FACTA UNIVERSITATIS
Series: **Mechanical Engineering** Vol. 12, N° 2, 2014, pp. 183 - 193

Original scientific paper

DFCL: DYNAMIC FUZZY LOGIC CONTROLLER FOR INTRUSION DETECTION

UDC [004.77+004.8]:681.5

Abdulrahim Haroun Ali[1], Shahaboddin Shamsirband[1], Nor Badrul Anuar[1], Dalibor Petković[2]

[1]Department of Computer System & Technology, University of Malaya,
[2]University of Niš, Faculty of Mechanical Engineering, Department for Mechatronics

Abstract: *Intrusions are a problem with the deployment of Networks which give misuse and abnormal behavior in running reliable network operations and services. In this work, a Dynamic Fuzzy Logic Controller (DFLC) is proposed for an anomaly detection problem, with the aim of solving the problem of attack detection rate and faster response process. Data is collected by PingER project. PingER project actively measures the worldwide Internet's end-to-end performance. It covers over 168 countries around the world. PingER uses simple ubiquitous Internet Ping facility to calculate number of useful performance parameters. From each set of 10 pings between a monitoring host and a remote host, the features being calculated include Minimum Round Trip Time (RTT), Jitter, Packet loss, Mean Opinion Score (MOS), Directness of Connection (Alpha), Throughput, ping unpredictability and ping reachability. A set of 10 pings is being sent from the monitoring node to the remote node every 30 minutes. The received data shows the current characteristic and behavior of the networks. Any changes in the received data signify the existence of potential threat or abnormal behavior. D-FLC uses the combination of parameters as an input to detect the existence of any abnormal behavior of the network. The proposed system is simulated in Matlab Simulink environment. Simulations results show that the system managed to catch 95% of the anomalies with the ability to distinguish normal and abnormal behavior of the network.*

Key Words: *Intrusion detection, Fuzzy system, PingER, Round Trip Time (RTT), Packet Loss*

Received June 21, 2014 / Accepted July 11, 2014
Corresponding author: Abdulrahim Haroun Ali
University of Malaya, Department of Computer System & Technology, Kuala Lumpur, Malaysia
E-mail: Haroun@gmail.com

1. INTRODUCTION

An anomaly is a deviation of normal behavior or common order. In computer networks, the behavior tends to follow a specific pattern. The followed pattern is due to the network operation time, user's activities or network usage policies. Network Base lining is a common technique for identifying the network behavior. In the case of attacks or network faults, the network behavior tends to be anything but normal. Hence it's a worthwhile approach to indicate the presence of attacks or faults. Ref. [1] suggests that Intrusion Detection System (IDS) uses an anomaly detection approach to estimate the normal behavior. Any deviation that exceeds predefined threshold is considered malicious. Unlike signature-based Intrusion Detection System, the anomaly detection approach is capable of detecting new attacks.

Network Anomalies is experienced due to internal and external factors. Internal factors include failure of network nodes or overload of traffic in network nodes. Network node such as router which is under pressure of handling traffic beyond its capabilities automatically delays the response time of networks or drop the extra packets. External factors are commonly described as attacks such as Denial of Service (DoS) attacks. Denial of Service (DoS) attacks floods the network with unwanted packets that fill up the host memory buffer to make the network unable to process any request. In DoS attacks, the response time of the network and packet loss are rapidly rising and it results in an abnormal behavior of the network.

In this paper, Dynamic Fuzzy Logic Controller (DFLC) mechanism is proposed to monitor and detect network abnormalities. Basically, fuzzy logic is a precise logic of imprecision and approximate reasoning [3, 8, 9, 10]. It is widely used in different research disciplines as potential solution [11, 12, 13, 14]. Ref. [2] suggests the use of fuzzy logic in controlling traffic in broadband communication networks. Ref. [4] shows how fuzzy logic technique is used for correcting climatological ionosphere models. The proposed Dynamic Fuzzy Logic Controller consists of a number of fuzzy logic rules that precisely detect any network abnormalities.

In order to evaluate the proposed system, this study uses PingER data. PingER project is Ping end-to-end Reporting network monitoring infrastructure. It uses a ping computer program to measure the performance of several networks around the world. A *ping* involves sending an Internet Control Messages Protocol (ICMP) echo request [1] to a specified remote node which responds with an ICMP echo reply [5]. PingER performance parameters include round trip time (RTT), packet loss, jitter, mean opinion score (MOS), ping predictability, ping reachability, zero packet loss frequency, directivity and TCP throughput. PingER is currently active in over 168 countries around the world. Malaysia alone is having three monitoring host and more than 30 remote hosts.

