Need for an Intrusion Detection System: A Systematic Review

Roohi Sharma

***Abstract*—The continuous increase within network size and its complexity, securing computer systems from attacks becomes important and a challenge. Because of dramatically increase in number of attacks, intrusion detection on internet becomes important and heated research field in computer science. The goal of intrusion detection is to identify or try to detects intrusion attempts like unauthorized use, misuse, abuse of computer systems by either internal or external penetrators, so that action may be taken to repair the damage later. This paper provides the review of existing techniques in intrusion detection to detect attacks.**

***Index Terms*—Attacks, intrusion detection system, intrusion prevention system, network security, worms.**

I. INTRODUCTION

With the rapid growth in the Internet based technology new application areas for computer network have emerged. All of these application areas made the network an attractive target for the misuse and a huge susceptibility for the community. Today there are two mechanisms which are mostly used to secure application servers i.e., firewalls and intrusion detection systems. Firewalls control the flow of communication to systems where as IDSs monitors this communication to detect all possible attacks. It is important to detect attacks as soon as possible and take feasible actions to stop them. These systems automatically detect intrusions and behavioral misuse. A simple firewall can provide no longer security as in past. Intrusion detection is mainly a security work to monitor activities of network for malicious or abnormal behavior. An ID has turn out to be an important activity in the all security policies and practices. The idea is that if it is not possible to prevent attacks against our computer, at least it may be possible to detect these attacks.

In the late 1990s, Intrusion detection systems (IDS) were developed to identify and report attacks. As hacker attacks and network worms began to affect the internet, IDS become a young field of research. Traditional IDS technologies detect hostile traffic and send alerts but do nothing to stop the attacks. Once the detection is done, next step is to protect the network.

The principle of intrusion detection is to prepare computer systems for and deal with attacks. From the variety of sources within computer systems and networks, intrusion detection system collects all relevant information. For nearly all systems, this information is then compared to recognize the attacks and vulnerability with predefined patterns of misuse.

Manuscript received on April, 2013.

Roohi Sharma is with Department of Information Technology, Model Institute of Engineering and Technology (Affiliated to Jammu University, Jammu), Kandoli Nagrota Jammu-181221, India.

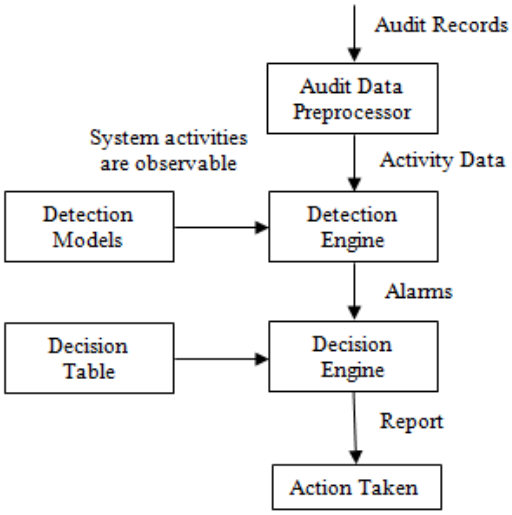

Figure 1: Components of IDS

The fig. 1 shows main elements of IDS. The primary assumptions are made, system activities must be observable. The normal and intrusive activities have distinct evidence. All evidences are extracted from audit data. To detect the intruder or attacker, various analysis approaches piecing the evidences together. Misuse detection is signature based where as anomaly detection is statistical based approach.

Even various preventive security tools are present; it is often possible for the intruder to bypass the protection. IDS system can identify and alert to the presence of unauthorized MAC addresses on the networks.

The area of intrusion detection is central to the concept of the computer security. While a number of methods can be employed to protect the data stored within a computer system, the ability to identify instances of an attack on the computer is paramount if an effective security mechanism is to be developed [24].

The objective of this paper is to present the current intrusion detection techniques, methodologies and tools. The remainder of paper is divided into three primary areas. The second section describes fundamentals of intrusion detection system. In Section III, related work in Intrusion Detection System is describes, and the paper ends with conclusion in Section IV.

II. INTRUSION DETECTION FUNDAMENTALS

The first observation made about the complex internet system is the number of attacks that continues to grow.

