ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 5, May 2016

A Novel Defense Mechanism against Distributed Denial of Service Attacks using Fuzzy Logic

Shivani, Er. Amandeep Singh, Dr. Ramesh Chand Kashyap

***Abstract*— In this advanced smart life, internet and computer are becomes the essential components of life. From the age of computer birth to now, each individual/organization used to store their data as a soft copy in computer. With the possibility of computer connection and internet was born the necessity to protect the data from attackers who like to get authentic data for their own use. There are several types of attacks (like Dos, Sybil attack, black hole attack, grey hole attack etc) that an attacker can perform within the network to break the network security. Here, our main focus is on the distributed denial of service attack in which attacker consumes the resources of user in distributed network. So, there should be possible methods to protect the system from DDoS attacks. In this paper, we are using fuzzy inference system for defense against DDoS attacks in HTTP server. The parameters of HTTP request (GET & POST) and delta time are considered for the measurement of denial of service attacks. Also a comparison is made with naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest and naïve bayes Multinomial on the basis of accuracy, true positive rate and false positive rate of each algorithm.**

***Index Terms*— Distributed Denial of Service Attack, HTTP Server, Wireless Network, Fuzzy Inference System.**

I. INTRODUCTION

Wireless communication networks use various packet delivery protocols to send data. There can be one receiver in the networks or more than one receiver and even there can be one or more than one sender and sending this information through a wireless medium can be critical and challenging because there are various type of attacks [1]. We can see the commercial and military applications of wireless communication networks. The usage of wireless network in a variety of applications is highly important with the emphasis on ensuring security. Still, defense against the malicious attacks of all levels may be high or low in wireless sensor network. A variety of attacks on the network like wormholes, DoS, DDoS, sinkhole, Sybil, sleep, and selective forward attacks in the network are being observed [2][3]. Here, we are using a fuzzy logic based defense mechanism for the detection of Distributed Denial of Service attack. Denial of service attack makes the resources unavailable for the intended users making it a major potential threat to availability. Denial of Service is defined as the prevention of authorized access to resources or the delay of time critical operations [4].

DoS attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised network on the Internet [5]. On the Internet, a DDoS attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system [6]. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker begins a DDoS attack by exploiting vulnerability in one computer system and making it the DDoS "master." It is from the master system that the intruder identifies and communicates with other systems that can be compromised [7].

In this research work, we have done the work for the detection of denial of service attacks against HTTP servers. Here, the parameters of HTTP request (GET & POST) and delta time are considered for the measurement of denial of service attacks. Also a comparison is made with naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest and naïve bayes Multinomial on the basis of accuracy, true positive rate and false positive rate of each algorithm.
Rest of the paper is organized in the following manner: Section II brief about the Fuzzy Logic. Section III presents the proposed algorithm. Section IV gives the result and comparison of the proposed concept with individual MAP algorithm. Section V concludes the paper.

II. FUZZY LOGIC

Fuzzy logic is a human reasoning based mathematical tool that deals with parameters like accuracy, uncertainty etc. It is used in network security since long ago and deals with degree of truth instead of complete true or false values [8].

Manuscript received May,2016.
***Shivani**, Research Scholar, Department of Electronics and Communication Engineering, Rayat Institute of Engineering and Information Technology, India.*
***Er. Amandeep Singh**, Assistant Professor, Department of Electronics and Communication Engineering, Rayat Institute of Engineering and Information Technology, India..*
***Dr. Ramesh Chand Kashyap**, Head of the Department, Department of Electronics and Communication Engineering, Rayat Institute of Engineering and Information Technology, India.*

The selection of fuzzy logic for intrusion detection is presence of values in the form of interval i.e. fuzziness of the approach. Fuzzy logic can be represented with the help of membership function. The membership function can be provided in various forms. In this denial of service attacks, we are using trapezoidal membership function which can be calculated as below:

Membership value = (x-a)/ (b-a)

Where
x=threshold value,
a = number of packets forwarded,
b = number of packets dropped.

