International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.103-112
http://dx.doi.org/10.14257/ijgdc.2014.7.3.10

Detecting Denial of Service Attacks by Analysing Network Traffic in Wireless Networks

R.Ragupathy[1] and Rajendra Sharma[2]

[1,2]*Dept. of Computer Science and Engineering*
Annamalai University, Chidambaram, Tamilnadu, India
[1]*cseraghu@gmail.com*, [2]*kingdomofraj@gmail.com*

Abstract

In recent wireless communication has become more popular because of its flexibility. That is, there is no need of large and complex physical establishment; one can connect with it easily using radio waves. But on the other part it also increases the chance for the unauthorized users to misuse it as there are fewer burdens in connectivity as compared to wired communications. The unauthorized access is called intrusions. Denial-of-service attacks are simplest but dangerous attacks which send excessive amount of false packets in order to jam and congest the network traffic. A technique is proposed in order to detect those intrusions by analyzing the network traffic pattern against suspicious pattern.

Keywords: *ad-hoc network, DoS attacks, intrusion detection system (IDS), network traffic, pattern matching, wireless sensor network (WSN)*

1. Introduction

The recent achievements in wireless networks technology have been giving the opportunity to use wireless networks in various spheres of academic research, commerce, and industry. A wireless network uses high frequency radio waves than wires to communicate between network enabled devices. It may consists of access point (AP) and other hardware devices which allow wireless communication enabled devices to connect to the network mostly called infrastructure based network and network without any physical communication set-up is known ad-hoc network [1]. Now-a-days the knowledge of adhoc network is vastly applied in wireless sensor network (WSN) [2]. Adhoc network is mainly interacted by human through PDAs, laptop etc. where as sensor network deals with environment rather than human interaction and that's make the difference between them [3]. . A common WSN consists of large number of sensor nodes, communicating with each other over short distances [2] and one or several base stations (BSs).

Sensor nodes are tiny, simple and cheap devices, constrained in energy, memory, processing power, and communication capabilities. They are vulnerable to physical phenomena and may be destroyed by environmental disasters. WSNs are susceptible to various types of attacks [4], because of simplicity of sensor nodes, dynamic network topology, and open medium for communication. Attacks may take place not only physical integrity of nodes, but also data, transmitted within the network. Sensor nodes monitor the environment and transmit the collected data in a hop-by-hop manner to a sink node (BS). Base stations are more resourceful and secure devices. They perform network's maintenance by broadcasting control messages.

The major aim in WSN is its functional architecture i.e. to place the sensor nodes wisely and cost effectively. Low cost establishment of wireless network makes the user attractive to

ISSN: 2005-4262 IJGDC

install it. But the loyalty of the networks is the matter of concerned. Since no security measure can guarantee that an attacker will not succeed eventually, intrusion detection techniques should be applied to detect anomalous behavior early and minimize its impact on network performance caused by the intruders [5, 6].

We have proposed an intrusion detection system in which each node monitors the traffic flow on the network and collects relevant statistics about it. By analyzing and comparing the traffic information, the nodes will be able to indicate if any attack performed or not. Figure 1 is the representation overall scenario of proposed intrusion detection system.

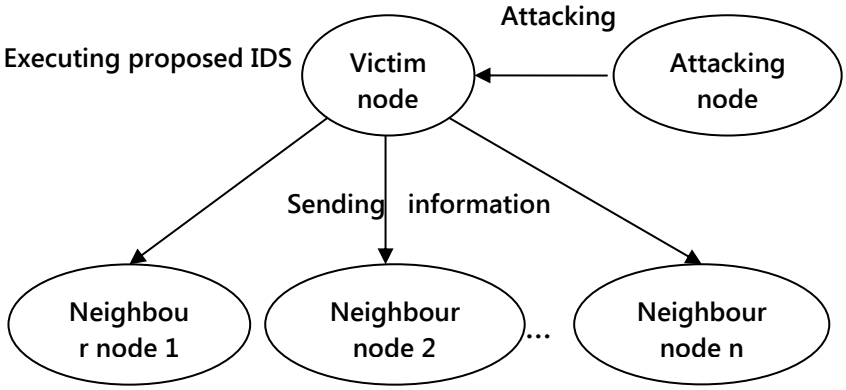

Figure 1. Overall Presentation of IDS

In this paper Section 2 contains literature review which provides the way of solving the problem. Section 3 is dealing with the basic need for an intrusion detection based on different types of attacks. Section 4 highlights the proposed work and Section 5 describes the implementation details and finally Section 6 is providing the conclusion along with the future works.