A. Classification of attacks

Several attack classifications have been described in literature. These classifications usually distinguish between the following basic categories [17], [22], [24]:

Physical attacks: attacks that damage the computer hardware and network hardware come under physical attacks.

Password attacks: attacks in which an unauthorized person tries to gain passwords, keys, etc. for any protected system.

Information gathering attacks: an attack that does not directly damage any system, but tries to captures information about the system. This category consists of network traffic sniffing and (port) scans.

Trojan horses: is a malware or harmful code that performs desirable actions against the targeted system. It is one of the major threats to the computer security.

Worms: is a self-replicating programs or malware that self-propagates across a network to spread to other computers. Self-replication is the characteristic that differentiates worms from viruses. A worm spread can be extremely fast: an example is the Sapphire/Slammer worm, which is known to have infected 90% of the vulnerable hosts in 10 minutes [24].

Viruses: is a self-replicating program that replicates from one computer to another. It needs user interactions to propagate to other system.

B. Detection Types

In this section the focus is on the three types of intrusion detection, signature-based, anomaly based and stateful protocol inspection [5].

1) Signature-based detection type (misuse detection):

This detection type is very quick and easy to configure. By relying on known traffic data, IDS can use signature-based detection to analyze potentially unwanted traffic. Once a new attack is launched, the attack patterns are carefully studied and a signature is defined for it. After studying the pattern of attack, action against that attack is to be taken. This approach is mainly used for known attacks and is not much capable for detecting novel attacks. Sometimes an attacker can slightly modify an attack to make it undetectable for a signature-based type. Although this type is limited in its detection capabilities, still it is very accurate.

2) Anomaly-based detection type:

Anomaly detection is general category of ID which works by identifying activities that vary from established patterns for users, or groups of users [24]. The approach used for anomaly-based detection is to learn the usual behavioral pattern of the network. This method is useful to detect unwanted traffic that is not known or new releases of the old attacks. Anomaly-based detection type is one that looks at network traffic and detects the incorrect, invalid or abnormal data.

3) Stateful protocol inspection:

Similar to anomaly-based detection is a stateful protocol inspection. The only difference between two is that stateful protocol inspection can analyze traffic at the network, transport and application layer, which anomaly-based detection cannot do.

C. Detection Methods or Technologies

This section presents the detection method, which are the approaches to distinguish malicious activities from normal one.

1) Host-based IDS (HIDS):

All system specific settings and network traffic is analyze by host-based IDS. System settings include policy and audits log for local security and also include software calls. System calls are used to diagnose the impact of attacks. A HIDS require to be installed on each machine and specific configuration to that software and operating system. Host-based intrusion detection has two major drawbacks [11]. Firstly, capturing activity is very time and space consuming. Secondly, for monitoring a large network several sensors are needed. These are the reasons why host-based intrusion detection is not successful in industrial community.

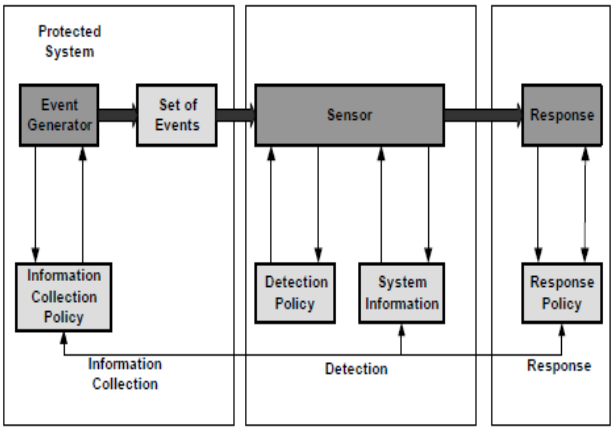

Figure 2: Host-based IDS [8]

2) Network-based IDS (NIDS):

When the system is used to analyze network packets, intrusion detection approach used is called network-based intrusion detection. This is in contrast to host-based intrusion detection, which relates to processing data that originates on computers themselves, such as events and kernel logs [19]. NIDS is widely used in industrial community. The reason for acceptance is that only one single sensor can monitor the activity of several hosts and their easy deployment.