The objective of this study is to detect a network anomaly using Dynamic Fuzzy Logic Controller (DFLC). All PingER matrices contribute to the normal behavior of the network. Unconditional changes in any of the matrices indicate abnormal behavior and hence it needs attention to prevent the network from potential threat of faults. DFLC is used for deciding whether the received matrices indicate a threat or safety.

This paper is organized as follows. Section 2 discusses literature review. Section 3 explains the architecture of the proposed DFLC system. Section 4 shows the results of the experiment and comparisons. Section 5 concludes the paper with discussion and conclusion.

2. RELATED WORK

PingER is a network monitoring infrastructure which sends a set of 11 pings of 100 byte packet size, followed by 10 pings of 1000 byte packet size from a monitoring host to a remote host at an interval of 1 second [5]. From the ping, ICMP packets returns two vital network performance parameters; round trip time and packet loss. Round trip time (RTT) is the time taken for the packet to be accepted by the router interface, any delays caused by queuing, and the time taken for the packet to be transmitted from the interface [5]. Round trip time needs to be very low for application; as such it requires high level of interactivity such as telnet, voice or video communications. Is it impossible to reduce RTT to less than the time taken by the medium to transmit data? In fiber networks, RTT is impossible to be less than the time taken for light to travel the distance along the fiber [5]. Packet loss is a parameter that gives a clear picture of congestions in network nodes. If a network node is congested (buffer is full), it discards all extra packets [6].

Ping program used in PingER, allows a number of other useful matrices to be calculated. It includes Ping Unpredictability which is derived from a calculation based on the variability of packet loss and round trip time [7]. Ping Unreachability which measures the extent of unreachability of the monitored host, if all 10 pings did not receive a reply the remote host would be declared unreachable. The opposite parameter of ping unreachability is Quiescence, if all 10 pings have received a reply the node or network is considered quiescence (non busy). Among other parameters are TCP throughput, Mean Opinion Score (MOS), Directivity which calculates how direct the link between Monitoring host and the remote host is.

PingER project methodology needs to take into consideration two major limitations; periodic sampling and the use of ICMP packets [5]. Periodic sampling allows ping to be sent at regular interval in order to understand the network performance. Hence, all network activities happening at a time outside the period of sampling are not going to be recorded. Also rare activities that can only occur during the period of sampling may result in making the network to be marked as poorer than it really is. The use of ICMP packets results in another limitation to PingER methodology due to its features in a network. In the networks which implements Quality of Service (QoS), ICMP packets are given low priority compared to other ones like TCP and UDP in the network. Some network blocks ICMP packets prevent the network from network attacks such as smurf attack uses ICMP packets [5].

3. METHODOLOGY

The Fuzzy Logic-Risk Analysis model is built on the following constituent parts and logic: Fuzzy linguistic variables and fuzzy expression for input and output parameters are shown in Table 1. For each variable, three membership functions are used which are Low, Medium, and High for inputs. The output variable (Output) uses only two membership functions, Normal and Abnormal. The characteristics of the Inputs and Output variables are shown in Table 1.

Table 1 Fuzzy linguistic and abbreviation of variables for each parameter

Inputs		Range
Parameters	Linguistic variables	
Maximum RTT		0–100
Minimum RTT	Low, Medium, High	0–100
Average RTT		0–100
Packet Loss		0–100
Outputs		
Output	Abnormal, Normal	0–1

The four inputs will be defined as Maximum RTT (which is the maximum Round Trip Time received after sending the 10 ping request), Minimum RTT (which is the minimum Round Trip Time received after sending the 10 ping request), Average RTT (which is the average Round Trip Time of the received 10 ping's reply) and Packet Loss (which is the percentage of packet lost during the 10 ping request and reply). A valid range of input is considered and divided into three classes, or fuzzy sets for all the inputs. Table 6 shows the range is low, medium and high for each input. Membership functions for input and output fuzzy model.

In choosing the membership functions for fuzzification, the event and type of membership functions are mainly dependent upon the relevant event. In this model, Gaussian-shaped membership function is employed to describe the fuzzy sets for input; for output variable triangular-shaped membership function is used [8, 9, 10]. The input variables have been partitioned according to the experiment parameter ranges. The degree of belongingness of the values of the variables to any selected class is called the degree of membership as shown in Fig. 3. The output defined in fuzzy sets "Normal" means the input from four features received indicate no anomaly, hence it is safe. While "Abnormal" meaning that there input received indicates the detection of abnormal behavior of the network.

