MANET에서의 전파방해 공격 탐지

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

Detecting Jamming Attacks in MANET

Rakesh Shrestha*, Sang-duk Lee**, Dong-you Choi***, Seung-jo Han****
****Corresponding author: Seung-jo Han

이 논문은 2008년도 조선대학교 교내연구비를 지원받았음

요 약

모바일 Ad-hoc 네트워크는 재해지역이나 빠른 구성을 필요로 할 때 중앙 집중 구조 형태가 없는 통신을 제공하여 준다. 반면에 악의적인 공격과 사전 보안 측정 부족으로 인한 개방형 Ad-hoc 네트워크 구조에 때문에 다른 계층에서 문제에 직면할 수 있다. DOS공격은 전파 전송 채널에서 방해를 하는 공격중 하나이며 전파방해 공격으로 알려져 있다. 이러한 종류의 공격은 공격자가 패킷을 방해하는 신호를 보내고 패킷이 전송되는 동안 많은 에러와 심각한 문제를 발생시킨다. 그 결과 이러한 종류의 공격을 방지하기 위한 방법이 요구된다. 따라서 본 논문에서는 네트워크 시뮬레이터인 OPNET을 활용하여 DoS 공격과 각 노드 상에서 전파방해 공격 시뮬레이션을 수행하였고, 모바일 Ad-hoc 네트워크에서 전파방해에 의한 채널 접근을 방해하는 공격에 대해서 분석하였다. 우리는 효과적인 이상적 분석 탐지 시스템 사용하여 방해전파 노드의 악의적인 행동을 탐지하고 모바일 Ad-hoc네트워크에서 전파방해 중에 부정적인 채널의 접속한 결과를 분석하였다.

ABSTRACT

Mobile Ad-hoc Networks provide communication without a centralized infrastructure, which makes them suitable for communication in disaster areas or when quick deployment is needed. On the other hand, they are susceptible to malicious exploitation and have to face different challenges at different layers due to its open Ad-hoc network structure which lacks previous security measures. Denial of service (DoS) attack is one that interferes with the radio transmission channel causing a jamming attack. In this kind of attack, an attacker emits a signal that interrupts the energy of the packets causing many errors in the packet currently being transmitted. In harsh environments where there is constant traffic, a jamming attack causes serious problems; therefore measures to prevent these types of attacks are required. The objective of this paper is to carry out the simulation of the jamming attack on the nodes and determine the DoS attacks in OPNET so as to obtain better results. We have used effective anomaly detection system to detect the malicious behaviour of the jammer node and analyzed the results that deny channel access by jamming in the mobile Ad-hoc networks.

키워드

Denial of Service, Mobile Ad-hoc Networks, IDS, Wireless Jamming

* 조선대학교 정보통신공학과 석사과정
** 조선대학교 정보통신공학과 박사
*** 조선대학교 정보통신공학과 조교수
**** 조선대학교 정보통신공학과 교수 (교신저자)

접수일자 2008. 09. 29

Ⅰ. Introduction

The Ad-hoc networking capabilities become essential in delivering overall next generation wireless network functionalities. A mobile Ad-hoc network is a peer to peer mode of communication without having a fixed infrastructure. MANET is a multi-hop wireless network capable of autonomous operation. The mobility of MANET nodes can lead to frequent and unpredictable topology changes. Routing from one node to another on such a "mesh" network typically uses on-demand routing protocol, which generates routing information only when a station initiates a transmission. MANETs are those nodes that are free to move randomly, have high mobility, organize themselves arbitrarily, dynamic network topology and hence they have decentralized network control. They may operate in a standalone fashion, or may be connected to the larger network and consume very low power and resources. The mobile nodes are energy consuming because they have a very limited bandwidth and battery power in addition an efficient host-based monitoring requires large amounts of CPU processing power.

Jamming is a kind of DoS attack which denies the service to valid users by generating noise or fake protocol packets. The jammer disrupts the wireless transmitting or receiving nodes by generating a continuous high power noise across the entire bandwidth. Generally, jammers are used in military with the purpose of generating noise to bring down the enemy network. Also it can be used to interrupt the critical communications or commercial hotspots or even wireless implemented classrooms or offices. The MANET node model is based on 802.11 wireless MAC protocol which listens before they transmits, if the medium is not clear it will postpone for a defined amount of time and then perform the CSMA/CA once again to listen for a clear medium before transmitting. But if there is continuous jamming signal that is constantly heard during the CSMA/CA intervals, the signals completely seizes until there is no signal present. The jamming in the wireless networks can be realized by generating continuous high power noise in the neighborhood of wireless receiver nodes. In this paper, the jamming is introduced within from the network itself.

