An Approach for the Analysis of Jamming Attacks in MANET

Rakesh Shrestha*, Kyong-heon Han*, Dong-you Choi*,
Seung-jo Han*, Sei-seung Park**
*Department of Information and Communication Eng,. Chosun University
**Department of Electronic Eng,. Chosun University
**Corresponding author E-mail : sspark@chosun.ac.kr

키워드
Denial of Service, mobile ad hoc networks, IDS, wireless jamming

목 차

Ⅰ. Introduction

A peer to peer mode of communication of mobile Ad hoc network without having a centralized infrastructure leads to frequent and unpredictable topology changes. On-demand routing protocols used in this type of topologies generates routing information only when a station initiates a transmission. MANET are the 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.

One of the DoS attack is jamming 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. Normally, jammers are used in military with the purpose of generating noise to bring down the enemy network as well as commercial hotspots. 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 wireless jamming can be realized by generating continuous high power noise in the neighborhood of wireless receiver nodes.

II. Related Work

The Security measures that has to be considered in ad-hoc network is discussed in [1] [2]. Zhang and Lee [2] discussed about the possible attacks in different layers as well as solutions 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. Problems faced by MANET

Different types of DoS attacks flood the network with so many additional requests that the regular traffic is either slowed or completely interrupted for some period of time which ruin the normal operation of the nodes. Hence, IDS can be used as second wall of defense to protect the network systems. 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

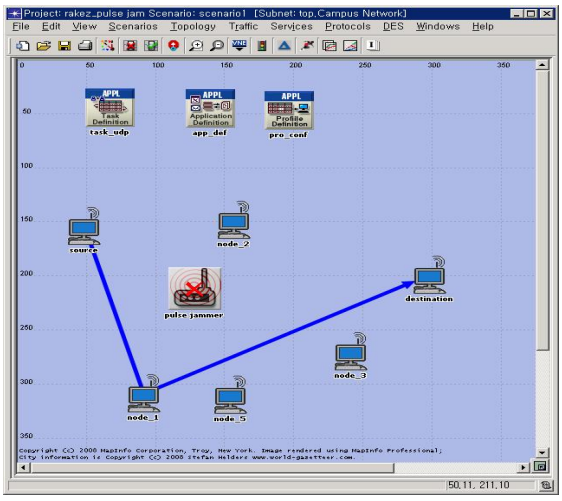
An IDS is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. Depending upon the detection model IDS is usually classified in one of two ways, with either signature-based or anomaly based detection.

In our model, anomaly detection model is implemented in 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 the 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 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 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 experimental set up is shown in Fig.1 with 6 similar wireless nodes stations and a jammer node within the campus network area of 500m X 500m. All the nodes use DSR as a routing protocol for mobile networks and all around data load environments [5]. The DSR route has been shown when the jammer node is disabled in Fig. 1.



<Fig. 1> Experimental setup for simulation

The node model of the jammer consists of a source and a 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. Control of the transmission pulses is performed by the process model which creates the packets and sends them through a radio transmitter. In our simulation we have used ideal jammer.

The simulation is run for 220 seconds and the results are analyzed. The summary of the simulation statistics is given in Table 1.

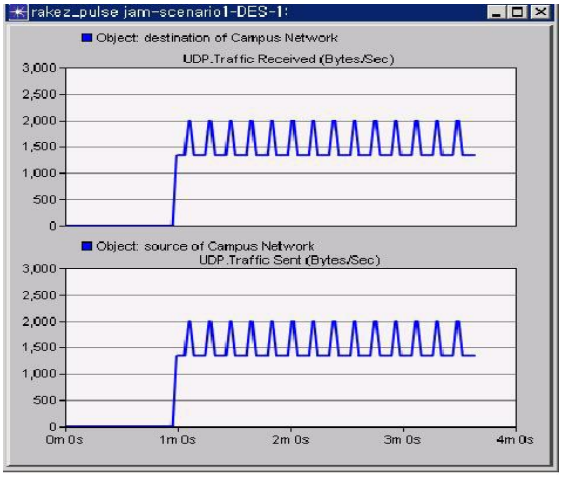
<Table 1> Scenario statistics

Statistics	Value
Scenario size	500m×500m
802.11b data rate	11 Mbps
Transmission Range	<200 meter
Power of each nodes	0.005W
Modulation	DPSK
Simulation Time	220
No. of nodes	6
No. of Jammer nodes	1

