Confined Anticipation Based Intrusion Detection System and Intrusion Prevention System In WSN

[1]K.Abinaya , [2]Mrs V.Sathya
[1]*M.E (CSE) , Avc college of engineering , Mayiladuthurai*
[2]*Asst prof , CSE , Avc college of engineering*
Mayiladuthurai

Abstract—

The importance of accurate intrusion detection system is growing tremendously the malicious network traffic activity have also grown significantly. Intrusion Detection Systems (IDSs) provide automatic detections to security violation like denial of service (DoS), virus, port scan, buffer overflow, CGI attacks, clogging or flooding etc., For network and host based system, the most widely used to and effective approach is data analysis with signature-based detection method. Thus, the success of the detection system depend on the real appearance of the security violation, detection of the violation and response times. IDS and IPS is one of the system that access the standard application which continuously monitor the network traffic to detect and prevent the attacks. It does not require prior Knowledge of the attack. It can prevent according to static and anomaly based rules. This work focus on IDS in the same network to detect the intruder from the filter of the IDS package. In this project, we are going to analyse the performance of Network Intrusion Detection System using snort tool. In existing system, inspects all snort rules applied for each incoming packets. It takes lot of time to examine all incoming packet using all snort rules and also create unwanted wrong alert. In order to overcome this, we are implementing two indexing methods (prefix and random indexing) to generate primary patterns, which have small number of rules from the set of snort rules.

Keywords— *IDS,IPS,WSN, prefix indexing, random indexing.*

I. INTRODUCTION

The network intrusion detection system is an important tool of the network security that helps in determining, discovering and identifying security violations like unauthorized uses, alteration, duplication or any destruction of information system. The network base IDS decides whether a specific activity is valid or intrusive based on network audit data, and most of the network based IDS can works in line with other security tools like firewalls, antivirus etc., Due to the large amount of network audit data, it is only possible to secure and monitor the network by a dedicated intrusion detection and prevention system. The NIDS can monitor the incoming packets and analyzes them to detect different type of attacks and probes. If we can detect the malicious packets in time. Then we can prevent the destruction by dropping the packets or taking proper action against it. This detection and prevention only can be done when system has high scalability and less human intervention. Snort is an effective open source network intrusion detection and prevention system based on rule signature and anomaly inspection method which can perform real time analysis for network traffic. Snort has four different deployment modes such as a packet sniffer, a packet logger, a honeypot monitor and a network intrusion detection system. So we have used snort to implement our both indexing methods. The snort IDS consists of several components such as packet sniffer, preprocessor, decode engine, detection engine, and logging/alert and output module. To analyzing techniques including pattern checking, statistical analysis, machine learning, file integrity checkers, and artificial immune system methods. We describe the implementation of algorithm and methodology for indexing.

II. LITERATURE SURVEY

Mishra & Shukla[1] Discuss about the attacks to protect end-users as well as the network infrastructure resources. The core of this work is to implement the Intrusion detection system (IDS) which is located at the Internet service providers (ISP) level. Using our self-developed simulation software, it will be shown that how ISPs form the protection rings around the host to collaborate and defend the traffic information. DDoS can shut down an organization for hours – or even days hence making it difficult for organizations to restore back to its place. Right now, the problem in today's world is the increase in growth of Cyber-attacks exponentially making it more difficult and difficult to identify the need for a better Intrusion Detection System. The problem are occurs with current Intrusion Detection System which generates high rate of false alarms. Our

