TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.3, March 2014, pp. 2110 ~ 2117
DOI: http://dx.doi.org/10.11591/telkomnika.v12i3.4062

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

Yang Shengju*, Shi Shaoting, Zhao Xinhui
Gansu Institute of Science and Technology Information, 730000,Gansu, China
*Corresponding author, e-mail: hwh_xa@126.com

Abstract

As known that Ad hoc networks are made of a group of portable terminals and has many wireless transmitter as multi-hops autonomy system. While Ad hoc networks are very easy to be attacked by various kinds of network attacks, because it has limited resources, dynamic topology and open communication channel, etc. The wormhole attack is the common attack method, and it is an internal attack against routing protocols in the Ad hoc networks, the research on security of routing protocols against wormhole attack in the Ad hoc networks is to avoid the wormhole attack. In the study, the security routing mechanisms against wormhole attack in the Ad hoc networks are presented, on the basis of deeply research on wormhole attack principles and models. The modelling method and related simulations are presented in detailed to verify the effectiveness of security routing mechanisms.

Keywords*: 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, 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 [1, 2] 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. The jump communication is not a new concept, because it has been widely used in the Internet. In the Ad hoc network, the nodes usually are mobile, and some nodes may disappear in the network sometimes, so some of the data transmission paths may become invalid, so the intermediate nodes are more important than the fixed nodes in the network, and they are more vulnerable to be attacked [3-6]. 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 [7-9], 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 this study, the “worm hole” attack security problems are taken as the main research topic in the Ad hoc network routing protocol, the research of “worm hole” in the Ad hoc network attacks and the corresponding security routing mechanism are analyzed. 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 an important role in the future.

Received August 1, 2013; Revised September 13, 2013; Accepted October 15, 2013

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

a) Based on the geographical location
b) Based on synchronous clock
c) The use of encryption algorithm
d) The use of the RF frequency watermark
e) SECTOR
f) Based on the directional antenna
g) DelPHI

In the study, the research of Ad hoc network routing protocols running mechanism is made, and select the typical Ad hoc routing protocols. The specific Ad hoc network routing protocols of the "wormhole" attack is the studied as core, and it also makes the analysis of "wormhole" attack principle, according to the Ad hoc network attack model of the "wormhole", the related algorithm is designed. The Ad hoc network security routing mechanism and its related algorithm in OPNET network simulation platform are obtained through the simulation, comparison and analysis, the validation of "wormhole" attack damage and the effectiveness of the security routing mechanism is verified.

2. Analysis of “wormhole” Attack

As 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 defence 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 be detected, because the 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.

3. Design of Adhoc Network Sectурity 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, the design of Ad hoc network security routing mechanism according to “worm hole” attack is presented.

3.1. 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:

a. Location-based routing protocols: GEAR.
b. Based on the synchronous clock "packet" (packet leashes).
c. The security strategy based on the encryption algorithm, such as SAODV, SEAD, SAR.
d. Method based on using of RF frequency watermark.
e. Method based on using of special hardware transceiver SECTOR.
f. Method based on using a directional antenna, SeRloc agreement is proposed.
g. Method based on statistical average jump each path .
h. Method based on the monitoring of adjacent nodes, according to the data packet transmission method of trust value.
i. Method based on the cycle method of trip time (RTT) .
j. Based on statistical analysis, the method of statistical link SAM agreement and neighbour number is put forward.
k. 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.
l. In the study [10] neighbour 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.

3.2. Analysis of the “wormhole” Attack Protection Method

It can be found that there exist two methods which can't position the malicious nodes, if the malicious nodes cannot be located, 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, it can be found that there are six kinds of methods need large calculation; so it is a challenge for Ad hoc network in the mobile terminal.

Table 1. Values of Parameters in Simulation

Simulation area	5×5 km^2	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		

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 [11, 12].

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.

3.3. 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:

a. The algorithm is simple, and it is easy to implement.
b. It does not need to use complex algorithm such as the digital signature technology,
c. Public/private key encryption system or hash function.
d. It does not need to use special high sensitivity, expensive equipment.
e. The routing information of node storage requirements is not high.
f. The routing operation of node energy consumption demand is not high.

5. Simulation and Analysis "Wormhole" Attack

Through basic steps of OPNET simulation, process model, node model and network topology model are built. The validation of “wormhole” attack damage and the effectiveness of the security routing mechanism according to the attacks of “wormhole” can be obtained. 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”.

