NETWORK INTRUSION DETECTION SYSTEM USING HYBRID CLASSIFICATION MODEL

Prof. Santosh T. Waghmode[1], Prof. Vinod S. Wadne[2]
Department of Computer Engineering,
[1, 2] JSPM's Imperial College of Engineering & Research, Wagholi, Pune.

Abstract: IDS is used to monitor N/W traffic or activity or file modification. If the system is being targeted by unauthorized person or intruder such as denial of service attack, SYN attack etc., it can be detected by the IDS. But Many times the system gets vulnerable to the new attacks. Today, most of Intrusion detection system cannot identify new attacks in the network for incoming packets from internet. So proposed model detects these unknown attacks with the help of optimized decision tree from available set of datasets. The proposed model presents an approach for building an intrusion detection system for a network by using hybrid classification model. This model works in two phases. In first Phase, Packet classifier mechanism filters incoming packets from internet as known or unknown packets into the local network i.e. plays an important role in many security-related system, such as intrusion detection and firewall. Second Phase proposes the simple method for data classification and decision tree creation using ID3 algorithm. The paper describes the design and implementation of new security architecture for identifying new unknown attacks or malicious attacks in a network using Hybrid classification model.

1. INTRODUCTION

Nowadays, many security systems are dealing with distributed database with many parties, while each party wants to keep its own information is private, as personal & business applications are becoming more widespread in a particular area on the internet, the network based applications and services can present security threats to individuals as well as information resources of companies. The hosts or servers in an intranet are making to the public access through the internet, and then such an exposed intranet can be attacked by unauthorized person or intruder. In such way Intrusion detection system refers to the act of detecting an unauthorized intrusion made by a personal computer on the network. An Intrusion Detection System is the software, hardware or a combination of both which is used to detect intruder illegal activity. Basically, IDS design and implemented can be either network based (NIDS) or host Based (HIDS). NIDS is an intrusion detection system that captures data packets traveling on the network and matching them to a database of signatures. Today, most of the available IDS tools are detecting unwanted i.e. malicious actions or activity by evaluating TCP/IP Connections or Log files, for attacks Instance. Intrusion detection systems (IDS) are also working with other security system in the markets such as VPN, authentication mechanisms etc. These IDS systems are used to resist an attack made on network with the various new threats in a network or host-based method with misuse or anomaly detection techniques. If the IDS find a malicious or suspicious action, it should creates a message or alert that Contains information about the source address, target address and type of an attack like buffer overflow, DOS, IP flood etc. When Intruder activity has creates by a single attack instance automatically are spread out across many network connections i.e. a single attack instance often results in hundreds or even thousands of alerts. IDS generally focus on identify attack types, but we will be work on differentiate instances for future scope. Whenever unknown attacks alerts are generated by IDS in into the network will provide to security administrators. In the proposed model classification approaches for classifying the incoming network traffic are implemented but here problem these approaches are insufficient for mining new packets. This drawback will reduced by identifying the behaviors of suspicious activity, classifying them again with update the signature database or Rule base of attacks. The proposed method uses both these security tools so as to protect a network Initially the incoming packets are captured by the packet sniffer the sniffed packets are then revert to the classifier which is based on SYN+ACK mechanism. This mechanism classifies the packets either as Known packets or Unknown Packets, Known packets are allow to travel on the network but the Unknown Packets are compared with the Historical base rule set created by an ID3 Algorithm. After this comparison packets will either be Innocent or malicious, Innocent packets are allowed to travel on the network whereas the malicious packets detected are instructed to the system administrator who blocks this packets using Firewall and also the behavior of malicious packets are extracted and again this are compared to Decision tree which is used to update the rule set.

ISSN: 2278 – 7798

2. **RELATED METHODOLOGY WORK**

In Proposed system use ID3 generates classifiers expressed as decision trees, but it can also construct classifiers in more comprehensible rule set form. The Efficient Dataset or a standard set of data which includes a wide variety of intrusions simulated in a network environment. Similarly, the two weeks of test data will take for the process around two or three week's connection records. A connection is a sequence of TCP packets starting and ending at some well defined times, between which data flows to and from a source IP address to a target IP address under some well defined protocol.