2. Literature Review

An Intrusion detection system (IDS) is software and/or hardware mainly designed to detect unwanted behaviours in the networks. These attempts may take the form of attacks, as examples, by crackers, hacker, malware and/or disgruntled employees. IDS may unable to directly detect attacks within properly encrypted traffic.

This intrusion detection system is used to detect different types of malicious behaviours that can compromise the security and trust of a computer system including network attacks against vulnerable services or data driven attacks on applications or host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses or sending excessive amount of false packets.

2.1. Types of IDS

There are several types of IDSs available based on different monitoring and analysis approaches. Each approach has its advantages and disadvantages. All approaches can be described in terms of a generic process model for IDSs. Here we have described some techniques of intrusion detection.

2.1.1. Anomaly detection: Anomaly detection techniques establish a "normal activity profile" for a system. We could flag all the system states varying from the established profile

by statistically significant amounts as intrusion attempts [4]. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same. Anomaly detection increases the false alarm rate [7], [8].

2.1.2. Misuse detection: It uses a pre known signature or pattern to compare with incoming traffic [9]. In the signature detection there are several methods to detect the intrusion patterns such as expert system, pattern recognition [10] are grouped on the misuse. The concept behind misuse detection is that these systems are not unlike virus detection systems, they can detect many or all known attack patterns. An interesting point can be noted that anomaly detection systems try to detect the complement of "bad" behaviour. Misuse detection systems try to recognize known "bad" behaviour. The main issues in misuse detection systems are how to build an efficient signature that encompasses all possible variations of the attacks, and how to build signatures that do not match non-intrusive activity too.

2.1.3. Network based Intrusion Detection: The most obvious location for an intrusion detection system is right on the segment being monitored. Network-based intrusion detectors [9] insert themselves in the network and they promiscuously examine every packet on the whole network.

2.1.4. Host based Intrusion Detection: Host based IDS [9] exploit vulnerabilities particular to specific operating systems and application suites. It examines the intrusions at host systems. Only host-based intrusion detection systems (the ones running as an application on a network-connected host) can correlate the complex array of system-specific parameters that make up the signature of a well-orchestrated attack.

2.2. Packet Sniffer

Packet sniffer is such a type of program running in a network attached device that actively or passively receives networking information passing through the device's network adapter [9], [11]. It is also known as Network or Protocol Analyzer or wireless network sniffer. Basic Components of sniffers are:

2.2.1. The hardware: Most sniffing products can work by standard adapters. Some sniffers support Ethernet or wireless adapters whereas some others support multi adapters and allow users to customize.

2.2.2. Capture driver: This is the core of a sniffer. Each sniffing product has its own driving program, after completing installation; a sniffer can start to capture traffic and data from network.

2.2.3. Buffer: A buffer is a storage device for captured data from the network. Generally there are two modes of buffers: keep capturing until the storage gets full, or keep capturing and overflowing as the latest captured data keep replacing the oldest data. Computer's EMS memory controls the size of a buffer. The bigger EMS memory is, the more data can be stored in the buffer.

2.2.4. Decode: Capture and analysis are both the most basic and important features of a sniffer. Sniffing products can provide real-time analysis of captured packets, this is the main reason why they are good assistants of network administrators, it record the errors and abnormity while they happening.

2.2.5. Packet editing: Some advanced sniffing products are able to resume the contents of captured packets; they may also allow editing the content and transmitting to the network.

2.3. Intrusion

Intrusion is an unauthorized access or anomalous behaviour in the network [6].

2.4. Network traffic

Network traffic is a flow of packets in network [12].

2.5. Signatures

Intrusion Signature is a suspicious pattern in network traffic.

3. Need for an Intrusion Detection System (IDS)

Intrusion detectors are an integral part of any network. The internet is growing constantly, and new vulnerabilities and threats are found regularly. Intrusion detectors provide an additional level of protection to identify the existence of an intruder, and help to inform accountability for the attacker's action. Generally four different types of attacks have been identified which makes the need for an IDS critical [3].

3.1. Denial of service (DoS)

Network-based denial-of-service attacks [5, 10, 13] are one of the easiest types of attacks. It often requires a very little effort to fully consume resources on the target computer, or to starve the target computer of resources, even to cause critical services to fail or malfunction. Typically corporate networks internally do not have internal filtering defenses against common denial-of-service attacks, such as flooding. Mainly DoS attacks try to send excessive amount of false packets in the network.