Fuzzy inference System is the mathematical framework of fuzzy logic. It works in three phases of fuzzification, rule generation and defuzzification [9]. Fuzzification is the process to convert the crisp values into terms of membership function. Then fuzzy rules generated in the form of If-Else form. Finally defuzzification is done to obtain the output user friendly results [10].

The If-Else rule based system is explained as below:

- If the output of both the modules is normal, then decision is normal.
- If the output of one module is normal and other one is abnormal then decision is abnormal.

If the output of both modules is abnormal, then decision is abnormal.

III. Proposed Algorithm

This work proposes to develop a Fuzzy logic based Distributed Denial of Service attack in HTTP server. In this approach, we have considered the routing protocols of Ad hoc On Demand Distance Vector. By using the AODV protocol with HTTP server, requests are send in the form of GET and POST parameters. The data is more secure with POST method which is routed for on demand packet transfer in http server. Attacker usually attacks in the form of huge traffic and marvellous information so that resources can be consumed. In this proposed concept, the http request methods are considered with delta time (time interval between two consecutive http request from a single IP address) of the nodes. More the value of delta time, lesser will be the chances of attack. The overall decision of system is performed by the fuzzy logic. Fuzzy logic involve basically three steps, (1) fuzzification, (2) Rule based inference mechanism and (3) Defuzzification. This proposed algorithm is structured as below:

Input: Virtual training dataset of packets.

Output: Distributed Denial of Service Attack Detection Model.

ALGORITHM

(1) $Z = \{(N_0, N_1, N_2 \ldots N_m), BS\}$

(2) For i = 1 to n

(3) Matrix= Nodes (N(id), N (Energy), N (delta time))

(4) E_t= Threshold Energy, D_{th} = Threshold Delta Time

(5) End For i

(6) For i = 1 to n,

(7) For j = 1 to m,

(8) $N_i \rightarrow$ Send packets by GET request $\rightarrow N_j$ & $N_j \rightarrow$ Receive Packets by POST request$\rightarrow N_i$

(9) Calculate 'E_n' for each node with fuzzy logic and Delta time between two consecutive nodes D_n

(10) If $E_n >= E_t$ and $D_n > D_{th}$

(11) Node not affected.

(12) Else,

(13) Node is affected by external attacker (DDoS Attack).

(14) Change the route for communication.

(15) End If

(16) End For j

(17) End For i

(18) End

Explanation

Step 1: Consider total N number of nodes that are randomly deployed in the network from a single base station (BS). Requests in HTTP server are send in the form of GET and POST method.

Step 2: During node creation, BS will send a request message to each node and will receive the reply message for the authenticity of nodes with their ID, Energy value and Delta Time.

Step 3: From the deployed 'N' number of nodes, number of authentic nodes 'm' are considered and defined the network structure of $Z= \{(N_1, N_2, N_3, \ldots N_m), BS\}$.

Step 4: Each node attains the Energy level of the HTTP server network. For a node at any location X, Y is represented by Ni= (rand(X), rand (Y)). A threshold Energy value and delta time is set for checking the denial of service attack as E_t and D_{th} respectively.

Step 5: Initialize the fuzzification parameters and consider the nodes as the fuzzification set of rules. To search the multiple copies of same example in D, if found then keeps only one unique example in D.

Step 6: Send the packets of different destination with different paths in the form of GET and POST request

methods in HTTP server. All the decision are to be made by the process of fuzzification in fuzzy logic.

Step 7: Fuzzy estimation is done for each node N= (N_1, N_2, N_3, ….N_m). Based on the threshold value E_t and D_{th}, the matrices values are calculated to check the energy level during the packet transaction process.

Step 8: Consider the matrix to store the values of node number and corresponding membership function which can be further calculated as RS[node number][member function value]. Trapezoidal membership method is used to calculate the member function value which is defined as below.

