Available online at www.sciencedirect.com

SciVerse ScienceDirect

Physics Procedia 33 (2012) 354 – 360

Physics Procedia

ELSEVIER

2012 International Conference on Medical Physics and Biomedical Engineering

An effective Denial of Service Attack Detection Method in Wireless Mesh Networks*

Liangyu Luan[1],Yingfang Fu[2*], Peng Xiao[3]
[1] *College of Applied Science, Beijing University of Technology, Beijing 100124, China;*
E-mail: luanly@bjut.edu.cn
[2] *College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China;*
E-mail: xp1984@emails.bjut.edu.cn
Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China;
E-mail: fuyingfang@bjut.edu.cn

Abstract

In order to detect the DoS attack (Denial-of-Service attack) when wireless mesh networks adopt AODV routing protocol of Ad Hoc networks. Such technologies as an end-to-end authentication, utilization rate of cache memory, two pre-assumed threshold value and distributed voting are used in this paper to detect DoS attacker, which is on the basic of hierarchical topology structure in wireless mesh networks. Through performance analysis in theory and simulations experiment, the scheme would improve the flexibility and accuracy of DoS attack detection, and would obviously improve its security in wireless mesh networks.

Keywords-wireless mesh network; denial of service attack; intrusion detection; distributed voting

1. Introduction

As a new wireless network technology, WMN (wireless mesh network) that depends on its high utilization ratio of frequency spectrum, wide coverage area, good expandability and reliability can get rid of some restrictions of Ad Hoc network, WLAN (wireless local area networks), WPAN (wireless personal

* Foundation Items: The National Basic Research Program of China (973 Program) (2007CB311100). Doctoral Fund of Ministry of Education of China(20100480173) .
Corresponding Author：fuyingfang@bjut.edu.cn

doi:10.1016/j.phpro.2012.05.074

area network), and WWAN (wireless wide area network). Nowadays WMN has been paid great attention to by more and more specialists from academic to commercial circles, especially security issues in WMN.

DoS attack means that a node couldn't provide normal required services to other legitimate nodes or terminals, and can be carried out on the every layer in network[1]. There are a lot of measures to launch DoS attack from the physical layer to the application layer in WMN because of its own characteristics. However, most DoS attacks are carried out in the network layer, whose manifestation are listed as follows[1-2]:

(1) Signal interference. The Attackers capture the frequencies of message signal sent and received by nodes in the network, and then continuously send the jamming signals.

(2) Modification of routing nodes sequence. Attackers modify the sequence and hop in AODV (Ad hoc On-demand Distance Vector) to create a false route, which significantly reduce the performance of the whole network[2].

(3) Faked legitimate nodes. Since message address isn't identified in routing protocols, attackers may fake certain legitimate nodes to access the network, and even mask legitimate nodes to receive their messages instead of them[3].

(4) Resources consumption. Attackers send a lot of useless messages, such as routing query messages, to consume resources of the network and nodes, such as bandwidth, memory, CPU and batteries power.

2. Related Work

Nowadays AODV routing protocol in ad hoc networks is also used in some WMNs, in which route establishment is carried out completely on the demands. When a source node needs to send messages to another node which current routes can not reach, it broadcast RREQ (route request), which are flooding in the network to inquire a reachable route. When receiving RREQ, a node will firstly check whether there is a recorded route to reach the destination node in its routing table or not. If not, it will temporarily store SNA (source node address), DNA (destination node address), UNA (upstream node address) and destination sequence number to set up a reverse route, and then broadcast RREQ again. If there is a current reachable route, or local node is the destination one, it will send RREP (route reply) back to the source one along with the route RREQ arrives. When the source node receives RREP, a route from the source to the destination is set up.

Link status is monitored through periodically broadcasting "hello" message in AODV. If a node finds a used link is broken off, it will delete all routes with the broken link from its routing table, and send RRER (route error) to initial nodes of the routes to inform them that correlative routes should be deleted from their routing tables. And those nodes forwarding RRER along the way will also modify their tables. When RRER arrives at the source node, it will delete the wrong routes, and query a new route if needed.