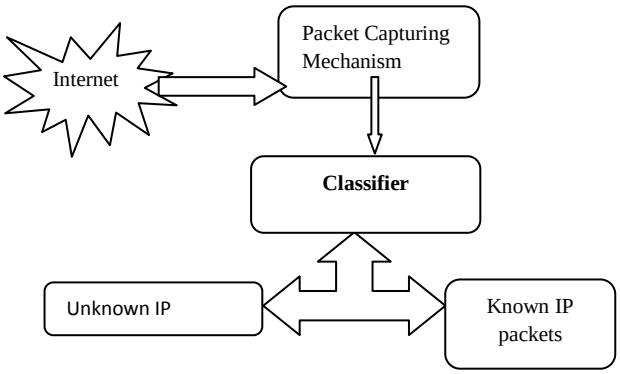

Fig. 01 IDS with Classifier

ID3 algorithm is a simple & typical decision tree algorithm. It has analyzes known types of objects according to a fixed set of attribute or properties and produces a decision tree, and then the decision tree put all the objects in the correct classification way. First, find out factors that have the best sense, and divide the data into several subsets, and then each subset can be divided by the factors that have best sense, till all subset contains the same type data thereby result in a decision tree. ID3 algorithm has clear theory, simple technique and strong learning ability; it is suitable for processing mass resources distribution issues. ID3 decision tree will be changed along with the increasing of training sets. Traditional ID3 algorithms choose the attributes that get more values, because the weighted sum method makes the classification of examples set to the metadata group that is discarding small data group, but the attribute has more properties is not always optimal one solution. The building process include the knowledge level of originally subject in learning ability database, the multiple factors of learning mode in learning mode database. The final decision tree classification results are not certainly consistent with the actual situation according to the traditional ID3 classification because there are many types of attributes based on Entropy.

2.1 IF-ELSE Rules

Rule 1

If packet Destination Address= Unknown
    If Protocol.Type ="TCP"
If Packet.Destination_Port (Known) =421
    Alert="YES"
If Packet.Destination_Port (Unknown)! =421
    Alert="YES"

Rule 2

If Protocol.Type ="UDP"
If Packet.Destination_Port (Known) =421
    Alert="YES"
If Packet.Destination_Port (Unknown)! =421
    Alert="YES

Rule 3

If packet Destination Address= known
    If Protocol.Type = "TCP"
If Packet.Destination_Port (Known) =421
    Alert="NO"
If Packet.Destination_Port (Unknown)! =421
    Alert="YES"

Rule 4

If Protocol.Type = "UDP"
If Packet.Destination_Port (Known) =421
    Alert="NO"

3. **PROPOSED SYSTEM ARCHITECTURE**

Now days providing the certain number of firewall, antivirus, and security tools become hectic even though which are not able to control the network type as anomalies or misuse activities. But we have maintain the security issue is introduced which produce online network intrusion detection system using hybrid classification model of current attack situation.

The design and implementation of a new security architecture for protecting exposed intranets or groups of computers in a network from malicious attacks. The proposed scheme presents an approach of building an intrusion detection system for a network by using the ID3 Algorithm. ID3 algorithm is a standard, popular, and simple method for data Classification and decision tree creation.

