THE PROPOSAL OF HYBRID INTRUSION DETECTION FOR DEFENCE OF SYNC FLOOD ATTACK IN WIRELESS SENSOR NETWORK

Ruchi Bhatnagar [1] and Udai Shankar [2]

[1]Department of Information Technology,
IIMT Engineering College, Meerut, G.B.T.U, Lucknow, India
ruchi.asmank@gmail.com,
[2]Department of Information Technology,
IIMT Engineering College, Meerut, G.B.T.U, Lucknow, India
shankar.udai@rediffmail.com

ABSTRACT

Data security is a huge responsibility for sensor network as there are various ways in which security can be breached, enabling hackers to access sensitive data. Threats to wireless sensor networks are numerous and potentially devastating. Security issues ranging from session hijacking to Denial of Service (DOS) can plague a WSN. To aid in the defense and detection of these potential threats, WSN employ a security solution that includes an intrusion detection system (IDS). Different neural methods have been proposed in recent years for the development of intrusion detection system. In this paper, we surveyed denial of service attacks that disseminate the WSN such a way that it temporarily paralyses a network and proposed a hybrid Intrusion Detection approach based on stream flow and session state transition analysis that monitor and analyze stream flow of data, identify abnormal network activity, detect policy violations against sync flood attack.

KEYWORDS

Wireless Sensor Network, Denial of Service, Intrusion Detection system, State Transition Hybrid Intrusion Detection System, Type of Service.

I. INTRODUCTION

A wireless sensor network is a network of simple sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Since sensor nodes are tightly constrained in processing ability, storage capacity and energy, routing and data aggregation in WSN are very challenging due to inherent characteristics. A notable feature of the architecture of a wireless sensor network is its hierarchy, rooted in a base station. A wireless sensor network often collects and relays data to a back-end server via a gateway or base station. Since sensor nodes are tightly constrained in processing ability, storage capacity and energy thus security and data aggregation in WSN are very challenging. Therefore, sensor network need to become autonomous and exhibit responsiveness and adaptability to evolution changes in real time, without explicit user or administrator action. This need is even more imperative when it comes to security threats, so an

attempt to apply the idea of implementation of an IDS that can detect a third party attempts of exploiting possible insecurities and warn for malicious attack in WSN makes a lot of sense.

As Sensor networks are constrained in resource compared to Ad Hoc and cellular networks (Aboelaze & Aloul, 2005). A typical sensor node such as MICA has an 8 MHz microprocessor, 128 KB program flash memories and 512 KB serial flash memories (Technology, n.d.). WSNs are deployed more densely and randomly in the environment and sensor node failure is likely to happen. So, it is impossible for a sensor node to store the signature data about malicious nodes for the whole network in a manner similar to additional misuse detection. Also, it is very difficult to use traditional anomaly detection methods in WSNs, because sensor nodes cannot monitor all the traffic traversing them and compute anomalous events. These specific characteristics of WSN demand a novel design of the security architecture for such an environment. Though wireless Ad Hoc networks and wireless sensor networks share some common characteristics, and there was development of IDS in a wireless Ad Hoc network (Mishra et al., 2004), R. Roman showed in his paper that they can't be directly applied in WSNs.. In this paper we have made an effort to document denial of service attacks on sensor nodes that is not just intervened the service of sensor nodes by flooding junk information but due to sudden breakdown of nodes loss of information flows as well, and proposed a hybrid system that combines anomaly, and signature based detection based on stream flow and state transition analysis that provide services to shut down the malicious node effectively.

II. RELATED WORK

Some vendors claim to have multi-gigabit statistical IDS's [1], they usually refer average traffic conditions and use packet sampling [2]. Different Artificial Intelligence techniques have been applied both to signature detection and for anomaly detection [6]. Yan [4] proposed hybrid intrusion detection system for Cluster-based Wireless Sensor Network (CWSN) that uses two major models of intrusion detection include anomaly detection and misuse detection. The CH is used to detect the intruders that not only decreases the consumption of energy, but also efficiently reduces the amount of information; therefore, the lifetime of WSN can be prolonged. While our proposal (STHIDS) use anomaly and signature based model with session state transition analysis. The key feature of our proposal (STHIDS) that it is not to violate privacy, since we are interested in only packet header to know whether a state has changed or not, to inspect header only also make this proposal efficient and best fit for a densely deployed sensor node.