In traditional defense models, the node creates a single table for each neighbor. It will start the timer when receiving a neighbor's message at the first time, and increase the value of correlative counter by 1 with each new received message before timeout. If the value exceeds a threshold designed, an attack alarm will be carried out. And if no attacks are detected before timeout, the value will set zero as its initial, until the timer starts again.

Yi et al. proposed a new detecting strategy based on priority[5], whose main idea is to change FIFS (first in, first served) to priority：

(1) The node sets a processing priority for each neighbor, which is related to their former sending frequency. When dealing with a lot of message, the node will query the senders' priority, and firstly process those that have the highest priority. The priority is set 1 as its initial value.

(2) When a neighbor sends *n* packets in a unit interval, its priority will be changed to *1/n*. For example, Node H's initial priority is 1. When H sends 10 packets in the former 1 second, then H's neighbors, one of which is marked as Node F, will change H's priority to 1/10 in F's table. And if now Node A sends a message, and A's priority in F's table is 1, then F will first deal with A's message, and put H's message behind A's.

(3) In order to further avoid excessive message sending, the threshold is set to the maximum of message which the node is allowed to send in one second in routing protocols. When a node's sending frequency exceeds the threshold, it will be recognized as an attacker and its successive message will be refused.

There are some shortcomings in Yi's scheme. Although adoption of priority can reduce malicious nodes' sending priority, but it can't prevent malicious nodes from modifying their IP address and then sending RREQ again. Since it is possible that packet sent frequency of the same IP address is managed not to reach the pre-assumed threshold, but all packets sent by the same IP address in total already consume all, so this scheme based on priority doesn't well protect resources of the network and nodes.

3. A New Dos Attack Detetion Scheme

3.1 Network Model for WMN

The detection scheme presented in this paper is based on a zone-based hierarchical network model for WMN[6], as shown in Fig.1. The whole network consists of one backbone network and one or more local area networks called zones. The backbone network consists of backbone routers, an off-line CA which only connects to the network under the condition that it is notified of the existence of an attacker, being it a terminal user, a zone router or a backbone router, and a database of authorized certificates that are shared only among the backbone routers. There are also at least two backbone routers connected to the Internet. Each zone network has two zone routers connected to the backbone network and to the users. There is also a database that stores user information, such as user ID, zone ID, authorized key, etc., which is shared between the two zone routers.

In the network model, it is assumed that communication between users has the following characteristics:

(1) One zone router may connect to one or more terminal users.

(2) Users in a zone network communicate with each other within a relatively shorter range and those in a backbone network communicate with each other within a relatively longer range.

(3) Terminal users connect to the Internet through backbone routers and any one of the two zone routers. Those in the same zone network may communicate directly. And those in adjacent zone networks may communicate with each other through their zone routers.

(4) Authentication between users would use authorized certificates. And cryptographic communication between users adopts the identity-based cryptosystem.

(5) The cost of communication through the backbone network is higher than that in zone networks.

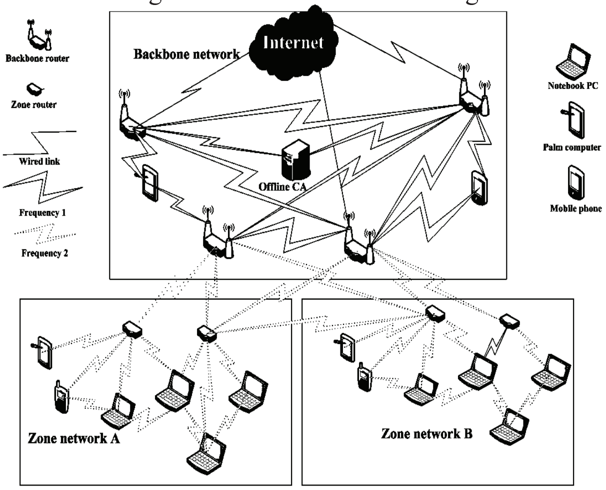

Fig.1. Network Model

3.2 Detection Mechanism

Paper [8] adopts priority mechanism to reduce malicious nodes' sending priority, however, resources of nodes being attacked is still expended, especially cache memory. Attackers can modify their IP to control its sending frequency less than the threshold and its total packets more than cache memory.