Ⅱ. Related Work

Security in Ad-hoc network is one of the essential part to protect the wireless network which is discussed in [1, 2]. Zhang and Lee discussed about the possible attacks in different layers and also discussed about the few of the possible solution and detection of those types of attacks. In [3], the authors introduced various types of jamming attacks including intelligent jamming attacks in the 802.11b wireless networks and focused on the energy efficiency of the jamming attacks.

Ⅲ. Difficulties in MANET

The wireless prevention techniques such as encryption, using password or biometrics are the first line of defense and are not sufficient in MANET due to its decentralized structure. DoS attacks flood the network with so many additional requests that the regular traffic is either slowed down or completely interrupted for some period of time. The DoS attacks cause disabling of service, exhaustion, service degradation and sometimes non-availability of the network infrastructure. Due to MANET's open network several types of DoS attacks can harm the normal operation of the nodes. Hence, IDS can be used as second wall of defense to protect the network systems. In general, DoS attacks are difficult to prevent and protect in wireless networks. According to V. Gupta ,S. Krishnamurthy and M. Faltous [4] some of the attacks like DoS attack keeps the channel busy at the surrounding of the node and results drainage of the battery life by continuous relay of bogus data at the MAC layer. The difficulties in Ad-hoc networks are discussed in [2]. Solving the problems will heighten the security fence of Ad-hoc networks a step

further than current IDS.

Ⅳ. Intrusion Detection System

Wireless communication is very vulnerable to different kinds of attacks. An intrusion detection system (IDS) is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. IDS involves capturing audit data and analyzing about the evidence in the data to resolve if the system is under attack or not. Depending upon the detection model IDS is usually classified in one of two ways, with either signature-based or anomaly based detection.

In our model, anomaly detection model is implemented within the MANET node module, where the normal behavior of each node is recorded as the audit report. Each node monitors the network which captures the traffic, creates the list of evidences and analyses them. These events include the number of packets send, idle periods, the number of corrupted packets etc. All the neighboring nodes communicate with each other and share as well as match those event lists which help them to distinguish between normal behavior and jamming attacks. This jamming attack results in the loss of large number of packets that are sent by the source to the destination node. The monitor placed in the source can see the frames sent on the channel where as that in the receiving node can not see anything. The sender will retry the transmission several times which is analyzed by the monitor within itself. By analyzing the evidences of both the source and destination's monitors it can detect any activities different from normal activities as an intrusive attack in the network and activates the intrusive alarm after iterative procedure of analysis.

Ⅴ. Simulation of Traffic Models

The simulation is carried out in OPNET which is a commercial network simulation tool with GUI interface [5]. The Fig.1 shows the simulation used in this paper to study the effect of jamming attacks on the networks consisting of 20 similar nodes stations and a jammer node. All the nodes use DSR as a routing protocol within the area of 100m x 100m office network. DSR protocol is a suitable approach for mobile networks and all around data load environments [6].

The node model of the jammer consists of a source and transmitter. The source model is used to generate jamming signals and the transmitter is used to transmit the signal to the neighboring nodes at a suitable frequency and bandwidth. All the packets are transmitted with adequate power so that there is never packet loss due to signal strength. For this simulation we assume that the jammer node have unlimited energy.

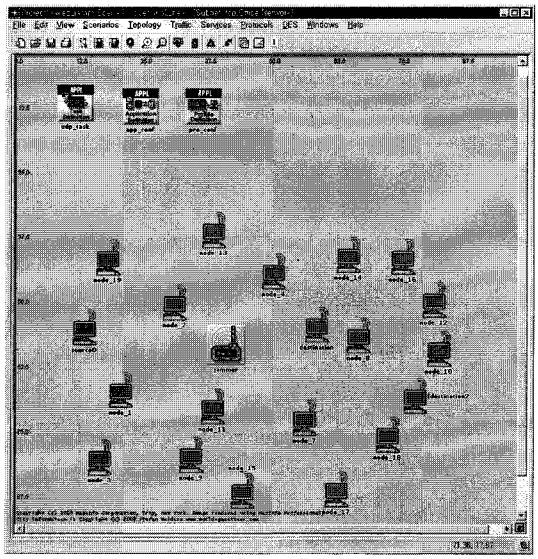

그림. 1. 시뮬레이션을 위한 실험적인 셋업
Fig. 1. Experimental setup for simulation

There is one source node and two destination nodes viz. destination and node_5 but for simplicity only source and the destination node is considered here. The simulation is run for 220 seconds and the results are analyzed. The summary of the simulation statistics is given in table 1.

