An Examination of Network Intrusion Detection System Tools and Algorithms: A Review

Jyoti Harbola
Mtech.(CSE)
BTKIT, Dwarahat

Kunwar Singh Vaisla
Associate Professor,CSE
BTKIT, Dwarahat

Aditya Harbola
Assistant Professor, MCA
GEU, Dehraun

ABSTRACT
Nowadays secured information communication has becoming at risk. Millions of users using the Internet at any instant of time and taking full use of the application's, services. DDoS flooding attacks are complex attempts to block the legitimate users. The Attacker normally gains access to a large number of computers by breaching their security loopholes and then they launch their attack to the target machine by these compromised machines. Intrusion Detection Systems have gained quick growth in command, scope and complexity. All IDS share an analogous primary structure: agents. Modern boost in malevolent network activity have hurried the need for IDS with global scope. A single IDS power can be grown by connecting an attack relationship engine with a database of events collected by distributed agents. This will help to provide global and single view of existing and rising attacks and will allow fast warning and ease development of countermeasures. A large number of distributed IDS with global and wide scope have been active for several years; three of these are discussed and compared with each other in this paper.

General Terms
Current IDSs cause challenges on not only unpredictable intrusion categories, but also huge computational command. So there is a number of existing literatures to IDS issues, and this paper will present a clear image for a comprehensive review.

Keywords
DDOS, Network attacks, IDS, IDS algorithms, IDS tools

1. INTRODUCTION
Nowadays secured information communication has becoming at risk because of threats from unknown and distributed sources and so the requirement for secured information assumes greater importance [1]. Attacks on network infrastructure are major threats With rapid growth of unauthorized actions in network, Intrusion Detection (ID) as a part of defense is very necessary because conventional firewall techniques cannot provide complete protection against intrusion [2].A DoS attack is a malevolent effort by an attacker (single or a group) to cause the target (server, site, node) to reject service to its customers. The single user attacks constitute a DoS attack and it is possible that a lot of malevolent hosts synchronize to flood the target with a large quantity of attack packets, so that the attack points can be scaled simultaneously and the attack becomes powerful. This attack is called a *Distributed Denial of Service*, or DDoS attack. The main motive behind DDoS attacks is to exhaust the target's resources, such as computing power, network bandwidth. To start on a DDoS attack, attacker need an infrastructure of computers that will be used to create the flood of traffic needed to deny services to legitimate users. To create an infrastructure, attackers discover weak hosts on the network. Weak hosts are usually those that are either having no antivirus software or non updated antivirus software or do not have any intruder detection system. The attacker as an intruder gains access to the vulnerable hosts system installs new programs or attack program on the compromised hosts. The weak hosts that run the attack programs on the behalf of the attacker are known as *zombies* because they do not have control over the attacker or the attacker tool. Many compromised systems together form an attack infrastructure.

2. BACKGROUND OF IDS
2.1: The Attack Types and Phases
The network is susceptible to many attacks and there are three types of network attacks as follows:

- ***Reconnaissance***
- ***Access***
- ***Denial of service (DoS)***

The first attack is to decide the goal of the attack. The second attack is to get access to a system network. The third attack is the genuine intrusion around the network assets. This attack comes with a DoS or an access attack. In it an opponent attempt to disturb, corrupt or tear down a network. It diminish the network's ability to perform its expected function [3]. Network Intrusion Detection Systems (NIDS) co-operate a major role on security deployment and assist organizations in safeguarding their assets from network attacks. NIDS was set up as a strategy to monitor and identify attacks on

