2012 International Conference on Networks and Information (ICNI 2012)
IPCSIT vol. 57 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V57.06

A New Hybrid Model Security Management in Wireless Networks

Sedighe Ahangari, Nasser Modiri and Ahmad Khadem Zadeh [+]

Computer Engineering Department, Islamic Azad University, Science and Research branch, Tehran, Iran

Abstract. Data security is a huge responsibility for the sensor network, as there are different ways in which security can be breached, allowing hackers to gain access to confidential data. Threats to wireless sensor networks are numerous and potentially devastating. Safety issues, ranging from session hijacking to a denial of service (DOS) can be annoying WSN. To assist in the defense and the identification of potential threats, WSN to use security solution that includes an intrusion detection system (IDS). Various methods have been proposed neuron in recent years for the development of intrusion detection systems. In this article we looked at denial of service attacks that spread WSN so that it temporarily paralyzes the network and the proposed hybrid approach based on intrusion detection in river flow and session-state transition analysis, monitoring and analyzing the data stream, identify abnormal network activity and detect violations policy on flood synchronization attacks.

Keywords: Wireless sensor network denial of service, intrusion detection systems, the State Transition hybrid intrusion detection system, the type of service, Hybrid detecting model.

1. Introduction

Wireless sensor network is a network of simple sensors that are capable of sensing some change in incidents / parameters, and communicate with other devices within a certain geographic area for certain specific purposes, such as target tracking, surveillance, environmental monitoring, etc. Since sensor nodes are severely limited in processing capability, storage capacity and energy, routing and data aggregation in WSN is very difficult because of inherent characteristics. A notable feature of the architecture of wireless sensor network is its hierarchy, rooted at the base station. Wireless sensor networks are often collects and transmits data to an internal server through a gateway or base station. Since sensor nodes are severely restricted in the processing capability, capacity, and thus energy security and data aggregation in WSN is very difficult. Thus, the sensor network must be autonomous and demonstrate the efficiency and adaptability to the evolution in real time, without explicit user or administrator action. This need is even more important to adding security threats, so tries to apply the idea of implementing IDS, which can detect third party attempts to use uncertainty and possibly prevent malicious attacks in WSN has a lot of sense.

As Sensor networks are limited in resources compared with the Ad and cellular networks (Aboelaze and Aloul, 2005). A typical sensor node, such as mica, 8 MHz microprocessor, 128 KB of flash program memory and 512 KB of flash memory serial (technology, d). WSNs deployed more densely and randomly in the environment and the sensor node failure is likely to happen. Thus, it is impossible for a sensor node to store the data label on the malicious nodes to the network in a manner similar to the additional detection of abuse. In addition, it is very difficult to use traditional methods to detect anomalies in WSNs, because the sensor nodes can not monitor all traffic through them, and the calculation of anomalous events. These specific WSN characteristics require a new security architecture design for such conditions. Although wireless ad hoc networks and wireless sensor networks, some common characteristics, and there was no development of the IDS in wireless ad hoc network (Misra et al., 2004), R. Roman has shown in his article, that they can not be

[+] Tel. Number : + 98 912 243 0668 ; fax: + 98 22574229.
E-mail address: *s_ahgr@yahoo.co.uk.*

directly applied in WSNs .. In this paper we have attempted to document denial of service attacks on the sensor nodes that are not only broke the sensor nodes flood of unwanted information, but due to the sudden collapse of the loss of units of information flows, as well, and proposed a hybrid system that combines anomaly, and signature-based detection, based on river flow and analysis of the transitions that provide services to close a malicious node efficiency.

2. Related work

Some manufacturers claim that the multi-gigabit statistical IDS [1], they usually refer to normal traffic conditions and use packet sampling [2]. Various methods of artificial intelligence are used for both signature detection and anomaly detection [6]. Yang [4] proposed a hybrid intrusion detection system for clusters, based on wireless sensor network (CWSN), which uses two basic models of intrusion detection and anomaly detection includes the detection of abuse. CH is used for intrusion detection, which not only reduces energy consumption, but also effectively reduces the amount of information, so the lifetime of the WSN can be extended. Although our proposal (STHIDS) use the anomaly and signature-based model analysis of the transition state of the session. The main feature of our proposal (STHIDS), that does not violate the privacy, since we are only interested in the packet header, to know whether the state has changed or not, just check the title and make this proposal effective and best suited for densely deployed sensor node.

