Journal of Applied Science and Engineering Innovation, Vol.2 No.11 2015, pp. 447-450
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

# Research for Intrusion Detection Technology of Ad Hoc Network

Jin Meng [1], Haiyan Zhao[1], Yuyang Du[1], Hui Li[1], Min Zhu[1]
[1] *Xi'an communication college, 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. Intrusion detection technology and its classification is described in this article. And based on the features of Ad Hoc network, the existing new network intrusion detection technology and its characteristics suitable for Ad Hoc network are summarized.

**Keywords** Ad Hoc network; Intrusion Detection Technology; Network security system

## 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.

Since Ad Hoc network itself has vulnerability, the research of security has already become an emphasis of studying Ad Hoc network. Intrusion detection can be defined as discerning those without authorization but using computer system illegal user and the users who have access right for system and abusing privilege. IDS(Intrusion Detection Systems) can complete real time monitoring, and sample and analyze monitoring data and judge whether it has intrusion behavior timely. As network security the second entrench line, IDS has increasingly become every security higher network indispensable part.

## 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. 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.

## IDS CHALLENGE IN AD HOC NETWORK

Intrusion detection system developed in wired network has been fairly grown, and has developed prodigious function for protecting network. But intrusion detection system structure of wired network is very hard to apply to mobile Ad Hoc network. Because there is huge difference between two networks, the research of intrusion detection system structure in mobile Ad Hoc network has faced many problems. If we want to realize mobile Ad Hoc network real safety, we have to face the following many challenges.

Wireless channel makes mobile Ad Hoc network to be very easy to suffer passivity eavesdropping, initiative intrusion, message block, message counterfeit and other ways attack. And since wireless channel bandwidth is limited, CPU computing power is lower and unable to realize fairly complicated monitoring algorithm in intrusion detection system. The monitoring algorithm not only need to adapt multiple threaten, but also has lower resource utilization rate.

In attack environment, physics protection of vagile node is relatively weaker, so intrusion detection system in Ad Hoc network should not consider hostile attack of network extern, but should consider betrayal node attack from network interior.

Since mobile Ad Hoc network has no concentrate entity, intrusion detection system in Ad Hoc network always can not collect whole system comprehensive message. It must rely on local message to judge intrusion behavior, which can increase judge difficulty of intrusion detection.

Compared with wired network, Ad Hoc network node quantity and network topology often can make transformation. Intrusion detection system in Ad Hoc system need to distinguish abnormal which is generated by normal network change, like route failure and network abnormal by spite intrusion.

## IDS CHALLENGE IN AD HOC NETWORK

Intrusion detection system developed in wired network has been fairly grown, and has developed

prodigious function for protecting network. But intrusion detection system structure of wired network is very hard to apply to mobile Ad Hoc network. Because there is huge difference between two networks, the research of intrusion detection system structure in mobile Ad Hoc network has faced many problems. If we want to realize mobile Ad Hoc network real safety, we have to face the following many challenges.

Wireless channel makes mobile Ad Hoc network to be very easy to suffer passivity eavesdropping, initiative intrusion, message block, message counterfeit and other ways attack. And since wireless channel bandwidth is limited, CPU computing power is lower and unable to realize fairly complicated monitoring algorithm in intrusion detection system. The monitoring algorithm not only need to adapt multiple threaten, but also has lower resource utilization rate.

In attack environment, physics protection of vagile node is relatively weaker, so intrusion detection system in Ad Hoc network should not consider hostile attack of network extern, but should consider betrayal node attack from network interior.

Since mobile Ad Hoc network has no concentrate entity, intrusion detection system in Ad Hoc network always can not collect whole system comprehensive message. It must rely on local message to judge intrusion behavior, which can increase judge difficulty of intrusion detection.

Compared with wired network, Ad Hoc network node quantity and network topology often can make transformation. Intrusion detection system in Ad Hoc system need to distinguish abnormal which is generated by normal network change, like route failure and network abnormal by spite intrusion.

## INTRUSION DETECTION TECHNIQUE IN AD HOC NETWORK

At present, traditional wired network intrusion detection technique research is sufficient and wide range. But the IDS research for traditional wired network can not directly be used in wireless Ad Hoc network. Wireless Ad Hoc network lacks fixed base installation. Physical layer facility is deficient. Wireless Ad Hoc network itself vulnerability makes it to be easier to suffer attack, which bring more challenge and requirement for IDS design.