As mentioned above, OPNET simulation can be divided into the three levels, network model, model of node, the process model. As to the functions, behaviour 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.

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 experiments, modifications should be made (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 Figure 1. Among them, the modified parts are mainly concentrated on the ip_encap, IP, manet_rte_mgr_Worm module.

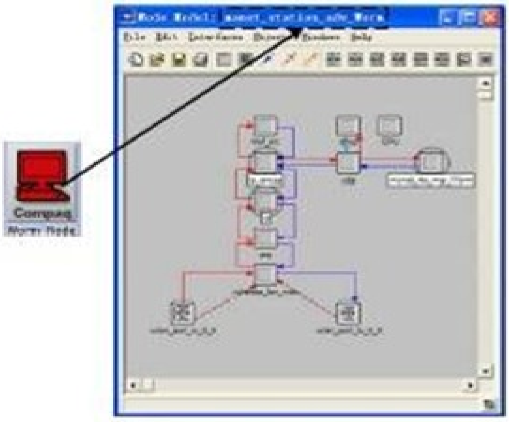


Figure 1. Wormhole Node Model in the Ad hoc Networks

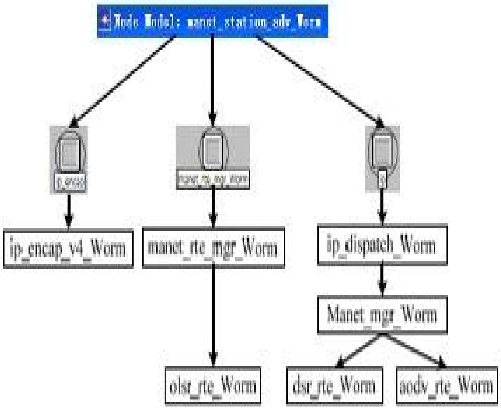
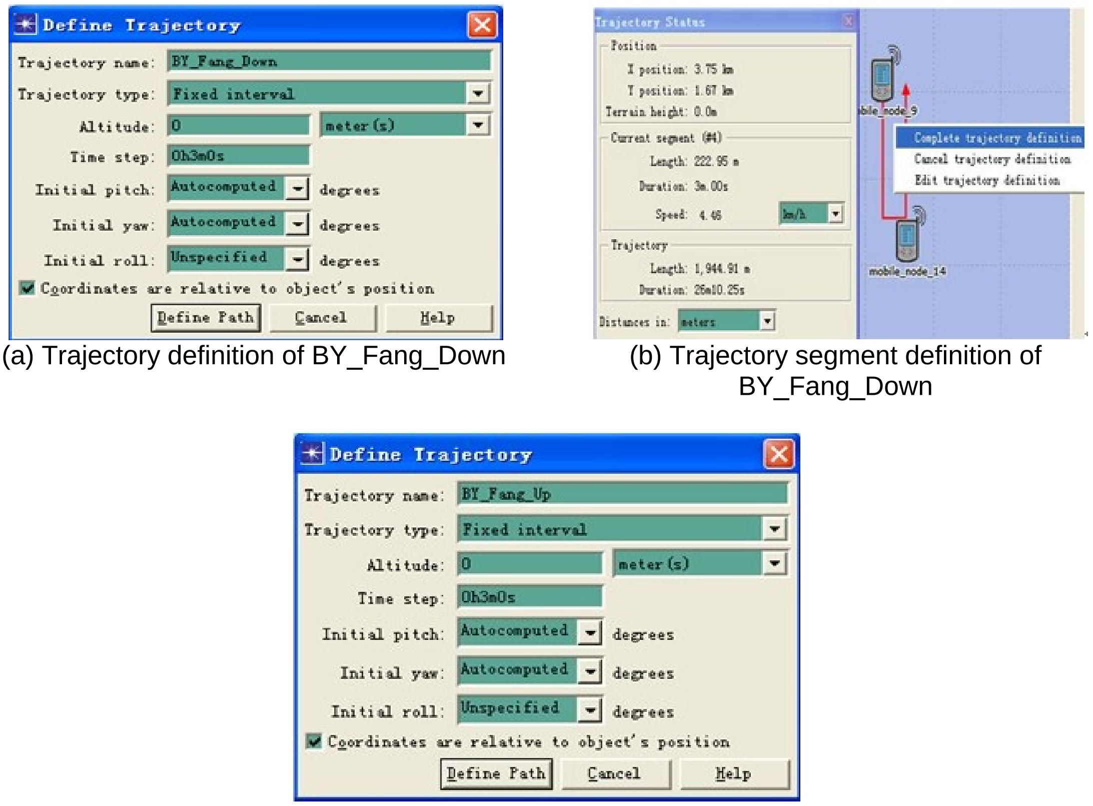


Figure 5. Wormhole Process Model in the Ad hoc Networks

5.1. The "worm hole" 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 a "worm hole" process model is also established. Figure 2 is diagram of the new connection between process model.



