Packet Header Intrusion Detection with Binary Logistic Regression Approach in Detecting R2L and U2R attacks

Muhammad Hilmi Kamarudin[1], Carsten Maple[1], Tim Watson[1]
[1]Cyber Security Centre, Warwick Manufacturing University of Warwick, CV4 7AL, Coventry, United Kingdom
m.h.b.kamarudin@warwick.ac.uk, carsten.maple@warwick.ac.uk, t.w@warwick.ac.uk

Hasliza Sofian[2]
[2]Department of Computer Science University of Warwick, CV4 7AL, Coventry, United Kingdom
h.b.sofian@warwick.ac.uk

***Abstract*—With the rapid growth of the Internet, there are an increasing number of computer threats and attacks. The prevalence of zero-day attack activities has given rise to the need to prevent these attack activities from spreading and damaging the computer system. As such, intrusion detection system (IDS) should satisfy complex requirements and must be durable, manageable and reliable. In this paper, we developed an anomaly-based detection model using a statistical method combined with a binary logistic regression approach. The model, Layer based Anomaly Detection (LbAD) is designed to detect remote to user (R2L) and user to root (U2R) attacks by statistically examining the degree of normal field values within three layer (data link, network, transport) of OSI Seven Layer. The results of the new method outperform the leading existing methods.**

Keywords—Anomaly Based Detection System; remote to local; user to root; binary logistic regression;

I. INTRODUCTION

Information security is one of the most important aspects in modern daily life. Many computer users are unaware of the fact that they might be exposed to risks and threats. Along with the continuous growth and high-speed development of the Internet technologies, widely available sensitive information makes the network environment becomes even more complex. Although the Internet brings convenience and real-time service to users, there are issues that can compromise confidentiality, integrity and availability (CIA) [1]. Many servers have been attacked and paralysed, many of them suffering from lost of information. In such cases, the impact can be a huge loss in terms of money, data and business availability. According to the FBI and the US-CERT, most exploits come from software vulnerability. The US-CERT National Vulnerability Database, reveals an average of 13 new vulnerabilities were reported daily in 2013, resulting in 4,794 vulnerabilities in that year alone, approximately 26.6% more than the number of flaws found in 2011.

The main focus of network security is on access control, firewall and information encryption. However, there are common issues related to bugs and deficiencies. For instance, a firewall alone is unable to detect inside intrusion [3], and therefore intrusion detection has become a popular option. An Intrusion Detection System (IDS) is one of the components in the security arsenal "defense in depth" [4], and acts as a compliment to the existing security appliances. Although there is no guarantee on security, when it is integrated with other security measures such as vulnerability assessments, data encryption, user authentication, access control, and firewalls, IDS can greatly enhance the network security. A major interest in defending a computer system is protection from exploits by intruders using zero-day attacks. A zero-day attacks are one that occurs when a hitherto unknown vulnerability is first discovered at the same time as the exploit [5]. An IDS is used to assist security analysts to detect and analyse the zero-day attacks. Since the attack is unknown, traditional signature-based approaches cannot be used. With that notion in mind, anomaly-based detection will be used in this research.

Intrusion Detection System

An IDS can be described as a device or an application that detects malicious activities or policy violations in a network. IDSs are considered not only as a part of surveillances, but also of network security. An IDS analyses captured traffic and triggers an alarm when signs of intrusions are detected, alerting the administrator for further action.

An IDS can be classified as either a host-based IDS (HIDS) or a network-based IDS (NIDS) [6], [7]. The classification is based upon the location of where the IDS is deployed to inspect suspicious traffic. NIDS captures the whole network segment and analyses it to identify signs of hostile traffic. HIDS focuses on a specific host and analyses information such as system calls, logs, and packets. In that manner, HIDS is more appropriate in helping to identify internal attacks compared to NIDS [8].

