Intrusion Detection System (IDS) by using Data Mining Techniques

Bhavesh.G.Pamwani[1] RavirajChauhan[2]
[2]Assistant Professor
[1,2]Department of Computer Engineering and Technology
[1,2]Parul Institute of Engineering and Technology, Vadodara, India

Abstract— Data mining has been used extensively and broadly by several network organizations. Intrusion Detection is one of the high priorities & the challenging tasks for network administrators & security experts. Intrusion detection system is employed to protect the data integrity, confidentiality and system availability from attacks. IDS use the data mining techniques to analyze the resources from the database over a network. It is also necessary to develop a robust algorithm to generate effective rules to get better results in terms of accuracy, false alarm rate, efficiency, capability to detect new type of attacks.

Key words: Data Mining, Intrusion Detection System, Knowledge Discovery Database

I. INTRODUCTION

Intrusion detection is performed to analyze and monitor the activities done by the individual host or by the network. Our main motivation is to safeguard the system from threats. It is possible only through Intrusion Detection System.

Intrusion detection system is a passive method. It just monitors the information over network or hosts and raises alarms when any intrusion happens. But data mining based ids can identify these data when it arrives and forecast it on its own, thus by gaining the function of active approach. Data mining has been popularly recognized as an important way to analyze useful information from large volumes of data that are noisy, fuzzy & random. Extracted patterns can be used to improve the business activities like sales, marketing and customer management. IDS are of two types namely Host and Network based IDS[1]. In HIDS the data come from audit record, system logs, application program etc, by comparing with network IDS to analyze network attack or an intrusion happened to particular hosts. Whereas the encrypted packets passes over the network from the system files and then decrypted in host machine. So the data are not affected and it does not require any special kind of hardware than monitoring system installed in specific host. In network based ids commonly one Intrusion Detection System is enough for the whole LAN. It is of low cost & capable of analyzing many attacks like DoS, DDoS, etc., but HIDS fails to analyze those attacks.[1]

Intrusion detection system has traditionally been classified into two classes namely anomaly detection and misuse/signature based detection.[1] Misuse detection compares the upcoming network traffic to the database of known attack with the help of signatures to detect intrusions. It works efficiently in analyzing known attacks that are stored in the database. But it cannot detect new attacks that are not predefined. On the other hand, the anomaly detection approach creates a profile (normal) based on the network and hosts under inspection & raises alarms or some kind of notification to make the administrator to handle the situation. However they have being able to detect new & unusual attacks. There are two types of false alarms in determining the any deviations from normal pattern false positive and false negative.[2] The main goal is to keep these alarms as low as possible. Data mining techniques such as association, classification, clustering and neural networks have been used in intrusion detection.

II. IDS

There has been a simultaneous increase in the number of attacks on networks, resulting in an increasing interest in network intrusion detection among the researchers. [2] The threat of a new wave of cyber or network attacks is not just a probability that should be considered, but it is an accepted fact that can occur at any time. In addition to the hacking, new entities like worms, Trojans and viruses introduced more panic into the networked society.

An Intrusion Detection System (IDS) [1] is a device or a software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection systems constantly monitor a given computer network for invasion or abnormal activity. The advantage of this service is the "round-the-clock" aspect, in that the system is protected even while the user is asleep or otherwise away from any computer hooked up to the network. Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. It is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic.

There are two basic types of intrusion detection: Host-based and Network-based. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages.

Host-based intrusion detection systems (HIDS) are IDSs that operate on a single workstation. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. [1]

Network-based intrusion detection systems (NIDS) are IDSs that operate as stand-alone devices on a network. NIDS monitors traffic on the network to detect attacks such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic. [1]

NIDS	HIDS
– Resides on the computer/ application connected to a part on an organization's network and monitors network traffic on that segment looking for indication of ongoing or successful	Resides on a particular computer or server, known as the host, and monitors activity only on that system looking for any malicious program running.

