Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 102 (2017) 44393-44397

ISSN: 2229-712X

SYN Flooding Attack Detection by Fuzzy Mechanism

Razieh Malekhosseini

Department of Computer Engineering, Yasooj Branch, Islamic Azad University, Yasooj, Iran.

ARTICLE INFO

Article history:

Received: 15 November 2016;

Received in revised form:

6 January 2017;

Accepted: 16 January 2017;

Keywords

Attack,

SYN Flooding,

Fuzzy.

ABSTRACT

A DoS attack is a type of attack which the attacker waste the resource of system. In DoS attack of the computer system an individual host will send huge number of useless packets to one machine so it makes the crash of the host. Among the different types of DOS attacks, SYN- Flooding attack is more important In the situation of attacking system is in non- linear mode so it seems the fuzzy logic work better other methods. In this paper we propose new hybrid mechanism of filtering and fuzzy for detection of DOS attack Source IP address and port, packet timeline, Number of packets, Entropy of Packet type, rate of request, Entropy of Source IP, and Entropy of Source Port some of the parameters that effect on attack detection. So in our study we infer fuzzy rules based on the value of these parameters. Performance analysis of the proposed approach is done by measure of the four parameters including Precision, Recall, F-measure, and Accuracy in different state of system. To similarity to real situations three modes: normal, LOW DOS Attack, and High DOS Attack for the system is intended. Two set of data e.g. train data and test data are provided to the analysis of the proposed approach. Results showed that for testing data in the situation of attack occurrences in system attack detection has a high degree of accuracy. Its accuracy is approximately 95%.

Introduction

In recent years, network's attack has been undergoing major challenges in network communications and services. A DoS attack is a type of attack which the attacker waste the resource of system. (s) He makes a computing or memory resources too busy to serve legitimate networking/service requests and hence denying legitimate users access to a resource of system. Some of the well- known of DOS attacks are Ping of Death, Smurf Attack, Spoofing ICMP Redirect Message, SYN Flood, Land Attack, RST Attack, and Teardrop Attack.

Among the different types of DOS attacks, SYN-Flooding attack is more important. The attack even in next-generation network infrastructure can also have a harmful impact [1]. The SYN flooding attacks exploit the TCP's protocol. TCP use three-way handshake mechanism. When a server receives a SYN request, it returns a SYN/ACK packet to the client. Until the SYN/ACK packet is acknowledged by the client, the connection remains in half open state. The server has built in its system memory a backlog queue to maintain all half-open connections. Since this backlog queue is of finite size, once the backlog queue limit is reached, all connection requests will be dropped. If a SYN request is spoofed, the victim target will never receive the final ACK packet to complete the three-way handshake. Flooding spoofed SYN requests can easily exhaust the victim machine's backlog queue. The stateless and destination-based nature of Internet routing infrastructure cannot differentiate a legitimate SYN from a spoofed one, and TCP does not offer strong authentication on SYN packets. Therefore, under SYN flooding attacks, the victim server cannot single out, and respond only to, legitimate connection requests while ignoring the spoofed. Figure 1 shows the mechanism of SYN flooding attack.

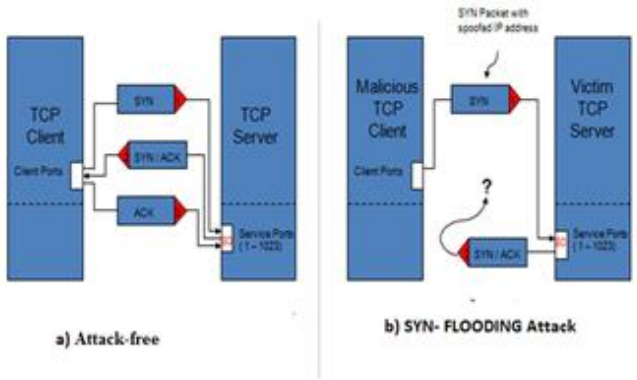

Figure 1a. Attack-free TCP 3-Way Handshake (b) DoS flooding-attacked system.

