International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Concept-Drift Based Identification of Suspicious Activity at Specific IP Addresses using Machine Learning

P V N Rajeswari, M. Shashi

Abstract – Network Intrusion detection systems(IDS), especially those that monitor Denial of Service(DoS) attack, aim at monitoring the network traffic continuously in order to identify suspicious activity possibly initiated at one or more nodes at specific IP addresses. Traditional anomaly detection based IDS methods rely on preset bounds on the magnitude of network traffic based on statistical measures and hence are not programmable based on the changes in the network traffic dynamics. The authors proposed a methodology for monitoring the changes in the network traffic received from individual source nodes based on concept drift in order to identify suspicious activity at specific nodes. The framework applies machine learning techniques to capture the normal traffic patterns of various source nodes and accordingly defines lower and upper bounds dynamically for each node. Based on the temporal analysis in successive time windows, it is able to discriminate an abrupt change from a gradual change in the magnitude of traffic received in a time window from a node to identify suspicious activity at the corresponding IP address. The effectiveness of the methodology is tested on real world data.

Keywords: Network anomaly detection, Concept drift measure, Parametric learning and Packet sniffer.

I. INTRODUCTION

Machine learning enables computers to improve their performance of doing a task through experience represented in the form of data records. Often statistical measures and models are used to extract the general patterns from the large collection of accumulated data records to capture the patterns of normality. Identification of suspicious activity in real time calls for anomaly detection methods that compare every activity with the patterns representing normality to check for the compliance. Any deviation from the normality implies either an anomaly or a changing trend. However, in domains with dynamically changing trends, in order to capture the changing trends, machine learning algorithms need to process data streams of records rather than accumulated collection of data records.

Manuscript published on 30 September 2019
* Correspondence Author
PVN Rajeswari*, Assoc. Professor, Dept. of Computer Science and Engineering, Visvodaya Engineering College, Kavali, AP, India.
Email: rajivrphd@gmail.com.
Dr. M. Shashi, Professor, Dept. of Computer Science and System Engineering., Andhra University, Visakhapatnam, AP, India. Email: smogalla2000@yahoo.com

Stream of records are processed in the order of their arrival to check for deviations from the extracted patterns which may possibly change with time representing time-variant trend that leads to identification of new patterns or otherwise anomalies. In this paper, the changing trends are identified based on concept drift with time, while differentiating them from anomalies specifically for anomaly based network intrusion detection systems.

A. Streaming Based Network Anomaly Detection

Internet is accepted as a vital and the most essential element of modern life to fulfill the communication and information requirements of people anywhere anytime; people are kept connected alleviating the differences in their geographical location, language and nationality. The other side of the coin of this global connectivity opens door for malicious users to attack the genuine users for gaining undue benefits or for destruction. Computers connected to other systems are prone to a variety of attacks which are termed as cyber-attacks. Competent Intrusion Detection System (IDS) is required for protection against from such attacks, threats and vulnerabilities, etc. Based on the scope of their activity, Intrusion Detection Systems are categorized as Host based and Network based. The Host based IDS is used to detect attacks /intrusions into individual computer systems whereas Network based IDS is used to trace anomalies in complex and large networks.

Broadly there are four categories of cyber-attacks namely Probe, User to root, Denial of service and Remote to super user. Denial of Service attack when initiated from multiple systems in a distributed environment referred to as Distributed Denial of Service (DDoS) attack has become more popular in the recent past and is considered as the most popular and brutal attack type in real-time networks.

B. Distributed Denial of Service Attack(DDoS)

The DDoS attacks mainly focus on the internet or cyber resources provided by the network service providers and its purpose is to disrupt normal operation of the server. The DDoS attacker, through multiple channels, overwhelms the target system by sending a constant flow of fraudulent requests causing severe disruption / delay in providing services to the legitimate users. An example for DDoS attack is BOTNET which is an army of hundreds or thousands of infected computers scattered all over the world to do a DDoS attack.

The main problems identified in the existing attack detection methods for dealing with real time systems:

1. Signature based attack detection is not effective since the network traffic dynamics change from time to time.
2. The algorithms such as D-FACE etc., are unable to predict DDoS attack if the input stream possess more number of features.
3. Traditional anomaly based machine learning models have high false positive rate along with high mean-squared error rate while handling real time traffic flow.