In the section III we describe the Denial of Service Attack model while the section IV explained the threat defence model and proposal of state transition HIDS. Section V presents a simulation model. Section VI presents method description simulation model & section VII provide the Method description. Section VIII concludes the work with extension.

III. ATTACK MODEL

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action and an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user [8]. The basic types of attack are: consumption of bandwidth or consumption of processor time,

obstructing the communication between two machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters Denial of Service attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network [3]. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming. The Table below presents the DoS attack at each layer and their defense mechanism:

Table 1.DoS Attack and Their Defence Mechanism

Protocol layer	**Attacks**	**Defenses**
Physical	**Jamming**	**Sleep**
	Node destruction	**Hide nodes or tamper proof packaging**
MAC (Medium access control)	**Denial of sleep**	**Sleep, authentication and anti-replay**
Network	**Spoofing, replaying**	**Authentication, anti-replay**
	Hello floods	**Geographic routing**
	Homing	**Header encryption**
Transport	**SYN flood**	**SYN cookies**
	De synchronization attack	**Packet authentication**
Application	**Path based DoS**	**Authentication and anti replay protection.**

In this paper we taken into account a sync flood attack in which a sequence of TCP session initiation packets, often from incorrect (or "spoofed") IP addresses. The result is that the target tries and fails to establish a number of TCP sessions, which consumes resources on the target.

IV. THREAT DEFENCE MODEL & PROPOSAL OF STHIDS

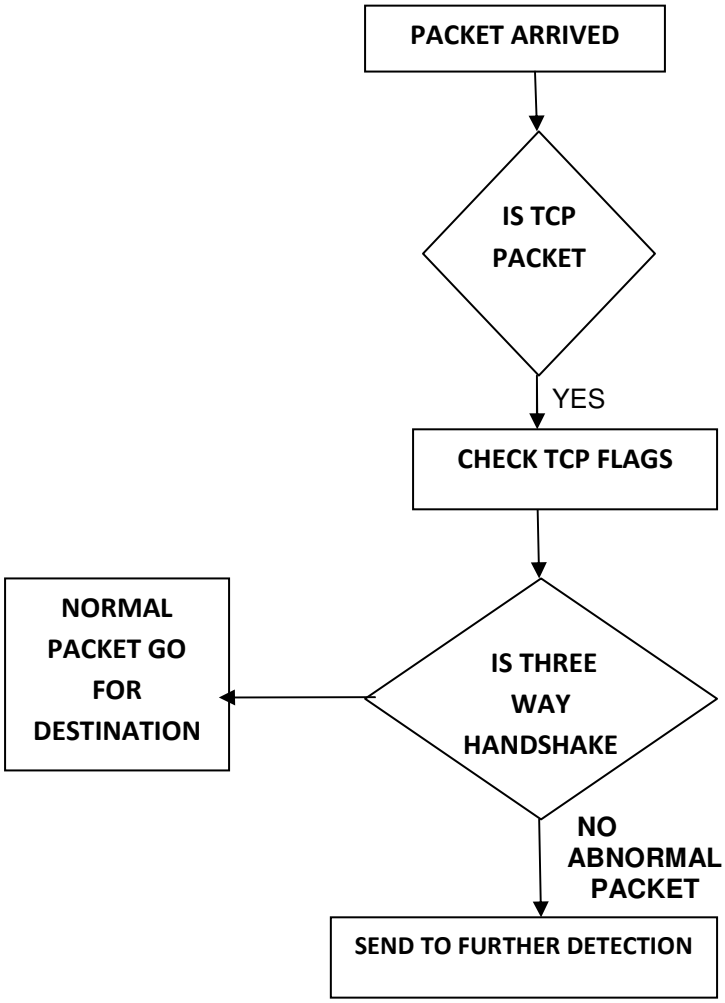
In our threat defence model there are two defense strategies for counter measure against sync flooding; first is filtering the data packets by anomaly based detection model while using signature based session state transition model for 100 % detection and removal of malicious node form the sensor network to protect paralyzing of network. Our approach consist of two models i.e. anomaly detection model and session state transition signature model.

The proposed STHIDS consists of two models i.e. anomaly detection and signature based detection and finally the outputs of anomaly detection and signature detection models report to base station for follow-up work.

