International Journal of Computer Applications (0975 – 8887)
Volume 5– No.2, August 2010

Intrusion Detection System Methodologies Based on Data Analysis

Shaik Akbar
Assoc. Profr, Dept. of C.S.E,
SVIET, Nandamuru,
Krishna Dist, Andhra Pradesh, India

Dr.K.Nageswara Rao
Prof & H.O.D, Dept. of C.S.E
P.V.P.S.I.T, Vijayawada,
Krishna Dist,
Andhra Pradesh, India

Dr.J.A.Chandulal
Prof, Dept. of C.S.E
GITAM University,
Visakhapatnam,
Andhra Pradesh, India

ABSTRACT
With the rapidly growing and wide spread use of computer networks the number of new threats has grown extensively. Intrusion and detection system can only identifying and protecting the attacks successfully. In this paper we focuses on detailed study of different types of attacks using in KDD99CUP Data Set and classification of IDS are also presented. They are Anomaly Detection System, Misuse Detection Systems. Different Data Analysis Methodologies also explained for IDS. To identify eleven data computing techniques associated with IDS are divided groups into categories. Some of those methods are based on computation such as Fuzzy logic and Bayesian networks, some are Artificial Intelligence such as Expert Systems, agents and neural networks some other are biological concepts such as Genetics and Immune systems.

Keywords – *IDS, KDD Data Set, Anomaly Detection System, Misuse Detection, Data computing Techniques.*

1. INTRODUCTION

At present networking revolution is main part of the communication era and internet is changing the computing. Too commonly there are main headlines about the Intruder attack. They attack into another system. They have stolen credit card lists, military secrets and trade secrets.
The goal of interconnected computer system is to more efficiency and better information exchange. The number of attacks are increases because of the integration of the computer system, which faces some attacks. An attack is a realization of threat, to find and exploit the system vulnerability.

Intrusion Detection concept was introduced by James Anderson in 1980[1]**,** defined an "Intrusion attempt or threat to be potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable".

Security of a network is always important, which monitors all network traffic passing on the segment. The following objectives are protecting the network against intruder's confidentiality, Integrity, Availability, Authentication and Non-repudiation.
Anderson discussed a frame work investigation of intrusions and intrusion detection. In this he discussed definition of fundamental terms Risk, Threat, Attack, Vulnerability and Penetration.
Risk: Accidental or unpredictable exposure of information, or violation of operations integrity due to the malfunction of hardware or incomplete or incorrect software design.
Threat: The potential possibility of a deliberate, unauthorized attempt to:
(a) Access information
(b) Manipulate information

(c) Render a system unreliable or unusable
Vulnerability: A known or suspected flaw in the hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.
Attack: A specific formulation or execution of a plan to carry out a threat.
Penetration: A successful attack; the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

Now a days amount of data available on the internet. Therefore, the attackers successfully attack the systems. As reported by the [CERT/CC], the number of computer attacks has increased exponentially in the past few years from 1980 to 2010 as shown figure.1.

An IDS is an important tool for the defense of a network against attacks. Since 1980 the sophistication of attacks has increased enormously. Fig1.1 shows this development of the increasing sophistication of attacks and the decreasing intruder knowledge very well. The result of these changes is a huge amount of sophisticated attacks, against which a network needs to be defended.

This is only possible with a multilayer defense strategy containing firewalls, content filtering, vulnerability and virus scanners as well as IDS's.

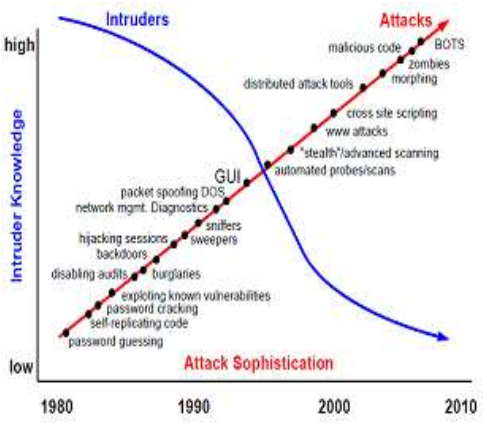

Figure.1 The increasing sophistication of attacks and the decreasing knowledge of the intruder.

