ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Configuration Based Statistical Analysis of Intrusion Detection System

Ashwini Araballi, Santosh Deshpande

Student, Dept. of Computer Networks Engineering, Visvesvaraya Technological University, Belgaum, India

Professor, Dept. of Computer Networks Engineering, Visvesvaraya Technological University, Belgaum, India

ABSTRACT: When we are operating on the Internet it is our responsibility to make network more proactive by examining network using appropriate tools and security settings. This paper presents a framework that is distributed intrusion detection system. DIDS is the device that examines network or systems for harmful activities. Its main goal is to secure the system from malwares and unauthorized access of a network or a system. DIDS is the combination of both network & Host IDSs, which are distributed over a large network with centralized analysis of data to examine a miscellaneous network of systems. This framework is idiomatic among the existing IDS's.

KEYWORDS: Intrusion detection system, Distributed Intrusion Detection System, Distributed monitoring, Probability distribution function (PDF), Router attacks, Data Aggregation and analysis, Network-User Identification(NID)

I. INTRODUCTION

An Intrusion is a group of actions that try to negotiate the security against privacy, availability, secrecy of resources [1]. An Intrusion Detection System (IDS) is a course of analysing & examining the incidents happening in the network & the system. It consists of three elements namely an incident generator (data source), a deconstruction engine and a reply manager. The data sources are of two types Host based & Network based monitors. A deconstruction engine receives information from incident generator and examines the received data for symbols of offenses. The reply manager acts only when probable malware offenses are found in the system by notifying someone or something by generating an alarm as a sign of response.
The deconstruction engine consists of two of the following approaches.

A. Signature/Misuse based Detection

This form of discovery engine detects intrusive behaviors that maintain known patterns of offenses or signatures that abuse known software liabilities. Limitation: unable to identify unknown patterns of offenses [3].

B. Statistical /Anomaly based Detection

A Statistical based discovery engine always looks for something abnormal. It examines the system for unusual behaviors using statistical techniques to find signatures of actions. Limitations: very expensive and may recognize a malicious behavior as normal behavior if inadequate data is collected for deconstruction [3].

The implementation layer includes two type analysis techniques namely; Pattern matching & Heuristic based deconstruction.

C. Pattern Matching

Simple pattern matching discovers a series of bytes in each and every incoming packet. Session Aware form of pattern matching requires detectors to conserve state related information on the TCP traffics. To negotiate the issue of fragmentation the packets are arranged by detectors before applying pattern rule. In Context based Signature detectors examine the occurrences of the exchange of messages and determine the correctness of certain patterns within packets. In Protocol Decode Analysis the type of deconstruction requires the detector to be aware of protocol [3].

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

D. Heuristic Analysis

In this type of analysis detectors are used to discover the form of traffic travelling in the network and uses Ping flood. If the number of pings received exceeds the average number of pings, an event is actuated. Traffic statistical deconstruction is used to define limits for interesting traffic forms. The detectors respond to the traffic patterns by generating an alarm when it exceeds the limit.

The architectural layers of IDS are of three types namely centralized, distributed and hierarchical. In centralized, data is received from single or multiple hosts and dispatched to central location for deconstruction. In Distributed, data is received at each host and deconstruction is distributed among all the hosts. In Hierarchical, data is received from multiple hosts and deconstructed as it passes through the layers.

DIDS contains multiple IDSs which are situated over a broad network with a good network design [1]. All these IDSs coordinate with each other with having single centralized server by facilitating improved network observations. IDSs are embedded into Agents and all these agents coordinate with each other. Distributed monitoring provides quick discovery of intrusive behaviors & there by allowing a network administrator to take preventive measures. DIDS also helps in controlling propagation of worms [1]. The main application of distributed compared to centralized gives rise to reduced control over expedients [1]. Multiple self-dependent systems produce more scanned data than individual system and the examined or scanned data is dissipated among different systems.

Router is the very important equipment in network. It forwards the data packets, based on addresses and tables which carry details of probable routes to reach to the destination between portions of the network [2]. Screening is another activity of router which is also called as filtering. Routing Information Protocol (RIP) is commonly used routing protocol that uses a hop count as its routing standard. The basic methodology of a RIP is to make a verdict on which is the best path by deciding the shortest path. The shortest path is calculated based on the minimum number of hops to reach to the destination.

