Anomaly Detection in IPv4 and IPv6 Networks Using Machine Learning

Department of Information Technology, Indian Institute of Information Technology, Allahabad, India
Bhanu Vrat[1], Nikhil Aggarwal[2], S. Venkatesan[3]
E-mail: bhanuvrat91@gmail.com[1], agg.nikhil12@gmail.com[2], venkat@iiita.ac.in[3]

Abstract: Anomaly Detection is an important requirement to secure a network against the attackers. Detecting attacks within a network by analysing the behaviour pattern has been a significant field of study for several researchers and application systems in IPv4 as well as IPv6 networks. For precise anomaly detection, it is essential to implement and use an efficient data-mining methodology like machine learning. In this paper, we contemplated an anomaly detection model which uses machine learning algorithms for data mining within a network to detect anomalies present at any time. This proposed model is evaluated against Denial of Service (DOS) attacks in both IPv4 and IPv6 networks while selecting the most common and evident features of IPv6 and IPv4 networks for optimizing the detection. The results also show that the proposed system can detect most of the IPv4 and IPv6 attacks in efficient manner.

I. INTRODUCTION

Intrusion Detection has been a critical technique of information security following continuous growth and complexity of Internet. With exhaustion of IPv4 addresses and emergence of IPv6 addresses, it has become more difficult for detecting intrusions since IPSec has been mandated as a built-in security measure for IPv6[1][2].

IPv6 although have been proposed in 1998 [3] but it is still a new technology and its use might gravel new vulnerabilities which could be exploited by attackers for gaining access into the networks [4]. Therefore it becomes necessary to implement intrusion detection for securing the networks from anomalous traffic. Intrusion detection systems for IPv4 networks can also be implemented for an IPv6 network, but analysing new features of IPv6 may become difficult because IPSec encapsulates and encrypts the packets which can only be decrypted at user end.

The overall goal of this paper is to propose an efficient intrusion detection model which can work effectively on both IPv4 as well as IPv6 traffic. The remaining of the paper is framed in following pattern. In section II, we explain the similarities and differences between IPv4 and IPv6 and review the security issues in each of them. In section III, we try to elaborate more about anomaly detection. In Section IV, we review and understand the relate works. In section V, we describe the proposed model of intrusion detection. Finally the section VI, outline our analysis and evaluate the results and conclude in section VII.

II. IPv4 AND IPv6

A. Comparison between IPv4 and IPv6

IPv6 also known as IPng is a new version of Internet Protocol for general use across Internet world. It is designed to overcome the most prominent limitations of IPv4 including the exhausting IP address space and lack of security. Besides IPv4 and IPv6 being similar in much of their basic model, there are also many differences. Table I summarizes the major differences between IPv6 and IPv4 [5].

Table 1 Comparison between IPv4 and IPv6

Description	IPv4	IPv6
Address	32 bit long(4 byte); 2^{32} (4,294,967,296) possible addresses	128 bit long(16 byte); 2^{128} (Approx. 3.4×10^{38}) possible addresses
IPSec	Optional, External	Mandatory, built-in
Fragmentation	Done by both sender and forwarding routers	Done only by sender; Routers doesn't support packet fragmenting
Checksum	Header contains Checksum field	Header doesn't contain checksum
Address resolution	Address Resolution Protocol (ARP) is used to resolve IPv4 addresses to MAC addresses	Neighbour Discovery Protocol (NDP) has replaced ARP
Broadcast messages	Available	Not available, can be done by using multicast address (FF02::1)
Address Configuration	Manual or using DHCP	Auto configuration functionality is available

B. Security Issues in IPv4 and IPv6 Networks

Even though IPv6 has improved in terms of security, there are certain areas where security issues may still prevail. Also there are some security threats which are not basically altered by emergence of IPv6 Protocol [6]. Some of the typical threats present in both IPv4 and IPv6 networks are:-

- *Flooding Attacks:* The target system is flooded with enormous amounts of illegitimate requests greater than it is able to process rendering it unreachable by legitimate user. It also called Denial of Service (DOS). In IPv4, this can be done as broadcast flooding attack or as Smurf attack [7]. While in IPv6, even though it lacks broadcast addresses but Smurf-type attacks are still possible for certain multicast addresses [8].