2. KDDCUP99 IDS DATASET

The KDDCUP'99 data set was created by processing the tcp dump portions of the 1998 DARPR Intrusion Detection System(IDS) evaluation dataset, created by Lincoln Labs, U.S.A. They acquired nine weeks of raw tcp dump data. This was processed into about five million connection records. The data set contains a total of 24 attack types(connections) that fall into 4 major categories: Denial of service(Dos) , Probe, User to Root(U2R), Remote to User(R2L). Each record is labeled either as normal, or as an attack, with exactly one specific attack type.

2.1 Denial of Service (Dos)

Dos attacks are probably the nastiest, and most difficult to address. These are most horrible, because they are very easy to launch, difficult (some times impossible) to track, and it is not easy to refuse the requests of the attacker.

2.2 R2L Attacks (Remote to Local)

The goal of these attacks is to access some resources that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should provide command shell access without being sure that the person making such a request is some one who should get it, such as a local administrator.
This kind of attack can be from local user who need to abuse administrative privilege or it can also be form remote users.

2.3 User to Root (U2R) Attacks

It is obviously undesirable for an unknown person to be able to execute commands on your server machines. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people etc.,) that an attacker should not be able to do.

This might, then, be all the access that an attacker needs on the other hand, an attacker might wish to make configuration changes to host perhaps changing its IP address, putting a start-up script in place to cause the machine. In this case, the attacker will need to gain administrator's privileges on the host.

2.4 Probing

Certain information (Such as personal record, company information, credit card details and others) would cause damage once gone into the hands of a competitor, an enemy or the public. In this case, it is possible that a normal users account on the machine can be enough to cause damage, while many of the perpetrators of this sort of break-in can be merely thrill-seekers interested in nothing or more malicious sort of break-in.

2.5 Training and Data sets

Training set used in this study – "10% KDD: Test set used in this study-"corrected KDD" The number of samples of each category of records present in data set is shown below.

Table1. Number of Attacks in Training KDDCUP99 Data Set

Data Set	Normal	Dos	U2R	R2L	Probe
10%KDD	97277	391458	52	1126	4107
Corrected KDD	60593	229853	70	11347	4106
Whole	972780	3883370	50	1126	41102

Table2. Attack types and Sample size in 10%KDD Data set

	Attack Type (Number of Samples)
Normal	Normal(97277)
DOS	Smurf(280790), Neptune(107201), Back(2203), Teardrop(979), Pod(264), Land(21)
U2R	Buffer_overflow(30), Rootkit(10), loadmodule(9), perl(3)
R2L	Warezclient(1020), Guess_passwd(53), Warezmaster(20), Imap(12), ftp_write(8), Multihop(7), Phf(4), Spy(2)
Probe	Satan(1589), Ipsweep(1247), Portsweep(1040), Nmap(231)

This dataset categorized into 5 classes (Normal, DOS, U2R, R2L, Probe) it contains 22 attack types and size of each attack as shown in Table-2.

Table3: List of Features of a Record in KDD dataset

Feature Number	Feature Name	Description	Type
1	Duration	Duration of the connection(in seconds)	Continuous
2	Protocol type	Type of the connection protocol	Discrete
3	Service	Destination service	Discrete
4	Flag	Status flag of the connection	Discrete
5	Source bytes	Number of bytes sent form source to destination	Continuous
6	Destination bytes	Number of bytes sent from destination to source	Continuous
7	Land	1 if connection is from/to the same host/port; 0 otherwise	Discrete
8	Wrong fragment	Number of wrong fragments	Continuous