Define Trajectory

Trajectory name: BY_Fang_Down
Trajectory type: Fixed interval
Altitude: 0 meter(s)
Time step: 0h3m0s
Initial pitch: Autocomputed degrees
Initial yaw: Autocomputed degrees
Initial roll: Unspecified degrees
☑ Coordinates are relative to object's position

(a) Trajectory definition of BY_Fang_Down

Trajectory Status

Position
X position: 3.75 km
Y position: 1.67 km
Terrain height: 0.0m

Current segment (#4)
Length: 222.95 m
Duration: 3m.00s
Speed: 4.46 km/h

Trajectory
Length: 1,944.91 m
Duration: 26m10.25s

Distances in: meters

bile_node_9
Complete trajectory definition
Cancel trajectory definition
Edit trajectory definition
mobile_node_14

(b) Trajectory segment definition of BY_Fang_Down

Define Trajectory

Trajectory name: BY_Fang_Up
Trajectory type: Fixed interval
Altitude: 0 meter(s)
Time step: 0h3m0s
Initial pitch: Autocomputed degrees
Initial yaw: Autocomputed degrees
Initial roll: Unspecified degrees
☑ Coordinates are relative to object's position

(c) Trajectory definition BY_Fang_Up

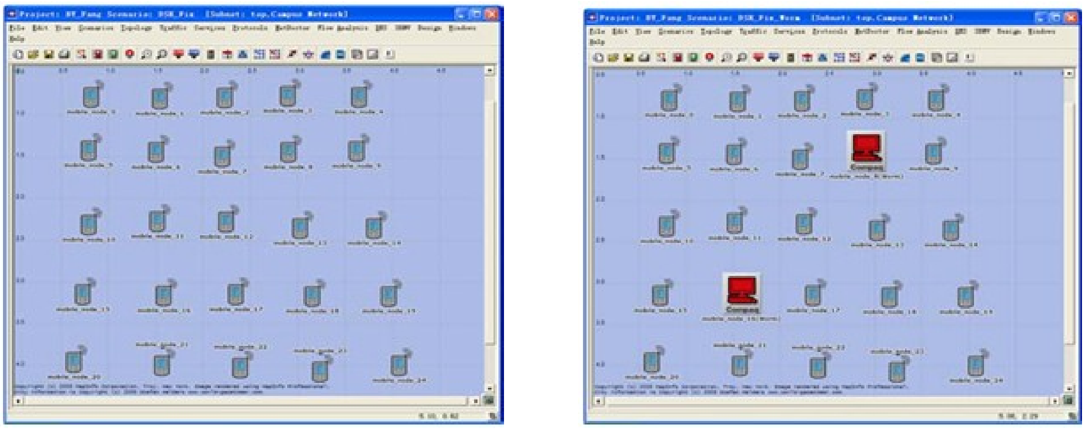
Figure 3. Trajectory Definition of BY_Fang_

5.2. Trajectory Define of the Node Movement

It defines 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 Figure 3.

5.3. 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. Figure 4(a), (b) are fixed basic model, the Ad hoc network on (a) of the Figure 4 is 25 common nodes, (b) of the Figure 4 is 23 common nodes and with 2 “worm hole” nodes.



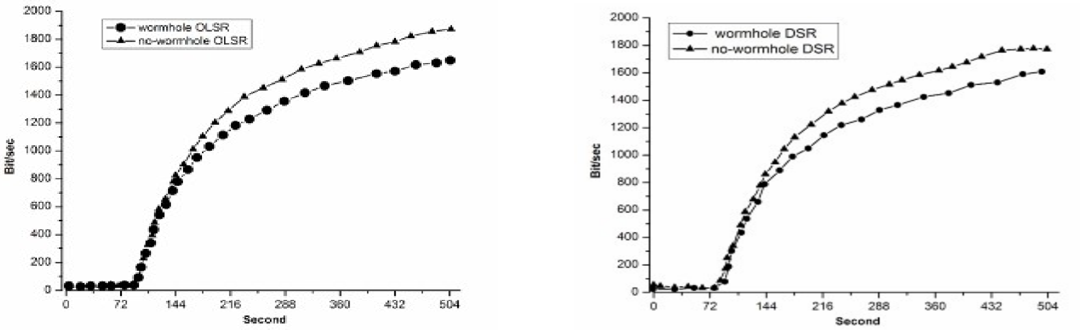
(a) Common nodes in Ad hoc network

(b) Common nodes and with 2 “worm hole” nodes in Ad hoc network

Figure 4. Fix Ad hoc Networks Model

The Figure 4 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. The parameters in the simulation are shown as Table 1.

