Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DENIAL OF SERVICE ATTACK DETECTION USING TRAPEZOIDAL FUZZY REASONING SPIKING NEURAL P SYSTEM

[1]RUFAI KAZEEM IDOWU, [2]RAVIE CHANDREN M. [3]ZULAIHA ALI OTHMAN

[1, 2]Centre for Software Technology & Management (SOFTAM), Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia (UKM)

[3]Centre for Artificial Intelligence Technology (CAIT), Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia (UKM)

E-mail: [1]ruffyk2001@yahoo.com, [2]ravie@ukm.edu.my, [3]zao@ukm.edu.my

ABSTRACT

Although 'Intrusion' is considered to be a bitter pill to swallow due to the havoc it unleashes on the cyber space, but it has become a household name to cyber-security experts because it appears to rebuff all possible solutions! Consequent upon this, there have been unrelenting efforts to reduce its negative impacts to the lowest ebb by the introduction of various Intrusion Detection Systems (IDS). Meanwhile, Spiking Neural P (SN P) system, a variant of Membrane Computing (MC), has proved to be a versatile class of distributed parallel computing model which embeds the idea of spiking neurons into P systems. Therefore, in this work, we have explored trapezoidal Fuzzy Reasoning Spiking Neural P (tFRSN P) system, which is an extension of SN P system in attack detection. Specifically, the focus is on detecting Denial-of-Service (DoS) attack with emphasis on SYN (synchronize) flood. Consequently, KDD Cup benchmark dataset was used for evaluation in series of experiments conducted. While we obtained very low False Negatives (FN) and False Positives (FP) of 0.02% and 0.25% respectively, the True Positives/Negatives were equally very high. These results have further lent credence to the fact that MC and indeed SN P system are yet-to-be tapped goldmine as far as Intrusion Detection is concerned.

Keywords: *SNP Systems, Attack Detection, Fuzzy Reasoning, Denial-of-Service, Membrane Computing.*

1. INTRODUCTION

Membrane computing despite the fact that it is just about a decade old, it is presently being applied to several fields. Spiking Neural P System *c*ombines the ideas of P systems and that of spiking neur*ons*. Simply put, Spiking neural P systems (SNPS) are a class of distributed and parallel computing models that incorporate the idea of spiking neurons into P systems [1]. Primarily, in SNP Systems, the process of information passage among neurons otherwise known as neuronal behaviours, is simulated. This is because it is believed that electrical impulses called spikes (carrying vital information) found in the neurons are exchanged when the axons of two or more neurons are linked via synapses. On the other hand, *Denial-of-Service (DoS)* attacks are now being accorded much attention simply because of the havoc it renders to the information system, since they are so easy to propagate. A DoS attacker may employ different tactics to render havoc on an information system. These include;

(i) bombarding the target machine with the sole aim of overwhelming it by generating a lot of meaningless and unimportant traffic
(ii) Crashing the target system by exploiting its software bug.

In all, DoS attacks make computing/memory resource to be fully engaged and disrupting its normal operation thereby denying its availability to legitimate users. Usually, a typical network is compromised and rendered inefficient with the influence of DoS attack type. This is because a simple DoS attack normally generates large amounts of traffics which are sent to the target machine [2]. Limitations in the TCP/IP protocols of a network are usually exploited by many of the DoS attacks, including Ping of Death and Teardrop.

Therefore, when one takes a deeper look at past works on fuzzy system and IDS, there is every need to propose a better method through which membership functions of network attacks (especially DoS attacks) could be intuitively and easily defined. Consequently, this research work

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

introduces a novel approach which engenders large data/packets handling in parallel manner and better means of knowledge representation in network systems.

The remaining part of this paper is structured as follows: Section 2 gives a brief description of related works. In section 3, a detailed analysis of DoS attack is presented. The link between SN P System and tFRSN P system is established in section 4. Meanwhile section 5 highlights the methodology adopted in the research work. The results of the experiments were presented and discussed in section 6. Finally, section 7 gives the summary and concludes the work.

