Layered Approach for Intrusion Detection in WSN

Mayur Dhaye
Department of Information Technology
Maharashtra Institute of Technology
Pune, India
mayur.dhaye8@gmail.com

Himangi Pande
Department of Information Technology
Maharashtra Institute of Technology
Pune, India
himangi.pande@mitpune.edu.in

***Abstract*—The essential component in WSN are the Intrusion Detection Systems. As the network technology is growing rapidly, the main focus of intrusion detection has shifted from simple signature matching approaches to detecting attacks based on analyzing contextual information. It may be specific to individual networks and application. Because of this reason, hybrid and anomaly intrusion detection approaches have gained significance. some of the common attacks that affect network resources are Denial of Service Attacks (DoS), Probe, User to Root (U2R) and Remote to Local (R2L) [1]. Intrusion detection faces a number of challenges like it must reliably detect malicious activities in a network and cope up with large amount of network traffic. We demonstrate that high attack detection accuracy can be achieved by using some features.**

Keywords- IDS; Layered Approach; Conditional Random Field;, Signature and Anomaly Based IDS

I. INTRODUCTION

The art of detecting, inaccurate, inappropriate or anomalous activity inside and the network environment is known as Intrusion detection. It is the network administrator's most important task. The main aim of intrusion detection system is to find the attacks which are specified in the signatures, as well as finding the new or unseen attacks effectively and to cope up with large amount of network traffics. Low FAR (False Alarm rate) value is the main key factor in any IDS, that is the System must be accurate enough to find the attacks. Many kinds of IDSs are present these days. Each has different features which detects different kind of network attacks[2][6].

*NIDS (Network Intrusion Detection Systems***)** are placed at a specific point or points within the network to monitor traffic to and from all devices on the network. It performs the task of analyzing passing traffic on the entire subnet, works in a promiscuous mode, and the traffic that is passed on the subnets is matched to the library of known attacks. The alert can be sent to the administrator once an attack observed having abnormal behavior is sensed.

HIDS (Host Intrusion Detection Systems) run on individual devices or hosts on the network. A HIDS monitors the outbound and inbound packets from the device only and will alert the administrator or user if suspicious activity is detected. It captures a snapshot of existing system files and try to matches it to the previous snapshot. If the critical system files were found to be modified, an alert is issued to the administrator to investigate.

A signature based IDS will try to monitor packets on the network and compare it with or against a database of signatures or attributes from known malicious threats. In the same way the antivirus software also works. The problem is that there may be a lag between a new threat being discovered and the signature for detecting that threat being applied to your IDS. During the lag time which is observed, your IDS would be unable to detect the new threat.

Anomaly Based IDS will monitor network traffic and try to compare it against an established baseline. The baseline will decide what is "normal" for that network- what type of bandwidth is generally used, what protocols we can used, what ports and devices may be connect to each other- and will alert the user or administrator when traffic is detected which is significantly different or anomalous, than the baseline. The problem is, it may raise a False Positive alarm for a authorized use of bandwidth if the baselines are not intelligently configure.

Another approach for detecting intrusions is that integrating the anomalies and Signatures in the network environment. Because of this, we can find the attacks which are newly found in the environment or specified in the database as well. This process will give the high efficiency of finding the different kind of network attacks which results in better classification test on the observed data. The Generic representation of this system is shown in figure 1.

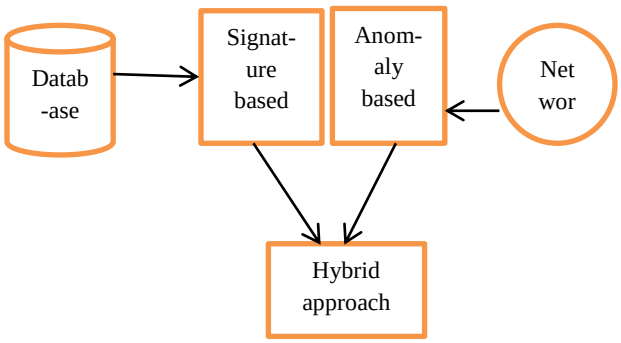

Figure 1. Generic representation of system

II. RELATED WORK

A. *Layered approach for Intrusion detection*

The concept of Layer-based Intrusion Detection System (LIDS) is like there should be a number of security checks that are performed one after the other in a sequence. So, the layers are deployed in a sequential manner. This approach having the advantages that we can increase or decrease the layers as we required, it will increase the high efficiency of the System. Each layer has the following units which are shown in Figure 2.

