International Journal of Engineering and Technology sciences (IJETS) 2(6): 533-539, 2014
ISSN 2289-4152

Research Article

Intrusion Detection Based On Degree of Nodes in Network Traffic Graph

Sara Hatami[a,*], Aliakbar Tajari Siahmarzkooh[b]

[a] Mirdamad University of Gorgan, Gorgan, Iran
[b] University of Tabriz, Tabriz, Iran

* Corresponding author. Tel.: +989118005033;
E-mail address: Sara.haatami@gmail.com

A b s t r a c t

Keywords:

Network graph,
Degree of graph,
Attack,
Intrusion detection,
DoS.

Nowadays with development of technology and variety of network services, communication and different needs of users with high speed and simplicity have been possible, but a way for the implementation of different types of destructive and illegal processes has paved. These processes are attacks with aim of reducing network performance or destruction of networks. So far, various types of attacks such as viruses, worms, Trojan horses, denial of service, distributed denial of service, Botnets have been attacked computer networks. In order to recognize and prevention with negative effects of this attacks, intrusion detection systems are designed and implemented. These systems are divided to two general groups; anomaly-based intrusion detection systems and signature-based intrusion detection systems. In Anomaly-based intrusion detection, the input data is compared with normal model or expected behavior of system and significant deviation from normal model is specified as an anomaly. The advantage of this method is that it could potentially detect attacks that have not been seen so far. We will propose a solution that create a graph in which nodes represents hosts and edges represents activity within hosts, computing degree of nodes in graph and compare with normal mode. This Method can be used for automatic detection denial of service attacks.

Accepted:27 December2014

1. Introduction

In recent years, large-scale attacks, including, viruses, worms, Trojan horses, buffer overflow, password, information gathering, social engineering, DoS[1], DDoS[2], and Botnets attacked to computer networks [11]. Learning that how some of the most important part of this attacks works, is a good way to find a way to

[1] - denial of service
[2] - distributed denial of service

deal with them. DoS attacks, reduce required services to legal users. These attacks often doesn't stop and doesn't failure victim server, but reduces quality of service provided by victim server and in most cases, server will not be able to provide correct services. In DDoS, several computer are used to attack to target. In this method, malicious software installed on computers and for an attack, attacker instructs to this computers that starts attack to a specified target [2]. Botnet consists of computers that are controlled by an attacker. These computers works under attacker's activities include the propagation of spam, viruses, DoS, etc. In order to face of these threats, researchers have created systems for intrusion detection to help to prevent injuries and damages. These systems are generally divided into two groups: 1. signature-based IDS[3], and 2. anomaly-based IDS. The first involves a process of identifying and comparing new data systems with knowledge base of known attacks. The power of this method is dependent on the accuracy and completeness of input data model, while the second group systems compared with the expected behavior of the system and significant deviation from the expected behavior will be known as an anomaly. Anomaly-based IDS is an important research topic that traditionally, did by checking contents of packets were sent. Since checking packets at high speed and high volume of work is not possible simply, another approach to complete packet-based methods, early detection in environments with large scale and move to automated systems used that called flow-based method. In this paper, based on the concepts of anomaly-based intrusion detection systems, we propose a mechanism that constructs an activity graph in which nodes represents hosts and edges represents activities within hosts, then calculate maximum and average degree of nodes in graph and compare with scenarios generated by the normal mode. This mechanism can be used for automatic discovery of DoS attacks.

In order to better understand of next sections, we will describe the relevant concepts briefly. An attack or an intrusion, is a sequence of Activities that want to gain control of a system [1]. Purpose of DoS attacks, is network failure for normal services that victim server cannot process user's request [2]. Intrusion detection and response to malicious activity are activities for deal with attacks [1].

Many techniques using for IDS, like: Fuzzy Logic Model, Markov model, Time series Model, Genetic Algorithm model and so on [3]. Flow is a set of IP packets. All packets of a particular flow have properties like IP protocol, source address, destination addresses source port number and destination port number that named flow keys [12]. These packets in a time interval passing from a point of network [12].