3.1.1. Ping of death: The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim node. The Ping command makes use of the ICMP echo request and echo reply messages and it is commonly used to determine whether the remote host is alive. However in a ping of death attack ping causes the remote system to hang, reboot or even crash [13].

3.1.2. Teardrop attack: Whenever data is sent over the internet, it is fragmented at the source system and reassembled at the destination system [13].

3.1.3. SYN - flood attack: In SYN flooding attack, several SYN packets with an invalid source IP address are sent to the target host. When the target system receives those SYN packets, it tries to respond to each system with a SYN/ACK packet but as all the source IP addresses are invalid the target system goes into wait state for ACK message to receive from the source [13].

3.1.4. UDP - flood attack: Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems. These services can be used to start DoS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic [13].

3.1.5. Land attack: A land attack is similar to SYN attack, the only difference is that instead of including an invalid IP address, the SYN packet includes the IP address of the target system itself. Consequently an infinite loop is created within the target system, which ultimately hangs and crashes the victim system.

3.1.6. Smurf attack: It Broadcasts ICMP packets with victim's spoofed source IP and causes all hosts on the network to reply to the ICMP request, results significant traffic to the victim's node.

3.2. Threat to confidentiality

Some intrusions like viruses attach themselves to existing files on the system they infect and they send the infected files to others. This can result in confidential [4] information being distributed without the author's permission.

3.3. Modification of contents

Intruders might be able to produce bogus press releases, modify news sites, and conduct other activities, all of which could make impact economically [4]. It hampers the integrity of the network security.

3.4. Masquerade

A masquerade [11] takes place when one entity pretends to be a different entity (a disguised entity). Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, and thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Any internet connected system and providing TCP-based network services (such as a FTP server or Web server, or mail server) is potentially subject to this attack.

4. Proposed Work

The flow chart of proposed work is given in Figure 2. Proposed work is following the basic components as.

4.1. Network Packet Sniffer

Packet sniffer is a program which runs in a network attached device that passively receives all data link layer frames passing through the device's network adapter [14].

4.2. Decoding the Packets

When network packets are captured the packet informations are not in a true format. So one need to convert the information in an understandable format. After capturing the network packets it is essential to convert or decode the network traffic information in true text to analyze the traffic pattern in an efficient and understandable way.

4.3. Categorize the informations

Categorization of network traffic [15], [16] is needed for extracting the required information from the large content of network traffic information to minimize the code and work load.

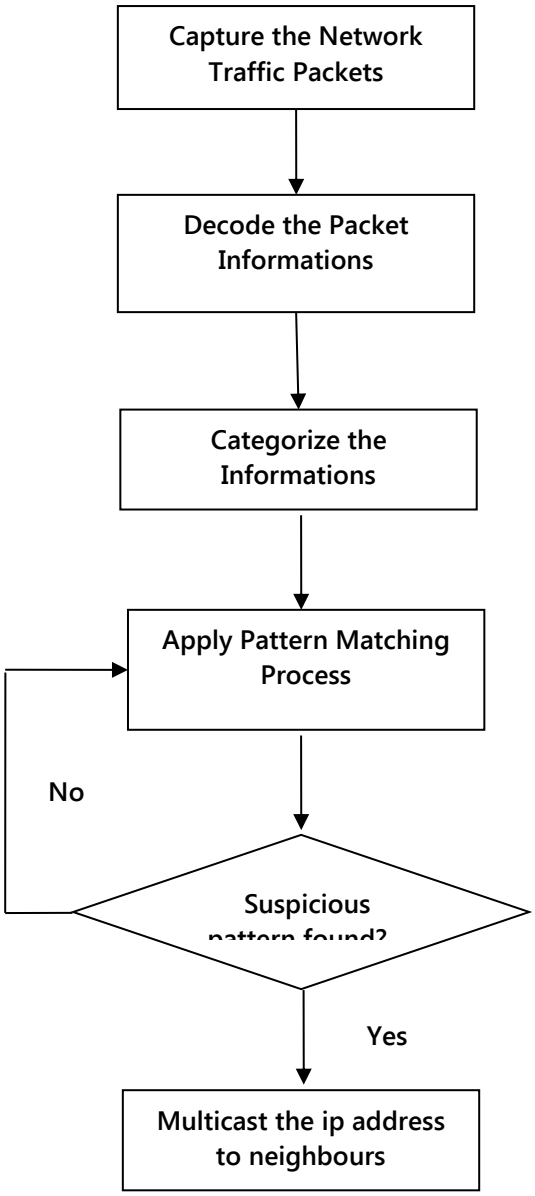

Figure 2. Flow Chart of Intrusion Detection System

4.4. Packets Information Matching and Detection Unknown Behaviour

The most important phase of this intrusion detection system is the analyzing the traffic pattern [9] and its behavior [17]. There are several pattern matching algorithms are available as: The Brute Force Algorithm, The Boyer-Moore Algorithm, The KMP Algorithm. Here we are focusing on Brute Force algorithm where a text pattern key [1 ...m]) tries to match the original text S [1...n].