9	Urgent	Number of urgent packets	Continuous
10	Hot	Number of "hot" indicators	Continuous
11	Failed logins	Number of failed logins	Continuous
12	Logged in	1 if successfully logged in; 0 otherwise	Discrete
13	Num Compromised	Number of "compromised" conditions	Continuous
14	Root shell	1 if root shell is obtained; 0 otherwise	Continuous
15	Su attempted	1 if "su root" command attempted 0 otherwise	Continuous
16	Num Root	Number of "root" accesses	Continuous
17	Num File creations	Number of file creation operations	continuous
18	Num Shells	Number of shell prompts	continuous
19	Num Access files	Number of operation on access control files	continuous
20	Num Outbound cmds	Number of outbound commands in an ftp session	continuous
21	Is hot login	1 if the login belongs to the "hot" list; 0 otherwise	discrete
22	Is guest login	1 if the login is a guest login 0 otherwise	discrete
23	Count	Number of connections to the same host as the current connection in the past two seconds	continuous
24	Srv count	Number of connection to the same service as the current connection in past two seconds	continuous
25	Serror rate	Percentage of connection that have "SYN" error	continuous
26	Srv serror rate	Percentage of connection that have "SYN" error	continuous
27	Rerror rate	Percentage of connection that have "REJ" error	continuous
28	Srv rerror rate	Percentage of connection that have "REJ" error	continuous
29	Same srv rate	Percentage of connection to the same service	continuous
30	Diff srv rate	Percentage of connection to different service	continuous
31	Srv diff host rate	Percentage of connection to host	Continuous
32	Dst host count	Count of connection having same dest hot	continuous
33	Dst host srv count	Count of connection having the same destination host and using same service	Continuous
34	Dst host same srv rate	Percentage of connection having the same destination host and using same service	Continuous
35	Dst host diff srv rate	Percentage of different service on the current host	Continuous
36	Dst host same src port rate	Percentage of connection to the current hot having same src port	Continuous
37	Dst host srv diff	Percentage of connection to the same service coming form different host	Continuous
38	Dst host serror rate	Percentage of connection to the current host that have an S0 error	Continuous
39	Dst host srv serror rate	Percentagof connection to the current host and specified service that have an S0 error	Continuous

40	Dst host rerror rate	Percentage of connection to the current host that have an RST error	Contin uous
41	Dst host srv rerror rate	Percentage of connection to the current host and specified service that have an RST error	Contin uous

3. INTRUSION AND DETECTION SYSTEM

The National Institute of Standards and technology classifies[2] Intrusion Detection as "The process of monitoring the events occurring in a computer system, or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, Integrity, availability or to by pass the security mechanism of a computer or network". An IDS is a system that attempts to identify intrusions. Which we done to be unauthorized uses, abuses or misuses of computer systems by either authorized users or external perpetrators.

Intrusion Detection provides the following:

1. Monitoring and analyzing both user and system activities
2. Analyzing system configurations and vulnerabilities
3. Accessing system and file integrity
4. Ability to recognize patterns typical of attacks
5. Analysis of abnormal activity pattern
6. Tracking user policy violation

IDS Classified into two categories

1. Host based or network based
2. Misuse detection or anomaly detection

3.1 Host-based intrusion detection

A host based IDS resides on the system being monitored and tracks changes made to important files and directories. It takes a snap shot of existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. Zirkle[6] described host-based IDS as "loading a piece of software on the system to be monitored". This software, which is generally defined as either host wrappers/personal firewalls or agent-based software, performs the following:

- Uses log files and or the system's auditing agents as sources of data, traffic in and out of a single computer
- Checks the integrity of system files, and watches for suspicious processes, including changes to system files and user privileges.

3.2 Network-based intrusion detection

A network-based intrusion detection system monitors and analyzes the traffic on its network segment to detect intrusion attempts. An I.D.S can be made of many sensors, each sensor being in charge of monitoring the traffic passing through its own segment.

The sensors cannot monitor anything outside their own segment or switch. Northcutt [7] described network based intrusion detection system (NIDS) as an ID system that monitors the traffic on its network segment as a data source. Implementation requires:

- The network interface card is placed in promiscuous mode to capture all network traffic that crosses its network segment; and packets traveling on that network segment.
- A sensor, which monitors the objective is to determine if packet flow matches with a known signature.