attacks. – Types of NIDS include Snort, Cisco NIDS, and Netprowler. – NIDS uses a monitoring port, when placed next to a networking device like hub, switch. The port views all the traffic passing through the device. Works on the principle of signature matching, ie comparing attack patterns to known signatures in their data base. – NIDS are suitable for medium to large scale organizations due to their volume of data and resources. So, many smaller companies are hesitant in deploying IDS.	– Types of HIDS, include Tripwire, Cisco HIDS, and Symantec ESM – Capable of monitoring system configuration data bases, such as windows registries, and stored configuration files like .ini, .cfg and .dat files. – Work on the principle of configuration and change management. An alert is triggered when file attributes change, new files created or existing files deleted. – Generally, most HIDS have common architectures, meaning that most host systems work as host agents reporting to a central console.
1) Advantages: – Large networks can be monitored by deploying a few devices with a good network design. – Ongoing network operations won't be disrupted by deploying NIDS, since they are passive devices. – NIDSs are not susceptible to direct attack and may not be detectable by attackers.	1) Advantages: – Attacks that elude NIDS and local events can be detected by HIDS. – HIDS functions on the host system, where encrypted traffic will be decrypted and available for processing. – The use of switched network does not affect a HIDS. – HIDS can detect inconsistencies in the application.
2) Disadvantages: – NIDS may fail to recognize attack when network volume becomes over-whelming. – Since many switches have limited or no monitoring port capability, some networks are not capable of providing all the data for analysis by a NIDS. – NIDS cannot analyze encrypted packets, making some of the traffic invisible to the process and reducing the effectiveness of NIDS. – Attacks involving fragmented or malformed packets cannot easily be detected.	2) Disadvantages: – More management efforts required to install configure and manage HIDS. – Both direct attacks and attacks against the host operating system results in compromise and/or loss in functionality of HIDS. – HIDS is susceptible to some DoS attacks. – Host OS audit logs occupy large amounts of disk space and disk capacity needs to be added, which may reduce system performance. – HIDS cannot scan /detect multi-host and non-host network devices.
NIDS	**HIDS**
– Resides on the computer/ application connected to a part on an organization's network and monitors network traffic on that segment looking for indication of ongoing or successful attacks. – Types of NIDS include Snort, Cisco NIDS, and Netprowler. – NIDS uses a monitoring port, when placed next to a networking device like hub, switch. The port views all the traffic passing through the device. Works on the principle of signature matching, ie comparing attack patterns to known signatures in their data base. – NIDS are suitable for medium to large scale organizations due to their volume of data and resources. So, many smaller companies are hesitant in deploying IDS.	– Resides on a particular computer or server, known as the host, and monitors activity only on that system looking for any malicious program running. – Types of HIDS, include Tripwire, Cisco HIDS, and Symantec ESM – Capable of monitoring system configuration data bases, such as windows registries, and stored configuration files like .ini, .cfg and .dat files. – Work on the principle of configuration and change management. An alert is triggered when file attributes change, new files created or existing files deleted. – Generally, most HIDS have common architectures, meaning that most host systems work as host agents reporting to a central console.

Table 1: Difference between NIDS and HIDS [1]

III. ATTACKS DETECTED BY DIFFERENT TYPES OF IDS

A. Denial-Of-Service (DOS) Attacks [1]:

It is an attempt to forbid the authorized users from utilizing the requested service/ resource. A more advanced Distributed Denial of Service occurs when in a distributed environment the attacker sends or rather floods the server or a target system with numerous connection requests knocking the target system to the knees, leaving them no other option to restart their system.

B. Eavesdropping Attacks [1]:

A form of external attack where there is an unauthorized interception of network communication and disclosure of exchanged information. This can be performed in different layers – for example, in network layer by sniffing into the exchanged packets or in physical layer by physically wiretapping the access medium.

C. Spoofing Attack [1]:

The attacker impersonates a legitimate user. IP spoofing is a common example where the system is convinced that it is

communicating with a trusted user and provides access to the attacker. The attacker sends a packet with an IP address of a known host by alerting the packet at the transport layer.

D. Intrusion Attacks or User to Root Attack (U2R) [1]:

An unauthorized user tries to gain access to system or root through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle leading to data loss.

E. Logon Abuse attacks [1]:

A successful logon abuse attack would bypass the authentication and access control mechanisms and grant a user with more privileges that authorized.

F. Application-Level Attacks [1]:

The attacker exploits the weakness in the application layer – for example, security weakness in the web server, or in faulty controls in the filtering of an input on the server side. Examples include malicious software attack (viruses, Trojans, etc), web server attacks, and SQL injection.

IV. MECHANISM OF INTRUSION DETECTION SYSTEM

A. Stack-Based: [2]:

Stack based intrusion detection system is the latest technology which works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.