In order to detect signs of intrusion in network packets network-based IDS are mainly used. Network-based IDS suffer from several drawbacks [11]. First, it is unable to analyzed ciphered traffic. Second, it is very challenging task to capture packets from the constantly increasing traffic bandwidth.

Table 1: Comparing Network and Host-Based Benefit [19]

Benefit	Host	Network
Deterrence	Strong deterrence for insiders.	Strong deterrence for outsiders.
Detection	a) Strong insider detection. b) Weak outsider detection.	a) Strong outsider detection. b) Weak insider detection.
Response	a) Weak real-time response. b) Good for long-term attacks.	Strong response against outsider attacks.
Damage Assessment	Excellent for determining extent of compromise.	Very weak damage assessment capabilities.
Attack Anticipation	Good at trending and detecting suspicious behavior patterns.	None.
Prosecution Support	Strong prosecution support capabilities.	Very weak because there is no data source integrity.

3) Behavior-based IDS:

The observed behavior of monitored system is compared with a system or model constructed previously. The model used for reference describes the expected behavior of this system. An intrusion is detected if there is a considerable deviation between the observed behavior of current system and the reference model.

The major drawback of behavior-based IDS lies in its inability to spot the exploited vulnerability explicitly [11].

4) Knowledge-based IDS:

In this approach, a model for known malicious activities is build. The elements that characterized the malicious activities are called signatures. The knowledge-based intrusion detection system is more accurate than behavior-based intrusion detection system.

The drawback of knowledge-based IDS is if no signature exists for coming attack, then it will go undetected.

III. RELATED WORK

Related work in the field of IDS is as follows:

1) Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems –

Kozushko. H have explored that combined network-based and host-based intrusion detection systems prevents attacks effectively from insider as well as outsider sources. The new techniques like neural networks machines and support vectors of intrusion detection were discussed. The difference between the host-based and network-based technology was study. Host-based technology examines events like what files were executed where as network-based technology examines events as packets of information exchange between computers (network traffic) [19]. Centralized real-time host-based ID and distributed real-time host-based ID architecture was described. Three attack scenarios for host-based ID are:

a) First scenarios are the abuse of privilege attack scenario.
b) Second scenario involves elevated privileges with contractors.
c) In third attack scenario ex-employees utilizing their old accounts.

2) BlueBox: APolicy-Driven, Host-Based Intrusion Detection System –

Chari. N. S, Cheng. C. P has proposed rules for important servers and for popular cgi-bin scripts. The rules are simple and very effective in detecting a large number of known attacks. They implemented BlueBox using two loadable kernel modules, i. e, system call interception module and rule enforcement module.

BlueBox is a simple system for sandboxing applications. It is a comprehensive way to incorporate checks on the execution of programs at the time of invocation of system calls [19]. With minimal impact on the performance they succeeded in achieving security. By combining signature-based systems, statistical profile-based systems and the sandboxing systems like BlueBox, an effective security can be achieved on much large scale.

3) Clustering Intrusion Detection Alarms to Support Root Cause Analysis –

Julisch. K has proposed a novel alarm-clustering method. This paper gives an approach that more efficiently handle the intrusion detection alarms. There are some reasons behind each alarm, which are called alarm's root causes. Some root causes are predominant, by identifying or by removing intrusion detection alarms were handled. The author proves that an attempt for identifying and removing root causes makes the future alarm load reduce by 87%. A semiautomatic process given by the author consists of two steps [18]:

a) step one is called root cause analysis. It identifies root causes that account for large numbers of alarms.
b) step two will removes the root causes identified in step one and reduces the future alarm load.

Input: An alarm clustering problem.
Output: A heuristic solution for problem.
Algorithm:

1: T := C;
2: for all alarms a in T do a[count] := 1;
3: while for all a ε T : a[count] < min_size do {
4: use heuristic to select an attribute A_i, i ε [1,...,n];
5: for all alarms a in T do
6: a[A_i] := father of a[A_i] ;
7: while identical alarms a, a' exist do
8: set a[count] := a[count]+a'[count]and delete a' from T;
9: }
10: Output all generalized alarms where a ε T with a[count] >=min_size;

Figure 3: Heuristic alarm-clustering algorithm [18]

The pseudocode for alarm-clustering methods is shown in fig. 3.

