모바일 Ad Hoc 네트워크를 위한 안전한 침입 탐지 시스템

Rakesh Shrestha*, 이상덕**, 최동유***, 한승조****, 이성주*****

A Secure Intrusion Detection System for Mobile Ad Hoc Network

Rakesh Shrestha*, Sang-duk Lee**, Dong-you Choi***, Seung-jo Han****, Seong-Joo Lee*****

이 논문은 2008년도 조선대학교 교내연구비를 지원받았음

요 약

침입 탐지 시스템은 무선 네트워크에서 활발한 연구 분야중의 하나이다. 네트워크 토폴로지가 있기 때문에 무선 모바일 Ad-hoc 네트워크의 침입 탐지는 동적과 집중화 부족의 공격을 받기 쉽다. 참가하고 있는 노드가 앞의 보안 연합을 가지고 있지 않고 열려 있는 Ad-hoc 네트워크의 악의적인 노드의 탐지는 이 논문에서 묘사하는 숫자에 직면한다. 이 논문이 모바일 Ad-hoc 네트워크의 중요한 조건에서 악의적인 노드를 결정하는 것에 대해 있고 보안과 더 좋은 실행과 침입의 탐지로 끝나는 취약점 이슈를 다룬다.

ABSTRACT

The intrusion detection system is one of the active fields of research in wireless networks. Intrusion detection in wireless mobile Ad hoc network is challenging because the network topologies are dynamic, lack centralization and are vulnerable to attacks. Detection of malicious nodes in an open ad-hoc network in which participating nodes do not have previous security association has to face number of challenges which is described in this paper. This paper is about determining the malicious nodes under critical conditions in the mobile ad-hoc network and deals with security and vulnerabilities issues which results in the better performance and detection of the intrusion.

키워드

Intrusion detection, Mobile ad-hoc network, IDS technique

Ⅰ. Introduction

MANET is the abbreviation of mobile ad-hoc network which is a kind of wireless ad-hoc network, and is a self-configuring network of mobile nodes and associated hosts connected by wireless links. Some of the characteristic features of MANET are the nodes are free to move randomly i.e. they have high mobility, organize themselves arbitrarily,

* 조선대학교 정보통신공학과 석사과정
** 조선대학교 정보통신공학과 박사
*** 조선대학교 정보통신공학과 전임강사
**** 조선대학교 정보통신공학과 교수
***** 조선대학교 컴퓨터공학과 교수 (교신저자)

접수일자 2008. 07. 16

dynamic network topology and hence they have decentralized network control. Such a network may operate in a standalone fashion, or may be connected to the larger network and consume very low power and resources. One of the differences between fixed wired and mobile wireless networks is that mobile nodes have a very limited bandwidth and battery power because efficient host-based monitoring requires large amounts of CPU processing power, and hence is energy consuming.

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are out of range use other nodes as relays or routers. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band, and follow the same hopping sequence or spreading code. The data-link-layer functions manage the wireless link resources and coordinate medium access among neighboring nodes. There are various applications of ad-hoc networks like emergency search-and-rescue missions, military, data collection etc. The following flowchart depicts the working of any general ad-hoc network.

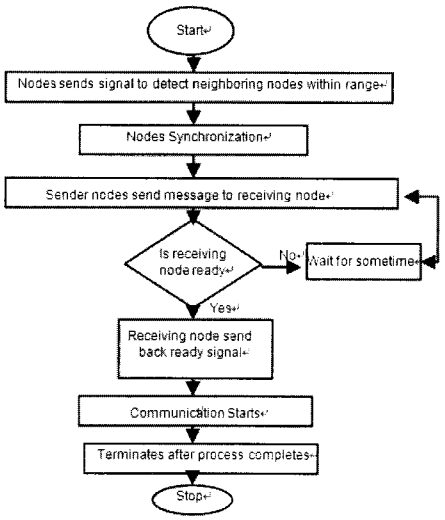

그림. 1. Ad-hoc 네트워크의 일반적인 활동
Fig. 1. Working of a general Ad-hoc network

1.1 Vulnerabilities in MANET

The very advantage of mobility in MANET leads to its vulnerabilities. But the inherent nature of the wireless medium makes it susceptible to variety of security attacks ranging from passive eavesdropping to active interference. The wireless intrusion detection system is more complex than wired systems. Authentication mechanisms are not sufficient and effective against internal attacks as the secret key is compromised when its node is compromised. In order to secure MANET, we need a second line of defense to detect the intrusions. For this purpose, Intrusion Detection Systems (IDS) are deployed to identify any set of actions that compromise the integrity, confidentiality and availability of resources. [1, 2]