ISSN: 2278 – 7798

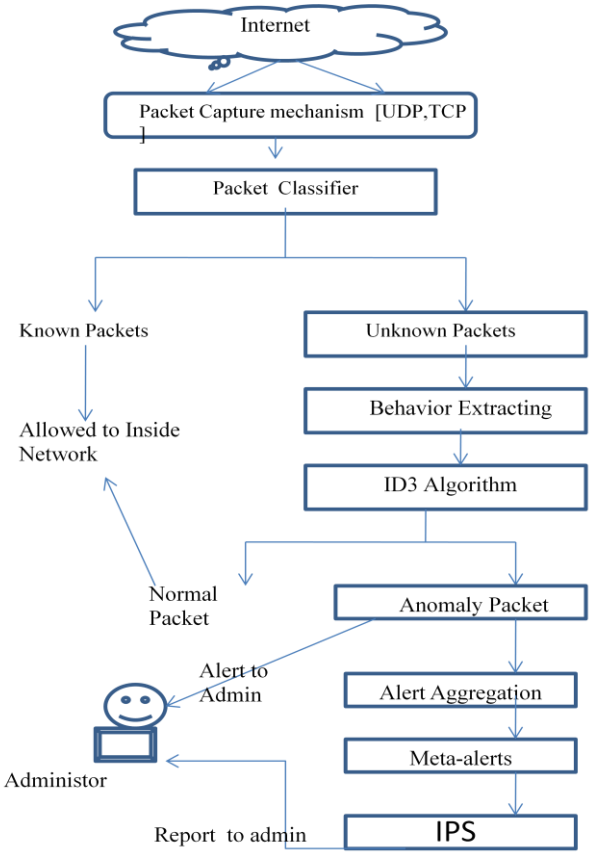

Fig. 02 Architecture of IDS

Traditional Intrusion Detection System (IDS) focus low – level attacks and only generate isolated attacks to achieve higher security in detecting malicious activities for a couple of years. Anomaly Detection is one of intrusion detection system i.e. Current anomaly detection is often associated with high false alarm with moderate accuracy and detection rates when it's unable to detect all types of attacks correctly. The proposed (Hybrid classification model) scheme is very fast in prediction as it processes training set only once to store statistics and use it to predict the unforeseen record. In the proposed method of First phase is packet Classifier module is the main module acts as the Intrusion Detection System. Module consists of the two layers work such as sensor layer for user actions involves detection layer, alert processing layer for incoming packets on user machine from internet. If IDS detected malicious packets then all messages of unknown packets is stored in the signature database for the references to predict future. This Message Log so called Log file for future references for any network environment. Second step, using ID3 Algorithm, generating good decision tree provide high reliability rules by removing unknown packets from incoming packets at the time of packets sniffer. The experiments results implemented using KDD'99, DARPA and Weka datasets indicate that, the accuracy of decision tree is provide good rules i.e. nothing but IF-ELSE rules. First, the sensors determine the values of attributes and then used as input for the detectors as well as for the clustering of attack alert.

If the determine value of Attributes in an event totally independent of a particular attack instance that can be used for classify at the detection level but value of Attributes that are depend on the attack instance that can be used for an alert. It is clearly dependent attribute such as the source IP address which can identify the attacker, and independent attribute such as the destination port which usually is 80 in case of web-based attacks.

4. EXPERIEMNTS AND RESULTS

Here implemented custom simulator software for online network intrusion detection system using C# dot net programming language. The User Interface screen for attack simulation is as shown in below figure real time Packet sniffer from internet or LAN network. In the below snapshot green color represented known or innocent packet detects from internet or LAN network and red color snapshot represented unknown or malicious packet detected from internet.