In order to preserve limited resources of the node, a improvement upon priority mechanism is introduced in this paper. An end-to-end authentication is used to prevent users modifying its IP for faked identity; and utilization rate of cache memory, two-threshold value, and distributed DoS attacker or not.

(1) Before communication, mutual authentication of two sides of communication is achieved using their issued authority certificate.

(2) A table of priority is set up by the node for its each neighbor, which is related to the neighbor's former sending frequency. When dealing with message, high priority is firstly considered. Each's initial value is set to 1.

(3) When a node has sent *m* message in the former 1 second, its priority will be changed to *1/m* by its neighbors.

(4) A certain size of buffer is allocated to each neighbor by the node, whose threshold is set to P_n. The neighbor with higher priority is allocated more buffers, which means its P_n is larger. When a neighbor's packets have reached the threshold, then its excessive packets will be directly abandoned instead of processed, and its excessive allocated buffer will be taken back.

(5) Each node set a threshold P for its total size of buffer, which is the sum of P_n. When some nodes unite to launch a collaborated DOS attack, and if the total used buffer exceeds the threshold P, a certain packets will be discarded, and their allocated buffer would be taken back. Packets with lower priority will be discarded more.

(6) Packets with highest priority in the buffer are processed at the first turn.

(7) If a node finds a terminal user, i.e., its neighbor node, being a DoS attacker, it would notify its zone router.

(8) If a zone router is notified of a terminal user being an attacker, the zone router would disassociate the terminal user with the zone network. Then, the zone router would revoke its authorized key and update the key pair of the zone network. Lastly, the zone router would announce that the terminal user is an ineligible user to the zone members in the same zone and to its neighbor backbone router. The backbone router will initiate any t-1 out of the n-1 backbone routers to revoke the terminal user's identity-based private key and authorized certificate along with itself. At the same time, the backbone router would send the result to the off-line CA so that the off-line CA would revoke the key pair and the public certificate of the terminal user [7].

4. Security Analyses

Comparing with current DoS attack detection schemes, the scheme presented in this paper based on a zone-based hierarchical distributed WMN has some advantages as follows:

(1) Zone-based hierarchical topology can be extended easily to deal with WMNs of any sizes and integrated easily with different networks.

(2) Considering some uncertain attacks, distributed voting is used in this scheme, which can enhance its flexibility and accuracy.

(3) In order to defend against DoS attack, mutual authentication of terminal nodes is carried out before communication, and utilization rate of cache memory is always monitored during communication. Its detection rate is higher than those who just monitor neighbors' sending frequency.

(4) Two-threshold value presented in this paper is able to resist collaborated DoS attack launched by multi-nodes.

(5) When collaborated DoS attack occur, packets with low priority will be discarded first, which can improve the accuracy to drop packets, and ensure stable transmission of legitimate nodes.

5. Simulation Analyses

Several experiments are carried out to simulate the presented detection scheme using OPNET 10.5A under Windows XP operating system. As shown in Fig.2, the simulation scenario is set as follows: the network covers an area of 1000m×1000m; transmission rate in backbone networks is set at 54Mbps, while that in zone network is set at 11Mbps; total simulation time is set to 10 seconds.