Routers can be attacked by having access to it directly, launching rejection of Service (DoS) offenses, increasing the bandwidth by making it overwhelming by flooding unnecessary traffic in the network, and exploiting the entries of the routing table to make router to behave abnormally [2]. Routers are the main target for DoS offenses. Distributed DoS offenses are other type of DoS offenses and are known as multiprotocol offenses. DDoS uses ICMP, UDP, and TCP packets to abuse the functionality of a router [3].

II. LITERATURE SURVEY

In [7] author proposed an architecture in which IDS is considered as substantial part in casting survivability of information system and securing their safety against offenses. Consolidated IDS is a one point of failure because it consumes huge amount of expedients of the network. Mobile Agent platform introduced in this paper addresses the drawbacks of consolidated IDS. Mobile agent platforms efficiently control the system and vigorously accommodate to the network changes also. IDS using Mobile agent shows superior performance than consolidated IDS and it report to the intrusive behaviors immediately by providing better accuracy of detection.

In [1] author proposed a framework in which it focuses on co-operative agents used in distributed environment. It also uses multi-agent techniques and computational frameworks to minimize data for deconstruction to improve malware detection efficiency and accuracy.

In [2] authors present overview of router; goals, attacks, detection and defence mechanisms. Also proposes one security paradigm that is generation of LOGS for detecting all kinds offenses which makes router to behave abnormally. Use of LOGS provides large amount of information in solving all type configuration issues.

In [9] author proposed a framework focuses on one of the substantial issue in governing security that is intrusion detection. It presents study of agent and multi-agent systems and advantages of using it to address the drawbacks of classical IDS. Our research is to develop new intelligent IDS which dominates the disadvantages of centralized approach.

In [8] author proposed architecture presents MA-IDS model, which uses signature based detection technique. Mobile agents used in this paper provide useful advantages in identifying offenses. Based on some simulated results of intrusions, they have demonstrated a relative experimental research by taking four IDSs into account, they have concluded that most of existing IDS are generally centralized and undergo from significant shortcomings when used in fast growing networks, especially offenses of distributed network. This depicts us to develop distributed model with mobile agent concept. We believe that the use of agent will help in aggregating effective and necessary information for IDS.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. PROBLEM STATEMENTS

Exploiting or negotiating router's routing table can degrade the network performance; reject network message exchange services. Negotiation in access control of router affects in exploiting the details of network infrastructure or rejection of services, and it eases offenses against other network elements.

A lack in screening router configuration may reduce the overall security of an entire network, exposure of network elements to scans and offenses, and makes it effortless for hackers to prevent detection. The following proposed DIDS helps in analyzing and recognizing the possibilities of offenses of the network specifically router offenses.

IV. PROPOSED ARCHITECTURE

The advanced IDS architecture is shown in Fig 1. The proposed DIDS architecture consists of the elements namely DIDS director, Host monitor, LAN Monitor. There is one director, and one LAN monitor for each LAN section. Per host one Host monitor. The information received from/by DIDS is forwarded & deconstructed at a central position, which allows aggregation of information from different sources. The primary function of Host and LAN monitor is to receive the witnesses of unauthorized or problematic activities. DIDS director is used for evaluating those witnesses. The final reports are directly sent to the DIDS directory one by one & asynchronously from both the monitors through the communication framework.

A. DIDS Directory

A two-way communication is demonstrated by DIDS directory. The communication message consists of request by the director for more accurate information from all the monitors and director uses appropriate commands to notify monitors to change their examining behavior. The exchange or message include two types of events namely, notable (distinguished) events & exception events. A large amount of deconstruction is carried out by host monitor to reduce the bandwidth of the network. The main function of Host and LAN monitor is the aggregation of witnesses for unauthorized activities.

B. Host Monitor

Type of monitor contains two elements, host agent & Host Event Generator (HEG). The function of HEG is collection & analysis of examined or scanned records from the host OS. The exchange of information between the host monitor and director is the function of Host agent.

C. LAN monitor and Agent

This type of monitor contains two elements, LAN agent & LAN Event Generator (LEG). Some doubtful scanned or examined records are directly dispatched to the expert system and other records are operated by the host monitor itself & only briefed reports are passed to the expert system.