main objective is to creates a model simulation showing the attack happen at the ISP level using the network node. Samrin & Vasumathi[2] Presented the data mining methods is broadly used for extracting useful information from the massive amount dataset. This paper present the investigation of different technique and intrusion classification on KDD Cup dataset. So, by classifying the different network issues a new and effective technique is implemented which can categorize and identify intrusions in the KDD Cup 99 dataset. The objective of the HIDS is the controlling state and dynamic behavior of the computer system. This detection system checks all the activities of inspected packets on a network. HIDS recognize what resources are being utilized and which program gets to those resources. If in the network any alternations or adjustment happens, system administer receive some network alerts. HIDS is progressively becoming essential to ensure the host computer frameworks and its network activities. HIDS with host based information is incorporated into the computer frameworks to identify the intruder abnormal activities, noxious Behavior, application abnormalities and preserve the Information Systems from intruders and report the occasions to the HIDS System Administrator. After surveying the various Anomaly based IDS technique concluded that single technique is not able to provide accurate detection rate. Korba et.al.,[3] Focus to avoid the fast forwarding process employed by rushing and wormhole nodes, we use a statistical anomaly-based technique. The idea is to enable cluster head nodes (CHs) to detect that malicious node has a high capacity of competition in route selection. The goal is to select routes that do not pass through loaded cluster nodes which have high selection rates. This approach not only detect malicious node but also balances load by eliminating traffic concentration points from the network. However a legitimate node may be placed at a key location of connectivity in the cluster, and thus can be detected as malicious node because of its high route selection rate. Lin et.al.,[4] Discuss the MAIS model, a non-self-detector set is trained using Negative Selection to identify self and detect non-self. A second detector set is trained to identify non-self and detect self. The second detector set is referred to as the self-detector set. These two detector sets are used in a Proportion Based Classification method (see below) to identify and detect new instances. The two detector set are used in a proportion based classification methods to detect unknown instances. The proportion of non-self-mature detector that match an instance is greater than the proportion of self-mature detector that match of instance, the instance is classified as non-self. Likewise, if the proportions of self-mature detectors that match are greater than the proportion of no self-mature detectors, the instance is classified as self. Since, false negatives (FNs) have the potential to cause significantly more damage than those of false positives (FPs), in the rare case that the proportions of the two independent detectors set are equal, the instance is classified as non-self. Fekolkin[5] Focus the proposed system includes both internal as well as external intrusion detection mechanisms. System contains two algorithms to detect intrusion. System detects both internal as well as external attacks, in integrated way. In proposed system, when multiple computers are attached to each other, each system has its internal intrusion detection mechanism and for external intrusion detection FGA is used. In internal intrusion detection system, signature matching algorithm is used. When user fires query on database, it is checked using algorithm. In processing of algorithm, fired query is compared with stored signatures of malicious queries. If similarity index exceeds defined threshold then it is classified as anomalous query and notification is given to admin to take further actions. Different techniques such as Neural Network, Clustering, and Genetic algorithms are present to detect intrusion.

III. ARCHITECTURE DIAGRAM

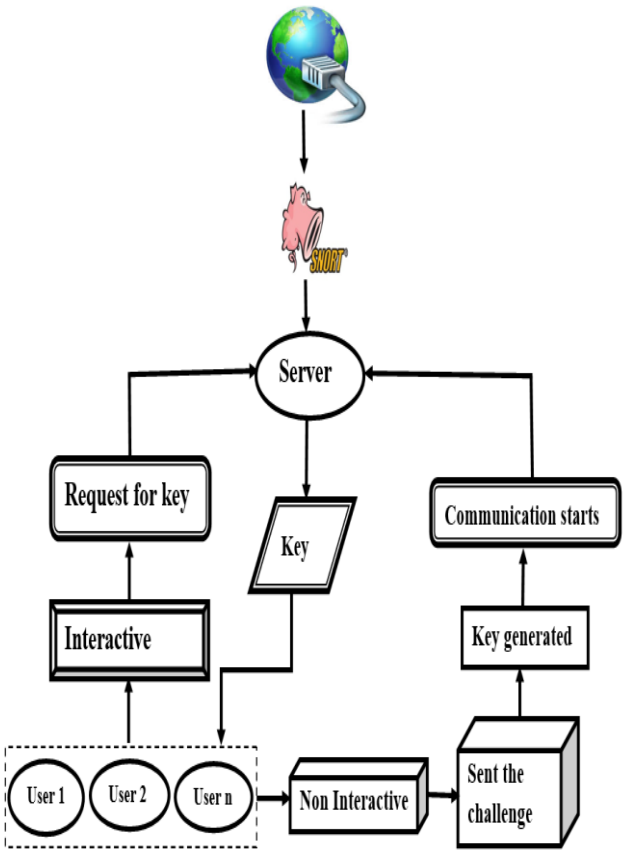

Figure1.1 System architecture

Lot of retinal images are stored in the database for training purpose. The test image is given to the preprocessing stage for the removal of noise. Then the filtered image is given to the feature extraction process.The hog and surf features are extracted from the corresponding image. The

extracted feature image is given to the SVM classifier for detecting the location of diabetic retinopathy and it classifies the affected and non affected part of that image.