Detection methods of IDS are divided into two types i.e. signature-based detection systems (known as knowledge-based detection) and anomaly-based detection systems (known as behaviour-based detection) [9]. Signature-based detection systems (SBDS) use pre-define rules that are previously stored in the database to detect attacks of known types. However, SBDSs also have its drawbacks due to it being solely dependent on regular signature updates, and cannot detect an unknown or new attacks [10] and thus such attacks may pass through the system. Anomaly-based detection systems (ABDS) are effective in detecting

978-1-4673-8499-5/15 $31.00 © 2015 IEEE
DOI 10.1109/CyberSec.2015.28

unknown attacks, and are based on behaviour analysis to establish a baseline of normal usage patterns. Anything that deviates widely from normal usage gets flagged as a possible intrusion [11]. This method is capable of detecting unknown attacks. However, anomaly based detection systems do have the drawback of raising more false alarms than signature-based detection systems [12]. A false alarm is an event where normal traffic is flagged as abnormal and an alarm is incorrectly triggered. The main focus in anomaly-based IDS is to design high detection and prediction with an acceptable number of false alarms.

II. Related Work

Packet Header Anomaly Detection (PHAD) has attracted the attention of numerous researchers [9], [13], [14], [15], [16]. In PHADs, packet characteristics and behaviours are used to identify unusual behavior. Normal packet behaviour is used to construct a normal profile, and then subsequent behaviour can be compared to this profile. Packets with characteristics and behaviours that differ significantly from the normal profile are considered to be anomalous packets. PHAD systems consider only packet header information rather than using IP addresses and port numbers [15]. It extracts values of 33 packet header fields that consist of packet information from layer 2 to layer 4 of the OSI 7 layers of the OSI model. PHAD systems calculate the probability of anomaly against each packet header field from the training session. Each field from testing data is compared to the training set data; if there is any dissimilarity detected anomaly score will be given. The total anomaly score of a packet are summed and the packet is classified as anomalous if the total score exceeds a defined threshold. This approach claimed to detect 72 attacks instance out of 201 inside DARPA dataset [15].

Unlike traditional PHAD systems, the Protocol-based Packet Header Anomaly Detection (PbPHAD) is implemented as host-based and network-based IDS [16]. In PbPHAD, the distinct value of normal behavior is used to create a profile that is based on three main protocols ICMP, TCP and UDP. As in traditional PHADs, these systems use statistics calculated from 33 packet header fields to produce the anomaly score. PbPHAD focuses on discovering the degree of incoming anomalous packets, which are individually rated with an anomaly score. Despite the fact that PbPHAD outperforms PHAD and the previously benchmarked DARPA Best Systems [14], the attack detection rate was only 57.83%.

Packet Analysis Anomaly Intrusion Detection (PAID) performs packet analysis in detecting intrusion [13]. Compared to PHAD and PbPHAD, PAID approaches use feature extraction and Bayesian analysis where packet features are transformed from continuous to discrete values before being fed into a Naïve Bayes Classifier. The classifier then categorises packets as benign or malicious. PAID systems focus on detecting DoS attacks and have an accuracy rate of just over 90%. However, the focus on DoS attacks makes PAID unsuitable for discovery of other types of attack.

In this research, the DARPA 1999 Intrusion Detection Data Set [14] has been chosen for evaluation. This data set is publicly available and was prepared by MIT Lincoln Lab. We are conscious of imperfection of DARPA dataset especially on the maturity over 15 years, but these are the most comprehensive and extensive used dataset in this field where we can easily make comparison with other researchers [18], [19], [20], [21], [22], and [23] since it has been accepted as standard benchmark for their IDS model. Lincoln Lab has provided 5 weeks of data that consist of 3 weeks of training data and 2 weeks of testing data in various formats such as tcpdump, NT audit data, and BSM solaris host audit data. For this research, tcpdump format has been chosen since it provides details of TCP/IP packet information for intrusion analysis. For the first and third week of training data, the data is free from any attacks, and this used to define normal traffic, suitable for training of anomaly-based IDS systems; the second week of training data contains labeled attacks. The testing data, consists of two weeks of network based attacks in the midst of normal background data. There are 201 attack instances of 56 different types distributed throughout the data. Of the 201 attack instances, only 176 attack instances are detected by the inside sniffer and it is this that is used by Shamsuddin [16]. For our experimentation we consider the same 176 attack instances.