D. Communication Manager

Communication Manager's (CM) main objective is to convey data between DIDS director & each of the monitors. CM receives incidents records from each host & LAN monitors & conveys those to the expert system.

E. Expert System

It is accountable for assessing & narrating on the security state of the examined system. The user interface of director helps the system security officer (SSO) to have an active access to the system entirely. The SSO watches all the conditions on each host and network traffic. Also it requests for more distinct information from the monitors.

F. The Network-user Identification (NID)

One of the vast fascinating challenges of an IDS functioning in a networked environment is tracing users (e.g., files) as they travel over a network. On single hosts, the user-id/password paradigm provides some degree of user accountability, but this is lost when multiple uncoordinated user-ids belongs to one person use. The solution to multi user identity issue is to create a Network user Identification once the user steps into the monitored infrastructure, and then to apply that to other further cases/illustrations of that particular user. All witnesses about the activity of any illustrations of a user are then responsible to that original NID. The issue involves the aggregation and estimation of data from both the Monitors. To address the issues related to false alarms when insufficient data is received for

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

deconstruction where malicious behavior is considered as normal behavior, the following analytical model (theoretical/mathematical model) is presented.

G. Analytical Model

Let Y^N & Y^A be random variables. Assume Y^N & Y^A are the models used to monitor network traffic for normal and attack condition respectively.

Considering Alarms are generated only when the monitor/sensor measurement reaches to threshold "t". Main concentration is on reducing false positive alarm and false negative alarm rates.

False Positive Alarm (FA): Probability that an alarm is raised during normal conditions.

False Negative (FN): Probability that an alarm not raised during condition that a network is under attack.

We can have the following expressions,

$$FA=P\ (Y^N > t) \quad \text{eq. (1)}$$

$$FN=P\ (Y^A \leq t) \quad \text{eq. (2)}$$

Let Y be the random variable, According to Chebishev's inequality.

$$P\ (|Y| \geq k) \leq (E\ (Y^2)\ /k^2) \quad \text{eq. (3)}$$

Assume that t=threshold, which is greater than $\mu=E\ (Y^N)$ Then,

$$FA \leq (Var\ (Y^N)\ /\ (t- \mu)^2) \quad \text{eq. (4)}$$

Where, $FA\ \alpha\ Var\ (Y^N)$,

If we set the value of threshold (t) as the following equation

$$t = \mu + r\ \sqrt{Var\ (Y^N)} \quad \text{eq. (5)}$$

Then *FA* rate is bounded by $1/r^2$.

As $Var\ (Y^N) \rightarrow 0, \quad FA \rightarrow 0$

Therefore reducing variance of normal traffic, False Alarm rate is reduced.

Similarly for FN rate,

Let Y^A random variable be sum of two random variables Y^N (under normal condition) & X (addition measurement caused during an attack).

$$Y^A = Y^N + X \quad \text{eq. (6)}$$

$$FN = P\ [(Y^N + X) \leq t] \quad \text{eq. (7)}$$

$$FN = P\ (Y^N \leq t)\ P\ (X \leq t) \quad \text{eq. (8)}$$

From (1) and (2)

$$FN = (1 - FA)\ P\ (X \leq t) \quad \text{eq. (9)}$$

Assume Y^N & X are independent.

If, $FA \rightarrow 0$

$FN \rightarrow FN_{ideal}$ (pure attack traffic without normal traffic added to it).

As a variant of normal traffic Y^N tends to zero, then false negative rate tends to the ideal false negative rate. Hence by reducing variance of the normal traffic false negative rate is reduced.

In the similar way if we consider 'n' sensors/monitors, Y_i^N reading monitor 'i' under normal condition. $Y_i^N + X$ reading monitor 'i' under attack condition. By averaging, the false alarm rate is reduced by factor 'n'. As readings from more sensors are averaged, the variance of the normal traffic goes down to zero & variance of an attack traffic stays above a positive lower bound.