Ⅵ. Analysis and Simulation Result

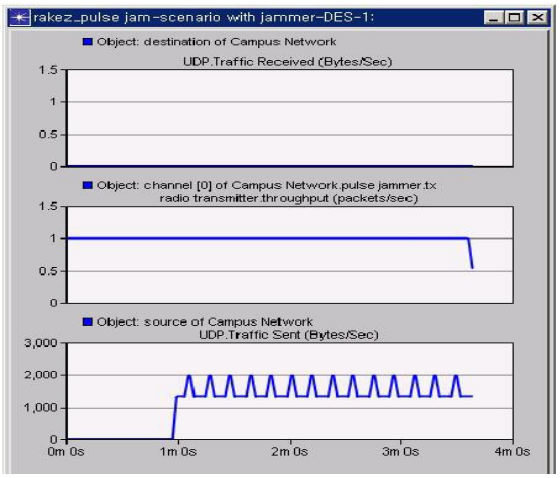
In our simulation, custom applications have been used with a streaming multimedia of packet size 1470 which starts at around 60 sec. We have used two simulation scenarios one without the jammer and the other with the jammer node. The given Fig.2 show the first scenario with UDP traffic before

the jammer node. Here, we have disabled the jammer node as if there is no jammer node during simulation. 2000 bytes/sec of UDP traffic that is sent by the source node is received by the destination node.



<Fig. 2> Traffic before jamming attack

In the second scenario, the jammer node is enabled in between the source and the destination nodes. When 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.

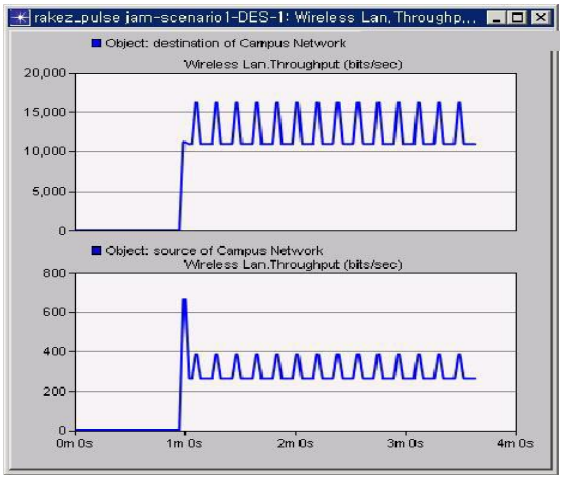


<Fig. 3> Traffic after Jamming attack

It is because the destination node first listens to the valid signal before transmission. The jammer node sends the jamming signal as soon as it is enabled. This jammer node denies the service between the source and the destination node of the network causing disruption in the network.

The detection module present in each node collects the data traffic. If there is no difference between the compared evidences collected by the nodes then it assumes as a normal behavior otherwise it declares the anomalous behavior as the intrusive behavior.

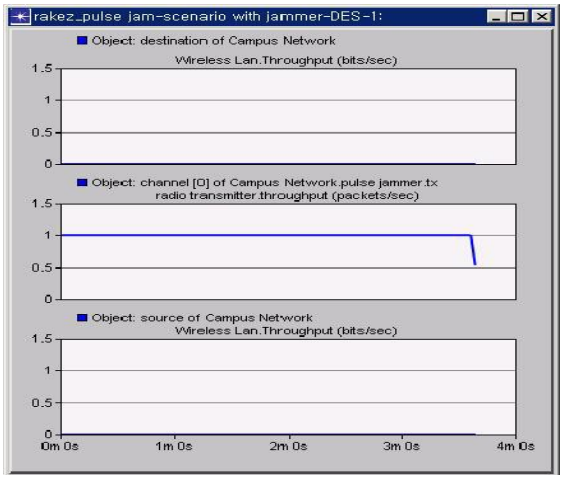
The Fig. 4 shows the throughput at the source and destination node before the jamming attack.



<Fig. 4> Traffic throughput jamming attack

The wireless LAN throughput of both the source and the destination is measured in bits/sec and the destination throughput is higher than the source throughput as the destination is receiving more data bits that is sent to it. The receiver and the transmitter port of the source is always busy because of the sending and receiving traffic.

The upper graph in Fig. 5 shows that the jammer lowers the traffic at the destination node to zero, the middle graph shows the jammer node throughput and it is busy.



<Fig. 5> Traffic throughput after the attack

And the last graph shows that the source node cannot transmit any packet due to jamming in its physical layer. 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.

Ⅶ. Conclusion

Hence, we examined the evidence collected by each node and identified the presence of jamming attack. We have seen that the communication between source and the destination node is interrupted by the jammer node hence acting as a DoS attack. An effective anomaly detection system has been implemented in our experiment which efficiently detects the malicious behavior of the jammer node. 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. Our future work is to introduce various types of attacks 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 hocnetworks," 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. 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.
6. OPNET Documentation, http://www.opnet.com