표. 1. 시나리오 통계
Table 1. Scenario statistics

Statistics	Value
Scenario size	100mx100m
802.11b data rate	11 Mbps
Transmission Range	<250 meter
Power of each nodes	0.005W
Modulation	dpsk
Simulation Time	220
No. of nodes	20
No. of Jammer nodes	1

The wireless lan transmitter attributes are shown in table 2 which is self explanatory.

표. 2.노드 송신자 특성
Table 2. Node transmitter attribute

Attributes	Value
data rate (bps)	1,000,000
packet formats	ip_datagram_v4, UDP_dgram, tcp_seg
bandwidth (KHz)	100,000
Minimum frequency(MHz)	2401
Modulation	dpsk
Power (W)	0.005
bit capacity (bits)	infinity
spreading code	disable

VI. Analysis and Simulation Result

In our simulation, custom applications have been used with a streaming multimedia of packet size 1470 which starts at around 100 sec. We have used two simulation scenarios one without the jammer and the other with the jammer node. The given Fig. 2 show the first scenario with UDP traffic before the Jammer node between the source and the destination node. Here, we have disabled the jammer node as if there is no jammer node during simulation. The same UDP traffic that is sent by the source node is received by the destination node before the jammer node is enabled.

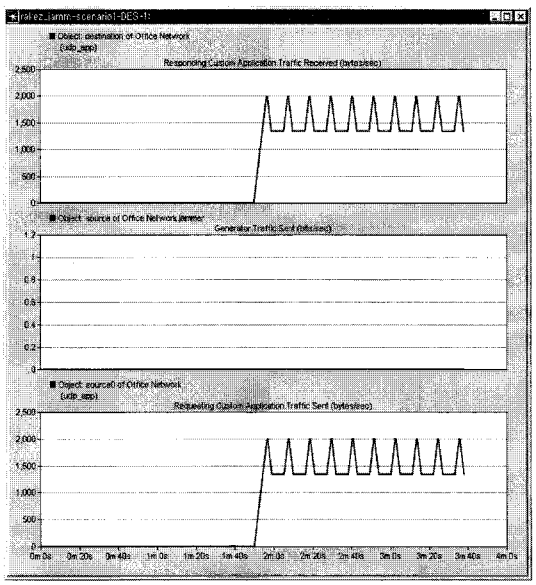

그림. 2. 전파방해공격 전의 트래픽
Fig. 2. Traffic before jamming attack

In the second scenario, the jammer node is enabled in between the source and the destination nodes . As soon as the jammer node is active it jams the signals so that the receiver node is unable to receive any messages sent by the source node which can be seen in Fig. 3. It is because the destination node first listens to the valid signal before transmission. This jammer node denies the service between the source and the destination node of the network causing disruption in the network. As mention in section 4, each monitoring node collects the network traffic of its surrounding nodes and then tries to compare the evidences of the traffic before and after the attack.

If there is no difference between the compared evidences then it assumes as a normal behavior. But if there is change in the evidence of the traffic collected between the nodes then according to the audit report, it declares the anomalous behavior as the intrusive behavior.

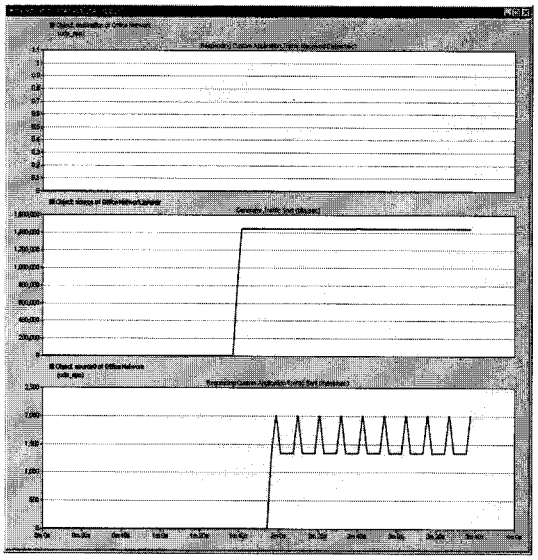

그림. 3. 전파 방해 이후의 트래픽
Fig. 3. Traffic after Jamming attack

The Fig. 4 shows the throughput at the destination node before the jamming attack. The receiver and the transmitter port of the source is always busy which shows that there is sending and receiving traffic.