There are three signatures that are particularly important:

- String signatures that look for a text string that indicates a possible attack.
- Port signatures simply watch for connection attempts to well known, frequently attacked ports.

- Header signatures that watch for dangerous or illogical combinations in packet headers.

3.3 Misuse detection

Misuse detection is also known as signature-based or knowledge-based systems. They follow the same principle as most anti-virus software and rely on the knowledge accumulated about previous attacks and vulnerabilities to detect intrusion attempts. Misuse detection systems compare current activities of the host or the network monitored with "signatures" of known attacks. If the current activities match any of the known signatures, an alarm is triggered.

Advantages and Limitations:
Low Rate of False Alarms: The main advantage of misuse detection systems is their ability to detect known attacks and the relatively low false alarm rate when rules are correctly defined. It is important to note that, as said above, the signatures which are used in rules must be as specific as possible to prevent false alarms.
Only Known Attacks Detection: The foremost drawback of misuse detection systems is their complete inability in detecting unknown attacks.

3.4 Anomaly detection

Anomaly detection systems are also known as behaviors-based systems. They rely on the fact that intrusions can be detected by observing deviations from the expected behaviors of the system monitored. These "normal" behaviors can either correspond to some observations made in the past or to some forecasts made by various techniques. Everything that does not correspond to this "normal" pattern will be flagged as anomalous. Therefore, the core process of anomaly detection is not to learn what is anomalous but to learn what is normal or expected.

Learning the Normal Behaviors and Detecting Deviations
The process of learning the normal behaviors of a system or a network and detecting deviations from these behaviors is an active area of research ever since the idea was first raised by Denning in 1987 [10]. Most of the methods currently investigated fall in any of the following five categories:

- Statistical-based detection,
- Payload-based detection,
- Protocol-based detection,
- Graph-based detection
- Machine-learning based detection.

Advantages and Limitations:

Unknown Attacks Detection: The main advantage of anomaly detection systems is that, contrary to misuse detection systems, they can detect unknown or novel attacks. They do not rely on any a priori knowledge concerning the intrusions. It is also important to note that anomaly detection systems have not for main purpose to replace misuse detection systems. The very good efficiency of misuse systems in detecting known attacks makes them a perfect complement to anomaly detection systems.
High Rate of False Alarms: Two factors may lead to a very high rate of false alarms or to a very poor accuracy of anomaly detection systems.

4. IDS METHODOLOGIES

In this paper we are concerned with different techniques used to process and implementing IDS. Classifying such techniques are very complicated because in the actual implemented system, a combination of such techniques may be used.

However, trace them individually helps better understanding the pros and cons of each, and how to improve a technique performance by combining with another technique.