Anomaly Detection Model

Anomaly IDS is built by studying the behavior of the system over a period of time in order to construct activity profiles that represent normal use of the system. The anomaly IDS computes the similarity of the stream flow in the system with the profiles to detect intrusions. The biggest advantage of this model is that new attacks can be identified by the system as it will be a deviation from normal behavior. This model plays a role like a filter in this research. Abnormal packets are delivered to the signature detection model for further detection. Because the anomaly detection uses a defined model of normal behavior, a packet is determined to be abnormal by the system when the current behavior varies from the model of normal behavior. As a result, the anomaly detection usually determines the normal communication as abnormal communication, and creates the problem of erroneous classification. Therefore, the anomaly detection model is used to filter a large number of packet records first, and make further detection with the signature detection model, when the amount of information decreases. In this proposed model which filters the infected packets from stream flow for further analysis the filtering of packets illustrate as follows:

The streams of packet go through the anomaly detection software that sniffs data packets and analyze the TCP header since TCP SYN Flooding is the main threat [7]. TCP header is built on top of IP header, which is unreliable and connectionless. TCP header occupies 20 bytes and has some limitations in header length. As mentioned, normal TCP header is 20 bytes but TCP can have another 40 bytes for option. So the header size is limited to 60 bytes. TCP Flags have six flags bits namely URG, ACK, PSH, RST, SYN and FIN, each of them has a special use in the connection establishment, connection termination or control purposes. Only few combinations of the six TCP flags can be carried in a TCP packet. URG and PSH flags can be used only when a packet carries data, for instance a combination of SYN and PSH becomes invalid. Since TCP SYN Flooding attack will flood the network with SYN packets, the three-way handshake application is checked in every packet. At this stage, packets are divided into two groups whether infected packets or normal packets. If the packet is infected, the system will distinguish the packet and go for analysis again to confirm whether the packet is truly comes from attackers. Otherwise, the normal packet will go through the network sending the data to the destination. The detection flow chart is shown below:

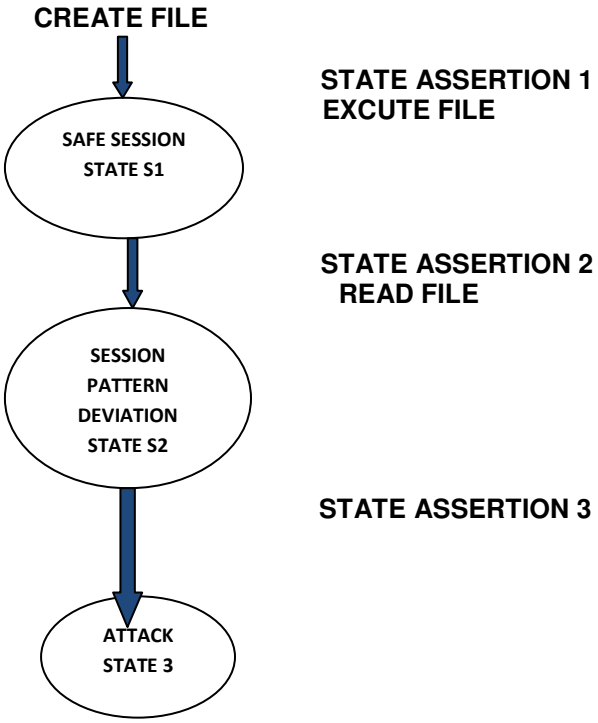


Signature Based Detection

The next prevalent form of intrusion detection model is through signature matching. Referred to as signature-based IDS, our system received the abnormal data packets and match packet attributes against a set of predetermined attack lists or signatures. As the particular network conversation match a signature configured on the IDS, the system alerts base station to take pre-configured action. This paper used the filter data packets and their TCP connection is a session state [5] and has shown that most of the illegal action performed would have something special ongoing in such sessions. Not only the strange packets itself, but the sequence of such packets caused an attack. The SYN flood will create a pile SYN-SYN ACK-RST packets in the network, the scan tools will create SYN-SYN ACK-RST and SYN-RST several kind of patterns in the network, all of these patterns indicate the failure of the connection.