To countermeasure SYN flooding attacks, several defense mechanisms have been proposed, such as Syn cache, Syn cookies, SynDefender, Syn proxying, and Synkill.

All of these defense mechanisms are installed at the firewall of the victim server or inside the victim server, thereby providing no hints about the sources of the SYN flooding.

Moreover, these defense mechanisms are state full, i.e., states are maintained for each TCP connection or state computation is required. Such a solution makes the defense mechanism itself vulnerable to SYN flooding attacks. Recent experiments have shown that a specialized firewall, which is designed to resist

SYN floods became failed under a flood of 14,000 packets per second [2]. The state full defense mechanisms also degrade the end-to-end TCP performance.

In this paper we propose new hybrid mechanism of filtering and fuzzy for detection of DOS attack.

Tele: +987433130291

E-mail address: malek.android83@gmail.com

The rest of paper is organized as follows. In the section of related work we review existing work, while in the "Methodology "section we describe the methodology that we use in our study. Then we discuss the mechanism of attack detection and details of fuzzy system. Simulation and performance analysis is described separately. Finally, in the section of Conclusions we conclude the paper

Related work

Many researches in the field of Denial of service (DOS) attacks identification have been conducted. Various mechanisms have been introduced to identify and deal with these types of attacks . Figure 2 shows taxonomy of identification of DOS attacks. Methods based on heuristic algorithms, fuzzy techniques [20, 21], Data Mining, Intrusion Detection System (IDS), Statistical Based Approaches, and identify abnormal behaviors, including methods that have been used in recognizing Denial of service attacks. In this section we explain the existing work in this field.

In Statistical Approaches normal profile creates using either based on statistical data [3] or if-than type rules and flags intrusion if network traffic deviates from normal profile. Moreover in statistical based approaches two methods used in detecting SYN attack. One is an adaptive threshold algorithm and other is CUSUM algorithm [4].

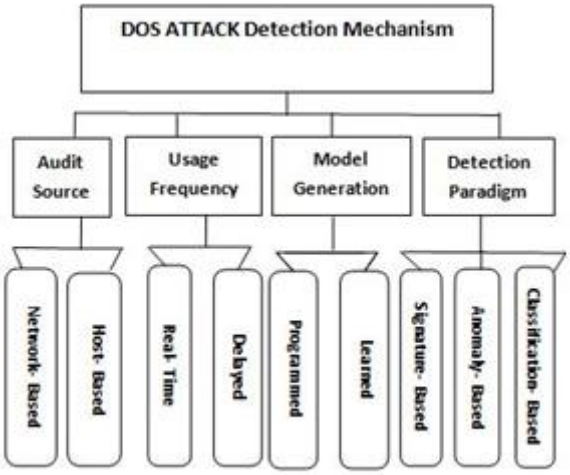

Figure 2.Taxonomy of Dos Attacks Detection.

In adaptive threshold algorithm intrusions are detected based on the exceeding of threshold. Threshold is set adaptively by the traffic or accumulated traffic measurements, as a normal profile. The direct application of this algorithm gives high number of false positives so anomaly is considered if number of violations exceeds certain threshold in a particular time interval [19].

Chi-Chun Lo et al. [5] proposed an intrusion detection system (IDS) framework in form of cooperative. When IDS identifies any attack then cooperative agents from IDS deployed in each cloud environment exchange alerts. In this mechanism there are different areas called clustering module that collected alerts and decision about accepting the alert as happened attack.

SampadaChavan et al. [6] proposed an intrusion detection system based on neuro-fuzzy approach. An Artificial Neural Networks and Fuzzy Inference System uses SNORT to detect abnormal traffic in real time. This mechanism used learning method to deal with dos attack. Moreover signature pattern create based on supervised and unsupervised learning method. Fuzzy logic is appropriate for approaching the nonlinear systems [7].