2. RELATED WORKS

Since over a decade ago when Membrane computing with its variants (including Spiking Neural P systems) made its debut, it has severally been applied probably due to its versatility. Gexian et al [1] proposed an extended spiking neural P system (ESNPS) by introducing the probabilistic selection of evolution rules and multi-neurons output and a family of ESNPS, called optimization spiking neural P system (OSNPS). These were further designed to adaptively adjust rule probabilities to approximately solve combinatorial optimization problems. On the other hand, Lei and Peter [3] addressed the problem of maximal independent set (MIS) selection in a graph in order to choose a set of nonadjacent nodes to which no further nodes can be added. So, they designed a class of simple neural-like P systems to solve the MIS selection problem efficiently in a distributed way.

However, from another perspective, in the work by Peng et al [4], Fuzzy Reasoning Spiking Neural P system with real numbers (rFRSN P system) was used for fault diagnosis thereby adding more to the literature on knowledge representation and reasoning. Also, in the efforts by Wang and Zhang [5], a fuzzy reasoning SN P system with trapezoidal fuzzy numbers in which a matrix-based fuzzy system based on the dynamic firing mechanism of neurons, was applied for fault diagnosis. More recently and in a related development for the very first time, Rufai et al [6] advocated the use of fuzzy reasoning spiking neural P system for detecting intrusion with specific emphasis on Brute Force Attack (BFA).

As it relates to DoS however, literatures abound including those by Dong [7] in which taxonomy of DoS detection was presented thus (Fig. 1):

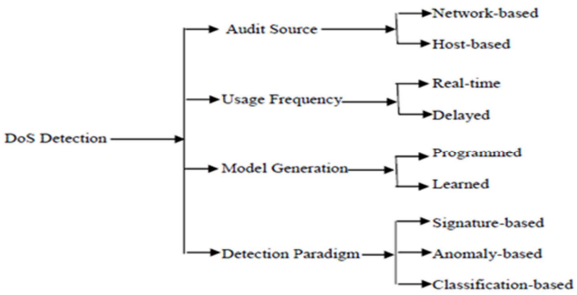


Fig 1: Taxonomy Of Dos Attacks Detection

An approach for detecting a Distributed Denial of Service (DDoS) attack using a fuzzy estimator on the mean time between network events was proposed by Stavros et al [8]. Quite well, before a victims machine suffers from resources exhaustion as a result of the attack, however, their technique could flag the malicious IPs and detect DDoS attack. Similarly, the idea of using a Genetic Algorithm (GA) based approach, for generation of rules to identify DoS attacks on the system was put forward by Anurag and Arvind [9]. In another dimension, Phyu and Kyaw [2] explored feature selection and classification methods for Denial-of-Service (DoS) attacks detection using with Random Forests (RDF) and k-Nearest Neighbor. Also, Peng and Yan [15], deduced normalized population diversity degree for identifying DDoS attacks under the complex network structure by employing an improved PSO-SVM (Particle Swarm Optimization Support Vector machine) algorithm. In the research work about DDoS carried out by Saravanan and Venkatachalam [16], statistical discrete wavelet transform was applied for the option fields of traffic stream identifier, internet time stamp, recording of data transmission route, and the flagging of loose and strict source routing. By so doing, some attacks were instantly detected within few seconds while some others could not until there was an aggregate consideration of a vast collection of events.

Generally, previous approaches are still considered to be deficient in their detection rate especially when large data is involved. Furthermore, for fuzzy detection approaches, understandability of membership function definition remains a concern. So, this approach addresses these gaps.

Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. DENIAL OF SERVICE ATTACKS

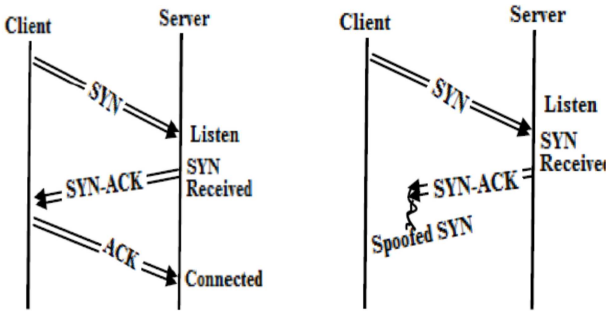
DoS is a grave network attack type which denigrates the network by flooding it with useless traffic which ultimately results in a compromised information system. It adopts the method of disallowing legitimate users of the information system from gaining access to it [7; 9; 10; 14].