Membership value = (x-a)/ (b-a)

Where x=threshold value, a = number of packets forwarded, b = number of packets dropped.

Step 9: Consider the membership function and calculate the energy level of each node and delta time using fuzzy rule based system.

Step 10: Apply Defuzzification and check the values of each node in energy form (E_n) and delta time (D_n) using fuzzy inference rule system.

Step 11: If E_n > = Et and $D_n > D_{th}$, then node is not affected by external denial of service attacks.

Step 12: If $E_n < E_t$ and $D_n < D_{th}$, then node is affected by external denial attacks. So, discard that nodes for packet transaction and change the path for packet transaction.

Step 13: Repeat the steps 7 to 12 and find the possible number of attacks.

IV. RESULT & COMPARISON

This section examines the performance of the proposed algorithm as compare to MAP algorithm on the basis of obtained results.

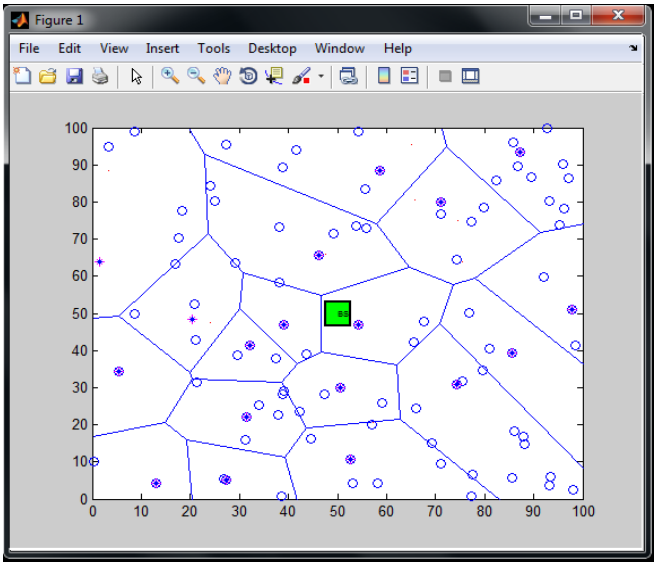

Figure 1: Packet Transaction from BS to each node

The proposed concept is implemented in MATLAB version 8.3.052. The Network size of 100 nodes is considered. At each iteration change in time for the sending and receiving of packet is calculated. The process of sending packets from base station to each node is shown in figure 1.

In figure 1, the base station is shown in centre. The circular nodes are the empty nodes that have already sent the data and filled circular nodes are those nodes that have received the data. Simple star structure shows data is in the path from one node to another one.

During this packet transaction, proposed concept checks for security parameters in the form of REQ and REP message and assure about the defense against the DDoS attacks. For the detection of DDoS attacks, fuzzy based network control system is generated having some fuzzy rules which are shared as below:

- If (Energy is **high**) and (Delta Time is **max**) then (Delay is **short**)
- If (Energy is **high**) and (Delta Time is **min**) then (Delay is **long**)
- If (Energy is **low**) and (Delta Time is **max**) then (Delay is **long**)
- If (Energy is **low**) and (Delta Time is **min**) then (Delay is **Denial**)

Fuzzy Inference System for Distributed Denial of Service attacks detection is shown in figure 2.