Tuncer and Tatar proposed a fuzzy technique for nonlinear system. The technique uses the fuzzy logic for nonlinear systems to detect DoS attack. In this method it is difficult to model the traffic network before, and after the attack due to linear and burst characteristics of packets flow. In addition, this technique depends on offset value in a TCP packet header which is a change due to network congestion and others states [18]. This technique shows a good result using a fuzzy logic compared to CUSUM algorithm, especially in false positive and false negative measurement in the low-rate flow packets [8].

Fuzzy logic is used for classifying quantitative and abstract features in normal and abnormal classes with smooth class boundaries [9]. Moreover Fuzzy logic is used with data mining methods for automatically discovering hidden patterns from large databases [9]. Fuzzy Association Rules [10] and Fuzzy Frequent Episodes, have been used to mine audit data to find normal patterns for anomaly based intrusion detection systems [2, 11]. Visconti, et al. [12] proposed a fuzzy system for detecting misbehaving nodes. The misbehaving nodes make abnormal traffic in network environment. For detecting of these nodes they collect sample data of various network parameters in distributed environment for Partial-anomaly based detection from misbehaving nodes. Fuzzy logic based forensic analysis [13], Fuzzy inference system based anomaly, Trust and fuzzy logic based detection system [14], Fuzzy Logic Controller based IDS [15] some of the fuzzy based mechanism for detection or dealing with intrusion detection system including DOS attack.

SYN flood defense mechanism classify based on Firewall based method, Server based method, Agent based, and Router based. In Firewall based methods filtering of packets and request done before the router so because of extra delay for processing each packet this approach can be overloaded. SYN Defender, SYN proxying are Firewall based method.

SYN Cache, SYN cookies are Server Based methods. In SYN cache first packets receives and then store states uses a hash table. For long uncompleted requested Removes half open connections. In Route-based we use packet information to determine if packet arriving at router has a spoofed Source/ Destination addresses [16]

Methodology

We will discuss the design of a hybrid approach against DOS attack based on the filtering method and fuzzy defense mechanism. Filtering mechanism define is based on the statistical behavior of parameters of network protocols. Each network regardless of network type, protocols, topology and packet size plays a crucial role in statistical anomaly detection. The parameters which were considered by Lee et al [10] to detect anomaly are as follows: Source IP address and port Destination IP address and port Packet type Occurrence rate of packet type (TCP SYN, UDP, ICMP) Number of packets. Under the normal condition, the difference between the collected number of SYNs and FINs (RSTs) is very small, as compared to the total number of TCP connection requests. SYNs Significant divergence of these parameters shows the attack in network traffic. Under SYN flooding attacks, the flooding SYN traffic has significant regularity and semantics that can be filtered out. Recent experiments with SYN attacks on commercial platforms [8] show that the minimum flooding rate to overwhelm an unprotected server is 500 SYN packets per second.

Our test bed consists of several components. Figure 3 shows the hardware configuration in test bed.

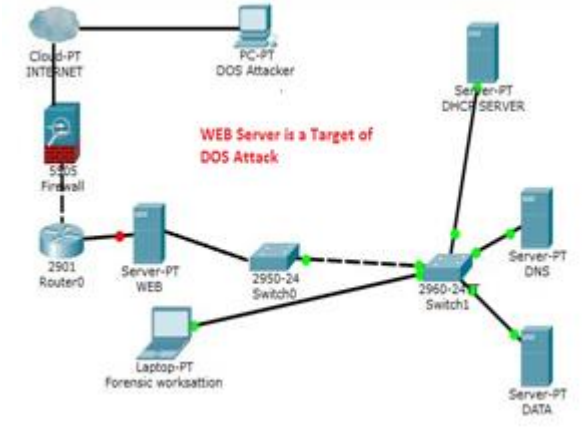

Figure 3.our test bed component.

As we can be seen in Figure 3the target of DOS Attacker is denied legal requests on the Web server. In the network we first launched an attack SYN- Flooding on web server.

In order to launch the TCP SYN flood attack on the victim server (web server) we use for this purpose we set the IP address for DOS Attacker and web server as victim system is and then we use the C Source Code (Linux) SYN Flood DOS with LINUX sockets [17] to send the large number of packets to server.