Ⅱ. Intrusion detection system

An IDS is a software or hardware tool used to detect unauthorized access of a computer system or network. An intrusion attempts to access information, or manipulate information causing a system unreliable or unusable. Intrusion detection involves capturing audit data and reasoning about the evidence in the data to determine if the system is under attack or not. Depending on the scope of protection or deployment and according to audit data used, IDS can be classified as network-based or host-based. Again, depending upon the detection model IDS is usually classified in one of two ways, with either signature-based or anomaly based detection. The anomaly detection observes the flag activities and if it is deviated from the normal activity profile then an anomaly alarm will be raised indicating possible intrusion and can identify the statically significant amounts of intrusion attempts. The basic idea behind misuse detection strategy is that the attacks are represented in the form of a pattern or a signature so that even variations of the same attack can be detected. [3]

2.1 Difficulties faced by current IDS techniques

The intrusion detection technique which is developed for wired network environment has to face many problems

when implementing these techniques in the MANET. Further, the available audit trace will be limited within the radio range and it often adopts disconnected operations. A node that has been compromised or that has been temporarily out of sync due to volatile physical movement may send out false routing information as a consequence it may be difficult for the intrusion detection to distinguish false alarms from real intrusions. So for developing a good intrusion detection system for MANET one should focus on the appropriate audit data sources and system architecture that fits the feature of mobile ad-hoc networks.

III Improved intrusion detection system architecture

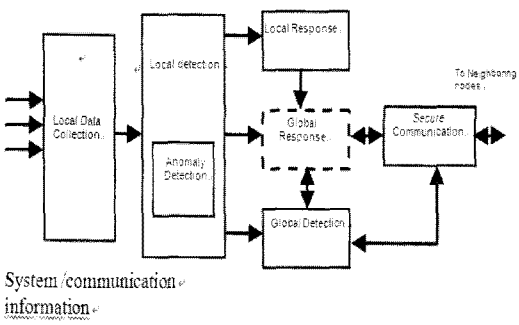

그림. 2. 침입방지 시스템의 아키텍처
Fig. 2. Intrusion detection system architecture

The intrusion detection and response system used in the mobile ad-hoc network should be both distributive and cooperative for better performance. This architecture is the improved architecture of Y. Zhang and W. Lee. Each IDS agent runs independently and monitors local activities. It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. But in this case no further investigation is done after local response.

The presented IDS architecture consists of six modules. The individual IDS agents are placed on each and every node which detects intrusions from local traces and initiates response. [4]

Algorithm for Intrusion Detection System:

- Inputs: The packet related information like System data, communication data, user data and network traffic related information are collected as inputs. It mainly uses statistical data processes from the packet information.
- Local Data Collection: The real time audit data from various sources is collected at the local level in a distributed manner. Each node IDS component will gather relevant data from network traffic, these data includes the user and system activities within the mobile node as well as the communication activities within the radio range of the node.
- Local Detection: The local detection engine examines the local data traces gathered by the local data collection module for evidence of anomalies. It can include both misuse detections as well as anomaly detections. Anomaly detection engine plays a greater role for newly created attacks on MANET networks. [3]
- Local Response: The type of intrusion response depends on the type of intrusion, the type of network protocols and the confidence in the authenticity of the audit trace data. According to the Local Detection, appropriate response should be made such as reinitializing communication channels between nodes, identifying compromised nodes and reorganizing the network to omit the promised nodes. It can also send a re-authentication request to all the nodes in the network to prompt the end users to authenticate themselves and those nodes which negotiate new communication channels is regarded as legitimate node. In case of Y. Zhang and W. Lee, after local response there is no further processing of information is done to detect the intrusion in the ad-hoc network. Here, after local response is done, it is sent to the global response module for further processing of the gathered information for re-conformation decision of intrusive data. [4, 5]
- Co-operative or Global Detection: If local data cannot fully support a decision and needs broader investigation then global or co-operative detection is initiated. If

anomaly detected is inconclusive and there is confusion about the local data or the local response data then neighboring IDS agents will co-operatively participate in global intrusion detection action. The information from the neighboring nodes is gathered through the secured communication channel. The objective of using collaborative decision making is to include information from different nodes in the decision making so as to make more accurate derision.