Since, the network traffic under DDoS attack manifests different or abruptly changed statistical features from IP addresses participating in the attack, long-term statistical models are found to be effective for identification of Distributed Denial of Service attacks. The authors proposed a strategy to monitor the real time network traffic dynamics from individual IP addresses based on 'concept drift' and accordingly change the thresholds if the change is gradual or otherwise suspect the stream of traffic from that IP address.

In this research work, DDOS attack detection is performed in two phases. In the first phase, packet level feature-wise threshold computation and filtering are performed for separating the suspicious packets from the network traffic data, while in the second phase, more intense machine learning approach is applied for focused analysis of the stream of traffic packets received from suspicious IP addresses to identify DDoS attacks with high attack detection rate and low false positive rate. The paper presents the details of the methodology for implementing the first phase of the framework. It analyses the amount of traffic received from individual IP addresses in fixed time windows to set lower and upper bounds on the traffic received from each IP address and also to update the thresholds dynamically. If the amount of traffic received from an IP address exceeds the specific threshold levels at any moment of time, then an alarm is set to closely monitor the traffic received from that suspected IP address.

In this research work, *History based filtering*[4] mechanism is implemented which uses the history of the normal traffic to filter the malicious traffic. The IP address specific recent history is captured in terms of thresholds which were set dynamically within the time windows and the latest thresholds are maintained in a database of IP addresses. This database includes only those IP addresses which are found to be legitimate for receiving communication. Therefore, when a bandwidth attack is targeted to this system, the system only allows those IP addresses found in the database and discarded all other IP addresses[10].

II. LITERATURE STUDY

In this section, some of the recent literature related to the statistical anomaly detection methods and machine learning models for network attacks detection are discussed.

2.1 Recent Anomaly Detection Techniques

J. J. Flores et.al, [3] developed an evolutionary programming technique in order to detect network anomalies. They have considered continuous Hidden Markov models for anomaly detection. They proposed an anomaly based technique for monitoring the bandwidth consumption of the sub-network. The normal behaviour scheme completely depends upon the bandwidth consumption of the sub-network. The most common variables of Hidden Markov models are bandwidth consumption and the total amount of time required for all network activities. Both the univariate and bivariate observation sequences are included during the evaluation phase and these are essential for identification of anomalous behaviour.

The *Sahoo et al.,* [5] proposed a new information distance (ID) as a metric to detect the network attack in networks. ID metric is used to find the deviation in the traffic distribution during the data communication. This technique is based on controlled parameters and is applicable to small datasets. It needs to be extended with a novel measure for detecting DDoS attacks and try to set the threshold more dynamic way in a real traffic scenario such that the detection can be done as early as possible.

Behal et al., [6] proposed a hybrid D-FACE attack detection model to prevent DDOS attack on networks data. This model is not able to detect DDOS if the number of traffic features is large. *Hoque et al.,* [7] proposed a novel correlation based DDOS attack detection in real time networks. This model select subset of small set of traffic features for DDoS detection. *T. Andrysia., et.al*,[12]reviewed and compared various network anomaly detection systems using the long-term statistical models [11]. In this work, they proposed an advanced network anomaly detection system based on long memory statistical models. They used three different statistical techniques, those are ARFIMA, A-FIGARCH and MIDAS.

2.2 Concept drift for Streaming Data

Monitoring network traffic online calls for the ability to identify changing trends. Processing data streams online to extract patterns and identifying the changes and countering them is an interesting research area in the current era of Machine Learning. This is an intrinsic problem of online learning, popularly known as Concept Drift[1]. Online and incremental learning algorithms such as DDM, EDDM, DWM, ECDD, EMWA, EDIST, ADWIN[2] are able to process data streams and detect the changes in context. In reality, changes in target concepts are often caused by changes in the hidden context.

In supervised incremental learning [13], a well-extended approach continuously monitors a performance measure such as accuracy, or speed etc., of the learning model to handle Concept Drift. Examples of real-life concept drift include junk mail recognition, monitoring systems, network intrusion detection, and automatic control systems. It is very common to enforce restrictions on these online change detectors [9]. The computational complexity required to process each performance value must be constant and the methods should be single-pass, where each record is processed only once. In this work, in order to record the online streaming data, a buffer is maintained with *time window*. Time windows have been used to process the input examples associating a time stamp that defines its age.