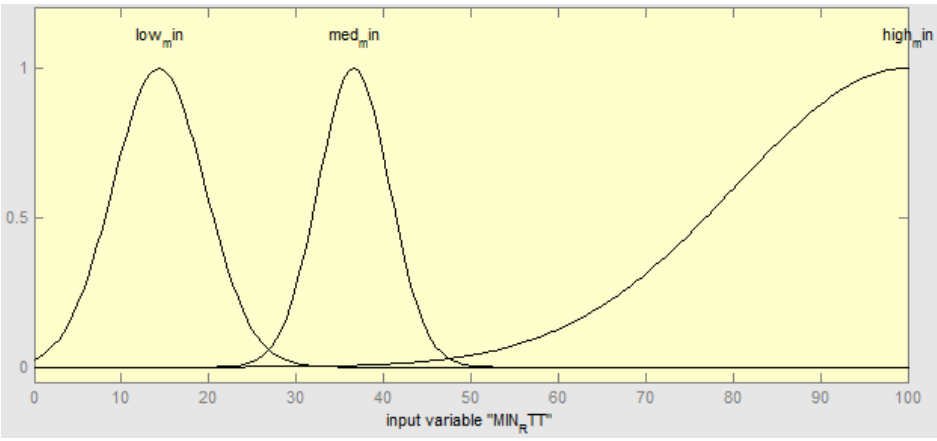

Fig. 1 Membership function Minimum RTT (Inputs MF)

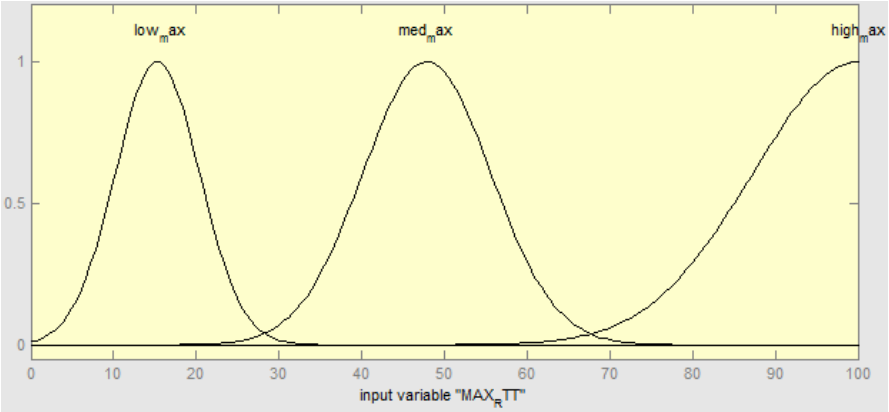

Fig. 2 Membership function Maximum RTT (Inputs MF)

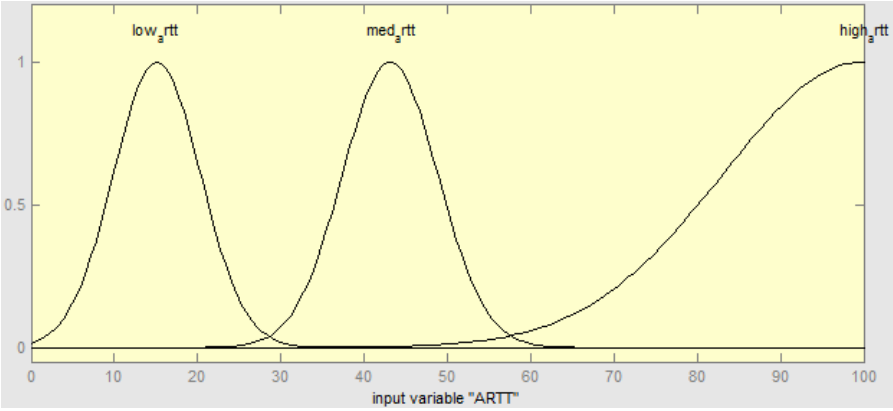

Fig. 3 Membership function Average RTT (Inputs MF)