IV. METHODOLOGY

Following the main stages in IDS and IPS

A. *Key Generated*

Challenging your Neighbor is defined to trust and authenticate a new node, we can challenge your neighbor to add that node into the network. A node having its neighbors in its friend list does not need to challenge them before a data session. When the networks is newly initialized to each nodes a stranger to another. Thus each node incorporates its neighbors in the unauthenticated list. The node pick to one of the neighbor, and perform the usual Share Friend Stage. As a response the neighbor node either sends its friend list or the nodes from its unauthenticated list if the friend list is empty.

B. *Generation of primary pattern*

To make a primary pattern two different indexing method is used.

Prefix Indexing: This method is pre-filtering process, to minimize number of rules to match against each packet for IDS based on an indexing algorithm. Prefix indexing finds common prefix strings that are shared by other rule signature.

Aho-corasick Algorithm: Extract N bytes of a substring from a snort signature string and compare them with other signature strings. The prefix indexing find common prefix string as primary patterns.

Random Indexing: To group the snort rules based on primary pattern. That generate randomly from snort rule's signature strings. To select the random string from its signature.

C. *Detection Engine*

The main functionality of a decoder is setting up the pointers into the packet data so the detection engine can analyze them later on. The detection engine applies the Snort rules against decoded packets to detect attacks. Rules maintain two main parts, Header and Options. The detection engine only examines those header and options that have been fixed up at run time by the rules parserThe detection engine applies the snort rules against decoded packet to detect the attack. Rules maintain two main part: Header, Option. The detection engine only examines only those header and option and fixed at run time.

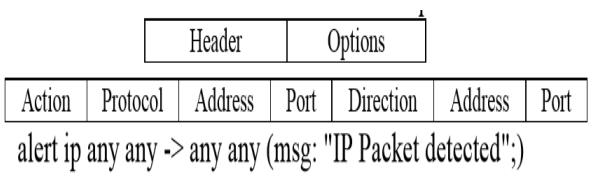

Figure3.3.1 Detection Engine

D. *Routing Efficiently*

The data can be send through the single routing path the data sending and receiving time should be increased and the data rate can be decreased and data sharing performance can be delayed by the present using algorithms. The data can be send and receive through set the path using the genetic algorithm to efficiently send the data to the receiver and the data rate can be increased and sets the different path to send the data and increased to data rate and the net rate efficient schedules the data and the shared to the data efficiently**.**

V. EXPERIMENTAL ANALYSIS

Our proposed project will be implemented with windows8 with i5 processor with the help of snort tool and R program.

Use the prefix indexing method pre-filtering process to minimize number of rules to match against each packet for IDS based on an indexing algorithm. We adopt an Aho-Corasik (AC) algorithm to generate primary patterns form Snort rule signatures. This algorithm extracts the first N bytes of a substring from a Snort signature string and compares them with other signature strings. By these comparisons, prefix indexing finds common prefix strings that are shared by other rule signatures. We use these common strings as our primary patterns for inspection of incoming network packets. Random indexing to group the Snort rules based on primary patterns that we generate randomly from Snort rule's signature strings. To select the random string from its signature, we used the naive approach based on random indexing. This naive approach extracts an N bytes substring from Snort rule signatures.