3. Attacking Model

Denial of Service (DoS) is produced by accidental failure of nodes or malicious actions and the apparent attempt to prevent a lawful user of services or data. A common method of attack involves overloading the target system with requests, for example, that he cannot respond to legitimate traffic. As a result, it makes the system or service is not available to users [8]. The main types of attacks: bandwidth consumption or the consumption of CPU time, prevent communication between two machines, a violation of a specific system or service person, a violation of the routing information, a violation of the physical components, etc. If the sensor detects a network denial of service attack, the attack gradually reduces functionality, as well as the overall performance of a wireless sensor network [3]. Projected use of sensor networks in a sensitive and critical applications makes the prospect of DoS-attacks even more alarming. The table below shows the DoS attack at every level of their defence mechanism:

Table 1.DoS attack and defense mechanism

Protocol layer	Attacks	Defense
Physical	Jamming	Sleep
	Node destruction	Hide nodes or tampering with evidence Packaging
MAC (Medium access Management)	Denial of sleep	Sleep identification and anti-replay
Network	Spoofing, Reproduction	Authentication anti-replay
	Hi, floods	Geographical routing
	Guidance	Title encryption
Transport	SYN-flooding	SYN cookies
	De-synchronization attack	Package identification
Application	The path is based DoS	Identification and anti-replay protection.

In this paper we consider the sync flood attack, in which a sequence of TCP session initiation, often with the wrong (or "spoofed") IP-addresses. As a result of trying to target and cannot set the number of sessions of TCP, which consumes resources on the target.

4. Anomaly hybrid detection model

Anomaly IDS is based on studying the behavior of the system over a period of time in order to build a profile of activities that constitutes the normal operation of the system. Anomaly IDS computes the similarity of the flow in the system with profiles for intrusion detection. The biggest advantage of this model is that new attacks can be identified in the system, as it will be a deviation from normal behavior. This model acts as a filter, as in this study. Abnormal packets are delivered to the signature-based detection model for future registration. Since anomaly detection using a model of normal behavior, the packet is defined as abnormal by the system when the current behavior depends on the model of normal behavior. As a result, the detection of anomalies usually determines the normal communication, as an abnormal connection, and creates a problem of erroneous classification. Thus, the anomaly detection model is used to filter the large number of packets the first and the further discovery of signatures to the model, when the amount of information decreases. In the proposed model, which filters packets with an infected stream for further analysis, packet filtering, illustrated as follows:

Packet streams to pass the software anomaly detection that sniffs packets of data and analysis of the TCP header TCP SYN flooding is a major threat [7]. TCP header is built on IP-based title, which is unreliable and the connection. TCP header is 20 bytes and has some limitations in the header length. As already mentioned, the normal TCP header is 20 bytes, but TCP may have an additional 40 bytes of version. Thus, the header size should not exceed 60 bytes. TCP flags six flag bits namely URG, ACK, PSH, RST, SYN and FIN, each of them has a special use in the connection establishment, connection termination or control. Only a few combinations of the six TCP flags can be carried in the packet TCP. URG and PSH flag can be used only when the package contains data, such as a combination of SYN and PSH become invalid. Because the TCP SYN-flooding attack will flood the network with SYN packets, three-step application is verified in each package. At this stage, the packets are divided into two groups, whether infected or normal package packages. If the package is infected, then the system will distinguish between the bags and go for an analysis to confirm that the package actually comes from the attackers. Otherwise, the normal packet will pass through a network of data transmission to the destination.