- *Malicious Code Distribution:* The malicious codes like viruses and worms are distributed and used to infect the target devices in the network. The small address space of IPv4 can easily be used to implicate this [7]. IPv6 have built-in authentication and encryption which make it difficult to determine whether the malicious code is transferred [4].
- *Reconnaissance attacks:* The attacker gathers all the essential information about the target network to perform further attacks. The information gathering techniques for both IPv4 and IPv6 are the same [6].
- *Man-in-the-middle attacks:* It is a kind of eavesdropping attack in which the attacker resides in between the two communicating users to intercepts the messages. In IPv4, this attack can be performed in various ways, such as ARP cache poisoning and DHCP spoofing. These attacks also find their ways in IPv6 network through spoofed ICMPv6 neighbour advertisement, spoofed ICMPv6 router advertisement and rouge DHCPv6 server [9].
- *Fragmentation Attacks:* This type of attacks use the fragmentation functionality to evade through the security monitoring device as since the fragmentation process is performed by source and destination device. One example for this attack is ping of death. While receiving each fragment, the size of the reassembled packet increases beyond the packet size limit of IPv4 which might crash the target system [7].

III. INTRUSION DETECTION SYSTEM

Intrusion Detection is a technique similar in manner to other security measures like firewalls, anti-malware solutions and access control mechanism schemes, which is aim to address Information systems security challenge and to minimize the threats. An IDS assists the three most significant security functions: it monitors, detects and responds to anomaly or unnatural behaviours in the activity patterns of stream data [10].

For research community IDS has always been a substantial field of interest, as it is impractical to set up a system without any vulnerability [11]. One challenging task in intrusion detection is to discover the hidden attacks from an enormous amount of day-to-day communication activities [13]. A good Intrusion detection system can be only judged by its capability of discriminating between normal and anomalous user behaviours [12].

Anderson [14] defined an intrusive threat as a potential likelihood of an attempt to (i) Access sensitive information (ii) Manipulate this information, or (iii) Even make a system unreliable or unusable. Also, Denning[15] describes that IDS have the function of analyzing the network traffic information and then applying detection algorithms to determine whether these are indicators of an attack or constitute a genuine use of the system.

While referring to intrusion detection, two main categories of detection are commonly emphasised [16]:-

- *Misuse detection:* It is a signature based detection of known attacks and known system vulnerabilities.
- *Anomaly detection:* At start it defines a profile for ‘‘normal behaviour’’, and then scrutinizing it with current behaviour data stream to determine likely deviation.

Misuse based detection systems are very efficient but are limited to the knowledge of the well-known signatures and would not work for new and unfamiliar attacks. Whereas the anomaly detection has capability of detecting attacks which were previously not encountered by analysis of their behaviour. This could also include more number of false positive. In this paper, we will focus more upon anomaly detection for reducing the false positive to a minimum and acceptable rate.

A. General Anomaly Detection Architecture

Although there are several anomaly detection mechanisms but generally all of them consists of the following stages or modules [17]:

- *Parameterization:* In this stage, the parameters (like attributes of network packet header and type of anomaly detection approach) are chosen and represented in a pre-established form.
- *Training stage:* The normal conduct of the system is profiled and a model is constructed, depending on the type of detection approach considered.
- *Detection stage:* As the model becomes available from the above, it is examined with the observed traffic data streams. If some deviations are discovered to exceed a given threshold, the alarm will be triggered.

B. Types of Anomaly Detection Mechanisms

On the basis of type of processing for “behaviour analysis”, anomaly detection mechanisms can be categorised into three important classes: knowledge based, statistical based, and machine learning based [18]. The class of knowledge based techniques analyse the default behaviour from usable target system data (protocol specifications, network traffic, etc.). In the statistical based class techniques, network traffic is captured and a behaviour profile (based on rate of traffic, packets number, etc.) of a system is created based on random view point. At last, machine learning mechanisms class are based on the establishment of a model that allows the behaviour to be categorized [19].