- Global Response: Once a global response is recommended for a detected intrusion, each node IDS components must communicate with other nodes to initiate and follow-through with action. When it detects intrusion with strong evidence, then the node can conclude intrusion happened and then initiate an alarm response.
- Secure Communication: In some cases, we may need to exchanged between node IDS in a secure manner. The communication relies on network protocols to exchange data and collaborate in intrusion decision making. Such protocols need to be secure and robust. [6]
- Output: It detects the intrusion in the mobile ad-hoc network and gives the response. Some of the methods can also detect the types of attack and the location of the intruder.

Ⅳ. Testing intrusion detection systems

Intrusion detection can be tested either by using actual attacks or by using predefined attack scripts. It is complicated and costly to collect a large set of attacks scripts for the purposes of IDS testing, a possible option is to use attack traces instead of real attacks. Such traces usually consist of files containing a network packets or systems log that corresponds to an instance of an attack. We need a better understanding of the advantages and disadvantages of replaying such traces as a part of an IDS test. DSR protocol is a suitable approach for mobile networks and all around data load environments. Here, in this experiment, the DSR protocol has been implemented in all the mobile nodes. [7]

Ⅴ. Simulation of intrusion

Network simulation can be done either in real environment or in experimental environment. Detecting and analyzing of intrusive activities in the real time scenario is difficult as the background traffic is realistic in nature. Real time scenario has some of the problems like risk of exposure of the testing environment during simulation from the internet and the normal system operation could be interrupted or compromised by the simulated attacks. Due to the high risks in the real environment most of the tests are performed in the experimental environment using simulation scripts and collecting real environment data and replicating in the simulated environment. [8, 9]

Ⅵ. Approach to simulation

The simulation tool we have used is OPNET a commercial network simulation package. OPNET provides a GUI for the topology design that has a performance data collection and various display modules and allow realistic simulation of networks. OPNET provides realistic analysis of performance measures and the effectiveness of intrusion detection.

6.1 Simulation environment

The simulation is done within the OPNET simulator. Our simulation model consists of 16 mobile nodes which are placed randomly and each mobile node runs on DSR routing protocol with in the area of 500m × 500m office network area. Each node has a radio propagation range of less than 300meters and the channel capacity implemented is 11Mbps. Among the sixteen mobile nodes 2 mobile nodes are used as malicious nodes for testing. The source and destinations are randomly selected and the simulation is run for 15 minutes or 900 sim seconds. The summary of the statistics is given in the table 1 below.

표 1. 시나리오 통계
Table 1. Scenario statistics

Statistics	Value
Scenario size	500m × 500m
802.11b data rate	11 Mbps
Transmission Range	<300 meter
Simulation Time	15 minute
No. of mobile nodes	16

6.2 Building network model

There are 16 mobile nodes placed randomly within the Office Network which communicate with each other with low quality video conferencing as shown in Fig. 3. In our model, Mobile node 2 and mobile node 4 are considered as an intruder which attacks mobile node 1 and mobile node 6 respectively as in Fig. 3. The intrusion packet is self generated in the task configuration which attacks to the victim node and these tasks are assigned to the attack nodes. TCP traffic is generated in the user defined task configuration. Basically, the nodes communicate with each other randomly however mobile node 0 and mobile node 1 tries to communicate with the mobile node 6 and in the same way mobile node 6 tries to communicate with these nodes. Here, the mobile nodes 1 and mobile node 6 are the victim nodes of the attacker nodes 2 and 4 respectively. The entire data communication pattern can be seen with help of the arrows which is a built in function of DSR route.

We can see the data transmission between the nodes by enabling the DSR record route in the Global attributes of the discrete event simulation. Since low quality video conferencing is done between the mobile nodes, we can take this traffic as normal behavior and record this traffic in the audit data.

First, all the traffics are collected by the data collection module and are analyzed by the detection module. Those node traffics which try to enter the system of the mobile nodes that has unusual behavior than the normal behavior are regarded as the intrusive activity and the nodes are viewed as intruder nodes. Before starting the simulation all the variables should be checked if they are correctly inserted and are related with the task configurations. This traffic can not be repeated more than once and therefore the attack traffic is present only once for the victim node.

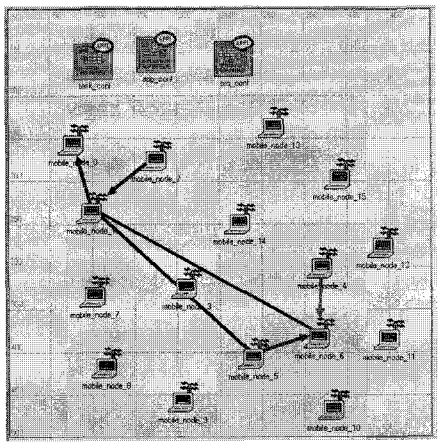

그림. 3. 시뮬레이션 시나리오
Fig. 3. Simulation scenario

Ⅶ. Analysis of simulation results

The simulation is executed and the results are obtained and compared the results with those expected. We setup several statistical measures in OPNET to study the performance of the intrusion simulation. The simulation has been run for several times and similar results have been obtained and these are discussed as follows.