4.5. Multicasting the Intrusion Related Information to Neighbours

If such kind of pattern is found then next procedure is to find the ip address of the attacker/intruder and the ip address of the victim computer. On the other part it is optional to find the type of attacks, *etc*. Once the required ips are found the attacking informations are sent/multicast to the neighbouring clients in order to make them aware of the attacking issues done by the intruder [18].

5. Implementation and Simulation

The proposed model is implemented in three different systems of virtual pc environment. Two of them are considered as authorized system and one as an intruder system. The intruder is having windows xp or ubuntu operating system. The victim node is windows 7 OS. And the neighbouring node has windows xp operating system. Apart from this virtual environment we have implemented in three different laptops. The proposed network intrusion detection system is implemented according to the following five steps:

5.1. Listening to the Network and Capturing the Packets

At this first step, a sniffer is developed using Jpcap library [6] In a Wireless network, each system has a network card which has its own physical address. Each packet is examined by the network card over the network and catches it once intended to the host machine. One machine withdraws from this package the various layers such as Ethernet, TCP, and IP etc. to forward information it contains to the application. When any network card is configured in the promiscuous mode through Jpcap library, every packets are captured without being out from the traffic.

The library WinPcap [6] is the Windows version of the library libcap. Supervision tools can use pcap (or WinPcap) to capture packets over the network; and to record captured packets in a file and to read the saved file.

The sniffer is implemented using the Jpcap library through the following steps:

i] Asking and showing all network interfaces available on the host machine using the method JpcapCaptor. getDeviceList(),

ii] Selecting of the network interface to be used by the sniffer,

iii] Activating of the network interface onto the proscimous mode thanks to JpcapCaptor.openDevice(),

iv] Starting the packets capturing process through the interface PacketReceiver.

5.2. Decoding the Packets

Packet decoding process also is based on the Jpcap library. The decoder receives all the packets one after another from the sniffer and finds their category (TCP, UDP, ICMP, etc.) by comparing them to different available classes in the Jpcap library namely TCPPacket, IPPacket, ICMPPacket, UDPPacket etc. For instance, if the concerned packet is UDP, the decoder collects its source and destination addresses, source ports and destination ports, data field and UDP flag *etc*.

5.3. Categorization of Network Traffic

Categorization of network traffic [16] is needed for extracting the required information from the large content of network traffic information to minimize the code and work load. The "StringTokenizer" class under "util" package provides the categorization of the informations *i.e.*, sub-divides the informations.

5.4. Detecting Specific Attacks (Pattern Matching)

For simplicity we used brute force matching algorithm in which each pattern will be checked thoroughly. Brute force pattern matching runs in time O (mn) in the worst case.

5.5. Sending the Information (multicasting)

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. Once the required ip is found the attacking informations are sent/multicast to the neighbouring clients. DatagramPacket is sent through DatagramSocket. (socket.send(DatagramPacket)).

Tested Attacks: Three different types of DoS attack named Ping of Death and LAND attack, and Flood attack are tested.

- For Ping of Death attack we used the PING tool through the command:

o ping "victim ip address" –t –l "no. of packets"

e.g. ping 192.168.93.1 –t –l 12000

(N.B: hping tool can also be used.)

- For Land attack we used the HPING tool installed on ubuntu OS through the command:

o sudo hping3 -n -c 2 -a "victim ip" "victim ip

e.g. sudo hping3 –n -c 2 –a 192.168.93.1 192.168.93.1

- In case of Flood attack a huge number of unwanted packets are sent at a quick time. For this attack we used the HPING tool installed on ubuntu OS through the command:

o sudo hping3 "victim ip" –flood -d "data size"

e.g. sudo hping3 192.168.93.1 –flood -d 12000

- Symbol descriptions:

–t : ping the specified host until stop.

--l: buffer size.

--n: packet count.

--a: spoof source address;

--d: data size.

--flood: flooding the packets.