III. PROPOSED METHODOLOGY

The architecture of the proposed framework for anomaly based attack detection is shown in figure 1. It starts with packet capturing module wherein the details of stream of packets received from specific IP addresses constituting the network traffic is collected in real-time.

An algorithm for packet capturing is implemented to collect each packet and its relevant fields from each of the connected systems using the network interface card. The second module of the framework namely 'identification of suspicious IP addresses', analyses stream of packets in successive time windows in the recent past to discover (and maintain a database of) lower and upper bounds on the number of packets received from each IP address during a time window to define normal activity patterns. A novel metric for suspicious activity at specific IP addresses is proposed based on concept drift[8]. Once the suspected IP addresses are found the stream of packets received from those sources will be more intensely analyzed to detect the attack packets among them. The details of the third phase are beyond the scope of this paper.

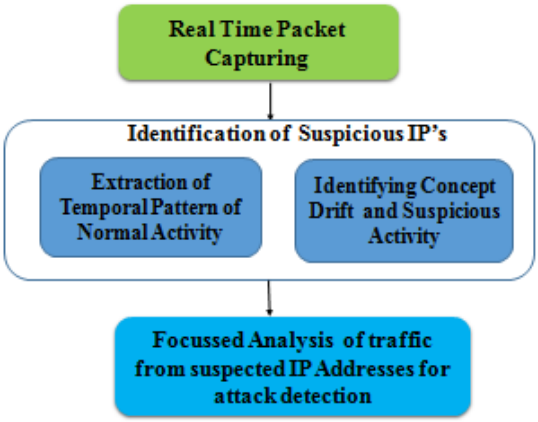

Figure 1: Proposed Framework for Attack Detection

In the packet capturing module, network packets are captured with various fields such as IP address, source IP, destination IP, source bytes, destination bytes, protocol type, timestamp etc. Algorithm1 implements packet capturing module of the frame work. A packet sniffer program is used on the real-time connected network and packets are captured using the network interface card and the windows packet capture drivers.

Algorithm 1: Packet Sniffer and Filter

Input: LAN network, Network Interfaces, Training network dataset NIDData[].

Output: Pre-processed Packets PP[].

1. Connect LAN network;
2. Start Monitoring Client System;
3. Capture all interfaces to the client system.
4. Network Interfaces:
   NI[]=getLANInterfaces[LAN];
5. NPFields[]=Null; //Network packets
6. for each interface NI[i]
7. do
   if(NI[i]==NULL)
8. then
9. continue;
10. else
11. NPData[]=getNetworkPackets(NI[i]);
12. end if
13. end for
   NProtocols[]=NULL;
14. for each packet in NPData[]
   do
15. if(NPData[i]!=NULL)
16. NPFields[]=ExtractField(NPData[i]);
17. end if
   return

3.1Extraction of Dynamic Patterns with Concept Drift

The second module of the framework, namely Identification of Suspicious IP addresses involves temporal analysis of the traffic packets captured in the previous module in order to extract the changing dynamics at different IP addresses. The packets received in a fixed length time window are partitioned based on their source IP address and the counts are monitored. The number of packets received from each IP address, i, in a time window t, is denoted by $f_i(t)$.

The pattern of normal activity at i^{th} IP address is modeled based on Guassian distribution with mean, μ_i and standard deviation, σ_i parameters. The gradual change in the activity at an IP address is monitored by the ***concept drift parameter*** $\Phi_i(t)$, which is the log normalized parameter used to capture the change in the network traffic from i^{th} IP address in time t. The first component of it indicates the proportion of traffic received from i^{th} IP address while the second component 'λ' captures the change in the frequency of packets in successive windows. It is estimated using the formula given below:

$$\Phi_i(t) = \frac{\ln(f_i(t))}{\sum_{j=1}^{N} \ln(f_j(t))} + \lambda \quad \text{for all i} - \text{Eq. (1)}$$

where

$$\lambda = \frac{\ln(f_i(t))}{\ln(f_i(t-1))}, \text{if } \ln(f_i, t) < \ln(f_i, t-1);$$

$$= \frac{\ln(f_i(t-1))}{\ln(f_i(t))}, \text{otherwise}$$

The pattern of normal activity is defined by the lower and upper bounds[14] on the number of packets received from individual IP addresses in a time window 't' which are calculated using the formulas given below:

lower bound, $B_L(f_i(t))=\mu_i - \Phi_i(t)*\sigma_i$; - Eq.(2)

upper bound, $B_U(f_i(t))=\mu_i + \Phi_i(t)*\sigma_i$; - Eq.(3)

