli Srinivas. Prventing replay attacks for secure routing in ad hoc Networks[J]. *Ad Hoc, Mobile, and Wireless Networks ,* 2003 ,(2865), pp.140-150.

[23] Lijun Qian, Ning Song, Xiangfang L. Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path[C]. *IEEE Wireless Communications and Networking Conference (IEEE WCNC),* New Orleans, USA, Mar 2005.

[24] Levente Buttyan, Laszlo Dora, Istvan Vajda. Statistical Wormhole Detection in Sensor Networks[C]. *Second European Workshop on Security and Privacy in AdHoc and Sensor Networks ESAS 2005* Visegad, Hungary, July 13-14, 2005,pp.128-141.

[25] Charles E., Perkins, Pravin Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers[J]. *ACM Computer Communication Review,*1994, 24,pp. 234-244.

[26] Jacquet P, Clausen T. Optimized link state routing protocol for ad hoc networks[J]. *IEEE Networking,* 2001, 11(28),pp. 62-68.