6. Conclusion and Future Works

The IDS system is designed in such a way that it can be reused very easily. The IDS is written completely in Java. Thus the present system is not platform dependent, and also it is tested on Windows 7, Windows XP and ubuntu. It can be employed and tested on various other machines which run on different Operating systems and which satisfy the requirements and pre-requisites for the IDS system.

In this paper we have applied three types of denial-of-service (DoS) attacks and implemented in three different nodes on three different environments. In future one can implement more types of DoS attacks (e.g. smurf attack etc) in more number of nodes.

References

[1] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A Survey of Routing Attacks in Mobile ad Hoc Networks", IEEE Wireless Communications, vol. 14, no 5, **(2007)**, pp. 85-91.
[2] Y. Wang, X. Wang, B. Xie, D. Wang and D. P. Agrawal, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks", IEEE Transactions on Mobile Computing, vol. 7, no. 6, **(2008)**, pp.698 – 711.
[3] M. S. Islam, S. A. Rahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology, vol. 36, **(2011)**.
[4] A. A. Rao, P. Srinivas, B. Chakravarthy, K. Marx, and P. Kiran, "A Java Based Network Intrusion Detection System (IDS)", Proceedings of the IJME - INTERTECH Conference, Session ENG 206-118, **(2006)** October 19-21; Kean University, US.
[5] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy," Denial of Service Attacks in Wireless Networks: The Case of Jammers", IEEE Communications Surveys & Tutorials, vol. 13, no. 2, **(2011)**, pp. 245-257.
[6] S. Boob, P. Jadhav, "Wireless Intrusion Detection System", International Journal of Computer Applications, vol. 5, no.8, **(2010)**, pp. 9-13.
[7] W. Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall, ch.18, **(2005)**.
[8] O. Adaobi and M. Ghassemian, "Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks", Proceedings of the1st International Conference on Communications Engineering, **(2010)** December 22-24; University of Sistan and Baluchestan, Iran.
[9] R. S. Shirbhate and P. A. Patil, "Network Traffic Monitoring Using Intrusion Detection System", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 1. **(2012)**.
[10] I. Demirkol, C. Ersoy, F. Alagöz and H. Deliç,"The Impact of a Realistic Packet Traffic Model on the Performance of Surveillance Wireless Sensor Networks", Science Direct: Computer Networks, vol. 53, no. 3, **(2009)**, pp. 382–399.
[11] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses ", Pervasive Computing, IEEE, vol. 7, no. 1, **(2008)**, pp. 74-81.
[12] I. Demirkol, F. Alag¨oz, H. Delic, and C. Ersoy, "Wireless Sensor Networks for Intrusion Detection: Packet Traffic Modeling", IEEE Communication Letters, vol. 10, no. 1, **(2006)**, pp.22-24.
[13] S. Rao, S. Rao, "Denial of Service Attacks and Mitigation Techniques: Real Time Implementation with Detailed Analysis", The SANS Institute, **(2011)**.
[14] Q. Wang, "Traffic Analysis & Modeling in Wireless Sensor Networks and Their Applications on Network Optimization and Anomaly Detection1", Macrothink Institute: Network Protocols and Algorithms, vol. 2, no. 1, **(2010)**, pp. 74-92.
[15] Y. Ponomarchuk, and D.-W. Seo, "Intrusion Detection Based on Traffic Analysis in Wireless Sensor Networks", Proceedings of the 19th annual IEEE Wireless and Optical Communications Conference, **(2010)** May 14-15; Shanghai.

[16] G. Kirykos, "Traffic Profiling of Wireless Sensor Networks", Thesis, Naval Postgraduate School, Monterey, **(2006)**.
[17] M.D. Aime, T. Politecnico, G. Calandriello and A. Lioy, "A Wireless Distributed Intrusion Detection System and a New Attack Mode", Proceedings of the 11th IEEE Symposium on Computers and Communications, **(2006)** June 26-29.
[18] B. Sun and L. Osborne, Y. Xiao and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks", IEEE Wireless Communications, vol. 4, no. 5, **(2007)**, pp. 56–63.

Authors

R. Ragupathy receives the M.E. degree from Bengal Engineering and Science University **(**currently Indian Institute of Engineering Science and Technology**)** and is on the way of his research work. He is currently an Assistant Professor at Dept. of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India.

E-mail: cseraghu@gmail.com

Rajendra Sharma receives the B.E. degree in Information Technology from University Institute of Technology, Burdwan University in 2011. In 2013 He completed M.E. in Computer Science and Engineering at the Dept. of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India.

E-mail: kingdomofraj@gmail.com