B. Simulation Model

To simulate the proposal, we fix the flow of TCP packets through the first-order Markov chain model, the model parameters (transition probabilities) are different for each application and make a "signature" of applications. Since the IP-traffic can be represented in three persons: the packet level, flow level, which corresponds to the sequence of packets with the same 5-tuple, and the session level, which is a sequence of streams (activity periods) applications. In the normal course of business, application sharing typical sequence of control packets (e.g., SYN, ACK, PSHACK, SYN-ACK, etc. ..) from a remote host (server or client). This sequence is modelled as a first order Markov chain, different types of control packets are exchanged (usually no more than 10, including the "rare" state) constitute the state space of the Markov chain and transition probabilities between states (transition matrix) to define different "signature" for each application. Thus, the identification of a Markov model associated with the applications can be divided into three stages:

1: is to define the state space. It comes down to defining the various types of control packets used by the applications.

2: is to restore the original order of packets in the stream, it comes down to the reorganization of flows according to their order of activation in the session, and packages according to their order in the radiation flux.

3: estimate the parameters of the Markov chain (transition probabilities) for each application. The transition probabilities P (I, J) for each model of the Markov chain is estimated as the number of transitions of the type of packets in a packet of type I have.

5. Summary

With all the security issues related to wireless sensor networks, it is difficult to determine where to focus their security resources with new implementations. In this section we briefly attack model based on a denial of service and the defense mechanism in which each of the layers of an attack can be defended against. Here we use a reactive approach to intrusion detection, i.e. filtering and detection. In line with this, the model detects abnormal traffic and attack with the transition of the session, observing all traffic without cooperation between neighbors. We assume that when the sensor node, first deployed in the field of environmental protection, the enemy takes some time to expand the attack. This means that no malicious node will appear in the initial deployment of sensor node. Using this model, we determine whether the output STHIDS this invasion. He will then report back to the base station to help them cope with the state system, and further corrections.

6. Conclusion

Security plays an important role in the proper functioning of the wireless sensor networks. Our proposed security system for synchronizing a flooding attack detection model of anomaly detection and signature-based detection model. It filters out a large number of packets entries using TCP packets and performs a second analysis of the detection of the transition state of a session of analysis model based on signatures. In this paper, the main threats is SYN Flood attack was traced back to the sensor network to analyze every packet for each category in the protocol TCP (port, flags, and TCP three-way handshake), and also noted that the threats are easier to detect once we know the behavior of the attack. Thus, the effective detection of the second to take to ensure full discovery. The proposed hybrid approach detection quickly and effectively in the case of densely deployed sensor network base station and the alarm of the infected or abnormal behavior in the flow of traffic. In the future we will implement the proposed scheme in the ns-2 to test its effectiveness in securing sensor networks.

7. References

[1] Arbor Networks. Intelligent Network Management with Peakow Trace. http://www.arbornetworks.com/download.php.

[2] N. Dueld, C. Lund, and M. Thorup. Flow sampling under hard resource constraints. In Proc. of ACM SIG-METRICS, 2004.

[3] Yan, Li and Chen,'A Dos Resilient flow level Intrusion Detection Approach for HighSpeedNetwork'http://list.cs.northwestern.edu/graid.html

[4] K.Q. Yan, S.C. Wang, C.W. Liu,' A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks'IMECS 2009, March 18 - 20, 2009, Hong Kong

[5] Zhang Qianli zhang@compass.net.edu.cn. Li Xing xing@ocean.net.edu.cn. CERNET CENTER, Main building 224 Tsinghua University Beijing 100084

[6] O. Depren, M. Topallar, E.narim and M.K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, 29(4), 2005, pp. 713-722.

[7] S.H.C. Haris, Ghossoon M. Waleed, R.B. Ahmad & M.A.H.A. Ghani 'Anomaly Detection of IP Header Threats' International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6)

[8] Mishra, A., Nadkarni, K. & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks, Wireless Communications, IEEE 11(1): 48 – 60

[9] H. Dahmouni, S. Vaton, D. Rosse' A Markovian Signature-Based Approach to IP Traffic classification'. MineNet'07, June 12, 2007, San Diego, California, USA.