Attack Detection by Traffic analysis

In this section we analysis the network traffic by fuzzy system. Effective parameter for proper detection are including Source IP address and port, packet timeline, Number of packets, Entropy of Packet type, rate of request, Entropy of Source IP

Entropy of Source Port. Base on theses parameters fuzzy system make a decision about the occurrences of DOS Attack. For simply we use these abbreviation for input parameters. Table 2 shows the notation of input parameters for fuzzy system.

Table 2.input parameters.

Input parameter	Abbreviation
Packet Timeline	PT
Rate of Request	RQ
Source IP address	S-IP
Source Port	SP
Entropy of Source IP	ES-IP
Entropy of Source Port	ES-P
SYN Segment	Tcp SYN

Fuzzy rules

To get the fuzzy rules we use a combination of input parameters together. The results of these rules may cause a normal mode, attack or high attack. In normal mode network traffic is detected as normal traffic. In other words, the attack has not occurred. In the attack mode we have an abnormal traffic. In the high attack mode all of the network traffic is abnormal and the system is out of service.

Fuzzy rules relating to detect denial of service attack is given below. In all these rules network traffic is shown by NT. Moreover for each of the input parameter values low, medium, and high is consider.

1. IF RQ is LOW and ES-IP is LOW THEN NT is Normal
2. IF RQ is LOW and ES-IP is MEDIUM THEN NT is Normal
3. IF RQ is LOW and ES-P is LOW THEN NT is Normal
4. IF RQ is LOW and ES-P is MEDIUM THEN NT is Normal
5. IF RQ is LOW and ES-IP is HIGH THEN NT is Normal
6. IF RQ is LOW and ES-P is HIGH THEN NT is Normal
7. IF RQ is LOW and ES-IP is MEDIUM THEN NT is Normal
8. IF RQ is LOW and ES-P is MEDIUM THEN NT is Normal
9. IF RQ is MEDIUM and ES-IP is MEDIUM THEN NT is Normal
10. IF RQ is MEDIUM and ES-P is MEDIUM THEN NT is Normal
11. IF RQ is MEDIUM and ES-IP is HIGH THEN NT is Attack
12. IF RQ is HIGH and ES-P is MEDIUM THEN NT is Attack
13. IF ES-IP is LOW and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
14. IF ES-P is LOW and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
15. IF ES-IP is MEDIUM and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
16. IF ES-P is MEDIUM and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
17. IF ES-IP is HIGH and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
18. IF ES-P is HIGH and RQ is LOW and Tcp SYN HIGH THEN NT is Attack
19. IF ES-IP is HIGH and RQ is HIGH and Tcp SYN HIGH THEN NT is HIGH Attack
20. IF ES-P is HIGH and RQ is HIGH and Tcp SYN HIGH THEN NT is HIGH Attack

Simulation

Fuzzy system is considered as shown in Figure 4. First the normal traffic as training data, attack traffic and fuzzy rules are inserted into system.

Then, using MATLAB fuzzy operations is done. Network traffics are collected form fuzzy system and finally the state of the traffic are classified in three modes Normal, Attack, and High Attack.

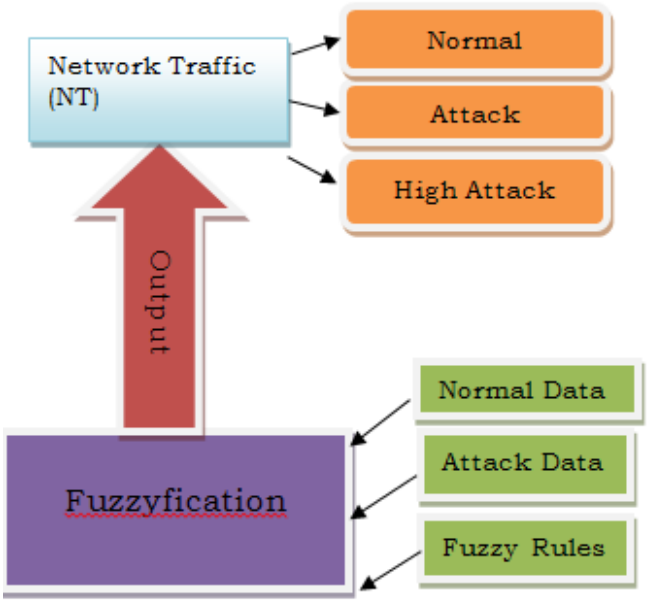

Figure 4.detailes of fuzzy system.

