TRAFFIC ANALYSIS BASED ANOMALOUS INTRUSION DETECTION IN WIRELESS SENSOR NETWORK

R.RAGUPATHY

Abstract : Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. A WSN tries to detect the unauthorized access in wireless network. The unauthorized access is called INTRUSIONS. So we need to protect the computer system from these intrusions i.e. wireless intrusion detection system (WIDS) is needed. By analyzing the network traffic and comparing the normal traffic pattern against the suspicious pattern we can detect those intrusions. Denial-of-Service attacks, and jamming in particular, are a threat to wireless networks because they are at the same time easy to mount and difficult to detect and stop.

Keywords: wireless sensor network(WSN),DoS attacks, intrusion detection, pattern matching, network traffic.

Introduction : The recent advancements in wireless networks technology have been giving the opportunity to use wireless sensor networks (WSNs) in various spheres of academic research, commerce, and industry. Since WSNs may monitor environment in unattended manner, have low price for installation and maintenance, and can be easily deployed, their popularity has been growing. A common WSN includes large number of sensor nodes, communicating with each other over short distances, and one or several base stations (BSs). Sensor nodes are simple and cheap devices, constrained in energy, memory, processing power, and communication capabilities. They are vulnerable to physical compromise and may be destroyed by environmental disasters. Sensor nodes monitor the environment and transmit the acquired 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. BSs collect sensed data, preprocess and send them to a user or another network, such as Internet. Though recently the research was mainly focused on protocols making WSNs operate efficiently, nowadays network security has been becoming one of the main concerns of research community. WSNs are susceptible to various types of attacks, because of simplicity of sensor nodes, dynamic network topology, and open medium for communication. Attacks may target not only physical integrity of nodes, but also data, transmitted within the network. The resource constraints of sensor nodes make the majority of traditional security policies unsuitable for WSN environment, therefore, new schemes and algorithms are needed . 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.

We propose a intrusion detection system in which each node monitors the traffic flow on the network and collects relevant statistics about it. By analyzing the traffic information the nodes are able to tell if (and which type of) an attack happened. However, this system opens the possibility for misuse. We discuss the impact of the misuse on the system.

In this paper Section 2 contains literature review which provides the way of solving the problem. Section 3 provides the different types of tools for network traffic analysis. Section 4 is dealing with the basic need for intrusion detection based on different types of attack. Section 5 highlights the proposed work and Section 6 describes the implementation details and finally Section 7 is providing the conclusion along with the future work.

Literature Review : An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses

A. Types Of IDS: There are several types of IDSs available today, characterized by different monitoring and analysis approaches. Each approach has distinct advantages and disadvantages. Furthermore,all approaches can be described in terms of a generic

process model for IDSs. Here we describe some techniques of intrusion detection.

A.1 Anomaly Detection : Anomaly detection techniques establish a "normal activity profile" for a system; we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts [3]. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities:

(1)Anomalous activities that are not intrusive are flagged as intrusive.

(2)Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are).

A.2 Misuse Detection : It uses a pre known signature or pattern to compare with incoming traffic. In the signature detection there are several methods to detect the intrusion patterns. The detection approaches, such as expert system [4], pattern recognition [5], 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, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity.

A.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 insert themselves in the network just like any other device, except they promiscuously examine every packet.

A.4 Host Based Intrusion Detection : Host based IDS exploit vulnerabilities particular to specific operating systems and application suites. 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.

B. Packet sniffer : Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter[2]. It is also known as Network or Protocol Analyzer or Ethernet Sniffer.

B.1. Sniffer Components: Basic Components of sniffers are:-

B.1.1. The hardware: - Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth.

B.1.2 Capture driver:-This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, and then stores the data in a buffer.

B.1.3. Buffer:-Once the frames are captured from the network, they are stored in a buffer.

B.1.4. Decode: - this displays the contents of network traffic with descriptive text so that an analysis can figure out what is going on.

B.1.5. Packet editing:-Some products contain features that allow you to edit your own network packets and transmit them onto the network.

Need For An Intrusion Detection System(IDS): Intrusion detection devices are an integral part of any network. The internet is constantly evolving, and new vulnerabilities and exploits are found regularly. They provide an additional level of protection to detect the presence of an intruder, and help to provide accountability for the attacker's action. Four different types of attacks have been identified which makes the need for an IDS critical.