Table 1: Identification Of Some Dos Attacks

TYPE	METHOD USED	HAVOC RENDERED	DETECTION	PREVENTION
Tear-drop	Sending of mangled IP fragment with overlapping	Crashing O/S, hence reboots the system.	Observation of Fragmentation flag in IP packet header.	O/S upgrade
ICMP Flood	Sending ICMP echo requests	Consume network bandwidth	Identifying packets with spoofed source address.	Filtering out ICMP packets
SYN Flood	Initiates many incomplete TCP connections	Denying legitimate traffic	If TCP 3-way handshake process can't be completed.	Hard to prevent so as not to disallow legitimate traffic
Ping of Death	Sending oversized ping packet	Crashing O/S	Looking for oversized ICMP packet.	O/S upgrade

3.1 SYN Flooding DoS Attack

The premise of a flood DoS attack is simple, send more requests to the machine than it can handle and then make it unusable! Ideally there should be a perfect synchronization of packets in a client-server relationship on the network. However, when a SYN flooding attack is to be perpetuated, the Transmission Control Protocol (TCP)s three-way handshake mechanism is exploited. A server normally reciprocates a SYN request made by a client with a SYN-ACK packet. This is also in turn, should be acknowledged by the client by sending back an ACK packet which signifies a perfect connection (Fig 2 (a)). Meanwhile, if the SYN request is spoofed, then the handshake process would never be achieved. This is because the connections are half-opened and server resources are being consumed (Fig 2 (b)). By this singular act, backlog queues limit would be reached, hence subsequent connection requests dropped [11; 12].



(a) (b)

Fig 2: (a) Attack-free TCP 3-Way Handshake (b) DoS flooding-attacked system

4. LINKING SN P SYSTEM AND tFRSN P SYSTEM

tFRSN P system is an extension of SN P system which allows some other elements to be succinctly defined. .

4.1 The SN P System

Spiking Neural P system is a non deterministic class of membrane computing systems which is similar to other P system variants such as Tissue-like and Cell-like. In general, an SN P system of degree m ≥ 1 is a construct of the form [17]:

$$\prod = (O, \sigma_1 \ldots\ldots \sigma_m \text{ syn, out}),$$

Where:

1. $O = \{a\}$ is the singleton alphabet. (a is called spike);
2. $\sigma_1, \ldots\ldots, \sigma_m$ are neurons, of the form $\sigma_1 = (n_i, R_i)$, $1 \le i \le m$, where:
   $n_i \ge 0$ is the initial number of spikes contained by the neuron;
   R_i is a finite set of rules of the following two forms:
   (i) $E/a^c \rightarrow a^p$;d, where E is a regular expression over O, $c \ge p \ge 1$, and $d \ge 0$;
   (ii) $a^s \rightarrow \lambda$, for some $s \ge 1$, with the restriction that as L€ for no rule E/a^c a; d of type (1) from R_i;
3. syn $\subseteq \{1, 2, \ldots., m\} \times \{1, 2, \ldots., m\}$ with $(i, j) \in$ syn, for $1 \le i, j \le m$ (synapses);

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. in, out respectively indicate the input and output neuron sets of $\prod$.

The rules of type (i) are called *spiking rules*, which is written in a shorthand notation as $a^c \rightarrow a^b$. The rules of type (ii) are referred to as *forgetting rules*. However, the neurons content determines how the rules are applied. By extension, it means that based on the total number of spikes contained in the neuron, the invocation of a rule is established. For the purpose of removing a predefined number of spikes from a neuron, the forgetting rule is possibly applied if no further spiking/firing rule could be applied at that computational instance.

4.2 The tFRSN P system

Typically, Fuzzy Reasoning is concerned with the process of firing and execution of the fuzzy rule which triggers when the consequent part of the IF-Then rule when the condition is met.

A tFRSN P system of degree m $\geq$ 1 [5], is a construct of the form:

$$\prod = (O , \sigma_1, \ldots , \sigma_m, syn, in, out)$$

where:

1) $O = \{a\}$ is the singleton alphabet (a is called spike);
2) $\sigma_1 , \ldots , \sigma_m$ are neurons of the same form

$$\sigma_i = (\theta, c_i, r_i), 1 \leq i \leq, m,$$

where:

i) θ_i is the potential value of spikes (i.e. pulse value) contained in neuron σ_i, and it is expressed by a trapezoidal fuzzy number in [0,1];
ii) c_i can be understood as either the fuzzy truth value of a proposition (when σ_i corresponds to a proposition neuron) or the certainty factor of a production rule (when σ_i corresponds to a rule neuron), and it is expressed by a trapezoidal fuzzy number in [0,1];
iii) r_i represents a firing or spiking rule contained in neuron σ_i with the form $E / a^{\theta} \rightarrow a^{\beta}$, where E ($E = a^n$) is the firing condition, and n is the number of presynaptic neurons connected to neuron σ_i which is expressed by an integer, θ and β are expressed by trapezoidal fuzzy numbers in [0, 1].