V. METHODOLOGY

This section explains the results of the proposed system implemented using MATLAB (8.1.0.604) simulation tool. Fig. 2 shows the presence of attacks analysis in the network in the form of flowchart. That too specifically attacks that occur on router. The communication recordings of router from the server are downloaded and three datasets are prepared by slicing the communication recordings. Each piece of recordings is considered as three different patterns. Each set pattern is observed and analysed for symptoms of attacks namely Host attack, Network attack and Flooding attack.

A. Network Attack

It is usually defined as mis-behavior in our network environment that will first monitor our network and aggregate the information in order to abuse the already opened ports or liabilities - this may include misuse or disallowed access to our expedients. To detect this attack the configured set of protocols are compared with the other types of protocols (LLMNR, NBNS, and TPKT). For any communications to take place the server must be configured with some set of

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

well defined protocols. The threshold value is set to trigger an event and is based on the condition; the use of other protocols for the communication should not exceed the number of configured set of protocols. That means the threshold is set at 50%. If the number of other protocols used in communication exceeds 50% than the set of configured set of protocols then the attacks are considered as Network Attacks.

B. Flooding Attack

It is simple attack similar to SYN flood appears with a broad range of IP addresses of sources, presenting the existence of DDoS attack. Completion of the request-response paradigm is not required in these types of attacks and these attacks attempts to break the destination SYN line or reduce the bandwidth of the server. The IP addresses of sources are slightly spoofed so that offenses could come from a restricted set of sources, or even may initiate by single host. The attack detection is based on the threshold. Here for every communication packet, service time is allocated that is considered as the threshold value. If the communication period exceeds the threshold value then the event is triggered as flooding attack. Threshold limit taken here is 0.2ns that is also known as service time.

C. Host Attack

If attacks are hosted by single host itself then it could be categorized as a DoS offense. Here the communication takes place continuously and periodically by the same host making resources unavailable for other hosts. If the communication with the server by single host exceeds threshold then the event is triggered as Host attack. The threshold value set is the average of number of times single host communicated with the server continuously and periodically. Thresh hold value set is 0.3.

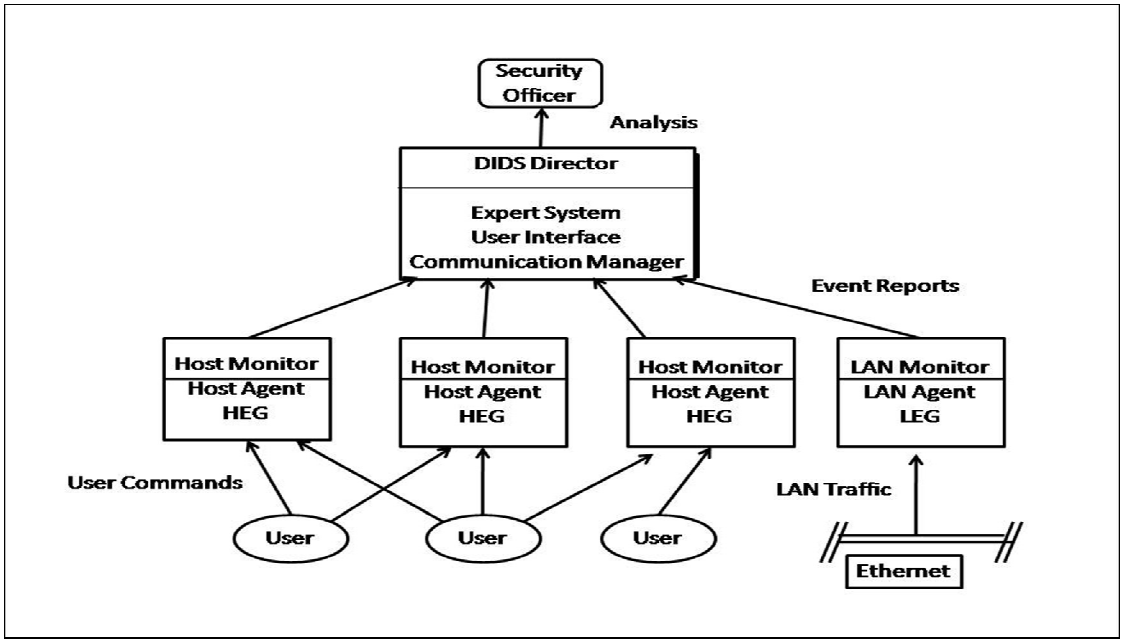

Fig. 1. Proposed Architecture

D. Probability Distribution Function (PDF)

MATLAB function evaluates the PDF for one element family of distributions which is prescribed by name.
Y = pdf (pd, x) which replicates the PDF of the continuous probability distribution (pd) at the values in x.
For all the above mentioned attacks threshhold values are set by using PDF and its fitting tool.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