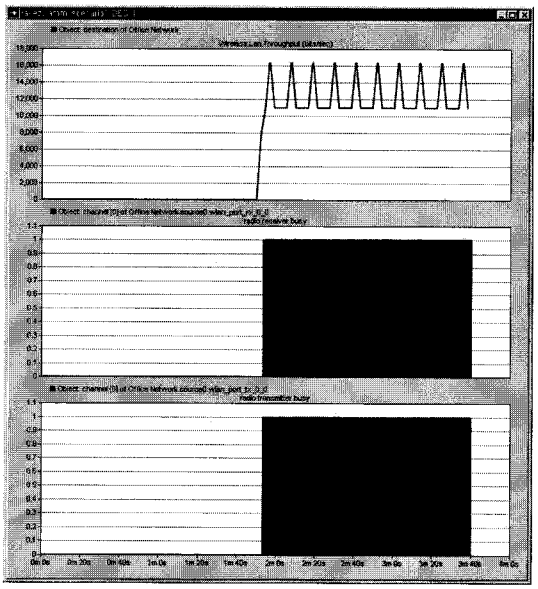

표. 4. 전파방해 공격전의 트래픽 처리량
Fig. 4. Traffic throughput before jamming attack

The Fig. 5 shows the throughput traffic of the destination node after the introduction of the jamming attack. The upper graph shows that the jammer lowers the traffic at the destination node to zero; the middle graph shows that the nodes is listening so it is busy. And the last graph shows that the source node cannot transmit any packet due to jamming. The jammer is constantly sending packets, the destination is forced to receive all of them trying to decipher but since the packets are useless it drops the packets.

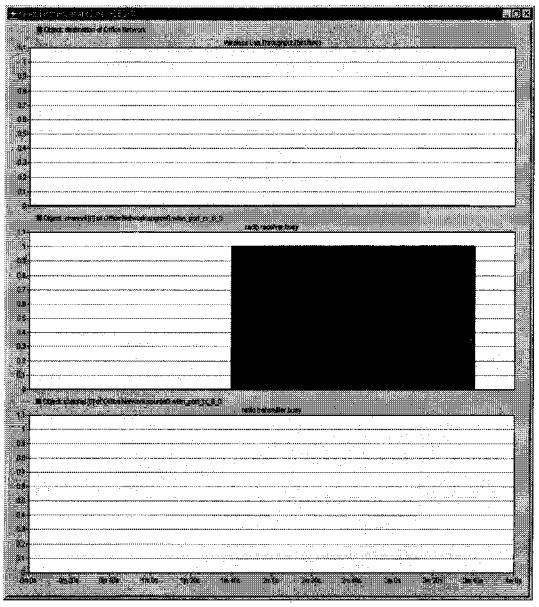

표. 5. 전파방해 공격이후의 트래픽 처리량
Fig. 5. Traffic throughput after the attack

Ⅶ. Conclusion

Hence, we studied the issue of detecting the jamming attacks and examined the evidence collected by each node and identified the presence of jamming attack. We obtained the result as our expectation when the jammer node is introduced. The jamming attack disrupts the data transmission between the nodes as well as the receiving nodes are prevented from receiving the data sent to it by

the source node. An effective anomaly detection system has been implemented in our experiment which efficiently detects the malicious behavior of the jammer node. On the other hand, a single system cannot fully solve the jamming problem. A collaborative approach of different detection schemes like carrier sense timing, signal strength consistency check etc is needed in order to fully detect different types of attacks including jamming attacks. So, our future work is to introduce various types of intelligent jamming attack and to implement collaborative detection approach of different attacks.

References

[1] L. Zhou and Z. Haas. Securing Ad-hoc networks. IEEE Network,13(6):24--30, November/December 1999.

[2] Y. Zhang and W. Lee, "Intrusion detection in wireless Ad ocnetworks," ACM MOBICOM, 2000

[3] Mithun Acharya, Tanu Sharma, David Thuente, David Sizemore. Intelligent Jamming in 802.11b Wireless Networks. In Proceedings of the OPNETWORK-2004 Conference Washington DC, USA, August 2004

[4] Vikram Gupta, Srikanth Krishnamurthy, and Michalis Faloutsos Denial of Service Attacks at the MAC Layer in Wireless Ad-hoc Networks, In Proceedings of Milcom, 2002

[5] OPNET Documentation, http://www.opnet.com

[6] 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

※ 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 (공학박사)
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