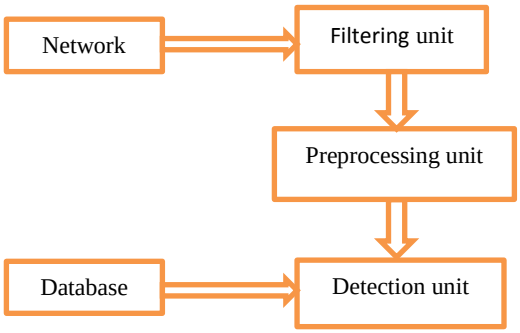

Figure 2. Layered representation

Filtering unit :

As shown in the figure 2, the software named WinCap provides facilities to capture raw packets and filter the packets according to user specified rules before dispatching them to the application.

Preprocessing unit :

One class called as a packet is defined by the preprocessor and this class will store all the packets that are generated by the Filtering unit.

Database:

It is a specially prepared pattern database. For the analysis of such patterns lot of signatures are present in the database. The use of snort is considered for this kind of purpose.

Detection unit :

It takes packets from preprocessor and compares them with special signatures from the database. Result of the comparison is sent to the output module, and a report is prepared.

B. *Multi Layered Approach*

A three layer system is proposed to ensure complete security viz. availability, confidentiality and integrity, each layer corresponding to one aspect of security. The layers are not overlapping and sequential i.e. layer one is followed by layer two which is followed by layer three, where each layer has some unique features and some features from its previous layers. This ensures that each layer is stand-alone and is able to effectively block the type of intrusion which it is meant to block. Sharing of some features from previous layers is necessary to ensure that the layers are linked together. Various semantic features needs to be related to the non-semantic feature such as connection features to ensure better detection capabilities [3].

C. *Feature Selection for Layers*

Feature work of selection is performed automatically. The various methods of automatic feature selection were not found to be effective. To detect a single type of attack category, each layer is separately trained. The attack groups are different in their impact and hence, it becomes very necessary to treat them differently. Based upon the type of attacks that the layer is trained to detect features are selected for each layer.

D. *Integration of layered approach with Conditional Random fields*

In previous sections we proposed two approaches called CRFs and Layered Approach for improving accuracy and efficiency respectively. To build the single system that is accurate in detecting attacks and efficient in operation integration of these two approaches is performed [4].

III. PROPOSED METHODOLOGY

Detection at single layer is not a good approach to remove most of the attacks. We should provide detection at different layers of model so that attacks which are occurring at different layers should be detected properly. So, we are providing such detection at different layers i.e probe, DoS, U2R and R2L layers so that most of the attacks are detected and our system will be more secure.

We are detecting the attacks at different layers using some features which are listed below. If that features matches then only detector allow it to go in next layer otherwise it will drop that packet. If it fulfills all the requirements then only packet will reach to destination. Following are the layers on which we are going to work.

The main goal of using a layered approach is to reduce overall and computation time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. This can be achieved by making the layers self-sufficient and autonomous to block an attack without the need of a central decision maker. Every layer in layered intrusion detection system framework is trained separately and after that deployed sequentially. We define four layers that correspond to the four attack groups mentioned in the dataset. They are probe layer, DOS layer, U2R layer and R2L layer. Each layer is then separately trained with a small set of relevant features[5].

Each record should be represented by 41 different features, each representing a separate connection and is therefore considered to be independent of any other record. The training data is either marked as normal or as one of the 24 different kinds of attack. The 24 attacks can be grouped into four classes: Probe, R2L,DoS, and U2R[6].