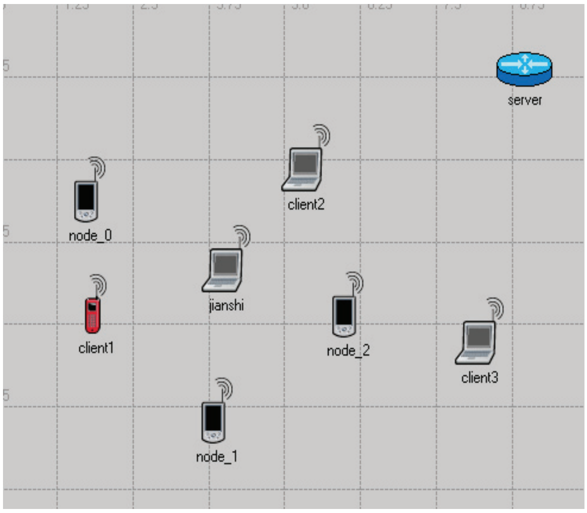

Fig.2. Simulation Scenario of DoS Attack

The simulation results of packet load and byte load in the network suffering from DoS attack are shown in Fig.3 and Fig.4: packet load is between 100 and 125 per second; byte load average is about 17,500 bits. And the simulation results of packet load and byte load after activating our scheme are shown in Fig.5 and Fig.6: packet load is between 20 and 40 per second; byte load average decreases to about 4,400 bits.

As far as packet received delay is concerned, the curve of packet received delay is instability in the network with DoS attack. The maximal packet received delay is 60 μs. After starting the DoS attack detection scheme, the curve of packet received delay is changed stability in the network, as the Fig.7 illustrated shows.

We can see that, when DoS attack occurs in the network, there will be full of a mass of void packets in the network, which reduces the reliability of the whole network and hamper data transmission between legitimate nodes. And after activating the scheme proposed in this paper, the harm causing by DoS attack is effectively reduced and the reliability of the network is also improved.

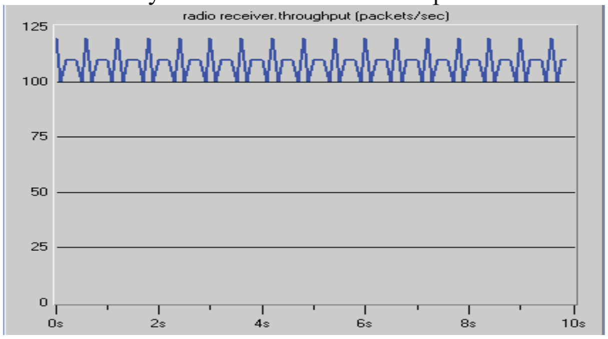

Fig.3. Data Packet Load in Network with DoS Attack

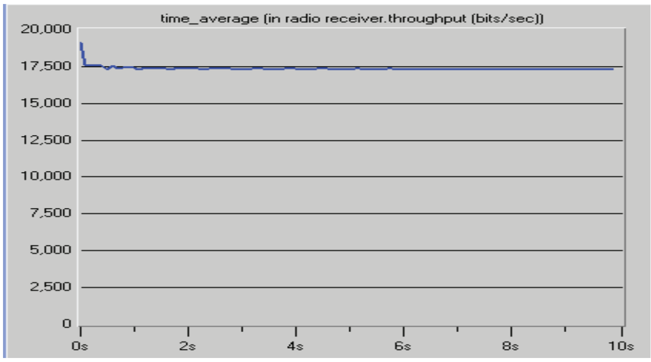

Fig.4. Byte Load in Network with DoS Attack

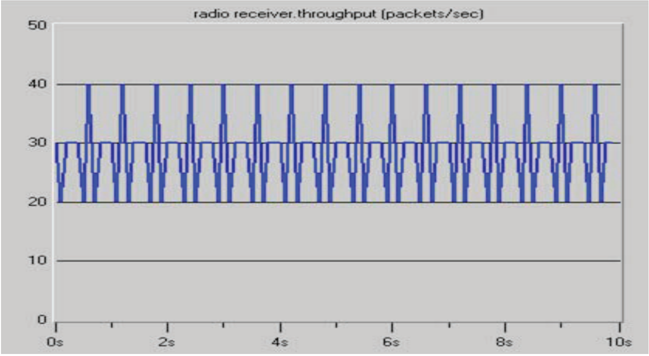

Fig.5. Data Packet Load in Network after Starting the DoS Attack Detection Scheme