B. Signature-Based/Pattern Matching-Based: [2]:

Signature based intrusion detection system use a rule set to identify the intrusions by watching for patterns of the events specific to known and documented attacks. It is typically connected to a large database which houses attack signatures. It compares the information it gathers against those attack signatures to detect a match.

C. Anomaly-Based: [2]:

Anomaly Based Intrusion Detection System examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies.

D. Hybrid-Based: [2]:

Hybrid based intrusion detection is the combination of stack, signature, and anomaly based detection. Because of the difficulties with the anomaly based and signature based detections, a hybrid model is being developed. Much research is now focusing on this hybrid model.

V. WIRESHARK AND TCPDUMP

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communication protocols development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark is software that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

A. Intrusion Detection Using Wireshark [4]:

Intrusion Can Be Detected Using Wireshark ->Expert Info's:
Wireshark in a capture file.Each expert info will contain the following things.

1) Severity:

Chat (grey): information about usual workflow
e.g. a TCP packet with the SYN flag set
Note (cyan): notable things e.g. an application returned a "usual" error code like HTTP 404.
Warn (yellow): warning e.g. application returned an "unusual" error code like a connection problem.
Error (red): serious problem e.g. [Malformed Packet]

2) Intrusion Can Be Detected Using Wireshark ->Chats:

Chats for the TCP connection should contain sequence of SYN, SYN+ACK and ACK messages.

3) Firewall Can Be Applied Using Wireshark->Firewall ACL (Access Control List) Rules:

A network conversation is the traffic between two specific endpoints. For example, an IP conversation is all the traffic between two IP addresses.

Any data mining technique such as association rule, classification, clustering etc can be applied to find the rules using either Weka or Rapid Miner Tool. Example: J48 algorithm which takes 0.09sec. It is classified based on the number of packet sent, packet received and port number.
Using wireshark firewall can be applied for any of the IP address to deny/allow packet from that particular IP.

4) Intrusion Can Be Detected Using Wireshark->Flow Graph:

Flow graph shows the communication between two or more different IP's.

5) Intrusion Can Be Detected Using Wireshark->Conversations:

B. TCPDUMP:

One of the most basic tools for analyzing packets is tcpdump.[5] Tcpdump runs from the command line and uses the libpcap module, which is an API for packetcapture and analysis. The program attempts to present packets in a more readable format, by decoding formats such as TCP (Transmission Control Protocol) and IP (Internet Protocol) headers to present them in a more user friendly way. This

The expert info's is a kind of log of the anomalies found by type of software is known as a protocol analyzer, since it combines the ability to retrieve packets from networks, but also to decompose the relevant protocols to make analysis more relevant.

VI. KDD CUP 99 AND NSL KDD

KDD Cup 99 data setcontains 23 attack types and their names are shown in table3and its features are grouped as:

A. Basic features:

It encompasses all the attributes of TCP/IP connection and leads to delay in detection.

B. Traffic features:

It is evaluated in accordance with window interval & two features as same host and same service.

1) Same host feature:

It examines the number of connections for the past 2 s that too from the same destination host. In other words, the probability of connections will be done in a specific time interval.

2) Same service feature:

It examines the number of connections in a particular time interval that too possess same service.

C. Content features:

Dos & probe attack have frequent intrusion sequential patterns than the R2L & U2R. Because these two attacks include many connections to several hosts at a particular time period whereas R2L and U2R perform only a single connection. To detect these types of attacks, domain knowledge is important to access the data portion of the TCP packets.

Ex. Failed login, etc. these features are called as content features.

NSL-KDD is a dataset proposed by Tavallaee et al. NSL-KDD dataset is a reduced version of the original KDD 99 dataset.[6] NSL-KDD consists of the same features as KDD 99. The KDD99 dataset consists of 41 features and one class attribute. The class attribute has 21 classes that fall under four types of attacks: Probe attacks, User to Root (U2R) attacks, Remote to Local (R2L) attacks and Denial of Service (DoS) attacks. This dataset has a binary class attribute. Also, it has a reasonable number of training and test instances which makes it practical to run the experiments on.

The NSL-KDD has the following differences over the original KDD 99 dataset: [6]

1) It does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records.
2) There are no duplicate records in the proposed test sets; therefore, the performances of the learners are not biased by the methods which have better detection rates on the frequent records. The number of selected records from each difficulty level group is inversely proportional to the percentage of records in the original KDD 99 data set. The numbers of records in the train and test sets are reasonable, which makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of different research works will be consistent and comparable.

