Journal of Applied Science and Engineering Innovation, Vol.2 No.11 2015, pp. 455-458
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

ACSS
Computation for Life ®

Research on Ad Hoc Network Security Mechanism

Junsheng Ma[1], Jing Zhao[1], Haiyan Zhao [1], Dezhi Niu[1], Xiaoshuang Wang[1]

[1] *Xi'an Communication Institute, Xi'an 710106, China*

Abstract*:* Ad Hoc network is a special kind of mobile multi-hop wireless networks, which has been widely used various occasions. In this paper, the main characters of Ad Hoc network are presented. Meanwhile, based on the inherent defect and security threats of Ad Hoc network, the corresponding security mechanism and strategy are proposed.

Keywords Ad Hoc network, Wireless Mobile Communication, Network security

INTRODUCTION

Ad Hoc network is a kind of self-organizing un-center network. Special occasions, such as cooperative communication for troops on the battlefield, the rescue after earthquake or flood, scientific investigation in wilderness, interim meeting, have made demands for a temporary networking technology which should possess characters like temporary, tasty and self-motion. That is the reason why a special mobile communication technology, Ad hoc network, was proposed. There is a basic difference between Ad hoc network and other mobile communication networks: all the nodes in Ad Hoc network have the equal status, which make Ad hoc network do not have to set any center control node. Such a characteristic attaches Ad hoc network strong destroy-resistance. In Ad hoc network, nodes do not only have the function required by normal mobile terminals but also be capable to transmit packets. When source node and destination node are not in the scope of direct communication, messages will be transmitted by intermediate nodes. Sometime, messages may go through multiple intermediate nodes. That is to say, a message has to go through multiple hops (Hop) to reach the destination.

CHARACTERISTIC OF AD HOC NETWORK

In Ad Hoc network, each node is both a network data terminal and a router. So the topology of the network is vulnerable to change. Resources of storage, power and wireless bandwidth are very limited. In general, it has features mentioned below:

The independence of network. Ad Hoc network does not have strict control center. All nodes have the equal status, which means Ad Hoc network is a peer-to-peer network.. Nodes can join or leave the networks at any time. Malfunction from any node does not affect the operation of the entire network. The destroy-resistance ability of Ad hoc network is remarkably strong. Besides, it has the ability of organizing network independently. Namely, the network layout do not have to rely on any network facilities constructed in advance. Nodes coordinate their behavior by the layered protocol and distributed algorithm. After the nodes starting up, they can form an independent network rapidly and automatically.

Multi-hop routing. when a node needs to communicate with nodes outside of the range it covered, message have to go through intermediate nodes to get the destination. Unlike the multiple hops of fixed network, the multi-hop routing of Ad Hoc network is done by the normal network nodes, rather than by appropriative routing equipments.

Dynamic change of network topology. In Ad Hoc networks, the mobile host can move optionally in the network. The movement of host can lead to the link between hosts increasing or disappearing or the relationship between hosts changing constantly. And the host may be a host or a router at the same time in Ad Hoc network. As a result, movement can make the network topology changes constantly. And the way and the speed of the change are unpredictable. So the network topology structure is relatively stable for the normal network.

INHERENT DEFECTS AND SECURITY THREATS IN AD HOC NETWORK

Inherent Defects. Ad Hoc network has bring in wireless access which is convenient and flexible. However, in the same time, many of its inherent characteristics has become fatal defects. These fatal defects are listed below.

(1) Vulnerability of channel. Like any kind of wireless network, it doesn't need the actual contact with network components to eavesdrop and insert fake messages to the network..

(2) Vulnerability of nodes. Network nodes usually consist of portable mobile devices which are lacking physical protection. So they are easy to loss ,be captured and fall into the attacker's control. In the same time, because of limited capacity and computing power of mobile nodes, It is hard for some mobile node to use some complex public key algorithms. In addition, some attackers can, drain the power of node by replay or forcing a node do a complex computing,

so as to initiate a special type of denial of service attacks.

(3) Lack of infrastructure. The lack of infrastructure make traditional security solutions for centralized certification bodies and online server be no longer suitable for Ad Hoc network.

(4) Dynamic change of the topology. In Ad Hoc network, continuous change of the topology requires complex routing protocol. So the security of routing protocols is critical to ensure the safety of the entire network.

(5) Vulnerability of routing mechanism. The operation of routing is completely distributed. Therefore, only every node in the network collaborating can routing functions be completed.

(6) Lack of central servers. The Lack of central servers makes the traditional form of web services is no longer suitable for Ad Hoc network. However, on the other hand, because of the independence on the central management, a single point of failure can not affect the entire network operating. This make it become a kind of security solution.

Security Threats. The routing security of Ad Hoc network aims to guarantee the availability of routing information, the integrity of routing information and the reliable routing of packets. As a kind of ceterless, self-organized networks, the discovery of routing and the maintenance need mutual cooperation among nodes in Ad Hoc network. On the other hand, due to mobility of nodes, the resources and capacity of network are limited. And the network also lacks effective physical protection[3]. All of these make the routing mechanism of Ad Hoc network face a variety of security threats. These threats can be roughly divided into the following categories.