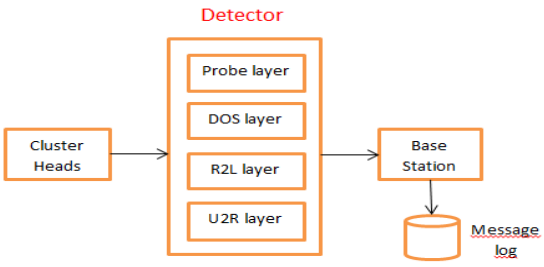

Figure 3. Architecture Diagram

Probe Layer

Probe attacks are detected by the Probe Layer. These attacks aim on acquiring the details about the target network from a source which is external to the current network. So, the basic connection level features such as the "source bytes" and "duration of connection" are significant for finding those kind of attacks[7].

TABLE I. PROBE LAYER FEATURE

Feature Number	Feature Name
1	Duration
2	protocol_type
3	service
4	Flag
5	src_bytes

DoS Layer

The DoS attacks are detected by this layer. These attacks force the target node to stop the services. Which are provided by flooding it with illegitimate requests. Hence, the traffic features such as the "percentage of connections having same destination host and same service" and packet level features such as the "source bytes" and "percentage of packets with errors" are enough for finding the DoS kind of attack[8].

TABLE II. DOS LAYER FEATURE

Feature number	Feature Type
1	Duration
2	protocol_type
3	Service
4	Flag
5	src_bytes
10	Hot
11	num_failed_logins
12	logged_in
13	num_compromised
17	num_file_creation
18	num_shells
19	num_access_files
21	is_host_login
22	is_guest_login

R2L Layer

The Remote to Local attacks are identified here. In a R2L attack, the vulnerability for local access is exploited. They are very difficult to detect which are present in the environment . The network level and the host level features for identification in the network are used. Network level features include the "duration of connection" and "service requested" and the host level features include the "number of failed login attempts" [9].

TABLE III. R2L LAYER FEATURE

Feature Number	Feature Name
1	Duration
2	protocol_type
4	Flag
5	src_bytes
23	Count
34	dst_host_same_srv_rate
38	dst_host_serror_rate
39	dst_host_srv_serror_rate
40	dst_host_rerror_rate

U2R Layer

This layer is used for detecting the U2R(User to Root) attack .Even this kind of attack is hard to identify. Such type of attack is often content based. The features for U2R attacks include "number of file creations" and "number of shell prompts invoked[13].

TABLE IV. U2R LAYER FEATURE

Feature Number	Feature Name
10	Hot
13	num_compromised
14	num_shell
16	num_root
17	num_file_creation
18	num_shells
19	num_access_files
21	is_host_login

We used domain knowledge as well as practical significance and hence high efficiency results are obtained for attack detection .Thus, from the total 41 features, we selected only 5 features for Probe layer, 9 features for DoS layer, 14 features for R2L layer, and 8 features for U2R layer. Since each layer is independent of every other layer, the feature set for the layers is not disjoint.

Algorithm

Training

Step 1: Select the number of layers, n, for the complete system.

Step 2: Separately perform features selection for each layer.

Step 3: Train a separate model for each layer using the features selected from Step 2.

Step 4: Plug in the trained models sequentially such that only the connections labeled as normal are passed to the next layer.

Testing

Step 5: For each (next) test instance perform Steps 6 through 9.

Step 6: Test the instance and label it either as attack or normal.

Step 7: If the instance is labeled as attack, block it and identify it as an attack represented by the layer name at

which it is detected and go to Step 5. Else pass the sequence to the next layer.
Step 8: If the current layer is not the last layer in the system, test the instance and go to Step 7. Else go to Step 9.
Step 9: Test the instance and label it either as normal or as an attack. If the instance is labeled as an attack, block it and identify it as an attack corresponding to the layer name.

IV. EXPERIMENTAL RESULTS

We are using Java as coding language for this experiment. This module is separate out in two parts node part i.e user and the server part. Node part will work differently. To capture the access of the node part the user has to logged on to system with its valid user id and password.