Performance Analysis

After the simulation of the system we evaluate performance of the system four criteria including precision, recall, F-measure, and overall accuracy. These criteria are normally used to estimate the rare class prediction. For this purpose we use the following equations for them.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (1)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (2)$$

In equations 1, 2 we have bellow definitions for TP, FP, and FN.

TP = True positive is defined as the proportion of positive cases that were classified correctly.

FP = False positive. The false positive rate (FP) is the proportion of negative cases that were incorrectly classified as positive.

FN = False Negative. The false negative rate (FN) is the proportion of positive cases that were incorrectly classified as negative.

$$F - \text{Measure} = 2.\frac{\text{Precision}.\text{Recall})}{\text{Precision}+\text{Recall})} \quad (3)$$

$$\text{Overall accuracy} = \frac{TP + TN}{TP + TN + FN + FP} \quad (4)$$

In equation 4 we define TN = True negative is refined as the proportion of negative cases that were classified correctly.

By considering the above criteria, we enter the training and test data in fuzzy system. For both normal and attack (including light attack and high attack) was measured Precision, Recall, F – measure, and Accuracy factors. The results show in Table 3.

Results and discussion

In this section the results of the parameters for both sample testing and training data is shown.

Table 3 shows the obtained values from the system simulation in MATLAB.

Table 3.Results of simulation.

Network traffic of system	Criteria	Training data	Testing data
Normal	Precision	0.9880	0.9875
	Recall	0.9885	0.9883
	F – measure	0.9883	0.9879
	Accuracy	0.9769	0.9761
LOW DOS Attack	Precision	0.9846	0.9807
	Recall	0.9785	0.9125
	F – measure	0.9815	0.9454
	Accuracy	0.9641	0.9761
High DOS Attack	Precision	0.9809	0.9789
	Recall	0.9685	0.9665
	F – measure	0.9746	0.9727
	Accuracy	0.9509	0.9469

In order to compare parameters in normal mode, Low DOS attack, and High DOA attack in the following separated charts for each metric is shown.

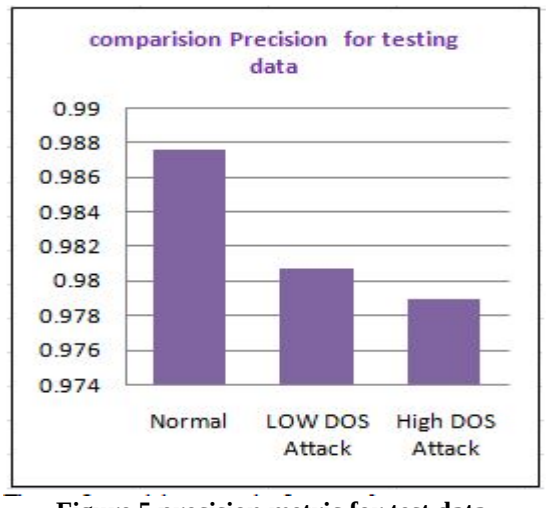

Figure 5.precision metric for test data.

As can be seen in Figurein both cases low and high DOS attack about 98% of attacks to be detected.