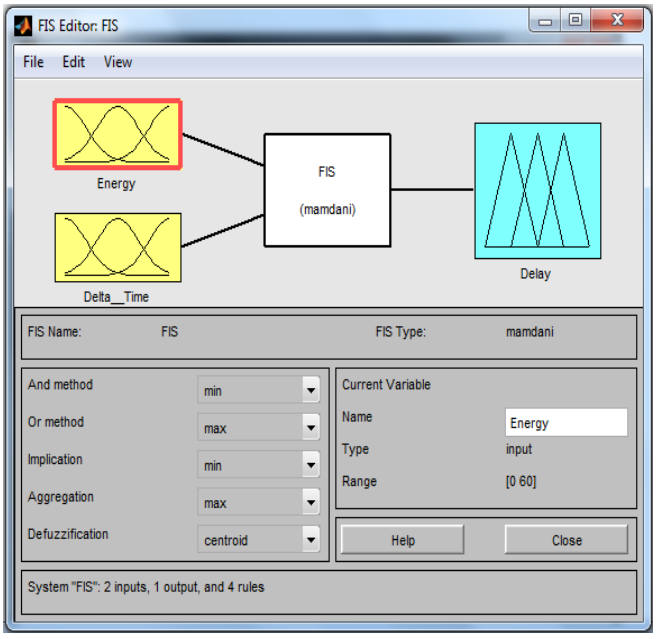

Figure 2: Fuzzy Inference System for DDoS attack Detection

Further, this concept is evaluated based on the Accuracy, True Positive and False Positive values of proposed concept. The comparison of the concept is made with the existing approaches of naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest and naïve bayes Multinomial [11].

To check the accuracy of our proposed algorithm, we have considered the parameters of Accuracy, True Positive and False Positive values. This comparison of naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest, naïve bayes Multinomial and proposed algorithm is presented in table I.

TABLE I: Evaluated parameters

Algorithm	**Accuracy**	**True Positive**	**False Positive**
Proposed Concept	95.238	96.774	2.564
Naïve Bayes	91.14	93.62	12.50
Naïve Bayes Multinomial	93.67	91.49	03.10
MLP	88.61	89.36	12.50
Random Forest	91.14	93.62	12.50
Logistic	92.41	93.62	12.50
RBFN Network	89.87	95.74	18.75

This comparison of proposed algorithm with naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest, naïve bayes Multinomial is shown also in figure 3 to 5.