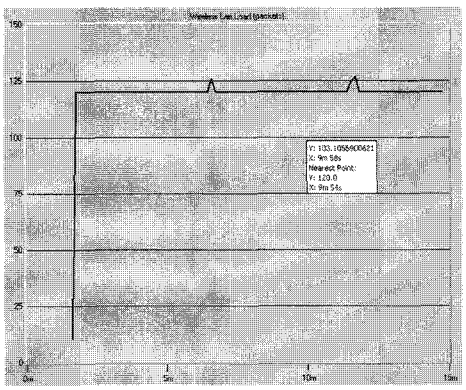

그림. 4. 공격전의 모바일 node 1 올림
Fig. 4. Load on the mobile node 1 before attack

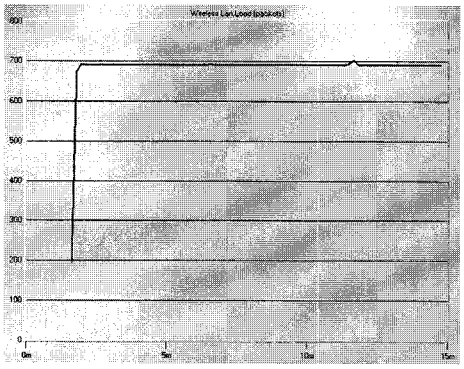

그림. 5. 공격 후의 모바일 node 1 올림
Fig. 5. Load on the mobile node 1 after attack

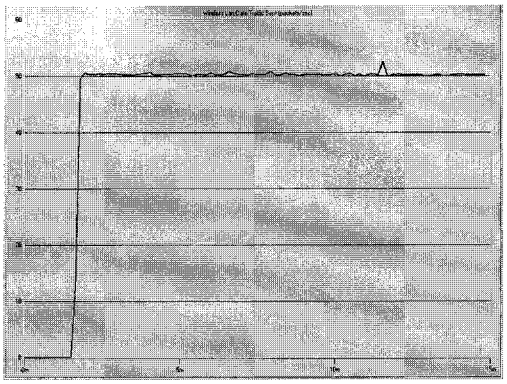

그림. 6. 공격전의 데이터 트래픽
Fig. 6. Data traffic before attack

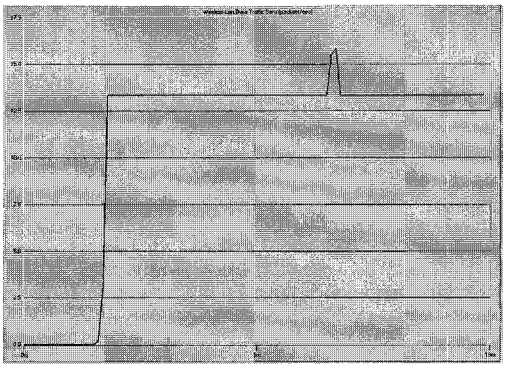

그림. 7. 공격후의 데이터 트래픽
Fig. 7. Data traffic after attack

Initially, the packet load on the mobile node is nearly 125 packets as shown in Fig. 4 but after the attacking node 2 attacks the mobile node 1 the result is that the packet load on the mobile node 1 is increased nearly up to 700 packets as shown in Fig 5. This is due to the TCP packet sent from the attacking node 2. As a result, the victim node is flooded with TCP packets which results in slow processing of certain services in the victim node. The detection system in the victim node can match the attack with the defined rule. If the attack does not match with the defined rule then it is regarded as abnormal behavior and the node is regarded as malicious node otherwise it is a normal node. If there is confusion whether the node is malicious or not then co-operative detection scheme is used. After detection of the intruder node, a response is given by the response module by sending an alarm message to the system. It is sent to the global response system for further response.

While analyzing the data traffic sent by the node 1 before the attack, the packet sent per second is as much as around 50 packets as in Fig.6 but while doing the simulation with the intruders the sent data traffic of the same node drops to around 14 packets as shown in Fig 7. Hence, there is data traffic congestion due to the attack in the node which reduces the performance of the mobile nodes. The intrusion detection technique present in each node can detect the intrusion during the communication between the different mobile nodes. Hence, providing a secure detection system for mobile ad-hoc network.