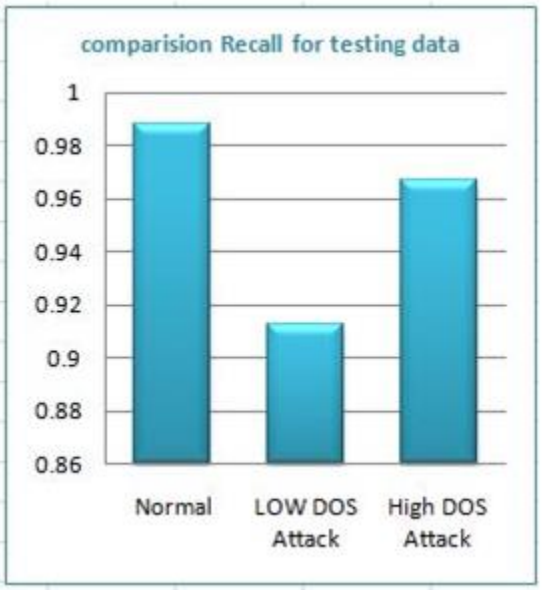

Figure 6.comparision of Recall metric for test data

Based on figure 6 we know that the number of samples in both low and high attack properly classify in their respective classes. In the situation that system is facing high attack our method well able to detect attack.

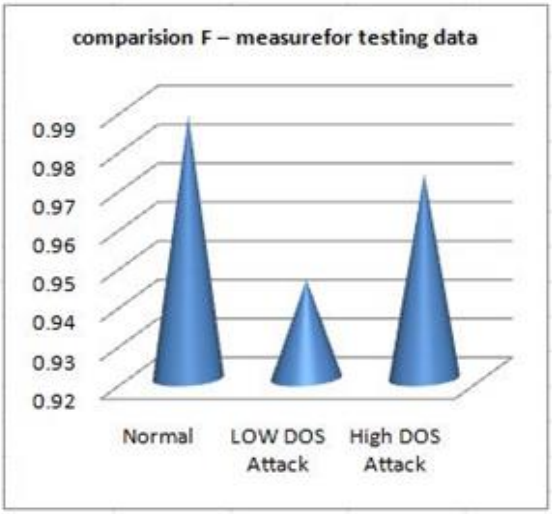

Figure 7.Comparision of F-measure metric for test data.

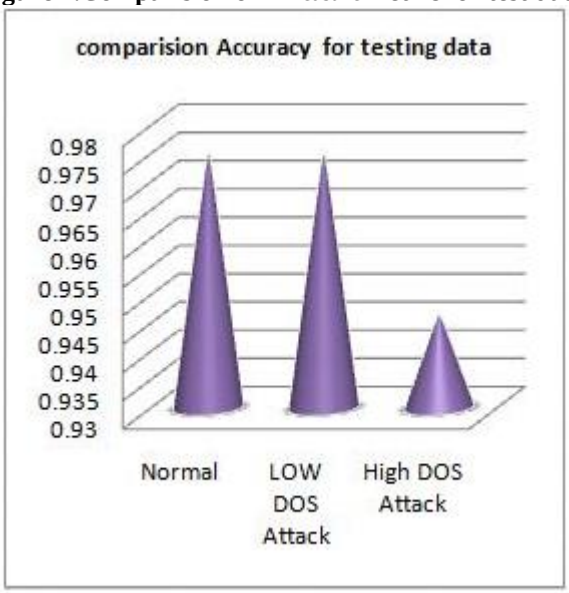

Figure 8.Comparision of F-measure metric for test data.

As can be seen in Figures 6 and 7 in the situation attack occurrences system attack has a high degree of accuracy. Its accuracy is approximately 95%.

Conclusion

DOS is a common attack that exhausts the computing resources of the system. By the various of different DoS attack tools launch of attack become easy.

In this paper we have proposed a fuzzy system to detection of attack packet in form of SYN Flooding attack. SYN Flooding attack initiates many incomplete TCP connections and denying legitimate traffic.

For this purpose e infer define rules and we use to set of data for system traffic.

The results show that, given that in the attack situation system is behaved non-linear so approach based on fuzzy logic can be more accurate.