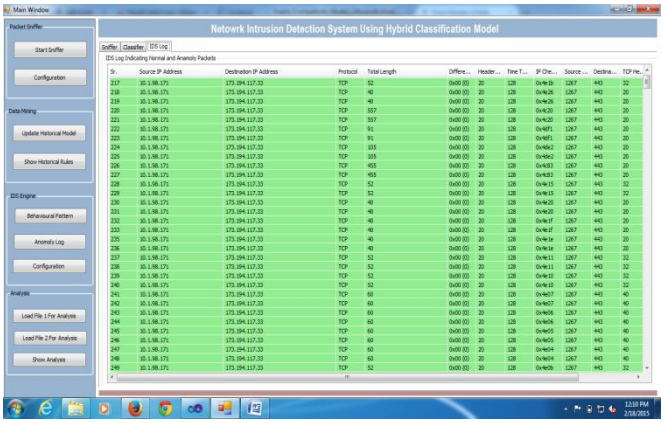

Fig. 03 IDS Log of Known IP Packets

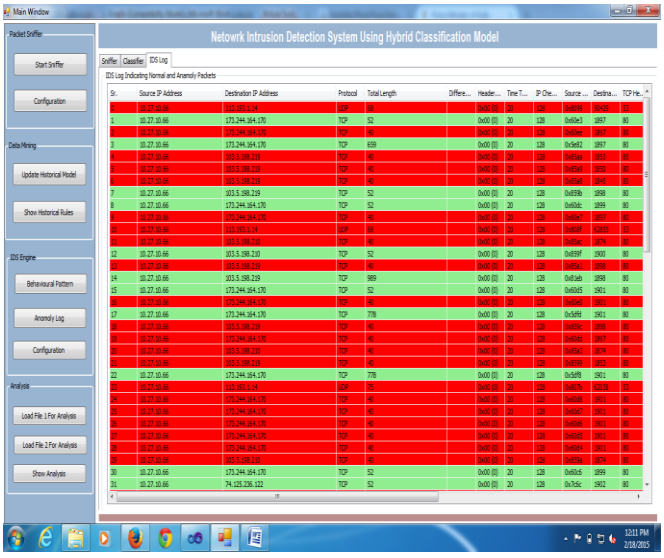

Fig. 04 IDS Log of Unknown or malicious IP Packets

ISSN: 2278 – 7798

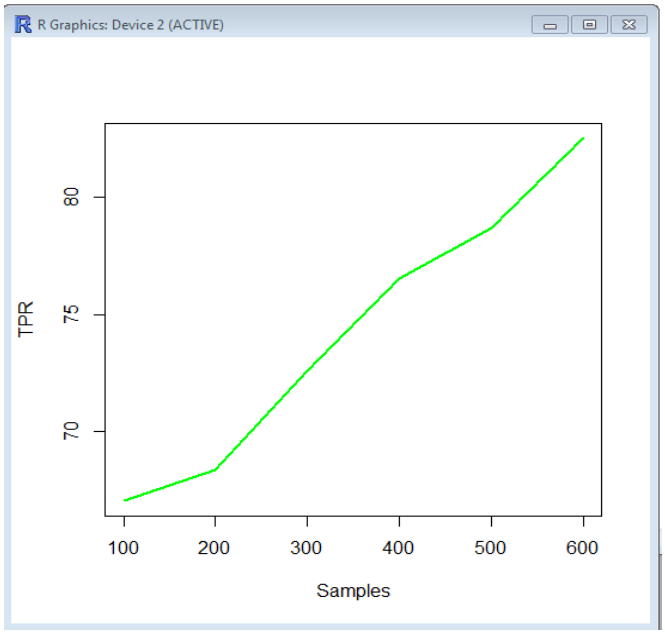

Fig. 05 True Positive Rate (TPR) using DRAPA & Weka datasets

----------True Positive Rate----------

x<-c (100,200,300,400,500,600)

y<-c (67, 68.33, 72.56, 76.548, 78.69, 82.54)

Plot(x, y, typ='l', xlab='Samples', ylab='TPR', lwd='2', col='Green')