III. Methodology

Our method is a network-based approach where the normal profile is developed based on the behavior of normal traffic packet headers at layer 2, 3 and 4 of the OSI 7 Layer model. This approach is designed to detect abnormal behavior by identifying the degree of normality packets from the sum of individually rated normal field values. In this experiment we used MySQL as database management system and SPSS statistical software for statistical data analysis.

The principal design concept behind this research was to learn the normal packet header attribute values during the attack free week 3 of data. The normal traffic, consisting of 12,814,738 traffic packets, was used to develop the normal profile. In creating the normal profile, we indexed each attribute as, i= 1,2, …, n, and the model was built based on the ratio of the normal number of distinct field values in the training data, Ri, against the total number of packets associated with each attribute, Ni. The ratio, Pi=Ri/Ni represents the probability of normal score for each attribute field.

$$NormalScore = \sum_{i=1}^{n} \frac{R_i}{N_i}, i = 1,2,3,...,n \quad \text{.....(1)}$$

Weighted Score

We performed group attributes within its own corresponding layer and performed weighted score rules to make each attribute fairly distributed. The weight score rules were based on the total attributes that were associated with the specified layer. For instance, in layer 2, we had 6 attributes and it gave a weighted value of 6/33, which was

equivalent to 18.18% for layer 2. The total weighted sum for layer 2, layer 3 and layer 4 is equal to 100%. The idea behind statistically modeling the score for each layer is to find a correlation of layers in detecting an outlier. Table 1 shows statistical model of Normal Profile. As the R value varies greatly, we used log ratio in our model where the value column Layer 2, Layer 3 and Layer 4 was calculated based on relative percentage ratio of log (R/N).

Table 1: Normal Profile

i	Field Name	R	N	Normal Score	
1	ethersize	1456	12814738	**2.042**	
2	etherdesthi	9	12814738	**3.186**	
3	etherdestlo	12	12814738	**3.121**	**Layer 2**
4	ethersrchi	6	12814738	**3.277**	
5	ethersrclo	9	12814738	**3.186**	
6	etherprotocol	4	12814738	**3.368**	
7	ipheaderlength	1	12715589	**4.1425**	
8	iptos	4	12715589	**3.959**	
9	iplength	1463	12715589	**2.3985**	
10	ipfragid	12489	12715589	**1.393**	
11	ipfragptr	2	12715589	**4.1425**	
12	ipttl	11	12715589	**4.3258**	
13	ipprotocol	3	12715589	**3.959**	**Layer 3**
14	ipchecksum	1	12715589	**4.1425**	
15	ipdest	1934	12715589	**2.3247**	
16	ipsrc	1918	12715589	**2.326**	
17	icmptype	3	7169	**2.057**	
18	icmpcode	3	7169	**2.057**	
19	icmpchecksum	2	7169	**2.164**	
20	tcpsrcport	22293	12715589	**2.0146**	
21	tcpdestport	22293	12715589	**2.0146**	
22	tcpseq	7357319	10617293	**0.1198**	
23	tcpack	6015527	10617293	**0.1856**	
24	tcpheaderlen	3	10617293	**4.9269**	
25	tcpflag	10	10617293	**4.5335**	
26	tcpwindowsize	10705	10617293	**2.2543**	
27	tcpchecksum	2	10617293	**5.059**	**Layer 4**
28	tcpurgptr	2	10617293	**5.059**	
29	tcpoption	3	10617293	**4.9269**	
30	udpsrcport	8051	2091127	**1.8165**	
31	udpdestport	8050	2091127	**1.8165**	
32	udplen	129	2091127	**3.1671**	
33	udpchecksum	2	2091127	**4.52856**	
n	**Total**	**13463719**		**100%**	