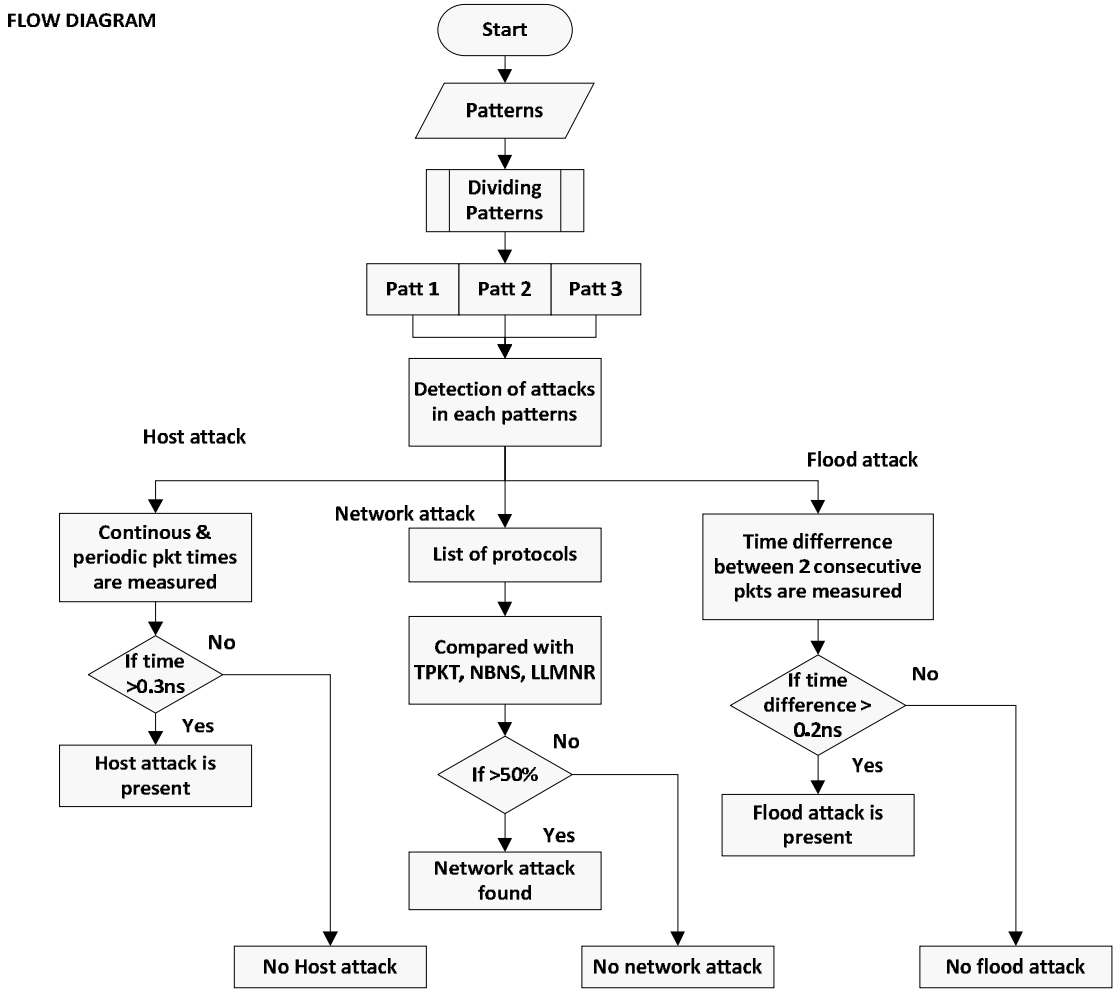

Fig. 2. Flowchart of Implementation

VI. EXPERIMENTAL RESULTS

This section depicts the results of the proposed system implemented using MATLAB (8.1.0.604) simulation tool. The positive alarm rate and negative alarm rates are calculated based on the values of false positive, false negative, true positive and true negative. The Fig. 3 indicates the positive and negative alarm rates present in all the three attacks.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