3) syn $\subseteq \{1,2,...,m\} \times \{1,2,...,m\}$, with $i \neq j$ for all $(i, j) \in syn$, $1 \leq i, j \leq m$, is a directed graph of synapses between the linked neurons;
4) *in*, *out* respectively represent the input and output neuron sets of $\prod$.

5. METHODOLOGY

In this work, the rule-based tFRSN P system method was applied to IDS with specific emphasis on DoS attack. Here, the rules were designed based on most significantly relevant features to DoS which could be found in KDD cup dataset [13]. Consequently, the experiments were carried out using CORE i5-2450M CPU 2.50 GHZ with 4.00 GB RAM, Windows 7 Home Premium. Matlab was adopted as the implementation programming language. Its mamdani inference mechanism was adapted to handle the reasoning using the four features of duration, src_bytes, dst_bytes and count.

The data used in this work which serves as benchmark dataset for IDS implementation is the widely available KDD CUP 1999 dataset which was created from DARPA Intrusion Detection Evaluation Program by MIT Lincoln Laboratory. Original KDD CUP 1999 dataset, consists of about 5 million connection records and 41 features. However, because the dataset was too large to analyze, concise set of 10% of it (as it is usually the practice) was used.

5.1 Assumptions, Definitions and Rules' Generation

5.1.1 Assumptions

In order that the IDS may attain high efficiency in detecting misuse of the computational resources, it is greatly essential that important and relevant features are identified from the network traffic data [10]. Although from the literature, there are no agreed number features that could be used to define DoS attacks, however, the following are some of the identified attributes. These include: Duration, Protocol_type, Service, Flag, Src_Bytes, Dst_Bytes, Land, Wrong_Fragment, Num_Compromised, Count, Srv_Count, Serror_Rate, Srv_Error and Dst_Host_Count. In this work therefore, the most significant attributes were used for our rule generation. These features as found in KDD Cup dataset are:

Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Duration: Length of connection made. It has label 1 out of the 41 features.

Src_bytes: This is the fifth feature which represents the number of data bytes sent from the source to destination machine.

Dst_bytes: This 6th feature carries the number of data bytes from the destination to source machine.

Count: Number of connections to the same host as the same service/connection within a given time interval (probably two seconds). The feature is labeled 23.

Table 2: Membership Terms of the Fuzzy Rules

Linguistic Terms					Trapezoidal Fuzzy Numbers
Src_bytes	Duration	Dst_bytes	Count	Attack Possibility	
AS	AT	AS	AS	AF	(0, 0, 0, 0)
VS	VT	VS	VS	VL	(0, 0, 0.02, 0.07)
S	T	S	S	L	(0.04, 0.1, 0.18, 0.23)
MS	MT	MS	MS	ML	(0.17, 0.22, 0.36, 0.42)
M	M	M	M	M	(0.32, 0.41, 0.58, 0.65)
ME	MG	ME	ME	MH	(0.58, 0.63, 0.80, 0.86)
E	G	E	E	H	(0.72, 0.78, 0.92, 0.97)
VE	VG	VE	VE	VH	(0.975, 0.98, 1, 1)
AE	AG	AE	AE	AH	(1, 1, 1, 1)

HINT: AS=Absolutely Small, VS=Very Smal, MS=Medium Small, M=Medium, ME=Medium Large, E=Large, VE=Very Large, AE=Absolutely Large, AT=Absolutely Short, VT=Very Short, VG=Very Long, H=High, E=Large, AF=Absolutely False, L=Low, S=Small

5.1.2 Definitions and Rules' Generation

For the purpose of detecting the DoS attack,

(a) the type of composite conjunctive fuzzy production rule below is applied:

$$R_i(c_i): p_1(\theta_1) \textcircled{\wedge} p_2(\theta_2) \textcircled{\wedge} \ldots \textcircled{\wedge} p_{k-1}(\theta_{k-1}) \rightarrow p_k(\theta_k);$$
$$\theta_k = (\theta_1 \wedge \theta_2 \wedge \ldots \wedge \theta_{k-1}) \textcircled{x} c_i$$