Since it lacks a centralized control node, which is similar to gateway and router, wireless Ad Hoc intrusion detection technique suffers restrict of every node flow. Moreover, distributed character of wireless Ad Hoc network itself requires intrusion detection technique to adopt an appropriate distributed algorithm. At the same time, we need to consider node bearing maximum flow in practical application. Since wireless Ad Hoc network has dynamic topological structure, every node can flexible migration which makes node to be easy to be capture to threat whole network safety. For saving limited bandwidth resource, wireless Ad Hoc network every node can not be like node in wired network to liberty communication any time any where. Thus, bandwidth and battery capacity further restrict IDS design of mobile network.

**Qualified IDS require of Ad Hoc network.** Qualified IDS system in mobile network must use as little as possible spending to accomplish correctly detecting intrusion behavior as far as possible. When we design IDS in Ad Hoc network, we should satisfy the following conditions to avoid unlawful intrusion.

(1) IDS can not introduce new loophole to network, and bring new security problem.

(2) IDS can not consume system too many resource, and affect normal node work.

(3) IDS should have advanced fault tolerance to recovery original data after system crash.

(4) IDS should have high reliability, false alarm rate and missing report rate is lower.

(5) IDS should adopt distributed structure.

(6) IDS should uninterruptedly and continue efficiently detect.

(7) IDS should use IDWG established intrusion detection exchange protocol IDXP that standardization intrusion detection message interchange format makes multiple intrusion detection scheme interplay.

**IDS system analysis of available Ad Hoc network.** Considering network node processing capacity, energy consumption, travel frequency and other factors, we divide Ad Hoc network into some clusters. In one cluster, every node can make direct communication with one jump any node. But when it exceeds one jump range, it must make communication through cluster head node. In the meanwhile, if distance of two nodes without one cluster is only one jump, it must make communication through cluster head node.

Multiple distributed intrusion detection system based on cluster is composed by interface module, local data collection module, mobile agent platform module, mobile agent module, analysis engine module and response module.

Communication interface module adopts general standard definition to compatible other standard definition intrusion detection system and offer cooperative work basis. Local data collection module is responsible for different data origin collecting audit data flow from locality. Mobile agent platform module is used to safely transfer mobile agent module, which supports TCP/IP protocol currently. Mobile agent module is responsible for collecting and treating data from other cluster. Response module of global analysis engine module can generate alarm information and chain scission operation of suspicious link.

Survivability is the meaning that when system is break down, accident or attack, system has accurately complete reserve basic task capacity timely. The architecture is divided as function into three layers, like driver layer, control layer and executive layer. In driver layer, it adds data recovery engine to improve system survivability based on currently intrusion feature analysis method. In control layer, it makes modular design to realize the layer portability from engineering technology. In executive layer, it uses new cluster head choice algorithm to vastly reduce system resource cost and improve system survivability.

The method improves system flexibility, and reduces system complex degree. Adopting agency technology and self-learning technology can improve network survivability. Dispersing monitoring agency and decision agency into a few dynamic chosen nodes can reduce whole network resource cost and enhance intrusion detection system efficiency, and improve network survivability to some extent.

Since anomaly detection algorithm has higher false alarm rate and misusing detection algorithm detection territory limited can not well apply network structure constant change. Mixture intrusion detection is based on rule matching, it statistically analyze network abnormal time rate without attack to set system design threshold to avoid false alarm rate and fail to declare. In data analysis aspect, if a series of anomalous events all show as the same attack feature and arisen probability in unit time is higher than threshold, it would judge as one attack. The algorithm not only can improve detection veracity, but also has no obvious effect for network performance, including data package transfer time and system response time.

## CONCLUSION

With the mobile Ad Hoc network widespread use, Ad Hoc network security problem has the significance. Dynamic state topological structure based on Ad Hoc network, limited wireless transmission bandwidth, mobile node finiteness and network distributed and other characteristics, this paper summaries research result of domestic and overseas about Ad Hoc network intrusion detection technique, and analyzes every kind of detection technique character and relative merits to have some certain referential meaning for research of Ad Hoc network intrusion detection technique theory and practice in future.

## 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.

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.

Zhou L D, Hass Z J. Securing Ad Hoc networks[J]. IEEE Nerworks Special Issue on Network Security, 1999, 7(06):24-30.