In 2011, V.K.Pachghare ,V.K.Khatavkar and Dr. ParagKulkarni proposed a system and tested it on both KDD cup99 and NSL KDD and experimental results showed that the detection rate for NSL-KDD dataset is greater than KDD CUP 10 % dataset. The false positive rate is also greater for NSL-KDD dataset than KDD 10% dataset.[7]

VII. IDS USING DATA MINING TECHNIQUES

In 2013 G.V.Nadiammai and M.Hemlatha proposed an improved Efficient Data Adapted Tree algorithm that achieved higher accuracy, less alarm rate and capable of detecting new type of attack efficiently. The data set used was KDD CUP99. [8]

They compared the results based on accuracy, sensitivity, specificity and FAR values and showed that their EDADT algorithm is 19.4% better than C4.5, 18.8% better than SVM, 19.6% better than C4.5+ACO, 19.2% better than SVM+ACO, 19.7% better than C4.5+ PSO, 19.3% better than SVM + PSO in terms of accuracy. Thus the proposed EDADT algorithm reduces the actual size of the dataset and helps the administrator to analyze the ongoing attacks efficiently with less false alarm rate respectively.

In 2014 G.V.Nadiammai and M.Hemlatha solved the issues like classification of data, high level of human interaction, lack of labeled data and effectiveness of DDOS by their algorithms: EDADT, Hybrid IDS model, Semi-Supervised Approach and Varying Hoperaaslgorithm. [9]

They gave the solution as follows:

1) To solve the problem of Classification of Data, an enhanced data adapted decision tree algorithm is proposed. This algorithm works different normal decision tree algorithm and classifies the data into normal and attack without any misclassification.
2) To minimize the workload of network administrator, SNORT is combined with anomaly based approaches.
3) The problem of implementing supervised and unsupervised method can be solved by using Semi-Supervised Approach where with small amount of labeled data, the large amount of unlabeled data can be labeled.

Distributed Denial of Service Attack can be greatly reduced using varying clock drift, with the help of varying clock drift in network based application, the adversary finds difficult to access the port that has been used by the legitimate client.

A. EDADT Algorithm:

For future issues they gave two issues to be considered: lack of resource consumption information and lack of model adjustment information techniques to be deployed to achieve automated IDS.

In 2014 Brijeshsharma and Huma Gupta proposed a system that can detect the attacks/intrusions and classifies them into different categories: U2R (User to Root), probe, R2L (Remote to Local), and Denial of Service (DoS). The prime task of the proposed IDS is to improve effectiveness with efficiency. An experiment was carried out to evaluate/calculate the performance of the proposed approach using KDD 99' dataset. The result shows that the proposed IDS technique performs better in term of efficiency (Execution Speed) & effectiveness. [10]

The system was divided into following modules:

1) Database Selection (Suggested Technique):
- Data source (KDD 99') is selected
- Data Pre-processing(Training and Testing)

2) Data Mining Techniques:
- Apripori
- K-Means Cluster Technique

3) Proposed System
- Apriori Technique
- Apriori with K-Mean

4) Performance

- Time Analysis
- Memory Analysis
- CPU Analysis

For the future work they considered to extend their system for host based IDS with some modifications.

In 2014, NedaAbdelhamid, Aladdin Ayesh and FadiThabtahinvestigated the problem of website phishing using a developed AC method called Multi-label Classifier based Associative Classification (MCAC) to seek its applicability to the phishing problem. Experimental results using real data collected from different sources show that AC particularly MCAC detects phishing websites with higher accuracy than other intelligent algorithms. Further, MCAC generates new hidden knowledge (rules) that other algorithms are unable to find and this has improved its classifiers predictive performance. [11]
The MCAC algorithm

B. Algorithm:

Input: Training data D, minimum confidence (MinConf) and minimum support (MinSupp) thresholds.
Output: A classifier

C. Preprocessing:

Discretise continuous attributes if any

1) Step One:
Scan the training data set *T* to discover the complete set of frequent attribute values. Convert any frequent attribute value that passes *MinConf*to a single label rule. Merge any two or more single label rules that have identical body and different class to derive the multi-label rules

2) Step Two:
Sort the rule set according to confidence, support and rule's length
Build the classifier by testing rules on the training data and keeping those in Cm that have data coverage

3) Step Three:
Classify test data using rules in Cm

The results revealed that the method outperformed the considered methods on detecting phishing with respect to accuracy rate. Further, the label-weight and any-label results of MCAC are better than those of the MMAC for the same phishing data. More importantly, MCAC was able to produce multi-label rules from the phishing data generating rules associated with a new class called ''Suspicious'' that was not originally in the training data set. This has enhanced further its classifiers predictive performance.