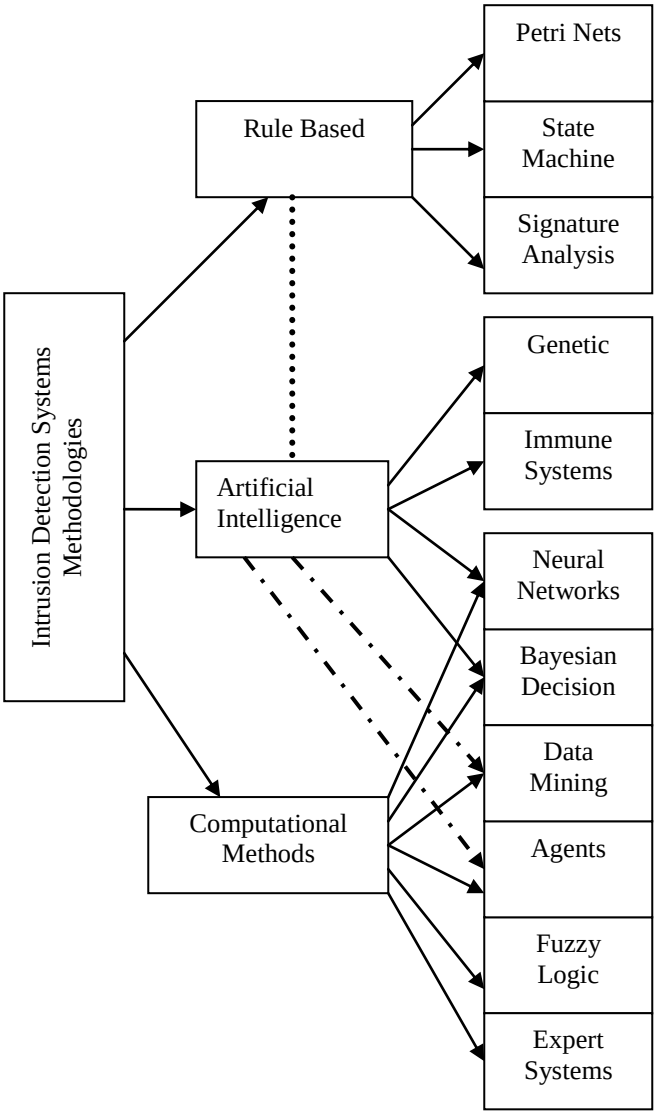

Figure.2 Methodologies for Intrusion Detection Systems

In the IDS there are totally eleven techniques are identified that are widely and currently used for processing input data of IDS [shown in Fig.2]. In the lower level of Fig. 2, techniques such as Agents and Data Mining belong to the Intelligent Data Analysis category. This is indicated by the dotted relation between Data Analysis and AI categories. The techniques: Expert systems and Fuzzy logic are intelligent model-based-rule-based systems shown by the dotted relation between Rule based and AI categories in Figure.2. The last level elaborates explanation about each technique.

4.1 Bayesian Inference

A Bayesian network consists of nodes and arcs representing variables and relations between the variables. Anomaly detection using Bayesian networks is a three-step process.

The first step is to select the variables used to monitor the system. There is no restriction on the kind of the variables. The second-step is to evaluate the relationship between these variables to construct a Bayesian network, so this step is the learning phase of the algorithm and it is called the "profile" of the system. The third step to determine the "support" by using profile, it gives the current state of the variables describing the system. The support is the probability of occurrence of the states observed. If this probability is less than the thresh hold, an alarm can be raised. In Bayesian networks, computing the "support" can be made by using mathematical formulas and the probability distributions computed for the profile.

4.2 Neural Networks

A neural network consists of Nodes and Edges. The value of the weight on edge defines how a node affects adjacent node. A subset of the nodes in the model is called the input nodes, which there is no connection themselves. The other subset contains the output nodes from which there is no connection themselves, their output is the result of the analysis. Anomaly detection using neural networks is a three-step process.

The first step consists of determining what kind of input data will be given and what output we want.

The second step consists in "training" the network -that is mapping the input-output by adjusting weights of the edges. This is the learning phase of the method.

The third step consists in using this network to detect anomalies. The input nodes are received data from a system and we observe the output of the network. Depending on the value of the output, we can determine whether the input vector was anomalous or not.

4.3 Data Mining

Data mining refers to a set of techniques that use the process of extracting previously unknown but potentially useful data from large stores of past data.

Data mining method excels at processing large system logs (audit data). However they are less useful for stream analysis of network traffic.

Decision trees[17] is one of the fundamental data mining techniques used in intrusion detection system. Decision tree models allow detecting anomalies in large databases.

Segmentation [18] technique refers to allowing extraction of patterns of unknown attacks. This is done by matching patterns extracted from a simple audit set with those referred to warehoused unknown attacks.

Association rules [19] technique is associated with to extract previously unknown knowledge on new attacks or built on normal behavior patterns. Anomaly detection often generates false alarms. With data mining it is easy to correlate data related to alarms with mined audit data, thereby considerably reducing the rate of false alarms.

4.4 Expert systems

The Expert Systems working principle is based on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of if-then-else rules.

4.5 Signature analysis

The Signature Analysis method is based on the attack knowledge. They convert the semantic format statement of an attack into the appropriate audit trail format.

Thus, attack signatures can be found in logs or input data streams in a straightforward way. Detection is accomplished by using common text string matching mechanisms.