4) Intrusion Detection using an ensemble of Intelligent Paradigms –

This paper shows the importance of ensemble approach for modeling intrusion detection systems. An ensemble helps to indirectly combine the synergistic and complementary features of the different learning paradigms without any complex hybridization [16]. The author shows that in terms of accuracy an ensemble of ANNs (Artificial Neural Networks), SVM (Support Vector Machines) and MARS (Multivariate Adaptive Regression Splines) is advanced and superior to any individual approaches of ID.

Experiment is performed by author on data, classifies in five classes. Class 1 contains normal data, probe belongs to class 2, class 3 contains DOS and class 4 contains user to super-user and remote to local covers in class 5.

Figure 4: Performance Comparison of Testing for Five-Class Classification [16]

Class	Accuracy (%) SVM	RP	SCG	Ensemble Of ANN, SVM and MARS
Normal	98.42	99.57	99.57	99.71
Probe	98.57	92.71	85.57	99.85
DoS	99.45	97.47	72.01	99.97
U2Su	64.00	48.00	0.00	76.00
R2L	97.33	95.73	98.57	100.00
Overall	98.85	97.09	80.89	99.82

Figure 4 shows performance of ANNs, SVMs and MARs for five-class classifications.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

5) A Taxonomy of Network and Computer Attacks –

Hansman. S, Hunt. R has analysis the various attacks of computer and network [17]. The taxonomy proposed by authors is used by information bodies to provide a common classification scheme. The taxonomy consists of four dimensions. The behavior of attack is covered in first dimensions. The classification of attack targets comes under second dimensions. The third section classifies vulnerabilities. The fourth dimension covers payloads.

6) Efficient Packet Classification for Network Intrusion Detection using FPGA –

The focus of this paper is on application of intrusion detection. Song. H, Lockwood. W. J has presented an architecture called BV-TCAM based on packet classification. To increase the throughput, authors combine Ternary Content Addressable Memory (TCAM) and the Bit Vector (BV) algorithms. The two major contributions given in paper are [15]:

a) TCAM is used as a component here, which avoids the need to expand the size of rule set.

b) Tree-Bitmap approach is used to implement the multi-bit trie Bit Vector algorithm.

By classifying the header faster and by using deep packet inspection function, processing overhead will be reduced.

7) Network-based Intrusion Detection using Adaboost Algorithm –

By using a machine learning algorithm called Adaboost, a network-based intrusion detection system is developed. Authors constructed a frame-work for network-based IDS that contain four modules. Computational complexity of Adaboost is lower than SOM, ANN and SVM. Paper presented four general types of attacks: DOS (denial of service), U2R (user to root), R2L (remote to local) and PROBE. The authors give the importance of balancing the normal samples for getting low FPRs [14].

8) Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks –

Hijazi. A has proposed the main security challenges of WAHNs. The paper addresses the two main types of wireless ad hoc networks namely: mobile ad hoc networks (MANET) and wireless sensor networks (WSN) [13]. Analysis of mobile agents and their attributes has been done against security challenges. Many features offered by mobile agents are just exact requirements of ideal WAHNs IDS. There are still features that have not been fully utilized.

Author compares three referenced designs i.e., local intrusion detection system (LIDS), static stationary database and distributed intrusion detection using mobile agents, against certain common design and performance parameters.

9) Focusing on Context in Network Traffic Analysis –

Goodall. R. J, Lutters. G. W, Rheingans. P, Komlodi. A in their research paper classifies intrusion detection work into three tasks: monitoring, analysis and response. They designed an information visualization tool [12]. The information visualization tool helps to reduce analyst cognitive burden.

Authors designed Time-Based Network Traffic Visualizer (TNV) to encourage network traffic exploration. With the help of TNV analysts can learn to understand the patterns of their networks traffic.

10) Intrusion Detection and Virology: Differences, Similarities and Complementariness –

In this paper authors main concentration is on information security. Morin. B, Me. L depicts all the differences, similarities and complementariness that exist between intrusion detection and anti-viruses [11]. In their literature survey, many examples on various types of intrusion detection are quoted. Only the scientific and the technical aspects are discussed in the differences among intrusion detection, virology and anti-virus.

11) Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks –

This research paper presents a comparison among various clustering scheme of intrusion detection for the ad-hoc networks. In the comparative analysis, scheme which proves to be fast, simple and only efficient was the CBID scheme. This scheme provides low overhead and also reduce the exchange of packets either it is required for cluster formation or for intrusion detection. Overhead is low in terms of memory usage and number of messages exchange [10]. The overhead seen will be uniform throughout irrespective of the various conditions.

Researchers test the effectiveness of the CBID with the existing techniques under different stress conditions.

12) High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS) –

Weinsberg. H, David. T. S, Dolev. D, Anker. T has built an algorithm for pattern-matching called RTCAM [9]. This algorithm uses concept of Ternary Content Addressable Memory (TCAM). The RTCAM is written in java. There are two pattern set that uses TCAM, Class AV pattern set and Snort pattern set.

This algorithm has two advantages. First is achieving line-rate speed and second is its compatibility with Snort.

13) Is Sampled Data Sufficient for Anomaly Detection? –

In this research paper, authors do a survey on sampling techniques. They study whether it is possible to deform network traffic features which are important for detecting any anomaly. An author gives many sampling techniques for measuring the high-speed network traffic. These techniques reduce the processing overhead and storage requirement [8].

They show that by sampling schemes, performance of anomaly detection system is degraded.

14) Agent Based Efficient Anomaly Intrusion Detection System in Adhoc Network –

Nakkeeram. R, Aruldoss. T, Ezumalai. R presents a system against wireless networks that has agents and data mining techniques. These techniques collect data by home agents that are present in each system and then by using data mining checks the local anomalies. Authors provide three different techniques, specifically a) Current node, b) Neighboring node, c) Global networks.

This system reduces the false alarm and halt all the successful attacks presents in an adhoc networks. In the system number of attacks has been tested to prevent attacks in wireless networks [4].

15) An Overview of IP Flow-Based Intrusion Detection –

This paper presents the need of flow-based intrusion detection. Authors provide an approach that consists of two stages [3]. In the first stage, flow-based approaches are used to detect some anomalies. In the second stage, packet inspection can be used to protect the systems against those anomalies that are detected in stage first. They provide a comparative analysis between traditional NIDS. In their study, they show that flow-based intrusion detection totally relies on header information of packets.

15) Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems –

This paper was completely a review paper which presents the current research in IDS and IPS. Authors show their complete involvement in cyber defense. The paper also discusses the limitations or drawbacks of using detection techniques. The major restriction of using intrusion detection is that, it was able to detect known anomalies or attacks only. They are completely unable to detect the unknown attacks.

To detect the attacks, predefined attack specification has been made which requires security experts that manually analyze attacks. Comparing a large volume of data for analysis requires human labor and time [2].

16) Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques –

Darji. M, Trivedi. B has provided a review of various intrusion detection and prevention systems in the paper. They compare all recent techniques based on architecture and data gathering for Mobile Adhoc Networks (MANETs) [1]. At the end they concluded that distributed and cooperative autonomous mobile agent based architecture is suitable for mobile adhoc networks. This architecture can efficiently detect the anomalies.

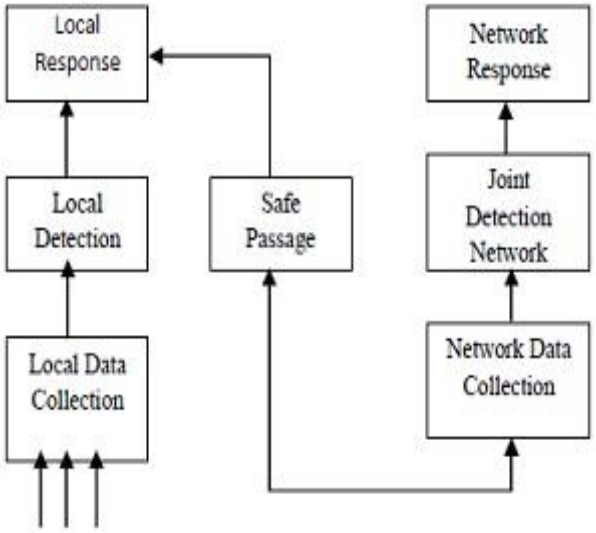

Fig 5: Intrusion Detection Process [1]

IV. CONCLUSION

Intrusion Detection techniques are used to secure a network against the novel attacks. An ID is distinct from other systems and network administration works. This paper presented a survey of various Intrusion Detection techniques that has been used in many systems.