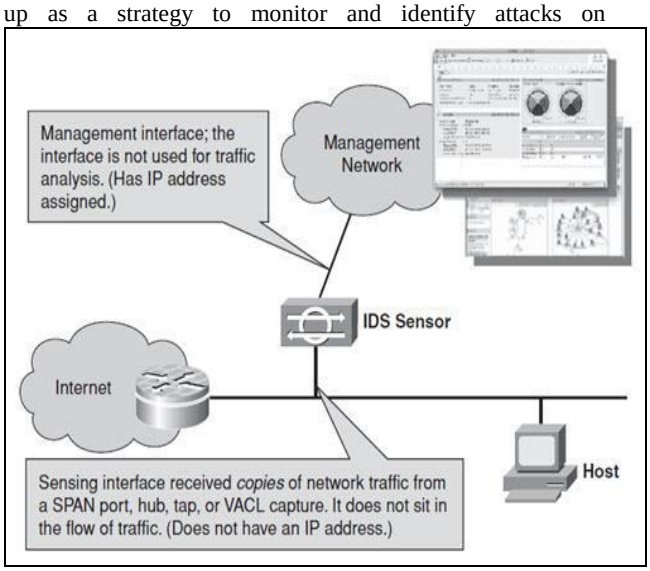

Figure 1: Intrusion Detection System

Weak services. Figure 1 shows the NIDS infrastructure.

2.2: Network Intrusion Detection Techniques

The techniques [4] [5] for the intrusion detection can be categorized into two categories:

- ***Anomaly Intrusion Detection***
- ***Misuse Intrusion Detection***

These techniques are based upon figures, Data mining, Neural Network and self manage Maps Based approaches etc. Based on [4], Anomaly Intrusion Detection is the process which attempts to see whether difference in the normal designs could be named as intrusion. Anomaly identification technique presumes that misuse detection is the most common approach used in the commercial IDS. Misuse Intrusion Detection uses the blueprint of known attacks of the system to balance and identity the attacks. Also all the computing resources are not utilized efficiently because of the inefficient use of the resources [23].

2.3: Existing Intrusion detection system and problems:

Many intrusion detection systems have been developed with time and all have merits and demerits. None of the system is able to provide complete and full proof IDS.

2.3.1. Snort: A free and open source network intrusion detection and prevention system was developed by M. Roesch in 1998 and now developed by Sourcefire. In 2009, this system entered InfoWorld's Open Source Hall of Fame as one of the "greatest open source software of all time" [8] [9].

2.3.2. OSSIM: The objective of Open Source Security Information Management, OSSIM is to supply a complete compilation of tools which, when working together, grant network and security administrators with a detailed vision over each and every aspect of networks, hosts, physical access devices, and servers [10].

2.3.3. BASE: The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools [11].

2.3.4: Sguil: Sguil is built by network security analysts for network security analysts [10] [11].Its main part is a sensitive GUI that provides real-time events from Snort. It includes components which assist the practice of network security monitoring and event driven investigation of IDS alert.

2.3.5: SAX2: SAX2 is a network based IDS. Sax2 is a professional intrusion detection and prevention system that performs real-time packet capturing, 24/7 network monitoring, advanced protocol analyzing and automatic expert detection [21].

Comparison between SNORT andSAX2*:*

1) SNORT is an open source IDS and SAX2 is shareware IDPS.
2) SNORT is supporting by all the major OS. SAX2 is only supporting by Windows.
3) SNORT analysis all the protocol. SAX2 also analysis IP, TCP, UDP, HTTP, FTP, POP3, SMTP protocols etc.
4) SNORT and SAX2are real time traffic analyzers.
5) SNORT and SAX2 are URL encoding, UDP port scan stealth port scans, packet logging and detecting signature attack.
6) SNORT throughput capability is 100mbps without packet loss. A SAX 2 throughput capability is high as compare to SNORT.
7) Rules set are flexible in SNORT so that changes are easily possible. SAX2 security rules are > 1500 but it can update rule set easily.

2.4: Problems with existing systems

The existing systems are prone to following problems [12].

2.4.1. Fidelity problem: Data has to traverse a longer path from its origin to the IDS and in the process can potentially be modified by an attacker. Then the intrusion detection system has to infer the performance of the system from the data collected, which can result in wrong events.