It can be seen from Table 1 that the distinct value of source IP (ipsrc=1918) and destination IP (ipdest=1934) fields represent the number of hosts that were simulated from the DARPA 1999 Test Bed. Figure 1 shows the process flow of building the Network Intrusion Detection System Model. The process flow can be divided into 3 stages as follows:

- Stage 1

  In stage 1, dataset training and testing were downloaded from MIT Lincoln Lab website where the data was compressed in tcpdump format [24]. Wireshark was used to read the data in tcpdump format and then running the tshark command inside the terminal to convert the format into (.csv) files, before exporting into My SQL database. As the dataset is huge to analyze, we copied the data into MySQL database, which made the process a lot faster.

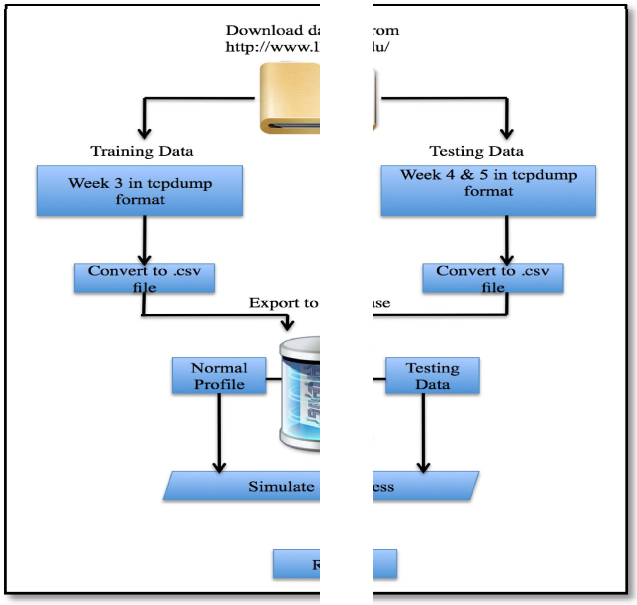

Figure 1: LbAD Process Flow

- Stage 2

  In stage 2, the program executed MySQL, creating the normal profile from week 3 of training data since it contained no attack for that week. Furthermore, distinct values for each 33 packet header fields in TCP/IP packet were inserted into normal profile table, and each fields were assigned with normal score.

- Stage 3

  In stage 3, the 2 weeks of network traffic testing data was simulated, containing both normal and attack traffic. Each one of the 33 packet header fields inside testing data was compared to its corresponding normal profile. A normal score was assigned to the packet, as modeled in Table 1, provided that the value existed inside the normal profile. We then summed up the normal score of each layer and performed binary logistic regression, using SPSS tools, to discover the relationship between each layer in predicting benign or anomalous packets. The prediction results from the binary logistic regression were then matched to the MIT Lincoln Lab data [25], to calculate the detection rate.

IV. Experimental Result

A binary logistic regression was conducted to ascertain the connection between three independent variable *x1* (Layer 2), *x2* (Layer 3), and *x3* (Layer 4) in predicting either attack

or normal traffics. Suppose y, (P=y) is the dependent variable with probability of 0 (attack) and 1 (normal).

$$\ln\left(\frac{p}{1-p}\right) = b_0 + b_1x_1 + b_2x_2 + ... + b_kx_k \quad \text{.....(2)}$$

The equation can be simplified into,

$$p = \frac{e^{b_0+b_1x_1+b_2x_2+...+b_kx_k}}{e^{b_0+b_1x_1+b_2x_2+...+b_kx_k}+1} \quad \text{.....(3)}$$

where p is the probability of attack (0) when p<0.5 and normal (1), when p>0.5.