A. **Denial of service(DoS):** Network-based denial-of-service attacks [1,6,11,12] are one of the easiest types of attacks. It often requires little effort to fully consume resources on the target computer, to starve the target computer of resources, or to cause critical services to fail or malfunction. Internal corporate networks typically do not have internal filtering defenses against common denial-of-service attacks, such as flooding.

1) Ping Of Death :- The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim.The Ping command makes use of the ICMP echo request and echo reply messages and it's commonly used to determine whether the remote host is alive. In a ping of death attack, however, ping causes the remote system to hang, reboot or crash.

2) Teardrop Attack :- Whenever data is sent over the internet, it is broken into fragments at the source system and reassembled at the destination system.

3) SYN - Flood Attack :- In SYN flooding attack, several SYN packets are sent to the target host, all with an invalid source IP address. When the target system receives these SYN packets, it tries to respond to each one 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 source.

4) Land Attack :- A land attack is similar to SYN attack, the only difference being that instead of

including an invalid IP address, the SYN packet include the IP address of the target sysetm itself. As a result an infinite loop is created within the target system, which ultimately hangs and crashes.Windows NT before Service Pack 4 are vulnerable to this attack.

5) 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 launch a DOS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.

B. Threat to Confidentiality : Some viruses attach themselves to existing files on the system they infect and they send the infected files to others. This can result in confidential [2] information being distributed without the author's permission.

C. Modification of contents : Intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact [2].

D. Masquerade

A masquerade [7] takes place when one entity pretends to be a different entity. Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Any system connected to the internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack.

Proposed Work : The flow chart of proposed work is given in figure 1.Proposed work is following the basic components as:

1)Network Packet Sniffer: Packet sniffer is a program running in a network attached [13] Device that passively receives all data link layer frames passing through the device's network adapter.

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 a understandable format.After capturing the network packets it is essential to convert or decode [15] the network traffic information in true text to analyze the traffic pattern in an efficient and understandable way.

3)**Categorize The Informations:** Catego- rization of network traffic [15] is needed for extracting the required information from the large content of network traffic information to minimize the code and work load.

4)Packets Information Matching And Detection Unknown Behaviour: The most important phase of this intrusion detection syetm is the analyzing the traffic pattern and its behavior. There are several pattern matching algorithms are available as: The Brute Force Algorithm, The Boyer-Moore Algorithm, The KMP Algorithm

5)Mutlicasting The Intrusion Related Information To Others: 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 attack. Once the required ips are found the attacking informations are sent/multicast(as on Figure 5.8) to the neighbouring clients in order to aware of the attacking issues done by the intruder.

.

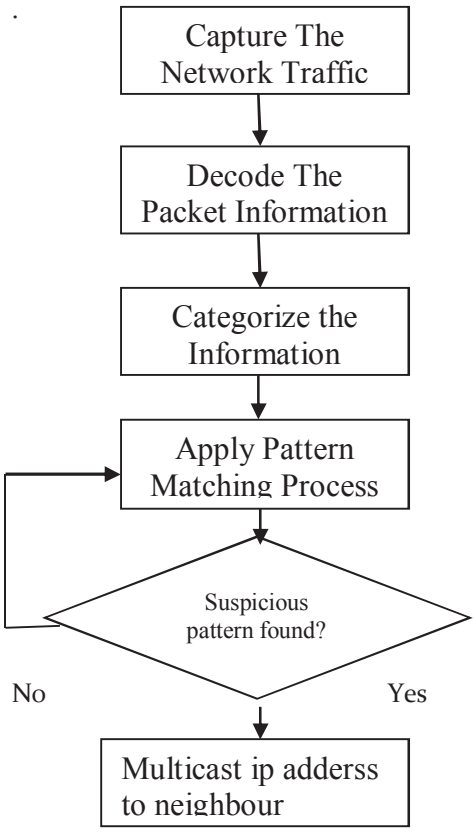

Figure 1:Flow chart of intrusion detection system

Implementation And Simulation : The proposed model is implemented in three different systems of virtual pc environment. Two of them is authorized system and one act as a intruder system.The intruder is having windows xp operating system. The victim node is windows 7 OS. And the neighbouring node has windows xp operating system. The proposed network intrusion detection system is implemented according to the following five steps:

1) Listening to the network and capturing the packets: At this first step, a sniffor is developed using Jpcap library In a Wireless network, each system has a network card which has its own physical address. The network card examines each packet over the

network and catches it once intended to the host machine. One withdraws from this package the various layers such as Ethernet, IP, TCP, etc. to forward information it contains to the application. When a network card is configured in the promiscious mode thanks
to the Jpcap library, all packets are captured without being out from the traffic. The sniffer is therefore implemented using the Jpcap library
through the following steps:
i] seeking and printing all network interfaces available on the host machine thanks to 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

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

3) Categorization of network traffic: Categorization of network traffic [15] 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.