A graph have a set of nodes (vertices) and a set of edges [4]. A graph with edge values ($e_{i,j} \geq 0$) named weighted graph [5]. A graph with $e_{i,j} \neq e_{j,i}$ named directed graph. A computer network can modeled with a graph [8]. Node degree is number of edges that are around of a particular node [7]. Node degree in directed graph can defined incoming node degree and outgoing node degree, sum of these degrees will be total node degree [6]. Figure [1] shows importance of flow based intrusion detection systems and path of researchers work in this field.

[3] - Intrusion Detection Systems

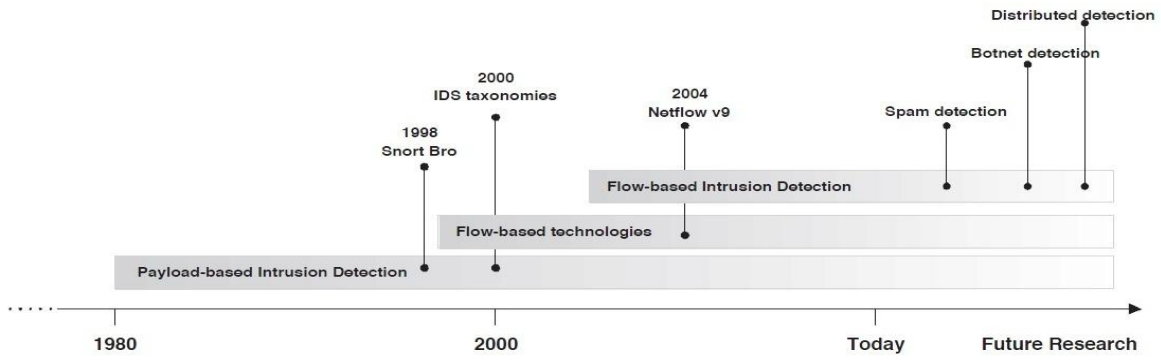

Fig. 1. Time line of evolution of intrusion detection and flow-based technologies [9].

Sperotto et al [1] shows detecting anomalies in flow with time series and describing how the number of flows, packets and bytes changes over time. In this work, flow based intrusion detection system performed for Scan, Worm and DoS attacks, but because a flow does not contain any payload, a flow-based method cannot be useful in detecting attacks related to packet payload.

Tomasek et al. [10] presents an anomaly filter SPAM and HAM as normal (normal pattern), that has been proposed in the email. SPAM filtering mostly uses Bayesian statistics to evaluate message with appropriate score. Each message is a sequence of words, depending on type of sequences, HAM or SPAM will be created. Another group that named UNSURE, presented for classification of dubious messages. This intrusion detection system has been implemented on Linux Fedora version. Mingqiang et al. [11] used clustering as one of data mining techniques and local deviation coefficient, for intrusion detection. For this process, three clusters CN, CA and CS as a normal cluster, abnormal cluster and suspicious cluster created by the calculation and determination of the metrics. CS cluster are not discarded and will used in next steps for calculating distance metrics. Despite acceptable results, some of disadvantages of this approach are including complexity of algorithm, increasing the computation and memory requirements. In addition in initial step, for normal and abnormal data, values of metrics needed to define more flexibility for new issues.

Jadidi et al. [13] employed an Artificial Neural Network (ANN) to detect anomalies in flow-based traffic. Two metaheuristic algorithms, Cuckoo and PSOGSA, examined to optimize the interconnection weights of a Multi-Layer Perceptron (MLP) neural network. This optimized MLP is evaluated with two different flow-based data sets. They compared the performance of these algorithms. This work uses centralized processing, but for providing real-time detection a distributed method should be developed.

David Zhao et al [14] proposed an approach to detect botnet activity in both the command and control and attack phases by classifying network traffic behavior using machine learning classification techniques for specific time intervals. They emphasize the detection in the command and control phase because of detecting the presence of a bot before any malicious activities can be performed, and they use the concept of time intervals to limit the duration they would have to observe any particular flow before they may raise

their suspicions about the nature of the traffic. They showed that using a decision tree classifier. Despite these advantages there are several limitations, they recognized their detection techniques based on the availability of existing malicious data and a detector to be truly robust, must developed a mechanism to evolve the classifiers to adapt to new threats. Also a malicious botnet designer can obfuscate the network flow behavior of a bot in order to evade detection, even if such evasion would come at the expense of the effectiveness of a bot.