Anomalous activity at specific IP address in the recent past, T, is suspected based on abrupt deviation in the number of traffic packets received from those IP addresses. The following formula defines a metric for differentiating suspicious activity from a gradual change in the trend at i^{th} IP address namely 'C_i'.

$$C_i = \frac{B_{U_i} - B_{L_i}}{\emptyset_i . \sigma_i} \text{ for each IP address } 'i'; - \text{Eq. (4)}$$

where $B_{Li} \rightarrow \min_{t\epsilon T}\{B_L(f_i(t)\}$

$B_{Ui} \rightarrow \max_{t\epsilon T}\{B_U(f_i(t)\}$ and

$\Phi_i = \max_{t\epsilon T}\{\Phi_i(t)\}$

and 'T' denotes the series of time windows in the recent past to be considered for analysis at macro level.

The IP addresses whose C value is higher than a predefined threshold are labeled as suspected IP addresses.

Algorithm 2 is used to implement the second module of the framework to identify suspicious activity at specific IP addresses.

Algorithm 2: Detecting Suspicious IP addresses using Concept Drift

Input: Stream of real-time traffic packets, list of recognized source IP addresses along with mean, μ_i and standard deviation, σ_i of number of packets received in a time window 't'.

Output: List of suspected IP addresses and time window.

1. For each time window 't'
   For each distinct source IP address, i
   Find the number of packets received $f_i(t)$.
2. Estimate the concept drift parameter $\Phi_i(t)$ using Eq.(1).
3. Estimate the lower and upper bounds $B_L(f_i(t))$ and $B_U(f_i(t))$ using Eq.(2) and Eq.(3).
4. For each time window, t, belonging to 'T', the recent past:

For every source IP address, i:

Estimate B_{Li} as the minimum over all $B_L(f_i(t))$.

Estimate B_{Ui} and Φ_i as the maximum over all $B_U(f_i(t))$,

Estimate metric for suspicious activity C_i, using Eq.(4).

5. If C_i is greater than a predefined threshold of C, then suspect the specific IP address.
6. Return the list of suspicious IP addresses with time window.

IV. EXPERIMENTATION AND RESULTS

Experimental results are performed on the real-time network with WIPCAP,JPCAP as network drivers for packet capturing and analysis in java environment and Netbeans IDE tool with 8GB RAM and third party libraries such as JAMA, JUNIT, statistical library and pattern miner. Experimental results prove that proposed anomaly detection model outperforms the traditional statistical models.

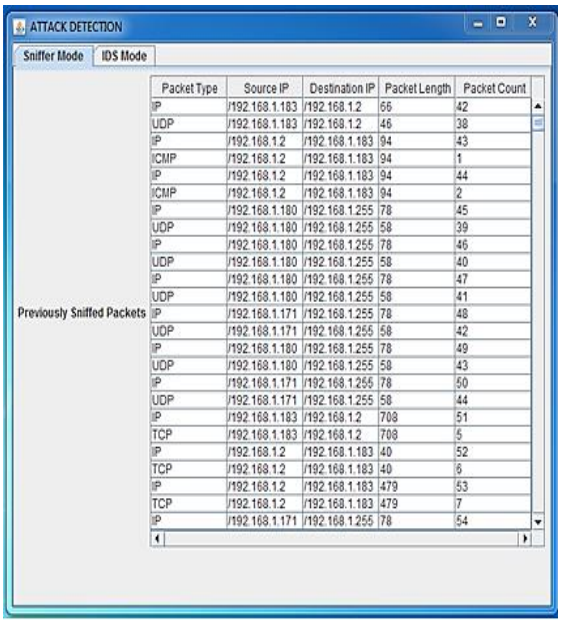

Figure 2:Sniffed packet details from TCP,UDP and IP protocols

Figure 2 gives the IP, TCP, UDP packets information in the real time connected network during attack detection process. Each packet and its relevant fields are visualized along with the flow count. The real time data set thus obtained by the above procedure in time T contains 43,291 packets, out of which 4 to 5% are attack packets. The distribution of packets based on protocol type include 560 ICMP packets, 6892 UDP packets, 15463 IP packets and 20380 TCP packets. These packets are used as training set to define lower and upper bounds and concept drift parameters for each of the recognized IP address for specific protocol type as described in algorithm 2.