Aho-Corasick Algorithm

Aho-Corasick(P={p^1,p^2,…p^r},T=t1,t2,…,t_n)

1. Preprocessing
2. AC€ Build_AC(P)
3. Searching
4. Current€ Initial state of the automaton AC
5. For pos c 1…n Do
6. While 6_{AC}(Current,t_{pos})=0 AND S_{AC}(Current) Ç 0 Do
7. Current € S_{AC}(Current)
8. End of while
9. IF 6_{AC}(Current,t_{pos}) Ç 0 Then
10. Current € 6AC (Current, t_{pos})
11. Else Current € initial state of AC
12. End of if
13. If Current is terminal Then
14. Mark all the occurrences (F(Current),pos)
15. End of if
16. End of for

Sample input:

Input text=”error_while_running_snort”

Set of strings P= {hey, ho, hey, error, error, hey} Output: ho, hey, error

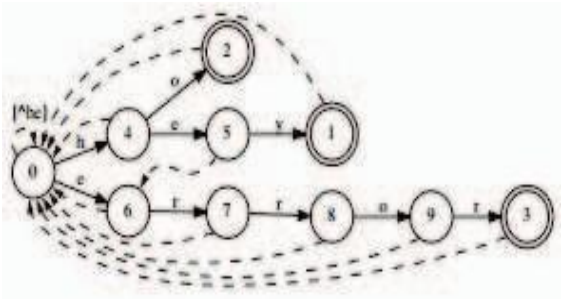

Figure:4.1.1 Aho-Corasick automaton with transitions

VI. CONCLUSION

In this implemented two indexing methods to improve the performance of intrusion detection systems. In general, IDS sensor examine packet against all signatures in signature based IDS. This approach is efficient to reduce false positive significantly but inefficient to improve the detection rate. In particular, IDS performance can be improved if we can reduce comparison time and the number of signatures that need to be examined. In our work, we applied prefix and random indexing that extracts strings to create primary patterns from Snort rules. Our research results shows that our approach has better performance in detection rate and in reducing false positives since primary pattern helps to reduce the rule signature comparison and improve the detection. It conducted a number of experiments at AEI, which shows very significant improvement of our IDS prototype. Our IDS prototype detection rate is improved by 42% and false positives decreases by 73% comparing to Snort IDS. Our proposed IDS can be used as cost effective and high efficient IDS in small to large network. So as a future opportunity it can work on how to improve the sensitive threat detection rate. We also need to do simulation to understand the estimated signatures that need to be examined for each incoming packet, and computational cost.

FUTURE WORK

To improve the sensitive threat detection rate. It also need to understand the estimated signatures that need to be examined for each incoming packet, and computational cost.

REFERENCES

[1] Mishra, V. P., & Shukla, B. (2017, December). Development of simulator for intrusion detection system to detect and alarm the DDoS attacks. In Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on (pp. 803-806). IEEE.

[2] Samrin, R., & Vasumathi, D. (2017, December). Review on anomaly based network intrusion detection system. In Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), 2017 International Conference on (pp. 141-147). IEEE.

[3] Korba, A. A., Nafaa, M., & Ghamri-Doudane, Y. (2016, November). Anomaly-based intrusion detection system for ad hoc networks. In Network of the Future (NOF), 2016 7th International Conference on the (pp. 1-3). IEEE.

[4] Su, M. Y., Yu, G. J., & Lin, C. Y. (2009). A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach. Computers & security, 28(5), 301-309.

[5] Fekolkin, R. (2015). Intrusion Detection and Prevention Systems: Overview of Snort and Suricata. Analysis.

[6] Mukkamala, S., Janoski, G., & Sung, A. (2002). Intrusion detection using neural networks and support vector machines. In Neural Networks, 2002. IJCNN'02. Proceedings of the 2002 International Joint Conference on (Vol. 2, pp. 1702-1707). IEEE.

[7] Mishra, V. P., & Shukla, B. (2017). Process Mining in Intrusion Detection-The need of current digital world. In Advanced Informatics for Computing Research (pp. 238-246). Springer, Singapore.

[8] Fekolkin, R. (2015). Intrusion Detection and Prevention Systems: Overview of Snort and Suricata. analysis, 10, 11.

[9] Hassan, M. M. (2013). Current studies on intrusion detection system, genetic

[10] algorithm and fuzzy logic. arXiv preprint arXiv:1304.3535.