2. Proposed Method

In order to make an IDS that has performance and ability to early detect, in large-scale environments and high speed activities, we need to check and make protection mode for system. In this context, we creat an activity graph in which vertices showes entities of system and edges showes relationship between entities. Number of outgoing packets in per flow is determined by labels on edges. For intrusion detection, our model is a type of DoS attacks. As mentioned, manner of DoS attacks is with sending requests to server and waste of time, difficults and sometimes impossible works of victim server. Ticket edges are a flow of packets and drawn from one node to another. From a logical point of view, the number of flows that received by victim server are more than other nodes.

We evaluated a system with 30 hosts at intervals of 10 minutes. System was attacked with DoS in first and third intervals. With based on number of input flows to server, we calculated input degree of per node and average degree of nodes (Table 1). We considered that if degree of each node is much higher than average degree of nodes (about 10 times) a DoS attack is happened.

Table. 1: Values of degree of nodes in four intervals

Interval	Node with maximum input degree	Input degree of suspicious node	Average of input degree of nodes	Average number of packets in suspicious node
First 10 minute(Figure2)	14	35	1	**7**
Second 10 minute(Figure3)	13	15	1	**71**
Third 10 minute(Figure4)	9	33	2	**4**
Fourth 10 minute(Figure5)	–	–	**1**	–

In Figure 2, results showed that input degree of 14th node was 35, which was more than 30 times of average of input degree of all nodes, was identified as a victim node with DoS attack and results that we have before this evaluation identified correctly. Similarly, in second interval that shown in Figure 3, input degree of 13th node was 15, which was more than 10 times of input degree of all nodes, was identified as a

victim node with DoS attack, but actual results of system, didn't show DoS attack. More reviews led us to this comment that although number of flows into a node is a good criterion for evaluation of DoS attacks, but is not enough criterion to exact determine. Therefore the next step is more evaluation of suspicious flows. Since an attacker create a false activity for server in DoS attacks, number of packets that are sent from each flow is much smaller number than packets are sent normally (averaging less than 10 packets per flow). Then, we considered number of packets per flow as next criterion for evaluation of suspicious nodes. In Figure 3 we repeat calculation, input degree of 13th node was 15 that was identified as suspect node, but with about 71 packets as average number of packets that was sent from each flow known as a normal mode. In Figure 4 (third interval), input degree of 9th node was 33, was identified as suspicious nodes then we calculate average number of packets per flow, with about 4 packets, known as a victim node and results that we have before this evaluation identified correctly. Figure 5 shows system in fourth interval. Maximum input degree of nodes was 3 and average degree of nodes was 2, so known as a normal mode and results that we have before this evaluation identified correctly.

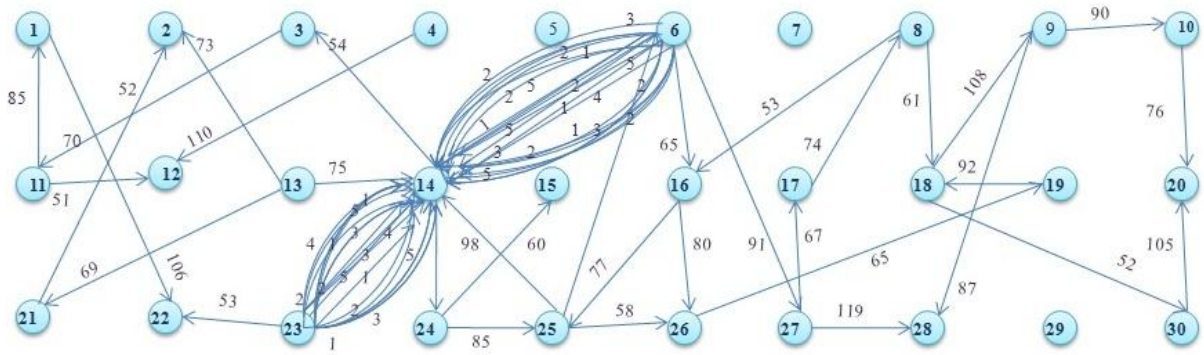

Fig. 2: A view of studied system that DoS attack occurred in the first interval.