(b) several rules were generated with the aid of tFRSN P system using the four identified features. These rules include:

(i) If Duration = G, Src_bytes = E, Dst_bytes = MS and Count = E
Then DoS is highly likely (MH)

(ii) If Duration = MG, Src_bytes = ME, Dst_bytes = M and Count = S
Then DoS is not suspected (L)

(iii) If Duration = M, Src_bytes = ME, Dst_bytes = M and Count = ME
Then DoS is probable (M)

(iv) If Duration = VG, Src_bytes = VE, Dst_bytes = S and Count = E
Then DoS is indisputably confirmed (AH)

(v) If Duration = MG, Src_bytes = E, Dst_bytes = MS and Count = ME
Then DoS is very unsuspected (VL)

5.2 tFRSN P system's Architecture and Model for DoS

5.2.1 tFRSN P System's Architecture

The architecture of the tFRSN P system shown in Fig. 3 begins by garnering the network traffic and subsequently analyzing it for the purpose of selecting the very important and highly relevant features which were needed for detecting the attacks. This stage is crucial because if redundant or irrelevant features were selected, they would consequently have negative impact on the final accuracy of detection. Within the second sub-system called reasoning/detection, several activities take place here. These include data normalization, fuzzy membership terms' determination, rule definition and application, reasoning, which eventually lead to the generation of fuzzified and defuzzified values for the attacks.

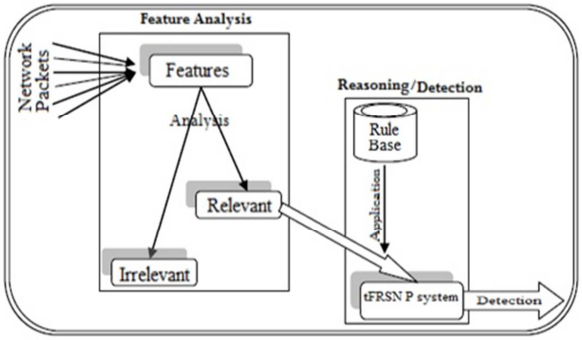


Fig. 3: Tfrsn P System's Architecture

5.2.2 DoS Attack-tFRSN P System's Model:

As captured below in Fig 4, the tFRSN P system's model for DoS attack has its fuzzy production rules defined as a construct:

$$\prod = (O, \sigma_1, \ldots, \sigma_{18}, \sigma_{19}, \ldots, \sigma_{23}, syn, in, out)$$

Where

(1) $O = \{a\}$

(2) $\sigma_1, \ldots, \sigma_{17}$ are proposition neurons having fuzzy truth values $p_1, \ldots, p_{17}$ respectively.

(3) $\sigma_{18}, \ldots, \sigma_{21}$ are "AND" –type rule neurons associated with production rules $R_1, \ldots, R_4$ respectively.

Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(4) *syn* = {(1,19), (2,20), (2,23), (3,21), (4,22), (5,19), (5,23), (6,20), (6,21), (7,22), (8,19), (8,23), (9,20), (9,21), (10,22), (11,19), (11,22), (12,20), (13,21), (13,23), (19,14), (20,15), (21,16), (22,17), (23,18)}

(5) *in* = $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}\}$
out = $\{\sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}\}$.

