© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Intrusion Detection in Wireless Sensor Network using Behaviour Based Technique with Real Time Network Traffic

Prof. Deepak Singh Rajput, Nitesh Kumar Singh

Gyan Ganga Institute of Technology and Science, Jabalpur, Madhya Pradesh, India

ABSTRACT

This paper will look at the nature and structure of wireless sensor network attacks and the tools, actions and processes that can be used to identify and respond to such attacks. A brief overview examining the anatomy of an attack and the creation of botnets will be presented and the motivation that drives such on-line malicious activity, the type of tools that are used in modern attacks, which is behind these and the impact they have will be discussed. Identifying attack streams and understanding the nature of TCP/IP traffic will be discussed through the use of Wireshark and their operation and contribution to combating malicious network activity will be considered. As practical, hands-on exercises, participants will be able to simulate a network attack and response scenario by trying to penetrate a remote network while at the same time protecting their own network from attack. This will be done using the tools and techniques discussed earlier and by remotely accessing a real wireless sensor network (WSN) running in the NS-3 Simulator.

Keywords : WSN, NS-3, TCP/IP, Wireshark

I. INTRODUCTION

Internet is forcing organizations into an era of open and trusted communications. This openness at the same time brings its share of vulnerabilities and problems such as financial losses, damage to reputation, maintaining availability of services, protecting the personal and customer data and many more, pushing both enterprises and service providers to take steps to guard their valuable data from intruders, hackers and insiders. Intrusion Detection System has become the fundamental need for the successful content networking.

IDS provide two primary benefits: Visibility and Control [1]. It is the combination of these two benefits that makes it possible to create and enforce an enterprise security policy to make the private computer network secure. Visibility is the ability to see and understand the nature of the traffic on the network while Control is the ability to affect network traffic including access to the network or parts thereof. Visibility is paramount to decision making and makes it possible to create a security policy based on quantifiable, real world data. Control is key to enforcement and makes it possible to enforce compliance with security policy.

1.2. Types of Ids

Depending upon the level of analysis IDS is classified into two major types:

Network based IDS (NIDS):

Monitors and analyzes the individual packets passing around a network for detecting attacks or malicious activities happening in a network that are designed to be overlooked by a firewall's simplistic filtering rules.

Host based IDS (HIDS):

Examines the activity on individual computer or host on which the IDS is installed. The activities include login attempts, process schedules, system files integrity checking system call tracing etc. Sometimes two kinds of IDS are combined together to form a Hybrid IDS.

II. METHODS AND MATERIAL

A. Related Wok

Anomaly Detection Pre-Processor

This module helps to detect network based intrusions which manifests in abnormal network behaviour. It runs in two phases, learning (Training) mode and detection mode. In the learning mode, the module learns the traffic pattern of the entire network and records the corresponding network parameters. Once the learning is over, the network profile is generated using the profiler program. This profile is used to detect the anomalies when the module runs in the detection mode.

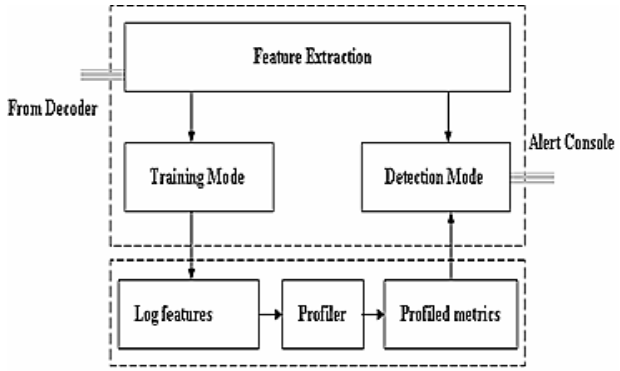

Figure 1 : Structure of Anomaly detection pre-processor

It performs following functionalities: In the Learning mode Measures the network parameters atregular intervalsasconfigured by user Stores these values into a log file at regular interval IntheDetection mode Measures the network parameters at regular intervals Reads baselined values from the file Finds statistical deviations (Mean and Variance) Computes values for Hotelling's expression and Bayesian discrimination function Triggers the alerts on detecting any abnormalities in the traffic pattern main part of the entire system which is responsible for detecting the attack signatures in the pre-processed packets. The overall system performance directly depends on this module. Some of the main functions handled by this modulearelisted below. Parses the rules and build an internal data structure that holds the rules in a customized tree structure. Once the tree is built, loads it into memory. Passes traffic through this rule tree for comparing the packet header anddata against the rules. (Uses strings matchingalgorithms) Report to Alert module on packets that have found to be carrying malicious data. If any new rules have been added or if existing rules are modified or deleted then updates the same to the detection engine treestructure. When the application is exited this will clean up all memory allocated for building the detection engine.

B. Proposed Work

We want to enhanced the time based mechanism and make real time IDS. [1] An attack on network can be in 5 phases, which are Reconnaissance, Scanning, Gaining access, Maintaining Access and Covering tracks [2]. Identifying the first 2 activities will let the administrator to prevent the attack from doing further damage to the service offered by the network. The attack can be launched in term of fast attack or slow attack.

Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [3]. Meanwhile, **slow attack** can be defined as an attack that takes a few minutes or a few hours to complete [4]. Both of the attack gives a great impact to the network environment due to the security breach. Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack. IDS acts as the monitoring tool to capture and analyze the network traffic for any anomalies activity.

Author of [1] used the Novel (Anomaly detection) approach to identify the intrusion (attacks). A novel methodology on detecting fast attack using time based detection technique for intrusion detection system.In this methodology the features capture from the network traffic is computed with respect to the time. The derived time based features from this methodology can help identify fast attack since the detection is based on the number of time the attacker made towards the host in second. Thus focusing in the time based features the early detection of the attack can be achieved and the security personnel can directly do the necessary action to stop further damages.

The efficiency of an IDS depends on the decision upon a set of features that the system is going to use for detecting the attacker especially the fast attacks. This is because the mechanism of a fast attack requires only a few seconds and the technique used by the attacker to

launch the attack is also different [12]. Figure 2 show the methodology used in time based IDS by [1].

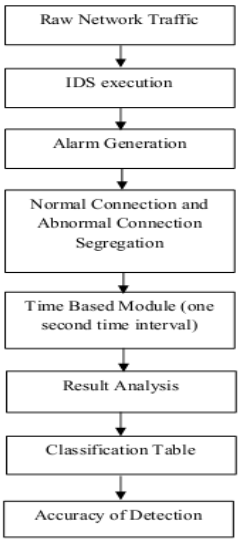

Figure 2 : Methodology of time based IDS

We have new idea to detect fast type attack that is the current requirement of an today's successful IDS because the today's Internet provide very high speed even to home users, so attackers easily attack to target machine if no security major have been adopted.

Following is our major concerned to improve the existing time based technique We used WIRESHARK [13] application to capture the network traffic.

We are also extend our research to different types of protocol used as carrier to launch attack like TCP protocol since TCP protocol is widely used protocol [14] as well as UDP and ARP (to detect MAC spoofing)and our future work will be to prevent DDoS (Distributed Denial of Service) attack .

Due to huge amounts of network traffic, it is difficult to distinguish the normal and abnormal behavior of network traffic [5]. Therefore we used current intrusion detection system Snort in default configuration to distinguish the normal and abnormal behavior of the network traffic.

System Domain

NS-3.20 will be used as a testbed of sensor network with ubuntu14.04.

III. RESULTS AND DISCUSSION

Simulation and Result

Our simulation is on ns-3 and All of are discrete-event network simulator, primarily used in research and teaching. Ns-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use. The goal of the ns-3 project is to create an open simulation environment for networking research that will be preferred inside the research community :

Our proposed method will be tested under NS-3.20 on Ubuntu 14.04 system Steps:

Processor and sensing capabilities	SA 1100,
Power for a node	Single 3.4v dc
Simulation area	1000*1000 Meter
Data Transmission renge	1 mb/s up to 10 meter`
Data Packet size	2500 byte
Data flow rate	20 kb/s
Mobility model	Constant mobility model
Routing protocol	AODV Routing Protocols

Figure 3 : Simulation Environment

1. **Creating of Sensor Network –** For creating sensor network we will use **Wi-Fi node** of NS-3 which is worked as **sensor node**.

   Then we will create **sinks nodes** which receive data from sensor node.

2. The number of nodes will be vary (number of sinks nodes are also) and tested under simulation.
3. **Types of topology -** Two types of topology we will prefer for better approximation of WSN Mobile (sensor moves are roam) Integrated Under different propagation loss model.
4. **Routing -** For better results we will use two famous routing protocols of different approach - AODV
5. **Energy Model –** This is the core thing of our proposed work. For calculating energy node we will apply energy module of NS-3 on each node.