4.6 Colored Petri Nets

This Petri Nets method is used to generalize attacks from expert knowledge bases and to represent attacks graphically. This technique is very easy and

useful for system administrators to add new signatures to the system. Audit trail data may be time-consuming. This technique is not used in commercial systems.

4.7 Agents

Agents are self contained processes that contain sensors and effectors to perceive and act on the environment respectively. Agents trace intruders and collect input data that is related only to the intrusion along the intrusion route. The major drawback with agents is that it needs a highly secure agent execution environment while collecting and processing input data. It is difficult also to execute onto large numbers of third-party servers.

4.8 Fuzzy Logic

Fuzzy Logic means to the model of uncertainty of natural language. In this case the logic depends on linguistics by taking the minimum of set of events or maximum instead of stating OR, AND or NOT operation in the if-then-else condition.

Basically, intrusion detection systems distinguish between two distinct types of behaviors, normal and abnormal. Fuzzy logic could create sets that have in-between values where the differences between the two sets are not well defined.

4.9 Genetic Algorithms (GA)

A Genetic Algorithm (GA) is a programming technique that mimics biological evolution as a problem-solving strategy.

GA uses an evolution and natural selection that uses a chromosome-like data structure and evolve the chromosomes using selection, recombination, and mutation operators.

This process usually begins with randomly generated population of chromosomes, which represent all possible solution of a problem that are considered candidate solutions.

An evaluation function is used to calculate the goodness of each chromosome according to the desired solution, this function is known as "Fitness Function".

During evaluation, two basic operators, crossover and mutation, are used to simulate the natural reproduction and mutation of species.

In intrusion detection the GA is employed to derive a set of classification rules from network audit data, and the support-confidence framework is utilized as fitness function to judge the quality of each rule.

4.10 State Machines

The State machines model is a collection of states, transitions and actions. An attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Sekar et al. [23] employ state-machine specifications of network protocols that are augmented with information about statistics that need to be maintained to detect anomalies. The protocol specifications simplified the manual feature selection process used in other anomaly detection approaches. The specification language made it easy to apply their approach to other layers such as HTTP and ARP protocols.

Peng, Leckie and Ramamohanarao [24] proposed a framework for distributed detection systems. They proposed a scheme to detect the abnormal packets caused by the reflector attack by analyzing the inherent features of the reflector attack.

4.11 Immune based

The Immune based IDS is based on human immune system concepts and can perform tasks similar to innate and adaptive immunity. The profile of normal behavior is generated by collecting appropriate behavior of services represented from audit data.

One challenge is faced to differentiate between self and non-self data which when trying to control causes scaling problems and the existence of flaws in detector sets.

5. CONCLUSION

In this paper we discussed a brief overview of Intrusion Detection System (IDS), related detection techniques and about the KDD Cup 99 Intrusion data. We are sure this brief survey is useful for all researchers those who want to investigate more efficient methods against intrusions.

In future we would like to investigate the efficient technique for feature reduction of the input dataset and find out how fuzzy logic, data mining, genetic algorithms along with neural networks can help to

improve intrusion detection and most of all anomaly detection.

6. REFERENCES

[1] Anderson. J. P. "Computer Security Threat Monitoring and Surveillance." Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, 1980.

[2] Baiju Shah "How to Choose Intrusion Detection Solution" SANS Institute Resources, July 24, 2001.

[3] Danny Rozenblum "Understanding Intrusion Detection Systems" SANS Institute Resources, 2001.

[4] KDD Cup 1999 Data, Information and Computer Science,University of California, Irvine. http://kdd.ics.uci.edddatabases/kddcup99/kddcup99.html

[5] N. Srinivasan and V. Vaidehi. "Timed Coloured Petri Net Model for Misuse Intrusion Detection" First International Conference on Industrial and Information Systems, 8-11 Aug. 2006.

[6] Zirkle, L., "What is host-based intrusion detection? "Virginia Tech CNS. SANS Institute Resources, Intrusion Detection FAQ, Hyperlink ID FAQ, 2000.