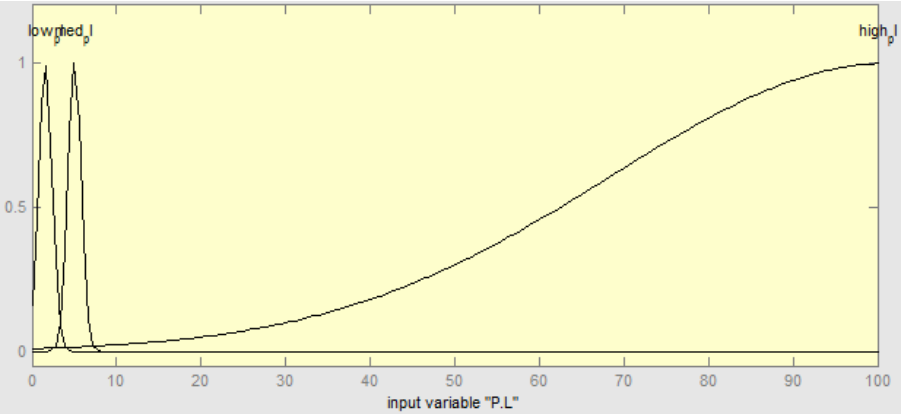

Fig. 4 Membership function Packet Loss (Inputs MF)

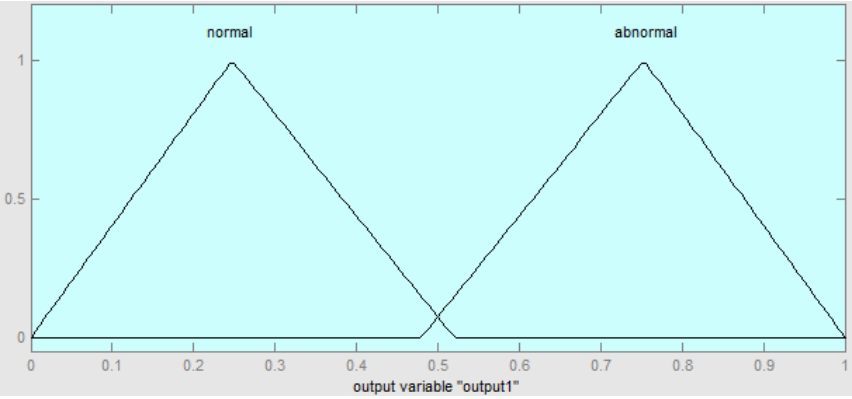

Fig. 5 Membership function represents Countermeasure (Output MF)

Expert knowledge is used to characterize inputs and outputs and connect the inputs and outputs by a set of inference rules using if/then statements; according to the number of the fuzzy sets of the inputs. The system will have sixteen possible combinations (inference rules). The fuzzy output set is the indication of the existence of an anomaly from the input received by the system. Fuzzy Inference System (FIS) for input and output parameters is shown in Fig. 6.

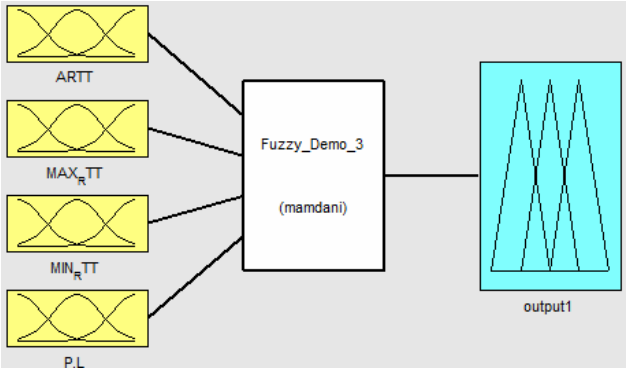

Fig. 6 Fuzzy Inference System

5. Structure of Fuzzy Rules

The type of the response of the Anomaly Detection System will be based on the calculated Average RTT, Minimum RTT, Maximum RTT and the Packet Loss. For example, if the packet loss is low while any of the remaining inputs is high, then the system will indicate an anomaly. If all four inputs are low, then the system will indicate it as a normal behavior of the network, hence no anomaly. The opposite of that (previous example) means that definitely the system will indicate anomaly. This methodology will catch any abnormal behavior of the network.

A set of 16 rules have been constructed based on the actual experimental qualitative analysis shown in Table 2 and the characteristics of the inputs and output variable are shown in Table 2. Experimental results are simulated in the Matlab using Matlab Simulink.