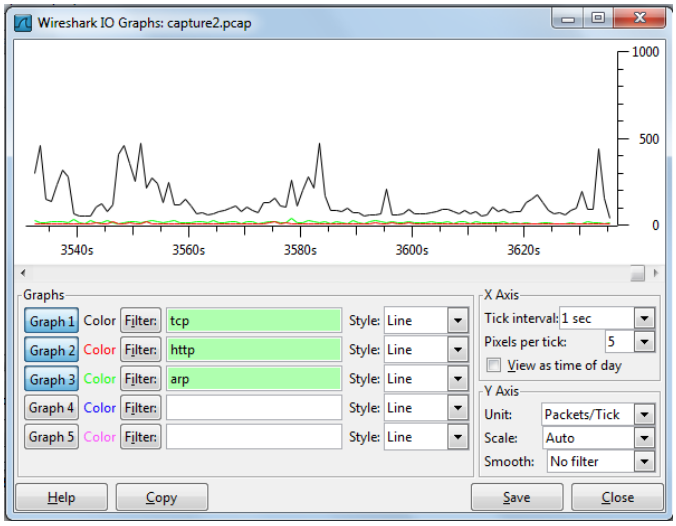

Figure 4 : Comparison Graph of Captured Trace TCP,HTTP and ARP Protocol

Comparisons table of existing work and proposed work as follows

Node id		Energy efficiency		PMR		PMIR		Execution time and packet	
Existing Work	Purposed Work	Existing work	Purposed work	Existing work	Purposed work	Existing work	Purposed work	Existing work	Purposed work
1	1	26J	0.50J	Not implement	10%	Not implement	0	1896(pkt) 38928 sec	3789(pkt) 62.57sec
2	2	26J	0.50J	Not implement	0	Not implement	0	1897(pkt) 38929sec	3913(pkt) 62.55sec
3	3	24J	0.50J	Not implement	60%	Not implement	8%	1898(pkt) 38930 sec	3937(pkt) 62.56sec
4	4	40J	0.50J	Not implement	0	Not implement	0	1899(pkt) 38931sec	3922(pkt) 62.55sec
5	5	21J	0.50J	Not implement	0	Not implement	90%	1900(pkt) 38932se	3914(pkt) 62.55sec

PARAMETE	BASE PAPER	OUR WORK
Routing	*Routing device*	*On demand routing protocol AODV*
Traffic	IDS device identification of malicious traffic	Wire shark is used identify malicious traffic in real environment(WSN)
Simulation	Hardware device	NS-3 simulator for crea Wireless sensor Network using Standard c++ language.
Energy Nodes	Yes	Yes
TCP strea	No	Yes
Nodes	40	Nodes based on requirement
Mobility model	No	Random Way point mob model
Reroute technique	Yes(Based threshold)	Use filtering rule on stream for isolation malicious traffic.
Energy	Calculated base routing	"Energy source model used for better energy calculation based on real time data

IV. CONCLUSION

This paper present framework of project, discussed the design and development of "Anomaly based intrusion Detection system in Wireless sensor network(WSN)" which is built on top of an existing open source signature based network IDS, called WIRESHARK so to have both the analysis techniques in a single package Presently, the work caters only to identify and classify the events into normal and attack classes. It can be extended to detect and classify the attacks into multiple attack classes. Dynamic updation of the Anomaly Model can also be considered for future enhancement. Different Analysis techniques like HMM and Fuzzy Logic can also be tried as alternative techniques for anomaly detection.

V. REFERENCES

[1] M. Mahoney and P. Chan, "PHAD: Packet header anomaly detection for identifying hostile network traffic", Technical report, Florida Tech., technical report CS-2001-4, April 2014,http://citeseer.ist.psu.edu/mahoney01phad.html

[2] Mahoney M. and P. Chan, "Learning models of network traffic for detecting novel attacks", Technical report, Florida Tech 2012, http://cs.fit.edu/~mmahoney/paper5.pdf

[3] D. Barbara, N. Wu and S. Jajodia, "Detecting Novel Network Intrusions using Bayes Estimators", Proceedings of the 1st SIAM International Conference on Data Mining, 2013.

[4] Jack Koziol, "Intrusion Detection with Snort", Pearson publications, 2013

[5] R. Dan Reid & Nada R. Sanders, "Operations Management", 3rd edition., Wiley ,2012

[6] P. Cisar, S. M Cisar, "Quality Control in Function of Statistical Anomaly Detection in Intrusion Detection Systems", SISY 2012 - 4th Serbian-Hungarian Joint Symposium on Intelligent Systems,

[7] DARPA Intrusion Detection Evaluation, Data Sets and Documentation, 2011
[8] Giorgio Giacinto, Fabio Roli, Luca Didaci, ”Fusion of multiple classifiers for intrusion detection in computer networks”. Pattern Recognition Letters 24(12): 1795-1803 (2013)
[9] R. Puttini, Z. Marrakchi, and L. Me. “Bayesian Classification Model for Real Time Intrusion Detection”, in 22th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering, 2012.
[10] A. Hossain, S. Chakrabarti and P.K. Biswas “Impact of sensing model on wireless sensor network coverage”, IET Wireless Sensor Systems, doi: 10.1049/iet-wss.2011.0101, 2011.
[11] Cardei, M., Wu, J.: ‘Energy-efficient coverage problems in wireless ad hoc sensor networks’,Comput. Commun. J., Elsevier Sci., 2014, 29,(4), pp. 413–420
[12] Tsai, Y.-R.: ‘Sensing coverage for randomly distributed wireless sensor networks in shadowed environments’,IEEE Trans. Veh. Tech., 2012,57, (1), pp. 556–564
[13] Elfes, A.: ‘Occupancy grids: a stochastic spatial representation for active robot perception’, in Iyenger, S.S., Elfes, A. (Eds.): ‘Autonomous mobile robots: perception, mapping and navigation’ (IEEE Computer Society Press, 2011), vol. 1, pp. 60–70
[14] Liu, B., Towsley, D.: ‘A study on the coverage of large-scale sensor networks’. Proc. 1st IEEE Int. Conf. on Mobile Ad Hoc and Sensor Systems (MASS 2014).