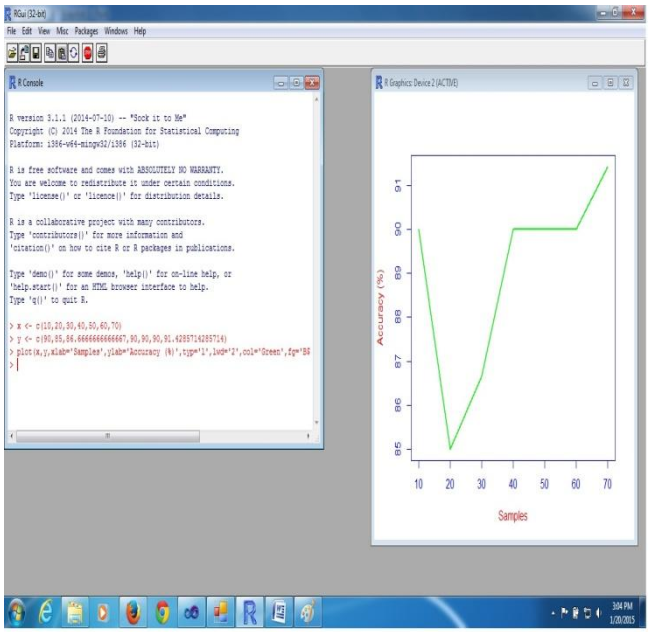

Fig.06 KDD'99 dataset classification

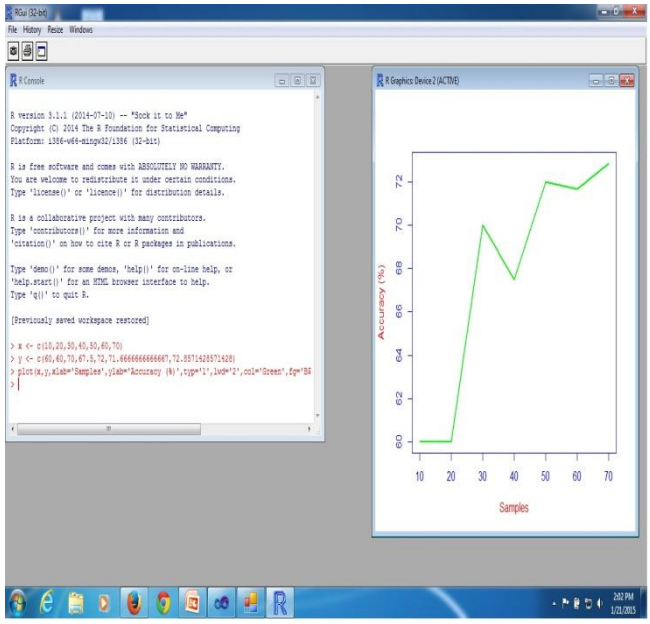

Fig.07 DARPA dataset classification

5. CONCLUSION

In the paper use of packet-filtering mechanism is building strong network intrusion detection systems, security architecture i.e. filtering known or unknown packets for incoming packets from the internet. After filtering, generating good decision tree using Improved ID3 Algorithm, provide high reliability rules for identify unknown attacks or malicious attacks. The experiments results implemented using KDD'99, DARPA and Weka datasets indicate that, the accuracy of decision tree is provide good rules i.e. nothing but IF-ELSE rules. Also biggest advantage of this system also it is real time update signature intrusion database.

6. REFERENCES

[1] Virendra Barot and Durga Toshniwal "A New Data Mining Based Hybrid Network Intrusion Detection Model" IEEE 2012.

[2] Wang and Wang Jun-Qing "Intrusion Detection System with the Data Mining Technologies" IEEE 2011.

[3] Dewan M.D. Ferid, Nouria Harbi, "Combining Naïve Bayes and Decision Tree for Adaptive Intrusion detection" International Journal of Network Security and application(IJNSA),vol 2, pp. 189-196,April 2010.

[4] M.Panda, M. Patra, "Ensemble rule based classifiers for detecting network intrusion detection", in Int. Conference on

ISSN: 2278 – 7798

Advances in Recent Technology in Communication and Computing, pp 19-22, 2009.

[5] R Rangadurai Karthick, Vipul P. Hattiwale and Balaraman Ravindran "Adaptive Network Intrusion Detection System using a Hybrid Approach" 2012 IEEE.

[6] JH Park, BH Choi, DS Go, "Real-time detection of malicious code using behavior pattern" , KI-IT pp. 124~130, 2008.

[7] Matthew M. Williamson, "Using Behavior to Detect and Classify Information-Stealing Malware" (2005).

[8] JH Ryou, JK Lee, SM Kim, HS Kim, "An On-the-fly Filtering Technique for Reducing Packet Inspection Overhead against Worms and DDoS Attack", KIISE pp. 57~6, 2008.

[9] Kristopher Kendall (1999): "A Database of Computer Attacks for the Evaluation of Intrusion Detection System" , Massa chusetts Institute of Technology, Journal of Computer Information technology.

[10] Wang Ling, Xiao Haijun ,"An Integrated Decision System for Intrusion Detection ", 2009 International conference on Multimedia Information Networking and Security.

[11] Wei Wang, Sylvain Gombault, Thomas guyet , "Towards fast Detecting Intrusion: Using key attribute of network traffic", 3rd International conference on Internet monitoring & Protection.

[12] Juan Wang, Qiren Yang, Dasen Ren,"An Intrusion Detection algorithm based on decision tree technology", 2009 Asia pacific conference on information processing.

[13] T. Jyothirmayi, Suresh Reddy "An algorithm of Better decision tree" International journal of computer science and Engineering.

[14] Mohammadreza Ektefa, Sara Memar, Fatimah sidi, Lilly Suriani Affendey," Intrusion Detection using Data Mining Technique", IEEE 2010.

[15] Shailendra k. Shrivastav, Preeti Jain" Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine" IJCSE Vol. 18, No-3, 2011

[16]http://kdd.ics.uci.edu/database/kddcup99/kddcup99.html.

[17] http://nsl.cs.unb.ca/NSL-KDD

[18] http://www.cs.waikato.ac.nz/ml/weka/datasets.html

ISSN: 2278 – 7798