Most of the scientific studies have shown that machine learning mechanisms have given promising results than other two techniques [19]. In this paper, four machine learning algorithms, namely Naive Bayes, Decision Tree, PART and J48, have been implemented to analyse the effectiveness of the suggestive model.

IV. RELATED WORK

There have been a number of research studies related to anomaly detection [25]-[28]. Such as, Zhao *et al.* [25] used entropy-based statistical approach to determine entropy for various variables in the Management Information Base. The only limitation in entropy based approaches is that two extremely different variables can display same entropy, resulting miscalculation in the statistics.

Phyu *et al.* [26] proposed an anomaly detection system for DDoS detection based on K Nearest Neighbour algorithm in order to develop a classification algorithm for attack detection. This system could not detect attack patterns in large quantities of legitimate traffic of service request and often falsely detect them as normal due to lack of detection instructions in proposed algorithm.

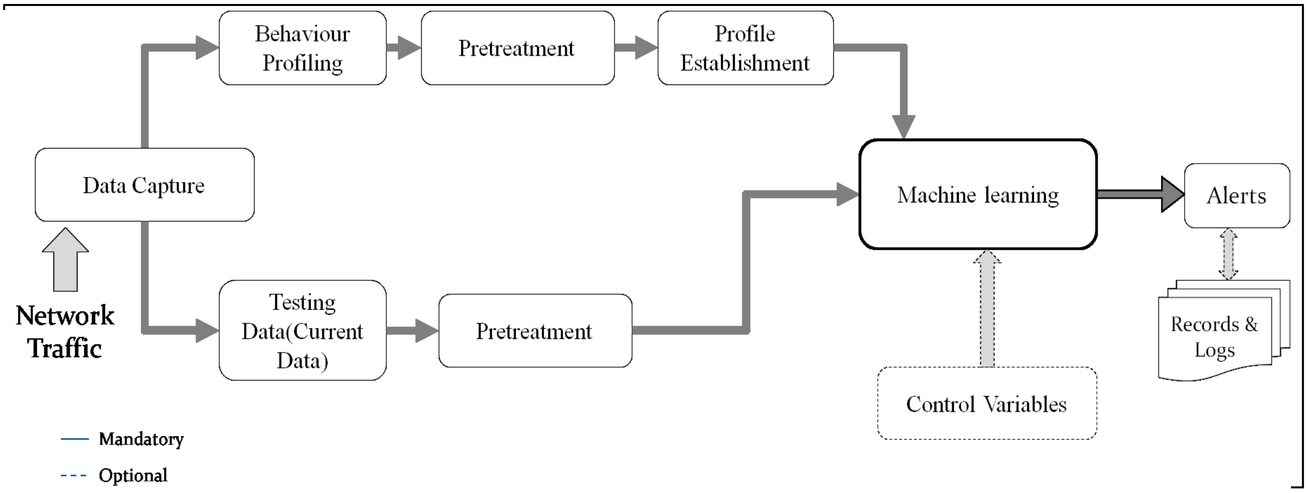

Figure 1 Proposed Anomaly Detection Model

Wei-Chao *et al.* [27] proposed a novel feature representation, the (CANN) cluster center and nearest neighbour approach for efficient intrusion detection by combining cluster centers and nearest neighbours. This approach is comparatively better than k-NN and SVM classifiers and display higher accuracy with low false alarm rate. This approach could not effectively detect User to root (U2L) and Remote to Local (R2L) attacks.

More closer to our approach, Sudhir *et al.* [28] used feature subset selection techniques to select features to improve accuracy and detection rate of attacks. This had a limitation of detecting only U2R attacks most efficiently while DOS and R2L attacks were not detected with same accuracy. Also this approach was found to be efficient only for IPv4 networks not for IPv6 networks.