Based on this thought, we have designed the session-state transition analysis. We will define some packets as the indication of the session state. The happening of such packets causes the change of the session state. We store these session states transition patterns into a database; thus we can calculate the happening rates of some specific patterns. Compared with the average level,

abnormal high happening rates often indicate the possible attack or information collection. As we collect all sessions SYN-SYN, ACK-RST pattern to decide whether a normal scan had happened. The session state transition model is as follows:



V. SIMULATION MODEL

For the simulation of proposal we capture the stream flow of TCP packets through the first order Markov chain model the parameters of the model (state transition probabilities) are different for each application and make up the "signature" of the application. As the IP traffic can be represented on three entities: the packet level, flow level which corresponding to a succession of packets with the same 5-tuple, and the session level which is a succession of flows (activity periods) of the application. During its activity period, an application exchanges a typical sequence of control packets (e.g., SYN, ACK, PSHACK, SYN-ACK, etc...) with a remote host (client or server).This sequence is modeled as a first order Markov chain; the different types of control packets exchanged (usually no more than 10, including a “rare” state) make up the states space of this Markov chain and the transition probabilities between states (transition matrix) identify a different “signature” for each application. Thus, the identification of the Markov model associated to the applications can be decomposed into three steps:

First Step: consists in identifying the states space. This amounts to determining the various types of control packets used by the applications.

Second Step: consists in reconstructing the original order of the packets in a flow; this amounts to reorganizing the flows according to their activation order in the session and the packets according to their emission order in the flow.

Third Step: consists in estimating the Markov Chain parameters (state transition probabilities) for each application. The transition probabilities P(i,j) for each Markov chain model is estimated as the number of transitions from a packet of type i to a packet of type j.

VI. METHOD DESCRIPTION

In the experimental description, the proposal is decomposed in to learning and decision step. In the learning step the transition probabilities for each application are obtained from a training dataset with a large number of applications and put into transition matrix. In the decision step to decide by which application a new sequence of packets has been produced; Neyman-Pearson [9] tested. In the case of two simple hypotheses H0 and H1 the Neyman-Pearson lemma states that the likelihood ratio test is the most powerful test of size α. The likelihood-ratio test rejects H0 in favor of H1when the likelihood ratio : $\Lambda(y) = L(y|H0) / L(y|H1)$ is lower than $\zeta(\alpha)$, where the threshold $\zeta(\alpha)$ is set so that the false alarm rate (size of the test) is equal to α : $Pr(\Lambda(y) \leq \xi(\alpha) | H0) = \alpha$.

For the detection of Intrusion the decision rule combines Maximum Likelihood estimation and Neyman-Pearson tests. More precisely, we estimate the likelihood of this sequence for each of the Markov models profiling the applications:

• If the likelihood of the packets sequence is very low for all the applications, we decide that this is probably a “new” application and eventually raise an alarm.

• If the likelihood is much higher for one of the Markov models than for the others, we decide that this sequence has been produced by the corresponding application.

• In some cases, the likelihood value is close for several Markov models. This can happen for example in the case of applications with very similar operation (for example http and https, or different activities using the same protocol).

On the basis of above decision rules the signature detector detects evidence of intrusive activity And also helps the user to handle the system with hybrid detection. In the future we observe the performance on the basis of detection rate, the false positive rate and accuracy.

VII. SUMMERY & DECISION MAKING

With all the security issues concerning with wireless sensor network, it is difficult to determine where to focus their security resources with new implementations. In this section we summarized the attack model based on Denial of service and their defensive mechanism, by which each of layer attack can be defended against. Here we used reactive approach for intrusion detection i.e. filtering and detection. According to this, model detects anomalous traffic patterns and attack with session transition, by observing all data traffic without collaboration between its neighbors. We assume that when a sensor node is first deployed in the environmental field, an adversary requires a particular period of time to deploy an attack. This implies that no malicious node appears during the initial stage of sensor node deployment. Through this model we determine whether or not an output of STHIDS is an intrusion. It then has to report the results to the base station to help them handle the state of the system and make further corrections.

VIII. CONCLUSION

Security plays a crucial role in the proper functioning of wireless sensor networks. Our proposed security framework for sync flood attack detection via an anomaly detection model and a signature based detection model. It filters a large number of packet records, using TCP packet analysis and performs a second detection with the session state transition analysis based signature detection model. In this paper, the main threats is SYN Flood attack had been traced in a sensor network By analyzed every packet to each category in TCP protocol (port, flags, and TCP three-way handshake) and observed that the threats are easier to detect once we know the behavior of an attack. Thus it is effective to take second detection to provide full detection. The proposed hybrid detection approach is faster and effective in case of densely deployed sensor network and alarming the base station about the infected or abnormal behavior in the flow of the traffic. In future we will be implementing the proposed scheme in ns-2 to check its effectiveness in securing sensor networks.

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.