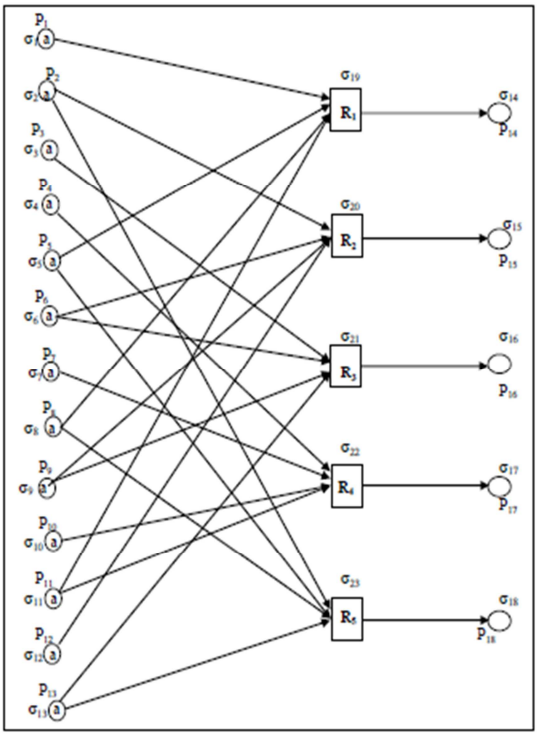


Fig. 4: tFRSN P System's Model for DoS Attack

6. RESULTS AND DISCUSSION

From the results obtained after the implementation using 10% of KDD Cup dataset, we establish here that our system performed well in the detection process. We employed the confusion matrix *CM* in Table 3 below. A CM is a square matrix in which each column corresponds to the predicted class, while rows correspond to the actual classes. An entry at row *i* and column *j*, *CM* (*i, j*), represents the number of erroneously classified instances that originally belong to class *i*, although wrongly identified as a member of class *j*. The entries of the primary diagonal, *CM (i,i)*, stand for the number of appropriately detected instances.

Table 3: Confusion Matrix

Actual	Predicted Normal	Predicted Attack
Normal	TP (19.35%)	FP (0.25%)
Attacks	FN (0.02%)	TN (80.37%)

As shown above, while 0.02% and 0.25% were flagged as False Negatives and Positives respectively, 19.35% and 80.37% were returned as True Positives and Negatives respectively.

Although, False Negative (FN) has a more dire consequence when compared to False Positive (FP), however, neither of them is desirable. Meanwhile, after our experiments, and by applying tFRSN P systems combined with fuzzy logic, many real attacks were captured in the dataset used (as TN returns the highest value). This is not unconnected to the fact that about 20% of the 10% of the KDD Cup dataset used ordinarily constitutes normal (i.e non-intrusive) traffic. Furthermore, the percentage of most dangerous FN which managed to escape undetected by our system was just 0.02%. Fig. 5 below also depicts the scenarios.

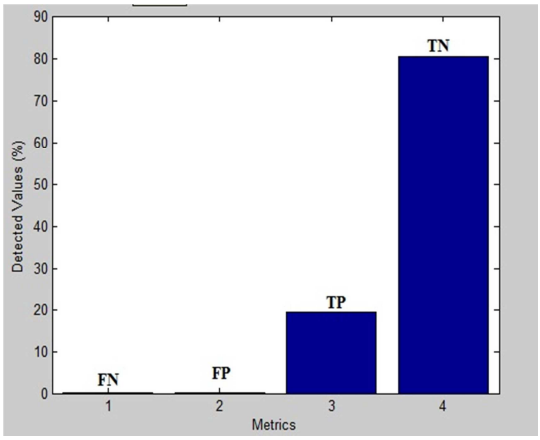


Fig. 5: Graph of Detected values of Metrics

Going a step further, applying the FN, TN, TP and FP obtained in the CM above to Attack Detection Rate (ADR) and False Alarm Rate (FAR), using the formulae:

$$\textbf{Detection Rate} = \frac{\textbf{TP}}{\textbf{TP + FN}} \quad (1)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\text{False Alarm Rate} = \frac{FP}{FP + TN} \quad (2)$$

we obtained 99.88% and 0.31% for ADR and FAR respectively.

7. CONCLUSION

From the experiments conducted so far, tFRSN P system has once again demonstrated its suitability for solving optimization problems. In this work, a DoS attack was detected by combining the powers of SN P system with fuzzy logic. The results obtained were promising with very high ADR and extremely low FAR.

In summary, the contributions of this article, among others, include:

- Proposing of architecture for the detection of DoS by using tFRSN P system. This applies a trapezoidal Fuzzy Reasoning Spiking Neural P system to detect intrusive traffic in a rule-based environment of a network detection intrusion system.
- Modeling the knowledge base and defining the membership functions of a DoS in a very intuitive, and remarkably simple and understandable form.
- Analyzing and processing large numbers of network packets at a high speed.

With the success recorded using this approach, it is hereby suggested to IDS researchers that more efforts may now be devoted to both hardware (e.g GPU) and software (e.g MC) platforms which support parallelization to further curtail the problem of data dropping arising from large data handling. This becomes very expedient now because the network super highway increases greatly by the day.