The stream of packets are partitioned based on protocol types and the concept drift parameters $\Phi_i(t)$ and lower and upper bounds on the number of packets received in a time window are estimated for each protocol based partition separately. Accordingly the metric for suspicious activity C_i, is estimated and compared against predefined threshold set by experimentation for each protocol type separately.

An appropriate threshold for the value of 'C' is selected for each IP address dynamically, such that the suspicion rate should be four to six times higher than the prevalence of attack packets in the dataset. For this data set, nearly 5% of the packets are attack packets and hence the threshold for 'C' is selected such that suspicious rate is in the range of 20% to 30% representing a proportion of 0.2 to 0.3.

Suspicion rate is defined as the ratio of the total number of suspicious packets to the total number of packets. Table 1 describes the estimation of suspicion rate separately for ICMP, UDP, IP and TCP packets at different threshold for 'C' for the training data set of 43,291 packets described above.

TABLE 1: NO OF SUSPICIOUS ATTACKS W.R.T C VALUES FOR ICMP, UDP, IP AND TCP PACKETS

Packets Type		C-value	No of Suspicious packets	Suspicion rate
Type	**Count**			
ICMP	560	1.9	560	1
UDP	6892		6892	1
IP	15463		15,463	1
TCP	20380		20380	1
ICMP	560	1.95	482	0.86
UDP	6892		3486	0.505
IP	15463		13982	0.904
TCP	20380		10563	0.518
ICMP	560	2	140	0.25
UDP	6892		1844	0.122
IP	15463		3058	0.19
TCP	20380		7875	0.386
ICMP	560	2.05	48	0.085
UDP	6892		281	0.04
IP	15463		2531	0.293
TCP	20380		4225	0.207
ICMP	560	2.1	0	0
UDP	6892		0	0
IP	15463		0	0
TCP	20380		0	0

TABLE 2: SUSPICION RATE W.R.T C VALUES FOR ICMP, UDP, IP AND TCP PACKETS

C Threshold	Suspicion Rate			
	ICMP	**UDP**	**IP**	**TCP**
1.9	**1**	**1**	**1**	**1**
1.95	**0.86**	**0.505**	**0.518**	**0.518**

2	0.25	0.122	0.19	0.386
2.05	0.08	0.04	0.293	0.207
2.1	0	0	0	0

Table 2, summarizes the results of experimentation in terms of suspicion rate obtained by the proposed model with different thresholds for 'C' ranging from 1.9 to 2.1 in steps of 0.05 separately for protocol types namely ICMP, UDP, IP and TCP. Figure 3 presents the graphical representation of the variation of suspicion rate with increased threshold on 'C' values for each of the protocols ICMP, UDP, IP and TCP separately in different colors. It can be observed that the best value of threshold for 'C' is 2.0 for ICMP, UDP and IP protocols while for TCP protocol the threshold value is fixed at 2.05 in order to limit the suspicion rate in the range of 0.2 to 0.3 to encompass all the attack packets into the suspicion set of packets.