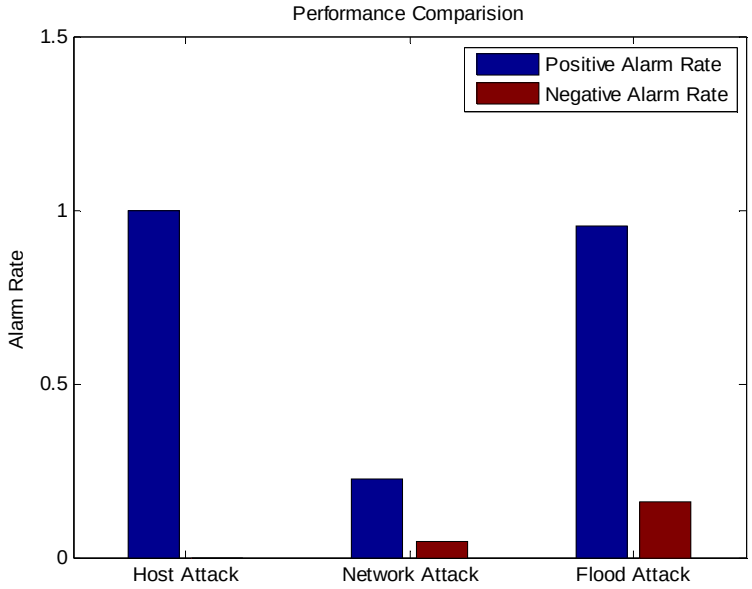

Fig. 3. Alarm rate of all attacks plot

The attack detection rate of each attack in terms of percentage in one pattern is shown in Fig. 4. Similarly for all the patterns are analysed. Overall detection rate is calculated which is approximately 77.07%.

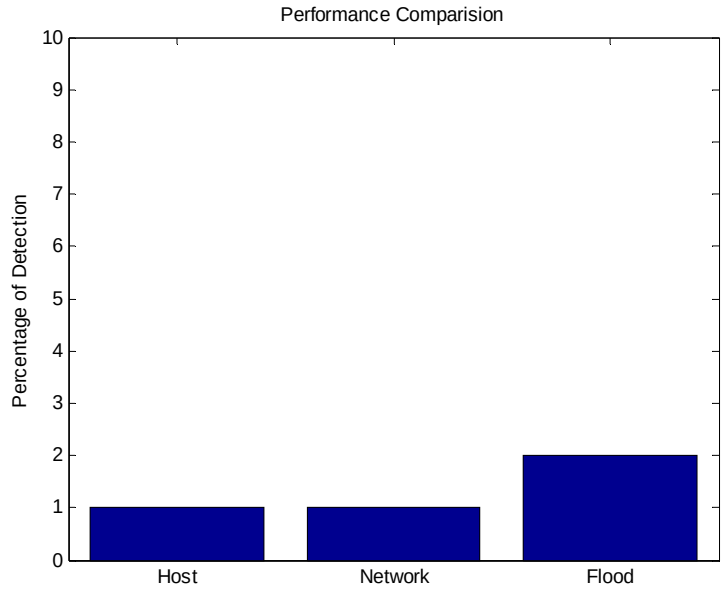

Fig. 4. Attack detection in terms of percentage in one pattern

From Fig. 5 it is clear that the implemented IDS detect attacks early. As we can see in fig the probability of detection of attack is increasing till the value 1.56. The average detection rate is 57.34% in considering all the patterns of the dataset.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