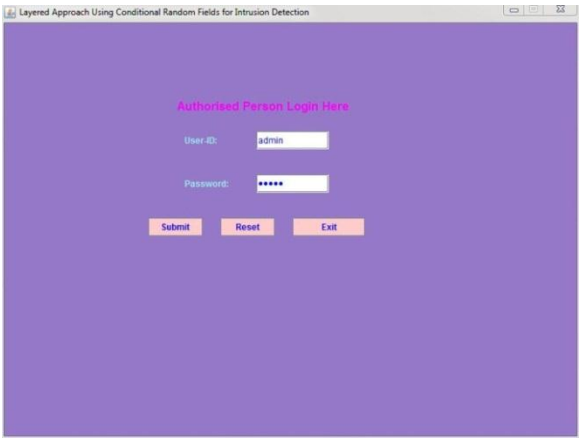

Figure 3. User login

After the successful login the user can fill the information for the systems reference like name, age, sex etc. It can send the file to the destination by choosing packet option in File menu. We can get desired results through get results.

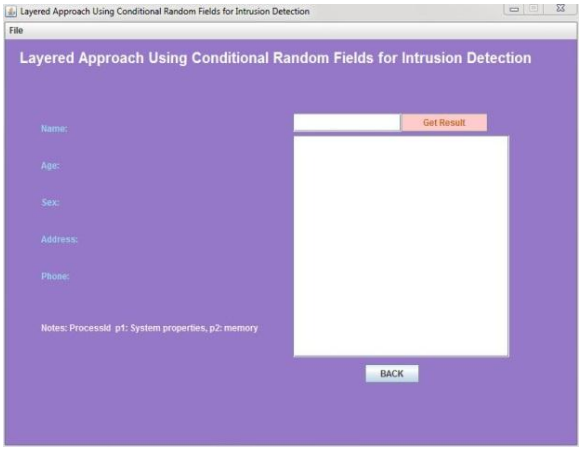

Figure 4. Extra information about user

If user wants to send the packet it can send by browsing the file. After clicking the send button the system will calculate the number of packets, size of packet and the status i.e the packet reached to destination or not.

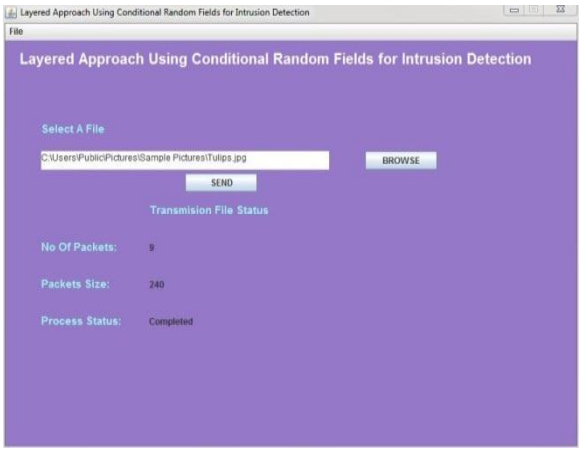

Figure 5. User sent the packet successfully

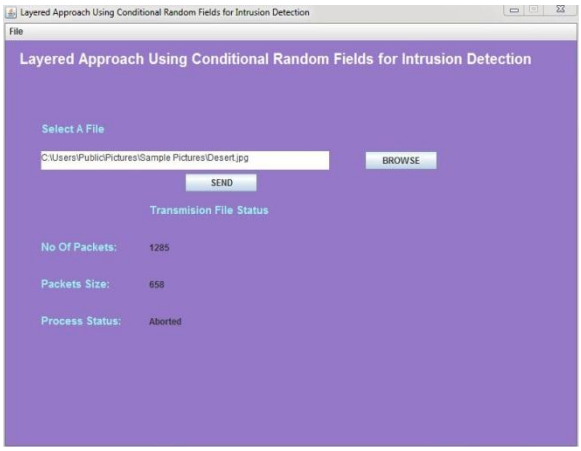

Figure 6. User failed to send packet

On the server side, when we send the packet from user side it travel through all the layers of the system. Each layer verify its features, if it matches then the packet will be send to next layer. If there is some problem with the packet the different layer shows different messages. That messages are stored in log file and the system will show status as aborted.