ACKNOWLEDGMENT

I wish to thank the referee for the careful reading of the paper and many valuable suggestions including recent references.

REFERENCES

1. M. Darji, B. Trivedi, “Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques,” IJAIS, 2012, pp. 38–43.
2. F. A. Mohammad, H. S. Syed, “Towards Cyber Defence: Research in Intrusion Detection and Intrusion Prevention Systems,” IJCSNS, 2010, pp. 316–325.
3. S. Anna, S. Gregor, S. Ramin, M. Cristian, P. Aiko, S. Burkhard, “An Overview of IP Flow-Based Intrusion Detection,” IEEE, 2010, pp. 343–356.
4. R. Nakkeeran, T. Aruldoss, R. Ezumalai, “Agent Based Efficient Anomaly Intrusion Detection System in Adhoc Network,” IACSIT, 2010, pp. 52–56.
5. *Intrusion Detection Systems.* IATAC, 2009, ch. 2.
6. V. Igure and R. Williams, “Taxonomies of attacks and vulnerabilities in computer systems,” *Communications Surveys & Tutorials, IEEE,* 2008, pp. 6–19.
7. L. Vokorokos, A. Balaz, M. Chovanec, “Intrusion Detection System Using Self Organizing Map,” Acta Electrotechnica et Informatica, 2006, pp. 1–6.
8. J. Mai, A. Sridharan, “Is Sampled Data Sufficient for Anomaly Detection?,” ACM, 2006.
9. Y. Weinsberg, T. S. David, D. Dolev, T. Anker, “High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS),” unpublished.
10. E. Ahmed, K. Samad, W. Mahmood, “Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks,” CERT, 2006, pp. 46–56.
11. B. Morin, L. Me, “Intrusion Detection and Virology: An analysis of Differences, Similarities and Complementaries,” Springer-verlag, 2006, pp. 39–50.
12. J. R. Goodall, W. G. Lutters, P. Rheingans, A. Komlodi, “Focusing on Context in Network Traffic Analysis,” IEEE, 2006, pp. 72–80.
13. A. Hijazi, “Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks,” unpublished.
14. H. Wei, H. Weiming, “Network-based Intrusion Detection Using Adaboost Algorithm,” IEEE, 2005, pp. 1–6.
15. H. Song, J. W. lockwook, “Efficient Packet Classification for Network Intrusion Detection using FPGA,” ACM, 2005, pp. 1–8.
16. S. Mukkamal, A. H. sung, A. Abraham, “Intrusion Detection using an Ensemble of Intelligent paradigm,” IJNCA, 2005, pp. 167–182.
17. S. Hansman, R. Hunt, “A Taxonomy of Network and Computer Attacks,” ELSEVIER, 2004, pp. 1–13.
18. K. Julisch, “Clustering Intrusion Detection Alarms to Support Root Cause Analysis,” IEEE, 2003, pp. 443–471.
19. H. Kozushko, “Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems,” 2003, unpublished.
20. S. N. Chari, P. C. Cheng, “BlueBox: A Policy-Driven, Host-Based Intrusion Detection Systems,” ACM, 2003, pp. 1–28.
21. S. Hansman, *A Taxonomy of Network and Computer Attack Methodologies.* NewZealand, 2003, pp. 15–50.
22. N. Weaver, V. Paxson, S. Staniford, R. Cunningham, “A Taxonomy of Computer Worms,” ACM, 2003, pp. 11–18.
23. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, “Inside the Slammer Worm,” IEEE, 2003, pp. 33–39.
24. J. Cannady, J. Harrell, “A Comparative Analysis of Current Intrusion Detection Technologies,” unpublished.

AUTHORS PROFILEL

Roohi Sharma received her M.Tech degree in Computer Science and Application from Thapar University Patiala, India. Currently she works as a Lecturer in MIET College Jammu. Her research interests include Network Management and Security. She publishes one paper in the Conference and one in the International Journal IJACR.