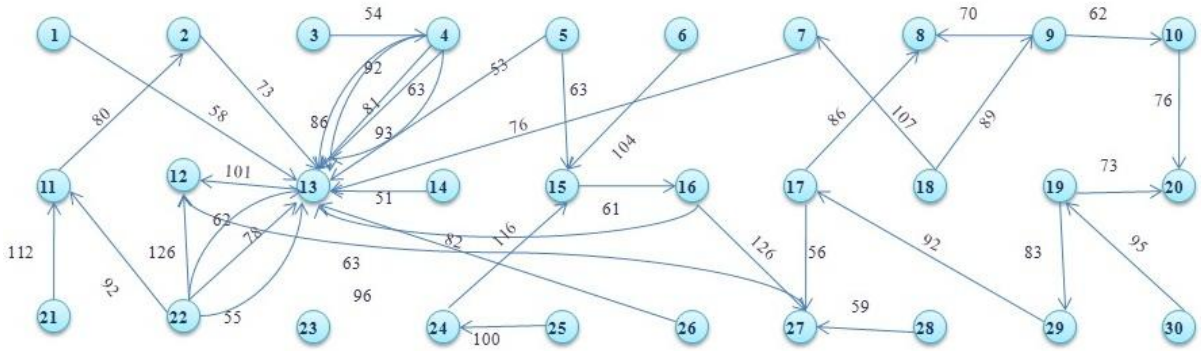

Fig. 3: A view of studied system that DoS attack doesn't occurred in the second interval

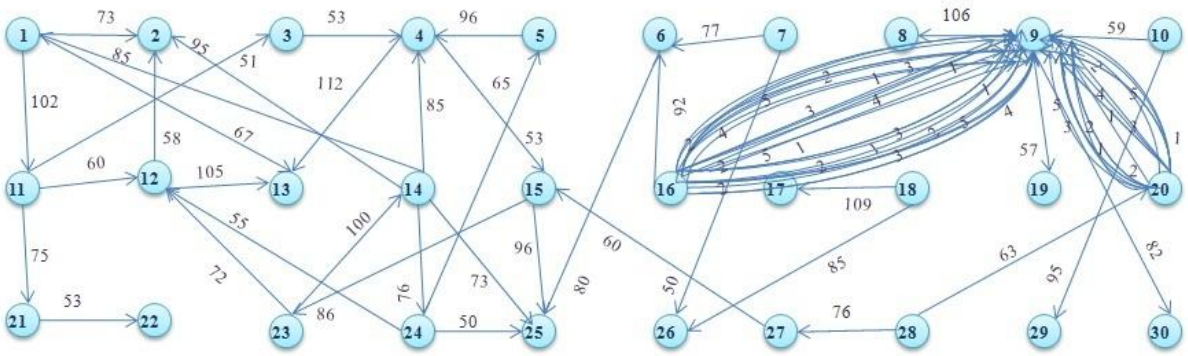

Fig. 4: A view of studied system that DoS attack occurred in the third interval

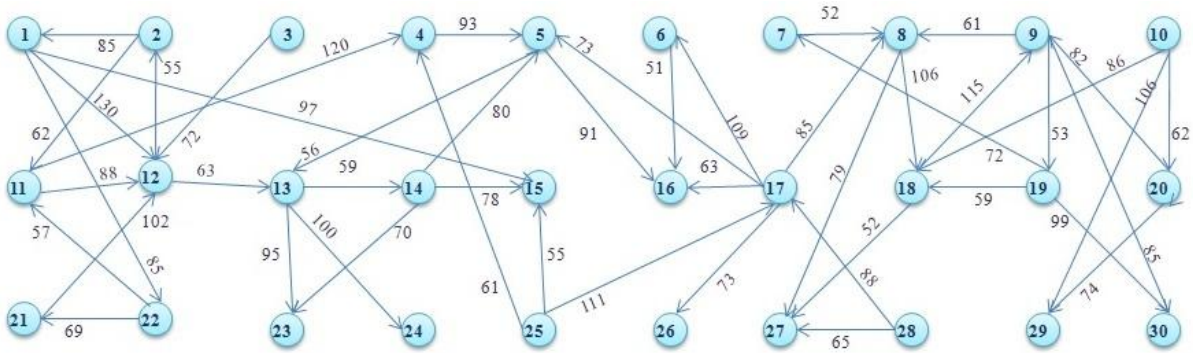

Fig. 5: A view of studied system that DoS attack doesn't occurred in the fourth interval