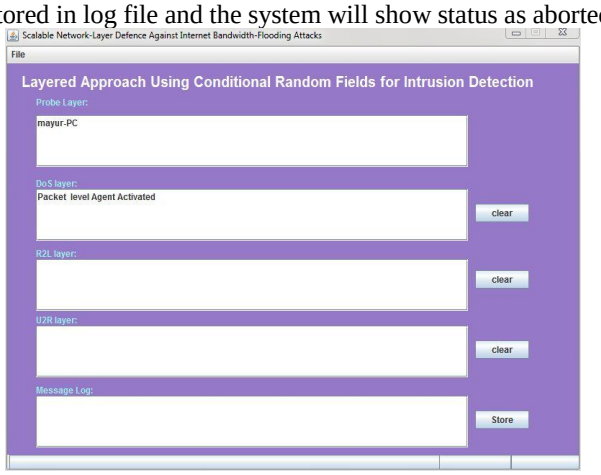

Figure 7. Packet reached to destination

Figure 8. user detected as intruder

V. CONCLUSION

In this paper we mainly focused on layered approach. There are many detection techniques are available but they are at single layer only. We are providing detection at multiple layers(Probe, DoS, U2R, R2L). Due to detecting the intrusion at multiple layers more attacks are detected and network becomes more secure. Our system can help in identifying an attack once it is detected at a particular layer, which expedites the intrusion response mechanism, thus minimizing the impact of an attack. The experimental results shows that our system is very effectively improve the attack detection rate and decrease the false alarm rate. Our system which is a sequence labeling method can be very effective in detecting attacks. System can be implemented to detect a variety of attacks including the DoS, Probe, R2L and the U2R.

REFERENCES

[1] Deepa V. Guleria, Chavan M.K " Intrusion Detection System Based on Conditional Random Fields" IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.12, December 2013.

[2] Ankita Gaur, Vineet Richariya "A Layered Approach for Intrusion Detection Using Meta-modeling with Classification Techniques" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1 , Issue 2, ISSN 2249-6343, 2013

[3] Siddheshwar V. Patil, Prakash J. Kulkarni "Intrusion Detection Using Conditional Random Fields" ACEEE Int. J. on Network Security , Vol. 02, No. 03, July 2011

[4] Abhishek Jain, Kamal Kant, M.R.Thripathi "Security solutions for wireless sensor network" 2012 Second International Conference on Advanced Computing & Communication Technologies.

[5] Prof.S.S.Manivannan , Dr.E.Sathiyamoorthy "An Efficient and Accurate Intrusion Detection System to detect the Network Attack Groups using the Layer wise Individual Feature Set" ISSN : 0975-4024 Vol 5 No 4 Aug-Sep 2013..

[6] Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri "Layered Approach Using Conditional Random Fields for Intrusion Detection" IEEE Transactions on dependable and secure Computing, VOL. 7, NO. 1, JANUARY-MARCH 2010.

[7] M. Naveen kumar , M. Pardha Saradhi , G. Rajeswarappa "Intrusion Detection System Using Pipelining Approach" International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org Volume 3 Issue 7I July 2014 I PP.46-50.

[8] Heba Ezzat Ibrahim ,Sherif M. Badr ,Mohamed A. Shaheen "Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems" International Journal of Computer Applications 2012 10.5120/8901-2928

[9] Suman Bharti, Dr. Savita shiwani, Dinesh Goyal, Vinit Agrawal "Intrusion Detection System (IDS) Using Layered Based Approach For Finding Attack" International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) Volume No.3 Issue No.8, pp : 1082-1084 1 Aug 2014

[10] B.Bhanu Chander, K. Radhika, D. Jamuna "An approach on layered framework for intrusion detection system" Asian Journal of Computer Science And Information Technology 2: 8 (2012) 230 – 23 2012.

[11] V.P Kshirsagar and Dharamraj R.Patil, "An overview of vadaboost-based NISD and performance evaluation on NSL-KDD dataset", International Journal of Computer Engineering and Computer Application, Vol. 1, 2010.

[12] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala "Security in Wireless Sensor Networks: Issues and Challanges" Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia.

[13] M. Naveen kumar , M. Pardha Saradhi , G. Rajeswarappa "Intrusion Detection System Using Pipelining Approach"International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 Volume 3 Issue 7July 2014 IPP.46-50

[14] Prof.S.S.Manivannan,Dr.E.Sathiyamoorthy "An Efficient and Accurate Intrusion Detection System to detect the NetworkAttack Groups using the Layer wise Individual Feature Set" International Journal of Engineering and Technology (IJET) ISSN : 0975-4024 Vol 5 No 4 Aug-Sep 2013