In our work, we have approached anomaly detection in two parts. In the first part, the features for anomaly detection are determined. In second part, the machine learning algorithms are used to analyse data for anomalies. One of the most important difference in our approach is that our method is able to detect anomalies in both IPv4 and IPv6 networks while most of the previous works focus on IPv4 networks.

V. PROPOSED ANOMALY DETECTION IDS MODEL

The proposed anomaly detection model as shown in figure 1 has several components, the following subsections describes each of them briefly:

A. Captured Data

For any intrusion detection system, data capturing is first and most important step for analysing the anomalies within a system. Especially for testing purpose, we took KDD'99 network traffic dataset to simulate real-time data along with certain attack behaviour. The KDD Cup 1999 is a revised version of DARPA 1999 dataset prepared by Stolfo *et al.* [21]. KDD training dataset contains approximately 5 million single connection instances where each instance comprises of 41 features or attributes and classified either as normal or an attack [20].

B. Behaviour Profiling and Pre-Treatment

Behaviour Profiling and pre-treatment consist of following two phases:

a) Feature selection

Every instance in captured data has certain features like duration of the connection, size of the payload, error rate, protocol-type (TCP, UDP, etc.) and service types (http, telnet, etc.).

As mentioned earlier KDD'99 dataset has 41 features. These features are categorised in 3 groups [20]:

- *Basic features:* these are the most fundamental features for any TCP or IP connection.
- *Traffic features:* these characteristics are calculated with respect to a time interval window and are classified in 2 groups:
  - *"Same host" features:* These examine the instances in the last two seconds which correspond to the same destination host as the current instance
  - *"Same service" features:* These examine the instances in the last two seconds which correspond to the same service as the current instance.
- *Content features:* These characteristic features correspond to understanding the contents of an instance as suggested by domain knowledge.

As X. Chen and J. Chen [22] suggested that along with the basic features like *flag*, *service*, *protocol_type*, *wrong_fragment, src_bytes* and *logged_in*, the time relevant features like *count*, *same_srv_rate*, *srv_count, diff_srv_rate* and *srv_diff_host_rate* are the most relevant features for IPv4 as well as IPv6 traffic. In this paper, we modified the training and testing data according to these 11 features (Table 2), analysed with different machine learning algorithms and compared them by taking the training and testing data with all the 41 features.

Table 2 Common Features and their Description

Feature Name	Description
protocol_type	Transport layer protocol type
service	Application layer network service requested on the destination
src_bytes	Size of data from source to destination
flag	status of the connection (normal or error)
land	1 if connection is from source or destination; 0 otherwise
logged_in	1 logged in session; 0 otherwise
count	number of connections to the same host in the past 2 seconds
same_srv_rate	Percentage of connections using same service
diff_srv_rate	Percentage of connections using different services
srv_count	number of connection to the same service in the past 2 seconds
srv_diff_host_rate	Percentage of connections to different hosts

b) Profile establishment:

In this phase, the training and testing data are modified according to selected features. Here these datasets are modified corresponding to the aforementioned 11 features.

C. Control Variables

Control variables are the inputs to the Machine-learning algorithm for controlling the processing of the anomaly detection. One such variable can be the rules to define the type of attack against which the anomaly detection is being done. The KDD'99 dataset is incorporated with several attacks which are classified into 4 categories:-

- *Denial of service (DOS) attack:* In this type of attack attacker utilize some computing, floods the target with large number of illegitimate requests, much more than it is able to process rendering it unreachable by legitimate user.
- *User to Root (U2R) attack:* In this attack, the attacker has accessibility to a legitimate user account in the system and tries to escalate his privilege to the root user level.
- *Remote to Local Attack (R2L):* In this attack, the attacker remotely finds vulnerable points in the system to gain access as a local user.
- Probe Attack: In this type of attack, intruder tries to collect all the essential information about the target area network to perform further attacks.