(1) Forgery of routing. Routing forgery means attackers make false routing information by methods such as tampering routing messages, forging routing messages, fabricating the chain-breaking information and copycatting ids of multiple nodes.

(2) Hide of routing. Hide of routing means the attackers hide reliable routings (Routings only contain internal legal nodes) by special ways. Attackers make network traffic flow to the controlled node by controlling routing protocol.

(3) Hidden discard of packets. Routing packets can go through the attacked nodes right. But the data packets would be discard or selective discarded. That means the routing protocol is considered a normal route, while the data messages failing to be sent.

(4) Attacks of denying service. Attackers make the routing table overflow by forging a large number of false routing messages or make nodes be busy for all kinds of signature verification, message certification, or oscillation for malicious manufacture of routing, for the sake of the large number of forged routing messages. All of these disable the routing protocol to provide routing information for communication between the nodes in time.

SECURITY MECHANISMS AND STRATEGIES FOR AD HOC NET WORK

In the traditional network, the connection between hosts is fixed. Network adopts a hierarchical architecture and has a stable topology. And it provides a variety of services including naming and directory services, to take full advantage of the existing resources. On the basis of this, relevant security policies, such as encryption, authentication, access control and rights management, firewall, etc, have been put forward. And there is no base station or central node in Ad Hoc network. All of the nodes are mobile. Nodes are connected by wireless channel. A node can acts as a router for itself. And there are also no network services such as naming service, directory service. All this leads to the traditional security mechanism not applicable to Ad Hoc network security methods.

Currently, security mechanism proposed for Ad Hoc network mainly includes the several ways mentioned below.

(1) Authentication protocol based on password. Password-based authentication protocol inherited the ideas of the key exchange protocol (EKE). All members of the communication are involved in the generation of session key, which ensures that the final key is not only generated by a handful of people. So the interference from attackers could not stop the production of key.

(2) Safety mode based on "resurgent duck". the principle of "resurgent duck" safety mode is based on the duck take the first moving object as its mother since it hatched. Taking the same mechanism, mobile node takes the individual which give it the key first as the owner of the key, and only accept controls from the owner. But mobile nodes can still communicate with other nodes, such a mechanism just being used to limit information dissemination.

(3) Asynchronous distributed key management. The method utilizes the encryption mechanism, such as digital signature, to protect the routing information and data exchange. Each node has a pair of key. And the key management service needs the corporation of several nodes. This is mainly based on the following assumptions. In Ad Hoc networks, although there is no single node worthy of trust, a collection of nodes can be trusted. In this strategy, the method that private key updates regularly is also adopted, which make the attacker be difficult to obtain the effective key for multiple nodes at the same time.

(4) Monitoring transmitting. When a node transmits messages, the transmitting behavior of the next node will be monitored. If the next node is discovered not transmitting message or the integrity message is

destroyed, the node will be considered as malicious node. Level parameters of this node will be reduced. And the behavior will also be reported. Each node generating and maintaining a brief monitoring table which ban reflect the past behavior of other nodes, such as data lost. Thus nodes can choose the "best" routing composed those behavior good nodes.

(5) Prevention for information eavesdropping. To deal with passive eavesdropping attacks, secure socket protocol (SSL) or encapsulation security payload(ESP) mechanism can be adopted according to the actual situation. ESP can provides end-to-end encryption for those nodes not supporting encryption. It can not only encrypt the application layer data and protocol header, but also encrypt the transport layer header, which can prevent the attacker speculate the kind of application in operating. In all, ESP has a perfect property for safety.

(6) Classification for nodes according to credibility. When node searching the path, the routing security level will be set. That is to say, the minimum reliability requirements for nodes involved in the transmitting is determined. Nodes having different reliabilities use the encryption and decryption key corresponding to their reliabilities. Intermediate node can simply transmit message according to routing. Although this scheme provides the integrity protection for the transmitting of routing protocol, it can't eliminate the wrong routing information provided by malicious nodes.

ACTIVE INTRUSION CORRESPONDING PROTECTION MODEL

Described in the previous section, we know that when the intrusion detection system detects intrusions, it will invade the information distributed decision agent behavior, decision-making by the decision agent. Once you make a decision to respond to the decision-making agent will generate sniper agent. It should be noted that the active response will consume large amounts of network resources, resulting in unnecessary occupation and consumption, when less harmful intrusion at this time, you can not cause active response. Finally, the formation of a mobile sniper proxy firewall to prevent intruders to send and receive their packets.

As shown in response to active intrusion protection model that can be seen from Figure 1, when the invaders attack, intrusion detection system into the stage, and then the information to respond to an intruder decision to determine whether to respond. If the decision by the implementing agencies to implement the response, and time to monitor the effect of execution, if an intruder halfway stop the invasion, immediately stop the execution of the response. Various functions by moving the agency to implement a network intrusion detection and response capabilities, to achieve the look and block intruders, when an intrusion is detected, you can find a timely and effective manner and respond to intrusion source. After the implementation of response, to assess, evaluate the results sent back to the appropriate decisions. This is the work of the whole process protection model.