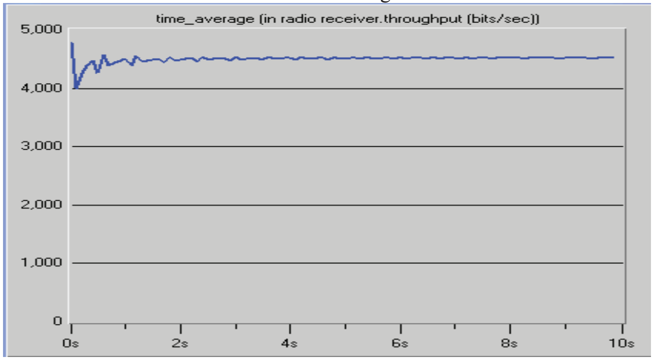

Fig.6. Byte Packet Load in Network after Starting the DoS Attack Detection Scheme

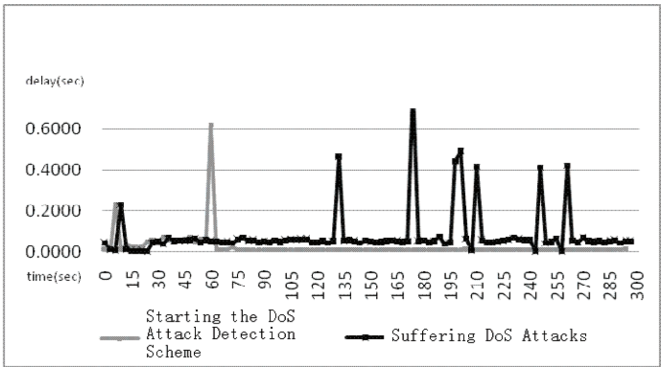

Fig.7. Packets Received Delay of applied Wormhole Attack Detection

6. Conclusions

Such technologies as an end-to-end authentication, utilization rate of cache memory, two-threshold value, and distributed voting are used in this paper to detect DoS attackers. Through performance analysis in theory and simulations experiment, the scheme would improve the flexibility and accuracy of DoS attack detection, and would obviously improve its security in WMN. In further research, distributed voting referred in this paper will be paid more attention to resist collaborated attacks.

References

[1] Xuming Fang, Next Generation Wireless Networks Technology: Wireless Mesh Networks, Peple's Post and Telecommunication Press, 2006.

[2] Wei Yu and K.J. Ray Liu, Defense against Injecting Traffic Attacks in Cooperative Ad Hoc Networks. GLOBECOM'05, St. Louis, MO, United States, 2005. New York, Institute of Electronical and Electronics Engineers Inc: 1737-1741.

[3] Ping Yi, DOS Attack and Defense in Mobile Ad Hoc Networks, Journal of Computer Research and Development, 2005, 42(4):697-704.

[4] Hongsong Chen, Zhaoshun Wang, Shurong Ning, Agent-based security protocol against DoS attack in Ad Hoc network, Journal of University of Science and Technology Beijing, 2007, 29(2): 166-171.

[5] Ping Yi, Intrusion Detection and Active Response in Mobile Ad Hoc Networks, Fudan University Ph. Degree thesis,2008.

[6] Yingfang Fu, Jingsha He, Rong Wang etc., Mutual Authentication in Wireless Mesh Networks.The 43rd IEEE International Conference on Communications (ICC 2008), Beijing, China, 2008. Piscataway, IEEE Press, 2008:1690-1694.

[7] Yingfang Fu, Jingsha He, Liangyu Luan, etc., A Zone-based Distributed Key Management Scheme for Wireless Mesh Networks. The 31st Annual IEEE International Software and Applications Conference (COMPSAC 2007), Beijing, China, 2007. Piscataway, IEEE Press, 2007:75-78.

[8] Ying Xu, Access Authentication and Key Management of Wireless Mesh Networks, Xi Dian University Master Degree thesis.