It has been observed in many cases that denial of service attacks are most frequent and most severe attacks on any target system. Back, land, neptune, pod, smurf, teardrop are some types of DOS attack present in KDD'99 as discussed below [24]:

- *Back:* In this DOS attack, the attacker makes a URL requests containing many front slashes. Consequently, the server will slow down while trying to process these requests and becomes unable to process other requests.
- *Land:* In this attack, a spoofed SYN packet is sent by an attacker, while keeping the address of source and destination same.
- *Neptune:* In this attack, the attacker generates a SYN Flood against the target system by sending session establishment packets through a forged source address.
- *Pod:* In this attack, attacker deliberately sends an IP packet larger than the allowed 65,536 bytes.
- *Smurf:* In this attack, the network is disabled by an enormous number of replies to spoofed ping requests that have been given the return address of the victim network or host.
- *Teardrop:* In this attack, the mangled IP fragments with overlapping, over-sized payloads are sent to the target system.

This research paper is based on analysis of these DOS type of attacks in a system.

D. Machine Learning Algorithm

There are several machine learning algorithm which exist for mining of the traffic data for anomaly detection namely, Bayesian networks, neural networks, fuzzy logic, clustering, etc. This paper uses Naive Bayes, Decision table, J48, PART algorithms to analyse and detect anomalies in the given dataset.

- *Naive Bayes Algorithm*: It is a classification technique based on Bayesian proposition with assumption (Naive) that each pair of features is independent. Mathematically, it is assumed that the effect of the value of a feature 'x' on a given class 'y' is independent of the other feature values [23]. Thus formulating the probability of feature over a given class as,

$$P(y|x) = \frac{P(y)P(x|y)}{P(x)}$$

  Where, $P(y|x)$→posterior likelihood of class over given feature.

  $P(y)$ → class prior likelihood

  $P(x|y)$→likelihood of feature for the given class.

  P(x) → feature prior likehood.

- *Decision Table Algorithm:* In this algorithm, all the possible combinations of conditions for a decision are represented in a tabular form. Based on the same set of features, it uses the nearest neighbour method to classify for each instance in the decision table [23].

- *J48 Algorithm:* It is an extension of ID3 (Iterative Dichotomiser 3) algorithm. It creates a decision tree and then progressively generalise it to generate rules to identify data [23].

- *PART Algorithm:* It generates rules from a partial decision tree. It uses C4.5's method to create the tree with user defined parameters [23].

E. Performance Metrics

The metrics and formulae used for evaluating the performance of the machine learning algorithms in finding the anomalies are as under:

$$\text{Precision}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}}$$

$$\text{Recall or True positive rate(TPR)}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}$$

$$\text{False positive rate(FPR)}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}$$

$$\text{F-measure}=\frac{2*\text{Precision}*\text{Recall}}{\text{Precision}+\text{Recall}}$$

$$\text{Overall Accuracy}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{FP}+\mathrm{TN}+\mathrm{FN}}$$

Where, TP =True positive, TN=True negative,
FN= False negative, FP= False positive

VI. RESULTS and ANALYSIS

After implementing the machine learning algorithms over our proposed model, the observed outcome results are shown in Table 3.

From our experiments, we compared the performance using all 41 existing features on the KDD dataset (Step A: Data capture) and 11 selected features (Step B: Behaviour profiling) for DOS attacks.

The experiments have also proved that algorithms (Step D: Machine learning) such as Decision Table, J48 and PART respond better in detecting anomalies (Step C: Control Variables) than Bayesian algorithm like Naive Bayes. It was observed that these algorithms are equally effective for U2R, R2L and Probe type of attacks.

Experiments also revealed that detecting anomalies in IPv4 is easier as compare to IPv6 because IPv6 data is encapsulated and encrypted by IPSec and few of the attacks can hidden easily within this encrypted data. One possible solution to this can be decrypting the packets at network IDS level while analysing them. This might raise several performance as well as information leakage issues and is beyond the scope of this paper.