Table 2: Variables in the equation of week 4 R2L attack

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Weighted_Score_L2	-.139	.005	818.061	1	.000	.870
	Weighted_Score_L3	1.194	.008	24957.453	1	.000	3.301
	Weighted_Score_L4	2.740	.050	3035.664	1	.000	15.484
	Constant	-156.406	2.080	5652.007	1	.000	.000

a. Variable(s) entered on step 1: Weighted_Score_L2, Weighted_Score_L3, Weighted_Score_L4.

Table 3: Variables in the equation of week 5 R2L attack

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	w5Layer2r2l	-.072	.010	51.704	1	.000	.931
	w5Layer3r2l	2.199	.020	11791.944	1	.000	9.017
	w5Layer4r2l	2.690	.053	2584.299	1	.000	14.725
	Constant	-197.219	2.440	6534.157	1	.000	.000

a. Variable(s) entered on step 1: w5Layer2r2l, w5Layer3r2l, w5Layer4r2l.

Table 2 and 3 summarised the descriptive statistics and analysis results in detecting R2L attack. Out of the three predictor variables, only two were statistically significant i.e. Layer 3 and Layer 4. Both Layer 3 and Layer 4 were positively and significantly correlated in detecting outliers. In contrast, Layer 2 (Data Link Layer) statistically showed negative correlation, showing that Layer 2 was not contributing in detecting anomalous traffic. An R2L attack happens when there is an attempt made from outside network that tries to gain inside local access - the Layer 2 information did not contribute much in detecting this type of attacks.

Table 4: Variables in the equation of week 4 U2R attack

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	w4u2rL2	2.758	67.710	.002	1	.968	15.766
	w4u2rL3	.057	.009	41.773	1	.000	1.059
	w4u2rl4	.264	.014	350.355	1	.000	1.302
	Constant	-63.510	1231.086	.003	1	.959	.000

a. Variable(s) entered on step 1: w4u2rL2, w4u2rL3, w4u2rl4.

Table 5: Variables in the equation of week 5 U2R attack

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	w5u2rL2	1.810	5.210	.121	1	.728	6.108
	w5u2rL3	.389	.005	5244.633	1	.000	1.475
	w5u2rL4	6.222	.022	80001.404	1	.000	503.917
	Constant	-310.855	94.737	10.767	1	.001	.000

a. Variable(s) entered on step 1: w5u2rL2, w5u2rL3, w5u2rL4.

On the other hand, from table 4 and 5, it shows that out of three predictor variables, Layer 2 (Data Link Layer) gave the highest contribution in detecting U2R attack as compared to Layer 3 and Layer 4. A U2R attack is triggered when an attempt is made from a local user trying to get root access, this is considered as an internal attack. For this reason, the Layer 2 information was of great significance in detecting U2R attacks. To evaluate the performance of the proposed method, the detected anomalous packets were then compared against the 176 attack instances provided in the MIT Lincoln Lab data [25]. The performance was evaluated based on attack instances detected.

Table 6: Detection Results of R2L attacks on Week 4 and Week 5

Date	Attack Instances inside Testing Week 4 and Week 5 Dataset	Attack Detected by Proposed Model
29/03/1999	6	5
30/03/1999	2	1
31/03/1999	9	9
01/04/1999	7	7
02/04/1999	6	6
03/04/1999	0	0
04/04/1999	0	0
05/04/1999	4	4
06/04/1999	5	3
07/04/1999	5	4
08/04/1999	2	1
09/04/1999	4	2
Total	**50**	**42**
Percentage Detected		**84%**

Table 7: Comparison between 1999 DARPA Best System, PbPHAD and Proposed Model on poorly detected attacks on R2L

Number	Name	Category	Total Instances	Instance Detected by Best System (2000)	Instance Detected by PbPHAD (2008)	Instance Detected by Proposed Model (2015)
1	ncftp	R2L	5	0	4	5
2	netbus	R2L	3	1	2	3
3	netcat	R2L	4	2	0	4
4	snmpget	R2L	4	0	0	3
5	sshtrojan	R2L	3	0	1	0
Total			**19**	**3**	**7**	**15**
Percentage Detected				**15.78%**	**36.84%**	**78.95%**