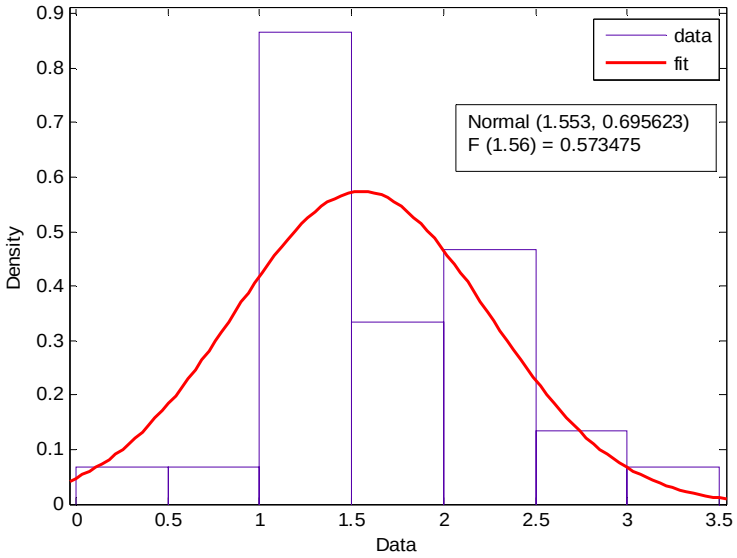

Fig. 5. Plot shows early detection of attacks using Difitting Tool

VII. CONCLUSION

As attacks on security are increasing rapidly, IDS tools are becoming necessary. Proposed IDS solve the issues of identifying disallowed usage and abuse by both system insiders and outsiders of computer systems. We have performed some low level screening and analysis on the components and thereby minimizing the usage of bandwidth of the network in passing witnesses to the director. Resultant graph shows the comparison of performance of our proposed system. The IDS used here is embedded into agents so the proposed DIDS includes multiple IDS's in order to facilitate early detection of attacks. The use of DIDS also reduces the control over the resources. It provides much better performance when compared to individual HIDS and NIDS. The proposed and implemented system early detects attacks. The average detection rate is given by approximately 57.34%.

REFERENCES

1. Ajith Abraham and Johnson Thomas "Distributed Intrusion Detection Systems: A Computational Intelligence Approach", School of Computer Science and Engineering, Chung-Aug University, Seoul, Korea.
2. Saili Waichal, B.B.Meshram "Router Attacks-Detection and Defense Mechanisms". International Journal of Scientific & Technology Research volume 2, issue 6, June 2013.
3. Chapter 8: Cisco Network-Based Intrusion Detection- Functionalities and Configuration
4. Mark Stamp "Information Security- Principles and Practices".
5. Paul Barford, Somesh Jha and Vinod Yegneswaran "Fusion and Filtering in Distributed Intrusion Detection Systems", University of Wisconsin Madison.
6. Patil, Nita, "Analysis of distributed intrusion detection systems using mobile agents," Emerging Trends in Engineering and Technology" ,IEEE, 2008.
7. Benmoussa,"Towards a new intelligent generation of intrusion detection system." Security Days (JNS4), Proceedings of the 4th Edition of National. IEEE, 2014.
8. Barika, F. A., N. El Kadhi, and K. Ghedira. "MA-IDS: Mobile agents for intrusion detection system." Advance Computing Conference, 2009. IACC 2009.
9. Eid, Mohamad. "A new mobile agent-based Intrusion detection system using distributed sensors." proceeding of FEASC (2004).
10. Jaydip Sen "A Distributed Intrusion Detection System Using Cooperating Agents", Innovation Lab, Tata Consultancy Services Ltd. Kolkata.
11. Zahra Hakimi, Karim Feaz, Morteza Barati " A Flow-based Distributed Intrusion Detection System using mobile agents", Department of Computer and Information Technology Engineering ,IJECE, Vol. 3, December 2013.
12. Harjinder Kaur, Nivit Gill. "Performance Comparison of Host based and Network based anomaly detection using Fuzzy Genetic approach." International Journal of Computing Trends and tachnology (IJCTT), volume 4, Issue 8, August 2013.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

BIOGRAPHY

Ashwini Araballi is a student in the department of Computer Networks Engineering at Visvesvaraya Technological University, Belagavi, India. She holds bachelor in Electronics and Communication from Jain College of Engineering, Belgaum, India. Her research interests are network security, digital signal processing, signal and systems.

Santosh L. Deshpande is a professor in the department of Computer Networks Engineering at Visvesvaraya Technological University, Belagavi, India. He has more than 10 years of international R&D experience and published 24 research articles in reputed international journals and conferences. He received his PhD in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, India. His research interests include network Security, data mining, and web services.