2.4.2. Reliability problem: An intruder can possibly stop or change the programs running on a system, exposing the intrusion detection system useless or unreliable.

2.4.3. Resource usage problem: The intrusion detection system always uses additional resources in the system it is monitoring even when there are no intrusions taking place, because the machinery of the intrusion detection system has to be running all the time.
All these above stated problems are actually been faced by the existing IDS so with time these problems are analyzed and the countermeasures been developed.

3. TYPES OF ALGORITHMS

In past with the advancement in DDoS attacks many intrusion detection techniques and algorithms have been developed.

3.1: GA (Genetic Algorithms):

Genetic algorithm is a combination of computational model for evolution and natural selection. GA translates the network issue into a model by make use of chromosomes like data structure and develop the chromosomes using selection, recombination and mutation operator [6]. Genetic algorithm

starts with a random selected known count of the

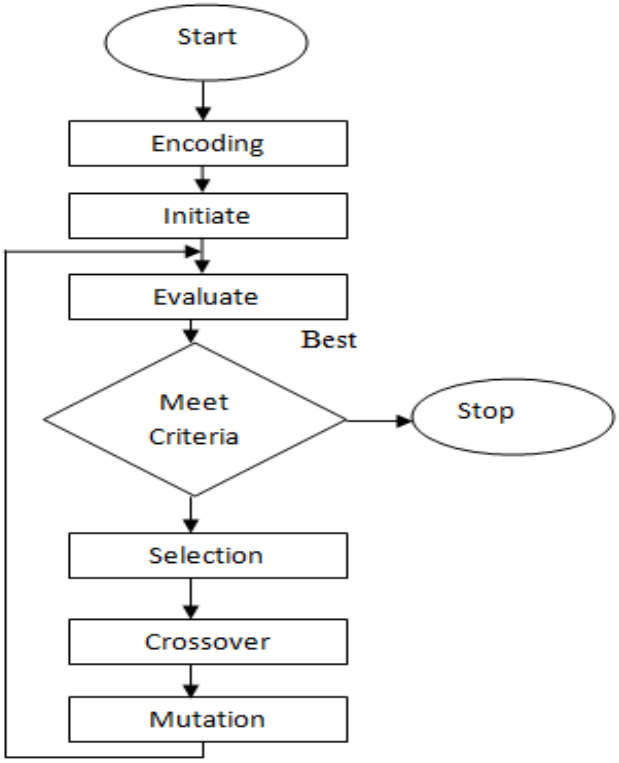

Figure 2: Genetic algorithm process

chromosomes, which indicate the issue to be solved. An assessment function can be used to calculate the goodness of every chromosome [7]. At first all various individual are selected according to user defined fitness function, others are discarded.

Then the various individual are combined with one another. Lastly a particular amount of individual are selected and alteration operator is applied randomly. Figure 2 Shows Genetic algorithm processes [6].

3.2: SVM (Support Vector Machine):

SVM are supervised learning models with associated learning algorithms that examine data and distinguish patterns, used for classification and regression study [13]. According to Guggenberger [14][17] the goal of the classification problem is to compute labels of latest input vectors to ensure that the error rate from the classification is minimal [18].

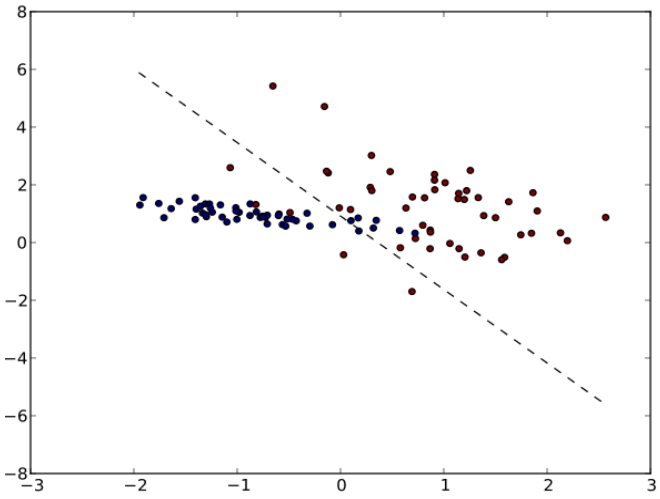

Figure 3. Linear SVM scarlet plot

3.3: K-means:

According to K-means Algorithm the classification is division clustering algorithm. The key idea [15] of the algorithm is to discover K centers (one for each cluster) of clusters. The major question here is how to choose

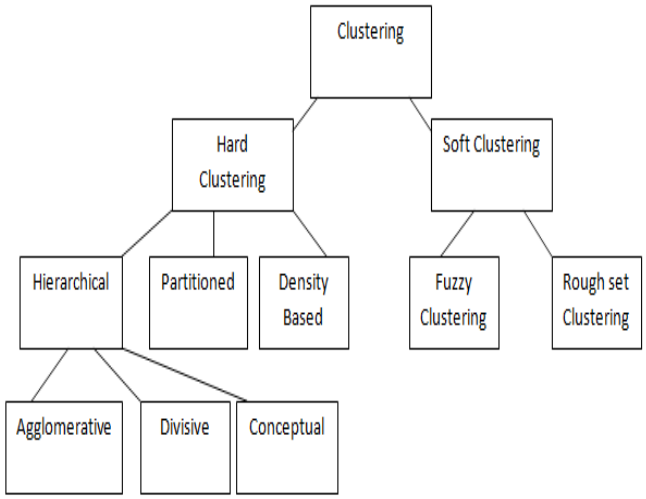

Figure 4: Different clustering approaches

Any centers of clusters, because this selection will significantly affect the resulting clusters [16]. The finest would be to pick center of cluster least similar to each other.

The next step is to assign each object from data set to the center of cluster, to which is for the most part similar. Once this take place, the next step in the classification is to decide the new center of all clusters.

3.4: COBWEB Clustering Algorithm:

This incremental clustering algorithm construct a hierarchical arrangement of clusters by using operator for construct a new cluster, include an object into an existing cluster, union of two clusters into one cluster and divide cluster into two clusters [19] and the classification utility .All these algorithms are basic algorithms which perform well on any of the IDS data set generated for the research purpose. Many other frameworks and packages are developed with time which provides a solution for intrusion detection system. Still there are many research challenges and areas where IDS needs refinement and progress.

3.5. CDAWG, Pattern Matching Algorithm for Intrusion Detection Systems:

In most Intrusion detection system's we need to check for a wider set of possibly known attack patterns. Pattern matching is an integral and necessary part of signature based IDS. Anithakumari et. al. [20] has implemented a CDAWG (compact Directed Acyclic Word Graph) in which String matching algorithm works 2.5 times faster than the currently used algorithm Aho-Corasick algorithm.

3.6. Knuth – Morris - Pratt Algorithm:

Knuth have suggested a string matching algorithm which fits the string to be searched into a finite state machine, and then checks the machine along the string to be searched as the input string. A matching time of O (n) is achieved taking some considerations [22]. B. Rajul et. al. has proposed a research paper in which it is shown that KMP algorithm can be used for IDS pattern matching and Prevention.

4. CONCLUSION AND FUTURE WORK

Some tools and algorithms for intrusion detection system are analyzed in this paper. Snort is powerful tool used for the network analysis and packet analysis. Each algorithm has some edge over other and researchers have used the algorithms as per their problem area. Clustering algorithm is basically deals with hierarchical arrangement of the clusters and classification purpose. Support vector machine approach for classification of error rate and any other variable decided by the user. Pattern matching is also important in IDS as there is a need of pattern match if we want to prevent the intrusion, by using previously gathered information about intrusion. All in all these all algorithms are not a complete solution for intrusion detection system. They suffer at the point of data analytics because at present the IDS data is a big data problem. So a new data analytics tool known as WEKA tool will be used for the analysis of the IDS data and analyzing the data sets. WEKA provides many inbuilt algorithms and classifiers which helps to analyze and visualize the problem very accurately and in a simple manner. In further work we will use WEKA with KDD cup 99 dataset for training and selection purpose. The future work will be based on these algorithms and WEKA tool.