VIII. SUMMARY

A. Types of IDS:

TYPES	ADVANTAGES	DISADVANTAGES
NIDS	– Large networks can be monitored. – Ongoing network operations won't be disrupted. – NIDS are not susceptible to direct attack.	– NIDS may fail to recognize attack when network volume becomes over-whelming. – Some networks are not capable of providing all the data for analysis by a NIDS. – NIDS cannot analyze encrypted packets. – Attacks involving fragmented or malformed packets cannot easily be detected.
HIDS	– Attacks that elude NIDS and local events can be detected by HIDS. – HIDS functions on the host system. – The use of switched network does not affect a HIDS. – HIDS can detect inconsistencies in the application.	– More management efforts required to install configure and manage HIDS. – Both direct attacks and attacks against the host operating system results in compromise and/or loss in functionality of HIDS. – HIDS is susceptible to some DoS attacks. – Occupy large amounts of disk space which may reduce system performance. – HIDS cannot scan /detect multi-host and non-host network devices.

Table 2:

B. Attacks Detected by IDS:

1) Denial-of-Service (DOS) Attacks:
It is an attempt to forbid the authorized users from utilizing the requested service/ resource.

2) Eavesdropping Attacks*:*
A form of external attack where there is an unauthorized interception of network communication and disclosure of exchanged information.

3) Spoofing Attack:
The attacker impersonates a legitimate user. IP spoofing is a common example.

4) User to Root Attack*:*
An unauthorized user tries to gain access to system or root through the network. Example Buffer overflow attack

5) Logon Abuse Attacks:
A successful logon abuse attack would bypass the authentication and access control mechanisms and grant a user with more privileges that authorized.

6) Application Level Attacks*:*
The attacker exploits the weakness in the application layer – for example, security weakness in the web server.

C. IDS Using Data Mining Techniques:

AUTHOR	PROPOSED SYSTEM	RESULTS	FUTURE WORK

Nadiammai, G. V., et al [8] 2013	EDADT algo. (Efficient Data Adapted Tree algorithm)	EDADT showed better results than C4.5, SVM, ACO, PSO in terms of accuracy. Reduces actual size of dataset and results in less FAR values.	For future, a hybrid intrusion detection system can bedeveloped which would be fast and robust in identifying the variety of new and unusual attacks.
Nadiammai, G. V., and M.Hemalatha [9] 2014	EDADT, Hybrid IDS model, Semi-supervised approach and varying hoperaalgo.	Issues solved: classification of data, high level of human interaction, lack of labeled data and effectiveness of DDOS.	For future two issues are to be considered: lack of resource consumption information and lack of model adjustment information techniques.
Sharma, Brijesh, and Huma Gupta. [10] 2014	Apriori technique with K-Mean technique.	Improved performance in terms of effectiveness and efficiency.	For future extend the system for HIDS.
Abdelhamid, Neda, Aladdin Ayesh, and FadiThabtah. [11] 2014	MCAC (Multi-label Classifier based Associative Classification)	Better accuracy compared to MMAC for same phising data.	For future, they consider content based features.

Table 3:

IX. Conclusion and Future Enhancement

Nowadays, the usage of network is growing rapidly and as well as it provides information rapidly. Likewise security violation like hackers, viruses, worms etc., also spread even faster across the network. Since the Intruder can compromise the confidentiality, integrity and availability of network resources. For the past few years, firewall acts as a gate wall for security measures. But it fails to detect the network traffic that has been done by the specific port or from the legitimate user port. So intrusion detection is necessary to handle the hackers from exploiting the data. Intrusion detection is possible only through Intrusion Detection System. Intrusion detection system is a passive method. It just monitors the information over network or hosts and raises alarms when any intrusion happens. But data mining based ids can identify these data when it arrives and forecast it on its own, thus by gaining the function of active approach.

The MCAC algorithm can be used to develop an IDS that will give better results in terms of accuracy, efficiency, effectiveness, false alarm rate. The system can also be modified to give the benefit of flexible architecture. New rules can be developed to detect and prevent the novel attacks.