Ⅷ. Conclusion and future work

In this paper, experimental results of network intrusion simulation using the low quality video conferencing as the know data traffic sources between mobile nodes is presented. An attack is generated in the task configuration in order to attack the mobile nodes by using OPNET tools. The intruder nodes are detected and identified by the suspicious behavior in the target node. The various performances of the mobile nodes are evaluated and the malicious behaviors of the nodes are detected by using anomaly IDS utilizing adaptive threshold algorithm which looks for different traffic volume variables and packet sizes. It sets a threshold after determining the average traffic and then compares the incoming traffic to the threshold generating an alarm if it is

crossed.. The detection of the intruder node intends to provide a functional and feasibility validation for our design, which is flexible in detecting attacks. The designed IDS seem to have good response in the small number of nodes usually located near each other.

As a future work, we will try to import predefined traffics as well as attacks in the OPNET simulator and try to analyze their effect in the MANET nodes which can be obtained from sources like SNORT, TCPDUMP, NMAP, NESSUS etc. We have planned to do simulation on increased mobile nodes as well as try to find out the effect of the mobility while implementing IDS on the mobile nodes.

References:

[1] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in Mobile Computing and Networking, pp. 275 - 283, 2000.

[2] Slobodan Petrovic. Vulnerabilities in wireless networks and intrusion detection.

[3] Yi-an Huang.Anomaly Detection forWireless Ad-Hoc Routing Protocols. A thesis submitted to the Graduate Faculty of North Carolina State University in partial fulfillment of the requirements for the Degree of Master of Science COMPUTER SCIENCE Raleigh, 2001.

[4] Yongguang Zhang Wenke Lee and Yi-an Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks. Kluwer. 2003. ACM/Kluwer Wireless Networks Journal, Sept; 9(5):545-56 ,2003.

[5] Jeff Dixon. Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy, 2006.

[6] Zheng Yan. Security in Ad Hoc Networks Networking Laboratory Helsinki University of Technology, 2002.

[7] Agustin Zaballos, Alex Vallejo, Guiomar orral, Jaume Abella. Ad-Hoc routing performance study using OPNET Modeler University Ramon Llull(URL-La Salle Engineering) Barcelona Spain, 2006.

[8] Guiomar Corral, Agustin Zaballos, Jaume Abella, Carlos Morales. Building an IDS using OPNET. Enginyeria i Arquitectura La Salle, Universitat Ramon Llull, Spain, EUROPE, 2005.

[9] Shabana Razak, Mian Zhou, Sheau-Dong Lang. Network Intrusion Simulation Using OPNET. University of Central Florida, Orlando, FL 32816, 2002.

※ This study was supported by research funds from chosun university, 2008.

저자소개

Rakesh Shrestha

2007년 Tribhuvan University electronics and communication(학사)
2008년 조선대학교 정보통신학과 (석사 입학)
※관심분야 : IDS, Mobile Ad-hoc Network, Security

이상덕 (Sang-duk Lee)

1997년 조선대학교 전자공학과 (학사)
1999년 조선대학교 전자공학과 (공학 석사)
2008년 조선대학교 전자공학과(공학 박사)
※관심분야 : 네트워크 보안, 임베디드

최동유 (Dong-you Choi)

1999년 2월 조선대학교 전자공학과 졸업 (공학사)
2001년 2월 조선대학교 대학원 전자공학과 졸업 (공학석사)
2004년 8월 조선대학교 대학원 전자공학과 졸업(공학 박사)
2004년 9월 ~ 2005년 6월 에너지 자원신기술연구소 전임연구원
2006년 3월 ~ 2007년 2월 청주대학교 이공대학 전자정보공학부 전임강사
2007년 3월 ~ 현재 조선대학교 전자정보공과대학 정보통신공학부 전임강사
※관심분야 : 전파전파, 이동통신, 통신 및 회로시스템

한승조 (Seung-jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학 석사)
1994년 충북대학교 전자계산학과(공학 박사)
1986년 6월~1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 : 택사스대학 객원교수
2000년 12월~2002년 3월 : 버클리대학 객원교수
1998년 3월~현재 : 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제 방지시스템, ASIC 설계

이성주 (Seong-Joo Lee)

1993년 광운대학교 전자계산학 (이학석사)
1994년 대구 카톨릭대학교 전자계산학 (이학박사)
1988년~1990년 : 조선대학교 전자계산소 소장
1995년~1997년 : 조선대학교 산업대학장
1981년~ 현재 : 조선대학교 컴퓨터공학부 교수
※관심분야 : 소프트웨어 공학, 프로그래밍 언어, 러프 집합