4) Detecting specific attacks/pattern matching::For simplicity we used broute force matching algorithm in which each pattern will be checked thoroughly. Brute force pattern matching runs in time O(mn) in the worst case.But most searches of ordinary text take O(m+n), which is very quick.

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 ips are found the attacking informations are sent/multicast to the neighbouring clients . DatagramPacket is sent through
DatagramSocket.(socket.send(DatagramPacket)).

Conclusion And Future Work : 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 platform independent, yet I have been tested on Windows 7 and Windows XP. 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 the one type of denial-of-service(DOS) attack called PING OF DEATH (POD) attack and implemented in three different nodes. In the next phase we are concerning about to implement more types of DOS attack(e.g. land attack, flood attack etc) in more number of nodes.

References

1. Kemal Bicakci, Bulent Tavli,"Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks",ScienceDirect:Computer Standards & Interfaces 31 ,2009,pp. 931–941.
2. William Stallings, "Cryptography and Network Security", Principles and Practices, Third Edition.
3. Ponomarchuk, Yulia and Seo, Dae-Wha,"Intrusion Detection Based on Traffic Analysis in Wireless Sensor Networks", IEEE Wireless and Optical Communications Conference (WOCC), 2010.
4. Md. Safiqul Islam, Syed Ashiqur Rahman,"Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches",International Journal of Advanced Science and Technology,Vol. 36, November, 2011.
5. Snehal Boob,Priyanka Jadhav,"Wireless Intrusion Detection System",International Journal of omputer Applications (0975 – 8887),Volume 5– No.8, August 2010.
6. Subramani rao Sridhar rao,"Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis",TheSANS Institute,2011.
7. Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, and P. Kiran,"A Java Based Network Intrusion Detection System (IDS)",IJME - INTERTECH Conference,Session ENG 206-118,2006.
8. Ilker Demirkol, Fatih Alag¨oz,Hakan Delic,and Cem Ersoy, "Wireless Sensor Networks for Intrusion Detection: Packet TrafficModeling",IEEE Communications Letters, vol. 10, no. 1, january 2006.
9. Yun Wang, Xiaodong Wang,Bin Xie,Demin Wang,and Dharma P. Agrawal,"Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks",IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008.

10. Okoli Adaobi, Mona Ghassemian, "Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks",international conference on communications engineering,22-24 dec,2010.
11. Anthony D.,Wood,John A.,Stankovic."Denial of Service in Sensor Networks", IEEE Computer, 35(10):54-62, October 2002.
12. Jonathan M. McCune Elaine Shi Adrian Perrig Michael K. Reiter,"Detection of Denial-of-Message Attacks on Sensor Network Broadcasts",Army Research Office, and grant CAREER CNS-034780.
13. Pallavi Asrodia*, Hemlata Patel,"Network Traffic Analysis Using Packet Sniffer",International Journal of Engineering Research and Applications,Vol. 2, Issue 3, May-Jun 2012, pp.854-856.
14. E. Denning, "An intrusion-detection model". IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987.
15. Georgios Kirykos," Traffic profiling of wireless sensor networks", naval Postgraduate school,2006.
16. Ilker Demirkol a, Cem Ersoy a,*, Fatih Alagöz a, Hakan Deliç,"The impact of a realistic packet traffic model on the performance of surveillance wireless sensor networks",Science Direct:Computer Networks 53 (2009) 382–399
17. Bo sun and lawrence osborne, yang xiao,sghaier guizani," intrusion detection techniques in mobile Ad hoc and wireless sensor networks", ieee wireless communications • october 2007.
18. Qinghua Wang,"Traffic Analysis & Modeling in Wireless Sensor Networks and Their Applications on Network Optimization and Anomaly Detection1,2",Macrothink Institute: Network Protocols and Algorithms ISSN 1943-3581,vol. 2,No. 1,2010.

***

Assistant Professor
Department of Computer Science and Engineering
Annamalai University