Table 8: Detection Results of U2R attacks on Week 4 and Week 5

Date	Attack Instances inside Testing Week 4 and Week 5 Dataset	Attack Detected by Proposed Model
29/03/1999	2	2
30/03/1999	3	2
31/03/1999	1	1
01/04/1999	0	0
02/04/1999	2	2
03/04/1999	0	0
04/04/1999	0	0
05/04/1999	2	2
06/04/1999	7	7
07/04/1999	2	2
08/04/1999	5	5
09/04/1999	7	6
Total	**31**	**29**
Percentage Detected		**93.54%**

Table 9: Comparison between 1999 DARPA Best System, PbPHAD and Proposed Model on poorly detected attacks on U2R

Number	Name	Category	Total Instances	Instance Detected by Best System (2000)	Instance Detected by PbPHAD (2008)	Instance Detected by Proposed Model (2015)
1	loadmodule	U2R	3	1	0	3
2	perl	U2R	4	0	3	3
3	sechole	U2R	3	1	1	2
4	xterm	U2R	3	1	1	3
Total			**13**	**3**	**5**	**11**
Percentage Detected				**15.78%**	**38.46%**	**84.61%**

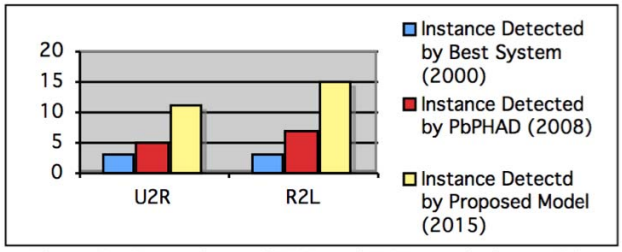

Figure 2: Comparison of U2R and R2L attack detected by three different methods.

Table 10: False Positive rate for both R2L and U2R attack over week 4 and week 5

	R2L	U2R
Week 4	17.1%	19%
Week 5	15.9%	14.5%
Weekly Average	**16.5%**	**16.75%**

V. CONCLUSION

Our LbAD model has shown to be a very promising model to be used in anomaly based detection systems. The experiment was conducted by statistically analysing the degree of normal field values inside three layers of the OSI 7 layer model (data link, network, transport) and a binary logistic algorithm was performed to find a correlation between the layers. The DARPA 1999 dataset has been used to identify two types of attack, R2L, and U2R. Based on the correlation results from SPSS, it showed that layers 3 and 4 contributed significantly to the detection of R2L attacks while Layer 2 and 4 contributed significantly to the detection of U2R attacks. Thus we can design our next model by only taking into account the most significant contributing layer or layers, so that the processing time will be shorter. The experimental results shows that our approach resulted on high detection rates on both type of attack with 84% on R2L and 93.5% on U2R. Our analysis showed that our approach managed to detect 15 out of 19 R2L attacks, and 11 out of 13 U2R attacks and compared favourably to the detection rate of current algorithms. In this respect, our approach indicated an improvement of 42.11% and 46.15% over PbPHAD, for R2L and U2R respectively [16]. However, false positive rate for both R2L and U2R attack was still high with weekly average of 16.5% for R2L and 16.75% for U2R.

VI. FUTURE WORK

By implementing statistical analysis alone, it has been found that it was possible to produce higher detection rate, but in contrast it also came with a high percentage of false positive rates. Thus, future work will continue to working on discovering data mining algorithm techniques [26] that can help to reduce the number of false positive into acceptable rate when combined with statistical analysis.

REFERENCES

[1] S.V. Thakare, D.V. Gore, "Comparative Study of CIA and Revised CIA Algorithm", Fourth International Conference on Communication System and Network Technology, 2014.