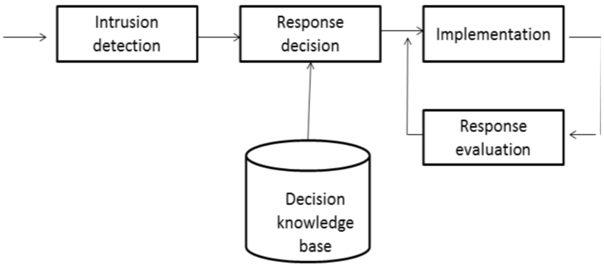

Figure 1. Active Protection intrusion response model

Mobile Firewall

As mobile ad hoc network nodes are not fixed, they can always move, and network boundaries are not very clear. Therefore, generally they do not have much effect on its firewall. To overcome this problem, researchers have designed a mobile firewall to attack the attacker. Mobile Firewall is the application of mobile communications from the principle that the aid must be between neighboring nodes in the network organization designed forwarded, if neighbor nodes refuse to forward packets, then the node will be isolated from the network, the communication can not be performed in a timely manner. This is in the security architecture which has a very important role when sniping agents surrounded by the intruder when the surrounding nodes form a mobile firewall to isolate intruders outside the network, preventing damage to the internal network structure.

Despite the formation of a solid mobile firewall, it cannot be sure that the intruder isolated intruder can be moved, resulting in the failure isolation. This requires a firewall to keep moving at all times in order to move to the path of the invaders, the invaders surrounded anytime, anywhere. To solve this problem, the designers of the mobile firewall fall into two layers, namely sniping layer and protective layer, layer by the internal nodes sniper, the main responsible role surrounded identification and isolation. Defense layer is composed of peripheral nodes, which is primarily responsible for preventing the escaped effect. Although usually used only for defense, the node will become an intruder defense sniper node timely intruder attacks when moving around the external node.

3.2 sniper agent moves

When agents discover the intruder, it will quickly produce sniper agents, and the formation of a firewall around the intruder, the intruder surrounded and isolated. In exceptional circumstances, the decision-making agency may not be intruders around, the agent intruder agency, which would take up too much channel, thus wasting network resources.

When the decision agent finds an intruder, the system in the form of a sniper agency moved to a node intruder and attacks around this quickly copying sniper proxy agent, and encircling the invaders. Finally the intruder is isolated by a mobile firewall.

CONCLUSION

Ad Hoc network is a special kind of network. The node number and type can be varied. Besides, its security measures has a high degree of flexibility, diversity and expansibility [4]. Due to the diversity of application environment and security weaknesses in Ad Hoc network, solving the security problem is very difficult. Currently, a satisfactory implementation strategy and mechanism for Ad Hoc security has not been found yet. This complicated open questions makes the future research work have a long march.

REFERENCES

Chen Z D, Kung H T, Vlah D. Ad Hoc Relay Wireless Net2 works over Moving Vehicles on Highways. ACM Special Interest Group on Mobility of Systems, Users, Data and Com2 puting . California,USA: ACM Press ,2001. 247 - 250.

Chung Weiho, Probabilistic analysis of routes on mobile ad hoc networks, IEEE. Communications Letters. 8 (2004)8 506-508.

Dai Y X, Lian Y F, Wang H. System Security and IntrusionDetection[M]. Beijing: Tsinghua Publishing Company, 2002.

will produce a large sniper decision to move to the

Garfinkel T,Matthews J,Hoff C,et al. Virtual machine contracts for datacenter and cloud computing environments[C] .Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds, ACM, New York,2009: 25-30.

J. Liu, X.B. An, C.S. Li, Principle and Application of Wireless Network Communication, Beijing, China, 2002.

Kachirski O, Guha R. Intrusion Detection Using Mobile Agents inWireless Ad Hoc Networks[C]. IEEE,July 2002:10-12.

Ljubica B, Levente B, Srdjan C, et al, Self-organization in mo2bile Ad hoc network : the approach of terminodes, IEEE Communication Magazine. 39 (2001)6 166-174.

Macker J ,Corson S. Mobile Ad Hoc Networks (MANET)[EB/OL].Http ://www. ietf . org/html . charter/manet - charter. Html,1997.

Rappaport S. Wireless communication s: principles and practice[M] . Upper Saddle River, NJ : Prentice H al l, 1995.72- 75.

Zhang Y, Lee W. Intrusion detect ion in w ireless ad hoc net works[J/ OL] . http: / / dependability. cs. virginia. edu/ bibliography/ p275- zhang. pdf , 2004-10-10.

Zhou L, Haas Z J. Securing ad hoc networks[J] . IEEE Net work Magazine, Special Issue on Network Security, 1999,13(6) : 24- 30.

Zhou Lidong, Zygmunt J Hass.Securing Ad hoc networks [J]. EEE Nerworks Special Issue on Network Security, 1999, 7(6):24～30