[7] Northcutt, S. "What the Hackers Know about You. "SANS Institute. SANS Institute Resources, Intrusion Detection FA*Q*, Hyperlink: ID FAQ, 1999.

[8] Ong, T.H., C.P. Tan, Y.T. Tan, C.K. Chew, and C. Ting. "SNMS-Shadow Network Management System "Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection, W. Lafayette, IN, 1999.

[9] Brenda McAnderson & Paul Ramstedt, "Intrusion Detection Technology: Today and Tomorrow", November, 18, 1999.

[10] [Denning 1987] An Intrusion-detection Model / Denning, D. E. – p. 118, IEEE Symposium on Security and Privacy, 1986.

[11] M. Mehdi, S. Zair, A. Anou and M. Bensebti "A Bayesian Networks in Intrusion Detection Systems" Journal of Computer Science 3 (5): 259-265, 2007, ISSN 1549-3636.

[12] Ryan, Meng-Jang Lin and Risto Miikulainen "Intrusion Detection with Neural Networks", In Advances in Neural Information Processing Systems 10, Cambridge, MA: MIT Press, 1998.

[13] Susan C. Lee and David V. Heinbuch "Training a Neural-Network Based Intrusion Detector to Recognize Novel Attacks", In IEEE Transactions on systems, man and cybernetics – part A: systems and humans, vol. 31, no. 4, July 2001.

[14] Anup K. Ghost and Aaron Schwartzbaard "A study in Using Neural Networks for Anomaly and Misuse Detection." In Pp. 141-152 of Proceedings of the 8th USENIX Security Symposium, Washington D.C, August 23-26, 1999.

[15] Theodoros Lapps and Konstantinos Pelechrinis "Data Mining Techniques for (Network) Intrusion Detection Systems" Department of Computer Science and Engineering UC Riverside, Riverside CA 92521.

[16] Fan W., Miller M., Stolfo S., Lee W., Chan P "Using Artificial Anomalies to Detect Unknown and Known Network Intrusions", In Proceedings of the First IEEE International Conference on Data Mining, San Jose, CA, November 2001.

[17] Lee W., Stolfo S, Mok K. "Adaptive Intrusion Detection: a Data Mining Approach", Artificial Intelligence Review, 14(6), pp. 533-567, December 2000.

[18] Bass T "Intrusion Detection Systems Multisensor Data Fusion: Creating Cyberspace Situational Awareness" Communication of the ACM, Vol. 43, Number 1, pp. 99-105, January 2000.

[19] Yao, J. T., S.L. Zhao, and L.V. Saxton, " A study on fuzzy intrusion detection ", Proceedings of SPIE Vol. 5812, Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, , Orlando, Florida, USA .,28 March - 1 April 2005.

[20] Gomez, J., and D. Dasgupta. "Evolving Fuzzy Classifiers for Intrusion Detection.", Proceedings of the 2002 IEEE, Workshop on Information Assurance, United States

Military Academy, West Point, NY., June 2001.

[21] Bobor, V. "Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms.", Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology, KTH/DSV, 2006.

[22] R. Sekar, A. Gupta, J. Frullo, T. Hanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-Based Anomaly Detection: a New Approach for Detecting", International Journal of Network Security, Vol. 1, No.2, pp. 84–102, 2005.

[23] T. Peng, C. Leckie and K. Ramamohanarao, "Information Sharing for Distributed Intrusion Detection Systems", Journal of Network and Computer Applications, Vol. [MAT02], No. 3, pp. 877-899, 2007.

[24] A. Pagnoni, and A. Visconti "An Innate Immune System for the Protection of Computer Networks", ACM International Conference Proceeding Series, Vol. 92 archive Proceedings of the 4th international symposium on Information and communication technologies, 2005.

[25] F.Sabahi, IEEE Member, A.Movaghar, IEEE Senior Member "Intrusion Detection: A Survey" The Third International Conference on Systems and Networks Communications, IEEE, 2008.

[26] Theuns Verwoerd and Ray Hunt, "Intrusion Detection Techniques and Approaches", Theuns Verwoerd and Ray Hunt, Department of Computer Science, University of Canterbury, New Zealand.