5.4. Simulation Results and Analysis



(a) Wormhole attack against OLSR protocol

(b) Wormhole attack against DSR protocol

Figure 5. Simulation Results of Wormhole Attack

Figure 5(a) 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.

Figure 5(b) 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.

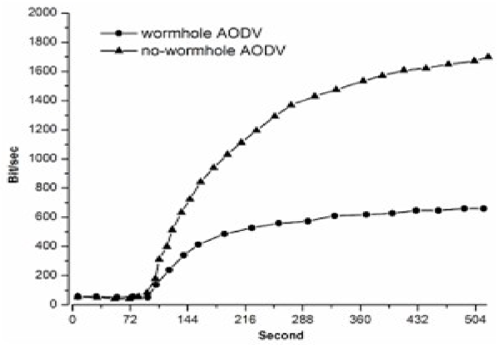


Figure 6. Simulation Results of Wormhole Attack Against AODV Protocol

Figure 6 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 study, it introduces the concept of wormhole and characteristics of the wormhole attack. It also proposes 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 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: The Tibetan of bilingual emergency relief Quality Control Issues in Multimedia Database Research Based on Ad Hoc Networks, National Natural science fund of China, 61162011, 2012.1.

References

[1] Jacquet P, P Muhlethaler, T Clausen, A Laouiti, A Qayyum, L Viennot. *Optimized link state routing protocol for ad hoc networks.* Proceedings of the 5th IEEE Multi Topic Conference, Springer, USA. 2001: 62-68.

[2] Zhou Z, Z Haas. Secuting ad hoc networks. *IEEE Networks.* 1999; 13: 24-30.

[3] Hu YC, A Perrig, DB Johnson. Ariadne: *A secure on-demand routing protocol for Ad Hoc networks..* Proceedings of the 8th Annual International Conference on Mobile Computing and Networking. ACM, Atlanta. 2002: 12-23.

[4] Bao L, JJ Garcia-Luna-Aceves. *Link-state routing in networks with unidirectional links*. Proceedings of the IEEE International Conference on Computer Communications and Networks, Boston-Natick, MA, USA. 1999: 358-363.

[5] Newsome J, E Shi, D Song, A Perrig. *The sybil attack in sensor networks: Analysis and defenses*. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA. 2004: 259-268.

[6] Kahn JM, RH Katz, KSJ Pister. *Next century challenges: Mobile networking for smart dust.* Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, WA. 1999: 271-278.

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

[8] Haas ZJ, MR Pearlman. *The performance of query control schemes for the zone routing protocol.* Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures and Protocols for Computer Communication. Vancouver, Canada. 1998: 167-177.

[9] Krishna P, N Vaidya, M Chatterjee, DK Pradhan. A cluster-based approach for routing in dynamic networks. *ACM SIGCOMM Computer Communication Revi*ew. 1997; 27: 49-65.

[10] Enkataraman R, M Pushpalatha, T Rama Rao, R Khemka. A graph-theoretic algorithm for detection of multiple wormhole attack in mobile ad hoc networks. *Int. J. Recent Trends Eng.*, 2009; 1: 220-222.

[11] Prakash R. A routing algorithm for wireless ad hoc networks with unidirectional links. *Wireless Networks.* 2001; 7: 617-626.

[12] Jetcheva JG, DB Johnson. *Adaptive demand-driven multicast routingin multi-hop wireless ad hoc networks.* Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, Long Beach, CA, USA. 2001: 33-44.

[13] Zhang Yu-quan, Wei Lei. A New Routing Protocol for Efficient and Secure Wireless Sensor Networks. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(11).

[14] Songchang Jin, Songhe Jin, Shuqiang Yang, Xiang Zhu. Design of a Parallel and Distributed Network Security Simulation Platform. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(6).

[15] Xin Yu, Jian Jun Fang, Zhao Li Zhang. *A Security Mechanism Based on Authenticated Diffie-Hellman for WSN.* 2013; 11(6).