The major drawback of this work is that it is only limited to existing and known attacks. By implication therefore, it implies that new attacks may escape without any detection alarm being raised. However, our future work would explore the possibility of applying the model (i.e tFRSN P System) to other classes of attack such as User-to-Root (U2R), Remote-to-Local (R2L) and Probing attacks.

ACKNOWLEDGEMENTS

The authors wish to thank the Faculty of Technology and Information Science, of the Universiti Kebangsaan Malaysia (National University of Malaysia). This work was supported in part by a grant from Grant Code: FRGS/1/2012/SG05/UKM/02/3

REFRENCES:

[1] Gexiang Zhang, Haina Rong, Ferrante Neri, Mario J. Pre-Jimnez: "An Optimization Spiking Neural P System for Approximately solving Combinatorial Optimization Problems", *International Journal of Neural Systems*, Volume 24, Issue 05, 2014.

[2] Phyu Thi Htun and Kyaw Thet Khaing: "Detection Model for Daniel-of-Service Attacks using Random Forest and k-Nearest Neighbors". *International Journal of Advanced Research in Computer Engineering and Technology* (IJARCET) Volume 2, No 5, May 2013.

[3] Lei Xu, Peter Jeavons: "Simple Neural-Like P Systems for Maximal Independent Set Selection". *Neural Computation* June 2013, Vol. 25, No. 6, Pg. 1642-1659. February 25, 2015.

[4] Peng H., Wang J., Mario J. Perez-Jimenze, Wang H., Shao J., Wang T.: "Fuzzy Reasoning Spiking Neural P System for Fault Diagnosis". *Information Sciences* 235(20), (2013)106-116.

[5] Wang T., Zhang G.: "Application of Fuzzy Reasoning Spiking Neural P System to Fault Diagnosis". *2nd Asian Conference on Membrane Computing, (2013).*

[6] Rufai K.I., Ravie C. M., Zulaiha A.O. : "Advocating the use of Fuzzy Reasoning Spiking Neural P system in Intrusion Detection". *3rd Asian Conference on membrane Computing* 18th-19th Sept, 2014. pg 201-209.

[7] Dong Lin: 'Network Intrusion Detection and Mitigation against Denial of Service Attack". WPE-II Written Report submitted to Department of Computer and Information Science, University of Pennsylvania. USA (2013)

[8] Stavros N. Shiaeles, Vasilios Katos, Alexandros S. Karakos, Basil K. Papadopoulos: "Real time DDoS Detection using Fuzzy Estimators". *Computer and Security* 31 (2012) Pg. 782 - 790.

[9] Anurag Andhare, Arvind Bhagat Patil: "Mitigating Denial-of-Service Attacks Using Genetic Approach". *IOSR Journal of Engineering* Mar. 2012, Vol. 2(3) pp: 468-472.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] Srinivas Mukkamala, Andrew H. Sung: Detecting Denial of Service Attacks Using Support Vector Machines.

[11] Zhengmin Xia, Songnian Lu, Jianhua Li: "Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic". *Informatica* 34 (2010) Pg 497 507.

[12] Haining Wang Danlu Zhang Kang G. Shin: "Detecting SYN Flooding Attacks". In *Proceedings of the IEEE Infocom. IEEE*, 2002 pp 1530 - 1539

[13] KDD Cup99 Dataset, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (1999).

[14] Usman Tariqa, Yasir Malik, Bessam Abdulrazak: "Defense and Monitoring Model for Distributed Denial of Service Attacks". The *2nd International Workshop on Internet of Ubiquitous and Pervasive Things* (IUPT 2012)

[15] Peng Yu, Yan Li: "A Novel DDoS Prediction Method Based on Population Entropy with Improved PSO-SVM Algorithm". *Journal of Computational Information Systems* 9: 10 (2013) pp. 41734183

[16] K. Saravanan, R. Asokan and K. Venkatachalam: "Detection mechanism for distributed denial of service (DDoS) attacks for anomaly detection". *Journal of Theoretical and Applied Information Technology*. Feb. 2014. Vol. 60 No.1

[17] Gheorghe Paun: Spiking Neural P Systems. A Tutorial Journal Bulletin of the European Association for Theoretical Computer Science, 2007, pp. 145-159.