[2] C. Florian, Report: Most vulnerable operation systems and application in 2013, February 3, 2014.

[3] A.D. Wankhade and P.N. Chatur "Comparison of Firewall and Intrusion Detection System" International Journal of Computer Science and Information Technologies (IJCSIT), 2014, 674-678

[4] S. Northcutt, J.M. Butler, and G.A. Board, Can you build a Defense in Depth architecture without an architect? May 13th, 2008(Version 1.1).

[5] E. Levy, "Approaching zero [attack trends]", IEEE Security & Privacy, July-August 2004.

[6] H.J. Liao, R. Lin, C.H. Lin "Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 2013.

[7] Z.Muda, W.Yassin, "A K-Means and Naive Bayes learning approach for better intrusion detection" IEEE Information Technology, 2011.

[8] K. L. I. Iii, "Anomaly Detection for HTTP Intrusion Detection: Algorithm Comparisons and the Effect of Generalization on Accuracy," no. May, p. 196, 2007.

[9] C.M. Chen, Y.L. Chen, H.C. Lin, "An efficient network intrusion detection" Computer Communications, 2010.

[10] P. Louvieris, N. Clewley, X. Liu, "Effects-based feature identification for network intrusion detection", Journal Neurocomputing, 2013.

[11] K. Leung, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters", Computer Science Conferences in Research and Practice in Information Technology, Vol. 38, 2005.

[12] H. Om, A. Kundu A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System, 1st International Conference on Recent Advances in Information Technology (RAIT), 2012.

[13] K.C. Lee, J. Chang, M.S. Chen, "PAID: Packete Analysis for Anomaly Intrusion Detection", Advances in Knowledge Discovery and Data Mining, 2008.

[14] R.P. Lippmann, J.W. Haines, D.J. Fried, J. Korba, and K. Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation. MIT Lincoln Lab Technical Report", 2000.

[15] M.V. Mahoney and P.K. Chan, " PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic." Florida Technology, Tech. Rep. CS-2001- 4, April 2001.

[16] S.B. Shamsuddin, and M. E. Woodward, "Modeling Protocol Based Packet Header Anomaly Detector for Network and Host Intrusion Detection Systems". Proceedings of the 6th International Conference on Cryptology and Network Security (CANS), Singapore, 2007.

[17] J.M. Esteves, G.T Pedro, J.E. Verdejo, "Measuring normality in HTTP traffic for anomaly-based intrusion detection", Computer Network, 2004.

[18] H. S-Jun, C. S-Bae, "Evolutionary Neural Networks for Anomaly Detection Based on the Behavior of a Program", IEEE Transaction on System, and Cybernetics, VOL. 36, NO. 3, JUNE 2006.

[19] X. Jinghu, L. Aiping, Z. Hui, Y. Hong, "A Multi-Step Attack Pattern Discovery Method Based on Graph Mining", 2nd International Conference on Computer Science and Network Technology, 2012.

[20] M. Salagean, "Anomaly Detection of Network Traffic based on Analytical Discrete Wavelet Transform", 8th International Conference on Communications (COMM), 2010.

[21] X. D-Xue, Y. S-Hong, L. C-Gui, "Intrusion Detection System based on Principal Component Analysis and Grey Neural Networks", Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[22] W. Xiong, N. Xiong, " Nework Traffic Anomaly Detection based on Catastrophe Theory", IEEE Globecom Workshop on Advances in Communications and Networks, 2010.

[23] W. Yassin, N. I. Udzir, A. Abdullah, and M. T. Abdullah, "Packet Header Anomaly Detection Using Statistical Analysis Warusia," *Springer*, p. 761, 2013

[24] MIT Lincoln Lab Intrusion Detection Dataset DARPA 1999, http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/1999data.html.

[25] MIT Lincoln Lab Intrusion Detection Attacks Database http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/docs/attackDB.html.

[26] Machine Learning "WEKA". Available from: http://www.cs.waikato.ac.nz/ml/weka