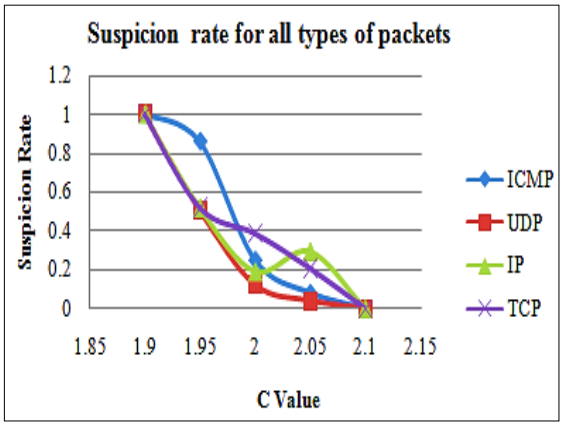

Figure 3: Analysis of the Suspicion rate w.r.t. C value

V. CONCLUSION

Real time attack detection is considered as the main issue of providing secure communication in connected or wireless networks. Since DDoS attacks are often made by a collection of fraudulent or spoofed IP addresses, this research aims to identify suspicious IP addresses at real time. A novel concept drift based identification of network anomaly detection model is designed and implemented on real-time networks. The proposed model analyzes the historical data at specific IP addresses to learn thresholds on concept drift and uses them to monitor online traffic packets received from specific IP addresses to detect suspicious behavior of the attackers. The performance of the proposed model in terms of suspicion rate is tuned by varying the threshold for 'C' values to define / refine the lower and upper bounds on the amount of network traffic received in a time window. The traffic received from the suspected IP addresses will be intensely analyzed by the second phase of the framework for accurate intrusion detection using advanced machine learning techniques. Experimental results showed that the accuracy of the attack detection is improved by setting separate bounds specific to the protocol type in addition to the IP address from which the packet is received.

REFERENCES

1. Bifet, A., de Francisci Morales, G., Read, J., Holmes, G., Pfahringer, B.," Efficient online evaluation of big data stream classifiers", in:Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM. pp. 59–68, 2015.
2. P.V.N. Rajeswari, Dr. M. Shashi, "Online parametric and non parametric drift Detection techniques for streaming data in Machine learning: a review", International Journal of Current Engineering and Scientific Research (IJCESR), Volume 5, Issue 3, March 2018.
3. J. J. Flores, F. Calderon, A. Antolino and J. M. Garcia, "Network anomaly detection by continuous hidden markov models: An evolutionary programming approach", Intelligent Data Analysis 19, pp. 391–412, 2015.
4. Tasnuva Mahjabin , Yang Xiao , Guang Sun and Wangdong Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques", International Journal of Distributed Sensor Networks, Vol. 13(12), 2017.
5. K.S.Sahoo, Deepak Puthal, Mayank Tiwary Joel J.P.C, "An Early Detection of Low Rate DDoS Attack to SDN Based Data Center Networks using Information Distance Metrics", Future Generation Computer Systems(Elsevier), pp. 685-697, Volume 89, December 2018.
6. Sunny Behal, Krishan Kumar, Monika Sachdeva, "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events", Journal of Network and Computer Applications, June 2018.
7. N. Hoque, H. Kashyap, D.K. Bhattacharyya, "Real-time DDoS attack detection using FPGA", Computer Communications(Elsevier), pp. 48-58, 2017.
8. Isvani Frıas-Blanco, Jos_e del Campo-_Avila, Gonzalo Ramos-Jim_enez, Rafael Morales- Bueno, Agust_ın Ortiz-D_ıaz, and Yail_e Caballero-Mota, "Online and Non-Parametric Drift Detection Methods Based on Hoeffding's Bounds", ieee transactions on knowledge and data engineering, vol. 27, issue no. 3, march 2015.
9. G. Ross, D. Tasoulis, and N. Adams: "Non-Parametric Monitoring of Data Streams for Changes in Location and Scale, Technometrics", , pp. 379– 389, Vol. 53, No. 4, 2011.
10. Juliette Dromard, Gilles Roudiere, Philippe Owezarski, "Online and Scalable Unsupervised Network Anomaly Detection Method", IEEE Transactions on Network and Service Management, IEEE, 14 (1), pp.34-47, 2017.
11. Muhammad Fahad Umer, Muhammad Sher, Yaxin Bi, " Flow-based intrusion detection: techniques and challenges", Computers & Security (Elsevier), pp 238-254, Volume 70, September 2017.
12. T. Andrysia., L. Saganowski, M. Choracco and R. Kozikco, "Proposal and comparison of network anomaly detection based on long-memory statistical models, Logic Journal of IGPL Advance Access published August 9, 2016.
13. M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "An Effective Unsupervised Network Anomaly Detection Method", ICACCI'12, Chennai, T. Nadu, India, pp. 533-539, August 3-5, 2012.
14. M. Mazini, B. Shirazi and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms", Journal of King Saud University – Computer and Information Sciences, March 2018.