3. Conclusions

Today, hackers attacks to network systems that very heavy damage to them, so detect and appropriate action to stop these attacks is important. Because of variation in form of attacks, this work is difficult and challenging. According to studies about intrusion detection process and traditional and modern methods, with relying on concepts of anomaly-based intrusion detection, a method proposed to improve detection of attacks on network systems. In proposed approach, we create an activity graph in which nodes represent hosts and edges represent network activity between hosts. Because of favourable properties of graph for large-scale networks, input degrees of nodes in graph created by calculating and compared with known patterns, and attacks detected easily. How to create and update activity graph can be one of things that with investigate and use of modern methods, will provides optimal performance of our proposed system in further. In large-scale networks with high traffic business, this mechanism can provide accurate detection, and with reducing time will provide good and satisfactory performance for organizations.

References

[1] Sperotto. A, Pras. A, Flow-Based Intrusion Detection. *12th IFIP/IEEE IM* 2011; 958 – 963.

[2] Chao-yang. Zh, DOS attack analysis and study of new measures to prevent. *International Conference on Intelligence Science and Information Engineering, IEEE* 2011; 426 – 429.

[3] Jyothsna. v, Rama Prasad. V, A Review of Anomaly based Intrusion Detection Systems. *International Journal of Computer Applications* 2011; 28(7): 26-35.

[4] Luxburg. U, A tutorial on Spectral Clustering, *Statistics and Computing* 2007; 17(4):395-416.

[5] S.V. N. Vishwanathan, Nicol N. Schraudolph, Risi Kondor and Karsten M. Borgwardt, Graph Kernels, *Journal of Machine Learning Research 11* 2010; 1201-1242.

[6] S. Boccaletti, V. Latora, Y.Moreno, M.Chavez and D.-U. Hwang, Complex networks: Structure and dynamics, *Physics Reports* 2006, 424 (4-5):175-308.

[7] Axelsson. S, Intrusion Detection Systems: A Survey and Taxonomy, Technical report Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden 2000; 99-15

[8] Henok. A, Graph Based Clustering for Anomaly Detection in IP Networks, Master's Thesis, Aalto University, School of Science Department of Information and Computer Science Espoo 2011.

[9] Sperotto. A, Flow-Based Intrusion Detection, CTIT Ph.D.-thesis Centre for Telematics and Information Technology University of Twente 2010; Series No, 10-180.

[10] Tomasek. M, Cajkovsky. M, Mados. B, Intrusion Detection System Based on System Behavior, *10th IEEE Jubilee International Symposium on Applied Machine Intelligence and Informatics*, Herl'any, Slovakia, 2012; 271 - 275

[11] Mingqiang. Zh, Hui. H, Qian. W, A Graph-based Clustering Algorithm for Anomaly Intrusion Detection, *The 7th International Conference on Computer Science & Education (ICCSE)*, Melbourne, Australia, 2012; 1311 – 1314.

[12] Sperotto. A, Schaffrath.G, Sadre.R, Morariu.C, Pras. A, and Stiller. B, An overview of IP flow-based intrusion detection, *Communications Surveys & Tutorials, IEEE*, 2010; 12: 343-356.

[13] Jadidi. Z, Muthukkumarasamy. V, Sithirasenan. E, Metaheuristic Algorithms Based Flow Anomaly Detector, 19th *Asia-Pacific Conference on Communications (APCC)*, Bali – Indonesia, 2013.

[14] Zhao. D, Traore. I, Ghorbani. A, Sayed. B, Saad. Sh, Lu3. W, Peer to Peer Botnet Detection Based on Flow Intervals, *27th IFIP TC 11 Information Security and Privacy Conference*, Heraklion, Crete, Greece, 2012; 376: 87-10.