Table 3 Results of using Machine Learning against DOS Attacks

Naive Bayes Algorithm										
DOS attacks	**41 Features**					**11 Features**				
	TPR	**F measure**	**FPR**	**Precision**	**Accuracy**	**TPR**	**F-measure**	**FPR**	**Precision**	**Accuracy**
Back	0.749	0.424	0.007	0.296	78.941	0.903	0.127	0.046	0.069	75.421
land	0.778	0.636	0	0.538		0	0	0	0	
neptune	0.995	0.998	0	1		0.997	0.99	0	1	
pod	0.92	0.008	0.065	0.004		0.931	0.692	0	0.551	
smurf	0.8	0.887	0.005	0.995		0.801	0.887	0.005	0.995	
teardrop	0.75	0.003	0.024	0		0.667	0.002	0.024	0.001	
Decision Table Algorithm										
Back	0.45	0.336	0.005	0.269	94.41	1	0.698	0.003	0.536	97.5617
land	0.556	0.714	0	1		0	0	0	0	
neptune	0.977	0.985	0.002	0.993		0.99	0.997	0.001	0.995	
pod	0.954	0.954	0	0.847		1	0.916	0	0.845	
smurf	0.958	0.971	0.018	0.985		1	0.99	0.27	0.98	
teardrop	0.75	0.02	0.003	0.01		1	0.393	0	0.245	
J48 Algorithm										
Back	1	0.997	0	0.995	97.62	1	1	0	1	97.9021
land	1	1	0	1		0.889	0.941	0	1	
neptune	0.984	0.992	0	0.999		1	1	0	1	
pod	0.977	0.881	0	0.802		1	0.916	0	0.845	
smurf	1	1	0	1		1	1	0	1	
teardrop	1	0.393	0	0.245		1	0.393	0	0.245	
PART Algorithm										
Back	1	0.997	0	0.995	97.5179	1	1	0	1	97.689
land	1	1	0	1		0.889	0.941	0	1	
neptune	0.9	1	0	1		0.999	1	0	1	
pod	0.977	0.909	0	0.85		1	0.916	0	0.845	
smurf	1	1	0	1		1	1	0	1	
teardrop	1	0.393	0	0.245		1	0.393	0	0.245	

VII. CONCLUSION AND FUTURE WORK

In this paper, we looked into four machine learning mechanisms namely, Naive Bayes, Decision table, J48 and PART against the proposed model. We determined that there are 11 features of the dataset which are common to both IPv4 and IPv6 networks. We also observed that reducing the feature will increase accuracy and decrease false positive rate. Experimental results also revealed that some algorithms display better performance as compared to others. Even though the model was tested against an offline dataset and under a small network environment, our next objective is to create a simulated environment especially for IPv6 and enhance our model against the attacks like router advertisement attacks, stateless auto-configuration attacks, etc which are not present for IPv4 networks.

VIII. REFRENCES

[1] Davies, J., *Understanding IPv6,* Microsoft Press, Redmond, WA, 2003.

[2] Popoviciu C.; Levy-Avegnoli, E.; Grossetete, P., *Deploying IPv6 Networks,* Cisco Press, Indianapolis, IN, 2006.

[3] Deering, S.; Hinden, R., *Internet Protocol Version 6 (IPv6) Specification*, RFC 2460, Dec. 1998, http://www.ietf.org/rfc/rfc2460.txt.

[4] Szigeti, S.; Risztics, P., *Will IPv6 bring better security?,* Proceedings 30th Euromicro Conference, 2004, vol., 532- 537, 31 Aug.-3 Sept. 2004.

[5] Amer Nizar Abu Ali, *Comparison study between IPV4 & IPV6,* International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

[6] Zagar, Drago, and Kresimir Grgic. *IPv6 security threats and possible solutions.* Automation Congress, 2006. WAC'06. World. IEEE, 2006

[7] Campbell, P.; Calvert, B.; Boswell, S., *Security+ Guide to Network Security Fundamental,* Thomson, Canada, 2003.

[8] Vives, A.; Palet, J., *IPv6 Distributed Security: Problem Statement,* The 2005 Symposium on Applications and the Internet Workshops, 2005. Saint Workshops 2005, vol., 18- 21, 31-04 Jan. 2005.