X. Acknowledgements

The Grateful thanks are extended to my guide, Asst.Prof.R.CHAUHAN, for all his diligence, guidance, encouragement, inspiration and motivation throughout. Without his treasurable advice and assistance it would not have been possible for me to attain this landmark.

References

[1] KR, Karthikeyan, and A. Indra. "Intrusion Detection Tools and Techniques–A Survey."
[2] Chowdhary, Mahak, ShrutikaSuri, and MansiBhutani. "Comparative Study of Intrusion Detection System." (2014).
[3] Sava, Neha, et al. "Survey on Intrusion Detection Systems." International Journal 2.1 (2014).
[4]] Gupta, S., and R. Mamtora. "Intrusion detection system using wireshark." Int. J. Adv. Res. Comput. Sci. Soft. Eng 2 (2012): 34-36.
[5] Gupta, A., "A Research Study on Packet Sniffing Tool TCPDUMP" Int. J. of comm. And comp. tech. (2013)
[6] Ibrahim, Laheeb M., Dujan T. Basheer, and Mahmod S. Mahmod. "A Comparison Study For Intrusion Database
[7] denial of service attacks. In: ACM symposium on applied computing, no. 26; 2011. p. 520–27. (Kdd99, Nsl-Kdd) Based On Self Organization Map (SOM) Artificial Neural Network." Journal of Engineering Science and Technology 8.1 (2013): 107-119.
[8] V. K. Pachghare, Vaibhav K Khatavkar, Dr. ParagKulkarni "Performance Analysis of Supervised Approach for Pattern based IDs" IJCA

Special Issue on "Network Security and Cryptography"NSC, 2011
[9] Nadiammai, G. V., et al. "an Enhanced Rule Approach for Network Intrusion Detection Using Efficient Data Adapted Decision Tree Algorithm." Journal of Theoretical and Applied Information Technology 47.2 (2013): 426-433.
[10] Nadiammai, G. V., and M. Hemalatha. "Effective approach toward Intrusion Detection System using data mining techniques." Egyptian Informatics Journal15.1 (2014): 37-50.
[11] Sharma, Brijesh, and Huma Gupta. "A Design and Implementation of Intrusion Detection System by Using Data Mining." Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on.IEEE, 2014.
[12] Abdelhamid, Neda, Aladdin Ayesh, and FadiThabtah. "Phishing detection based Associative Classification data mining." Expert Systems with Applications 41.13 (2014): 5948-5959.
[13] Vincenzo Gulisano, Zhang Fu, Mar Callau-Zori, Ricardo Jim Enez-Peris, Marina Papatriantafilou, Marta Patino-Martınez. STONE: a stream-based DDoS defense framework. In: Technical report no. 2012-07, ISSN 1652-926X, Chalmers University of Technology; 2012.
[14] Sethuramalingam S. Hybrid feature selection for network intrusion. Int J ComputSciEng 2011;3(5):1773–9.
[15] KDD Cup99 intrusion Detection Dataset. Available from: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>. Monowar H. Bhuyan, Bhattacharyya DK, Kalita JK. An effective unsupervised network anomaly detection method. In: International conference on advances in computing, communications and informatics, no. 1; 2012. p. 533–9.
[16] Lane T. A decision-theoretic, semi-supervised model for intrusion detection. In: International conference on machine learning and data mining for computer security; 2006. p. 157–77.
[17] Zhang Fu, Marina Papatriantafilou, PhilippasTsigas. Off-thewall: lightweight distributed filtering to mitigate distributed denial of service attacks. In: IEEE international symposium on reliable distributed systems, no. 31; 2012. p. 207–12.
[18] Zhang Fu. Marina Papatriantafilou, PhilippasTsigas, Wei Wei. Mitigating denial of capability attacks using sink tree based quota allocation. In: ACM symposium on applied computing, no. 25; 2010. p. 713–18.
[19] Zhang Fu. Marina Papatriantafilou, PhilippasTsigas. CluB: a cluster based framework for mitigating distributed
[20] Vincenzo Gulisano, Zhang Fu, Mar Callau-Zori, Ricardo Jim Enez-Peris, Marina Papatriantafilou, Marta Patino-Martınez. STONE: a stream-based DDoS defense framework. In: Technical report no. 2012-07, ISSN 1652-926X, Chalmers University of Technology; 2012.