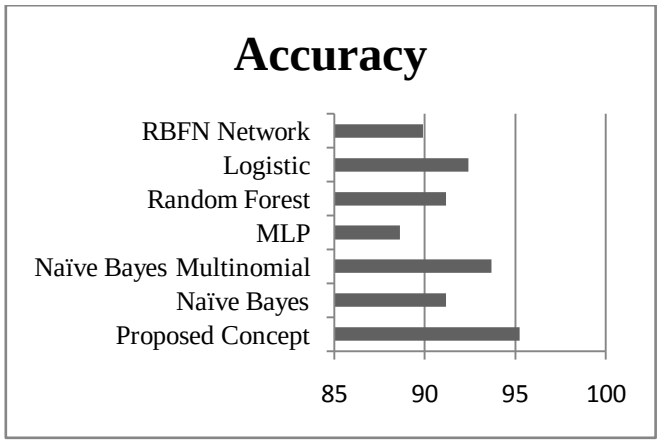

Figure 3: Comparison of Proposed Algorithm with others based on Accuracy

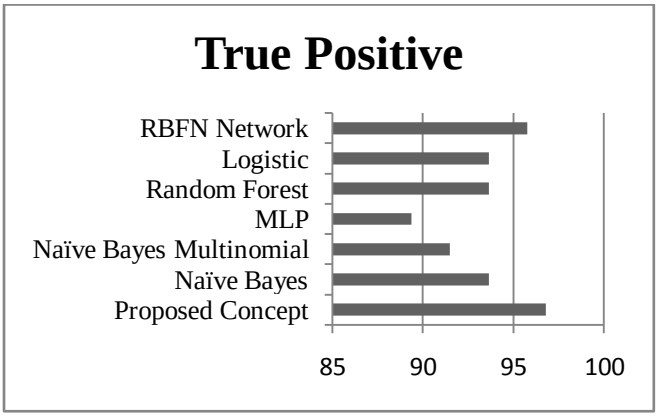

Figure 4: Comparison of Proposed Algorithm with others based on True Positive

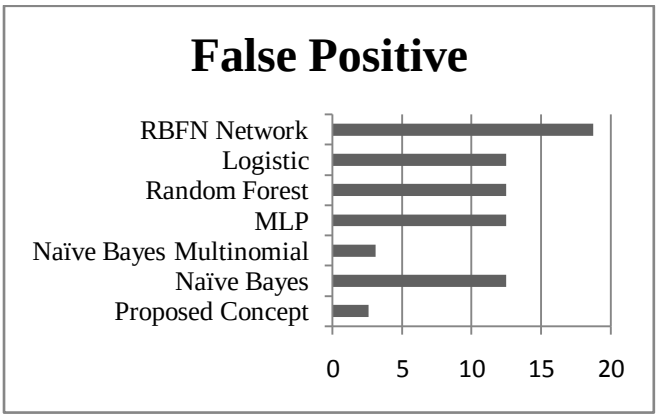

Figure 5: Comparison of Proposed Algorithm with others based on False Positive

V. CONCLUSION

The main goal of this research thesis is the improvement of defence mechanism to ruin the DDoS attack in HTTP server based wireless network. DoS attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. Here, we have proposed Fuzzy Logic based algorithm for the defense against the Distributed Denial of Service Attacks. To check the accuracy of our proposed algorithm, we have considered the parameters of Accuracy, True Positive and False Positive values. This comparison of naïve bayes classifier, RBF Network, Multilayer Perception, Random Forest, naïve bayes Multinomial and proposed algorithm. The overall results for proposed algorithm as compare to other existing approaches shows better accuracy and other results as shown in table I and figure 3, figure 4 & figure 5. In this way, we can say that the proposed concept is efficient enough to defense against DDoS attacks.

REFERENCES

[1] Byers, Paula K., and Suzanne Michele Bourgoin. "Encyclopedia of World Biography. Ford-Grilliparzer." (1998).

[2] Wu, Hongyi, Chunming Qiao, Swades De, and Ozan Tonguz. "Integrated cellular and ad hoc relaying systems: iCAR." *Selected Areas in Communications, IEEE Journal on* 19, no. 10 (2001): 2105-2115.

[3] Djenouri, Djamel, Lyes Khelladi, and Nadjib Badache. "A survey of security issues in mobile ad hoc networks." *IEEE communications surveys* 7, no. 4 (2005): 2-28.

[4] Lau, Felix, Stuart H. Rubin, Michael H. Smith, and Ljiljana Trajković. "Distributed denial of service attacks." In *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 3, pp. 2275-2280. IEEE, 2000.

[5] Peng, Tao, Christopher Leckie, and Kotagiri Ramamohanarao. "Protection from distributed denial of service attacks using history-based IP filtering." In*Communications, 2003. ICC'03. IEEE International Conference on*, vol. 1, pp. 482-486. IEEE, 2003.

[6] Specht, Stephen M., and Ruby B. Lee. "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures." In *ISCA PDCS*, pp. 543-550. 2004.

[7] Carl, Glenn, George Kesidis, Richard R. Brooks, and Suresh Rai. "Denial-of-service attack-detection techniques." *Internet Computing, IEEE* 10, no. 1 (2006): 82-89.

[8] Dickerson, John E., and Julie A. Dickerson. "Fuzzy network profiling for intrusion detection." In *Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American*, pp. 301-306. IEEE, 2000.

[9] Botha, Martin, and Rossouw Von Solms. "Utilising fuzzy logic and trend analysis for effective intrusion detection." *Computers & Security* 22, no. 5 (2003): 423-434.

[10] Ross, Timothy J. *Fuzzy logic with engineering applications*. John Wiley & Sons, 2009.

[11] Singh, Khundrakpam Johnson, and Tanmay De. "An Approach of DDOS Attack Detection Using Classifiers." In *Emerging Research in Computing, Information, Communication and Applications*, pp. 429-437. Springer India, 2015.