Refernces

[1] R. MalekHoseini, N. MalekHoseini SYN flooding Attack countermeasures in Next Generation Network, International Journal of Computer Science and Information Technology & Security (IJCSITS),Vol. 3, No.2, 2013

[2] W. Lee, S. Stolfo, and K. Mok "Mining audit data to build intrusion detection models", In Proceedings of the fourth international conference on knowledge discovery and data mining, New York, New York, August 27-31, 1998.

[3] V.A Siris, F.Papagalou "Application of an anomaly detection algorithms for detecting SYN flooding attacks" IEEE communications Society Globecom ,2004.

[4]B. E. Brodsky and B. S. Darkhovsky. Nonparametric Methods in Change-Point Problems. Kluwer Academic Publishers, 1993.

[5] L. Chi-Chun, C.C.Huang, and J.Ku. "A cooperative intrusion detection system framework for cloud computing networks," IEEE 39th International Conference on Parallel Processing Workshops , San Diego, pp. 280-284, 2010.

[6] S.Chavan, K. Shah, Neha Dave, S.Mukherjee ,A.Abraham ,S.Sanyal, "Adaptive neuro-fuzzy intrusion detection systems," International Conference on Information Technology: Coding and Computing, Las Vegas, Vol. 1, pp. 70-74, 2004.

[7] L. A. Zadeh, "Fuzzy sets," Information and control, vol. 8, pp. 338-353, 1965.

[8] T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in International Conference on Information Security and Assurance, 2008, pp. 321-325.

[9] A Susan, M Bridges, R. B. Vaughn, and A Siraj. "AI Techniques, Applied to High Performance Computing". Proceeding of the Tenth International Conference on Telecommunication Systems, Modelling and Analysis, Monterey CA, Volume 2, pp. 100-114, October 3-6, 2002.

[10] C. Kuok, A. Fu, and M. Wong, "Mining fuzzy Association rules in databases". SIGMOD Record VOL. 17 NO. 1 1998, PP. 41-46.

[11] J.E. Dickerson and J.A. Dickerson. "Fuzzy network profiling for intrusion detection" in proceedings of NAFIPS 19th Int'l conference of the North American Fuzzy information processing Society. Atlanta USA July 2000, Pp 301-306.

[12] A. Visconti, H. Tahayori, " A Biologically–Inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad hoc networks," International Journal for Infonomics,Vol. 3, No. 2, 2010, pp. 270-277.

[13] S. Ahmed, S. M. Nirkhi, "Fuzzy Forensic Analysis System for DDoS Attack in MANET Response Analysis," International Journal of Science and Modern Engineering (IJISME), Vol. 1, No. 7, 2013, pp. 52-55.

[14] V.Manoj, M. Aaqib, N. Raghavendiran, and R.Vijayan, "A Novel Security Framework Using Trust and Fuzzy Logic in MANET," International Journal of Distributed and Parallel Systems (IJDPS), Vol. 3, No. 1, 2012, pp. 285-299.

[15] S.Sujatha, P. Vivekanandan, and A.Kannan,"Fuzzy logic controller based intrusion handling system for mobile adhoc networks,"Asian Journal of nformation Technology, Vol. 7, No. 5, 2008, pp. 175-182.

[16] H.Wang, D. Zhang, and K.G. Shin Serhat , Detecting SYN Flooding Attacks TURKMEN N10163791

[17] code for lunch SYN-Flooding- Attack, http://www.binarytides.com/syn-flood-dos-attack/

[18]T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in International Conference on Information Security and Assurance, 2008, pp. 321-325

[19] V.A Siris, F.Papagalou "Application of anomaly detection algorithms for detecting SYN flooding attacks" IEEE communications Society Globecom 2004.

[20] R.IDOWU, R. CHANDRENM, and Z.ALIOTHMAN , DENIAL OF SERVICE ATTACK DETECTION USING TRAPEZOIDAL FUZZY REASONING SPIKING NEURAL P SYSTEM, Journal of Theoretical and Applied Information Technology, Vol.75. No.3, 2015., pp. 397-404

[21] N.Ch.S.N. Iyenga, A. Banerjee, and G. GanapathyA Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 3, December 2014, PP. 233-245.