[9] Atik Pilihanto, *A Complete Guide on IPv6 Attack and Defense,* GIAC Paper, November, 2011

[10] Marcos M. Campos, Boriana L. Milenova, *Creation and Deployment of Data Mining-Based Intrusion Detection Systems in Oracle Database 10g,* Fourth International Conference on Machine Learning and Applications, 2005.

[11] Anazida Zainal, Mohd Aizaini Maarof and Siti Maryam Shamsudin , *Research Issues in Adaptive Intrusion Detection,* 2nd Postgraduate Annual Research Seminar Faculty of Computer Science & Information Systems, Universiti Teknologi Malaysia, 24 – 25 May, 2006.

[12] Dr. Fengmin Gong, *Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection,* White Paper from McAfee Network Security Technologies Group, 2003

[13] Jian Pei, Upadhyaya, S.J., Farooq, F., Govindaraju, V, *Data mining for intrusion detection: techniques, applications and systems* 20th International Conference on Data Engineering, pp: 877 - 87, 2004.

[14] James P. Anderson, *Computer security threat monitoring and surveillance,* Technical Report 98-17, James P. Anderson Co., Fort Washington, Pennsylvania, USA, April 1980.

[15] Denning, D. E., *An intrusion detection model,* IEEE Transactions on Software Engineering, 1987,13(2), 222–

[16] Debar, H., Dacier, M., & Wespi, A., *Towards a taxonomy of intrusion detection systems,* Computer Networks, 1999, 31(8), 805–822

[17] Este´vez-Tapiador JM, Garcı´a-Teodoro P, Dı´az-Verdejo JE, *Anomaly detection methods in wired networks: a survey and taxonomy,* Computer Networks 2004;27(16):1569–84

[18] Lazarevic A, Kumar V, Srivastava J, *Intrusion detection: a survey, Managing cyber threats: issues, approaches, and challenges,* Springer Verlag; 2005. p. 330

[19] P. Garcı´a-Teodoroa, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez and E. Va´zquez, *Anomaly-based network intrusion detection: Techniques, systems and challenges,* Elsevier, Computers and Security, Vol. 28, pp. 18-28, 2009

[20] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, *A detailed analysis of the KDD CUP 99 data set,* Second IEEE international conference on Computational intelligence for security and defense applications, pp. 53-58, Ottawa, Ontario, Canada, 2009

[21] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, *Cost based modelling for fraud and intrusion detection: Results from the jam project, discex,* vol. 02, p. 1130, 2000

[22] Cohen S, Rokach L., Maimon O, *Decision-tree instance-space decomposition with grouped gain-ratio*, In J. Information Sciences, vol. 177, issue 17, pp. 3592–3612. Elsevier. 2007

[23] *Data Mining- Practical Machine Learning Tools and Techniques* by Ian H.Witten,Eibe Frank, Mark A. Hall

[24] DARPA intrusion detection evaluation, *http://www.ll.mit.edu/IST/ideval/data/data index.html,* Lincoln Laboratory, MIT,1999

[25] Lei Zhao, Fu Wang, *An Efficient Entropy-based Network Anomaly Detection Method Using MIB,* IEEE international conference on Progress in Informatics and Computing, pp. 428 – 432, Shanghai, 2014

[26] Thwe Thwe Oo, Thandar Phyu, *Analysis of DDoS Detection System based on Anomaly Detection System,* International Conference on Advances in Engineering and Technology, Singapore, 2014

[27] Wei-Chao Lin , Shih-Wen Ke , Chih-Fong Tsai, CANN: *An intrusion detection system based on combining cluster centers and nearest neighbours,* Elsevier, Computers and Security, Vol. 78, pp. 13-21, 2015

[28] S. K. Sharma, S. Bahl, *Improving Classification Accuracy of Intrusion Detection System using Feature Subset Selection,* Fifth International Conference on Advanced Computing & Communication Technologies, pp. 431-436,201