5. REFERENCES

[1] Aneetha, S., Indhu, T.S. & Bose, S. (2012). *Hybrid Network Intrusion Detection System Using Expert Rule Based Approach.* Paper presented at the CCSEIT '12 Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology Pages 47-51,ACM New York, NY, USA ©2012

[2] Casella, E.L. Lehmann and G. (1998). *Theory of Point Estimation* Springer Texts in Statistics Vol. 2nded.(pp. 590 p). doi:10.1007/b98854

[3] M. Sadeghi, F. Khosravi, K. Atefi, M. Barati. (2012). Security Analysis of Routing Protocols in

Wireless Sensor Networks *International Journal of Computer Science Issues*, *9*, 465-472

[4] Carter, Earl. (2001). *Cisco Secure Intrusion Detection System* (Vol. 1). 800 East 96th Street,

Indianapolis, Indiana 46240: Pearson Education, Cisco Press.

[5] Yuebin Bail, Hidetsune Kobayashil (March 27-29, 2003). *Detection Systems: Technology and Development.* Paper presented at the 17th International Conference on Advanced Information Networking and Applications (AINA'03), Xi'an, China.

[6] Sharmila Devi, Ritu Nagpal. (2012). Intrusion Detection System Using Genetic Algorithm-A Review. *International Journal of Computing & Business Research*.

[7]Whitley, Darrell. (1992). *Foundations of Genetic Algorithms and Classifier*. Morgan Kaufmann Publishers Inc., 297-318.

[8]Snort(software); http://en.wikipedia.org/ wiki/Snort_% 28 software%29

[9]InfoWorld, The greatest open source software of all time, 2009; http://www.infoworld.com/d/open-source/greatest-open-source-software-all-time-776?source=fssr

[10] SecTools.Org: Top 125 Network Security Tools; http:// sectools .org/tag/ids/

[11]Sectools.Org: 2006 Results; http://sectools. org/tools 20 06.html

[12]Houque,Mukit,Bikas"An mplementation of Intrusion Detection System Using Genetic Algorithm" IJNSA,Vol. 4, No. 2,March 2012

[13] http://en.wikipedia.org/wiki/Support_vector_machine

[14] Guggenberger, Andre. (2008). Another Introduction to Support Vector Machines. Retrieved from http://mindthegap.googlecode.com/files/ AnotherIntroductionSVM.pdf

[15] P. Berkhin. A Survey of Clustering Data Mining Techniques. Grouping Multidimensional Data, p. 25–71, 2002

[16] A. Abraham and R. Jain. Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies in Computational Intelligence, p. 191–207, 2005

[17] S. Abe. Support Vector Machines for pattern classification. London, Springer, 2005

[18] N. Cristiani and J. Shawe-Taylor. An Introduction to Support Vector Machines and other kernel-based learning methods. Cambridge, Cambridge University Press, 2000.

[19] D. H. Fisher. Knowledge Acquisition Via Incremental Conceptual Clustering.Kluwer Academic Publisher, 1987.

[20] Anithakumari, S.; Chithraprasad, D., "An Efficient Pattern Matching Algorithm for Intrusion Detection Systems," Advance Computing Conference, 2009. IACC 2009. IEEE International , vol., no., pp.223,227, 6-7 March 2009

[21] Bhavani sunke, Research and Analysis of Network Intrusion Detection systems, Internet, 1-88, 2008.

[22] B. Raju1 and B. SrinivasNetwork Intrusion Detection System Using KMP Pattern Matching Algorithm, IJCST,33-36, January 2012.

[23] Aditya Harbola et.al. "Green computing research challenges: A review", IJARCSSE, Volume 3, Issue 10, October 2013