Table 2 The pseudo code for Dynamic Fuzzy Logic Anomaly Detection (DFLAD)

1. If (ARTT is low_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is normal)
2. If (ARTT is high_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is abnormal)
3. If (ARTT is med_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is normal)
4. If (ARTT is low_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is med_pl) then (output1 is abnormal)
5. If (ARTT is low_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is high_pl) then (output1 is abnormal)
6. If (ARTT is high_artt) or (MAX_RTT is high_max) or (MIN_RTT is high_min) or (P.L is high_pl) then (output1 is abnormal)
7. If (ARTT is med_artt) and (MAX_RTT is med_max) and (MIN_RTT is med_min) and (P.L is low_pl) then (output1 is normal)
8. If (ARTT is low_artt) and (MAX_RTT is low_max) and (MIN_RTT is med_min) and (P.L is low_pl) then (output1 is normal)
9. If (ARTT is low_artt) and (MAX_RTT is med_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is normal)
10. If (ARTT is low_artt) and (MAX_RTT is med_max) and (MIN_RTT is med_min) and (P.L is low_pl) then (output1 is normal)
11. If (ARTT is med_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is normal)
12. If (ARTT is med_artt) and (MAX_RTT is low_max) and (MIN_RTT is med_min) and (P.L is low_pl) then (output1 is normal)
13. If (ARTT is med_artt) and (MAX_RTT is med_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is normal)
14. If (ARTT is med_artt) and (MAX_RTT is med_max) and (MIN_RTT is med_min) and (P.L is low_pl) then (output1 is normal)
15. If (ARTT is high_artt) and (MAX_RTT is low_max) and (MIN_RTT is low_min) and (P.L is low_pl) then (output1 is abnormal)

6. DEFUZZIFICATION

Defuzzification is the conversion of a fuzzy quantity to a precise value, just as fuzzification is the conversion of a precise value to a fuzzy quantity. In this method, the resultant membership functions are developed by considering the union of the output of each rule, which means that the overlapping area of fuzzy output set is counted as one, providing more results. Fig. 9 is an example to demonstrate the appropriate assent between input parameters change and output values predicted by fuzzy based model. The close assent of output values obviously displays that fuzzy logic model can be used to predict output values under consideration Thus, the proposed fuzzy logic model gives a promising solution to predict output value in the specific range of parameter.

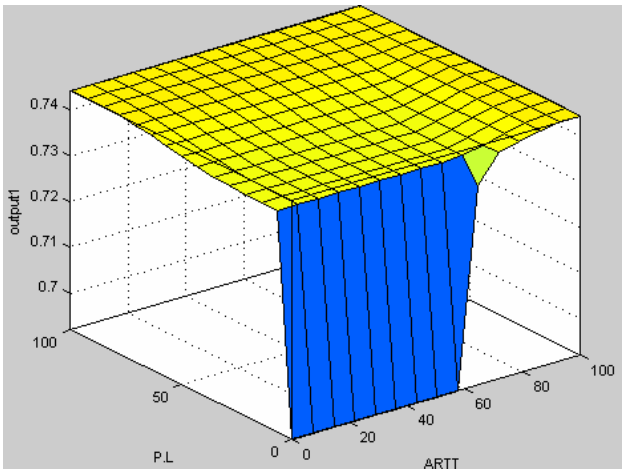

Fig. 7 Output value in relation to change of Average RTT and Packet Loss

7. SIMULATION

The experiment is simulated in Simulink environment using the required components to achieve the objectives. The components used include multiplexers, fuzzy logic controller and a scope that relates to the output. Fig. 10 illustrates the design of the Simulink environment used in this experiment.

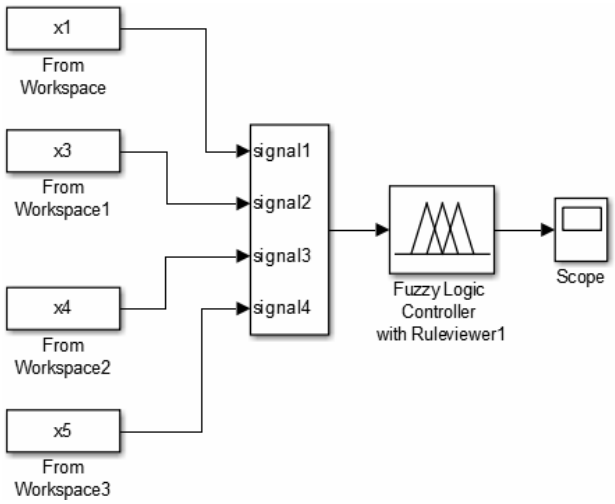

Fig. 8 Simulink design

Fig. 8 shows our four inputs being multiplexed to the fuzzy logic controller. It is the fuzzy logic controller where we install our fuzzy logic instance which we have created using the fuzzy rules shown in Table 8 and the membership functions. After the fuzzy system makes the decision, it will push the results to the scope and stored in the system.

Fig. 9 shows the simulation in the fuzzy logic block. The results obtained from this simulation are highly accurate as the all predicted anomalies are caught by the system leaving the remaining inputs as normal behavior of the network.

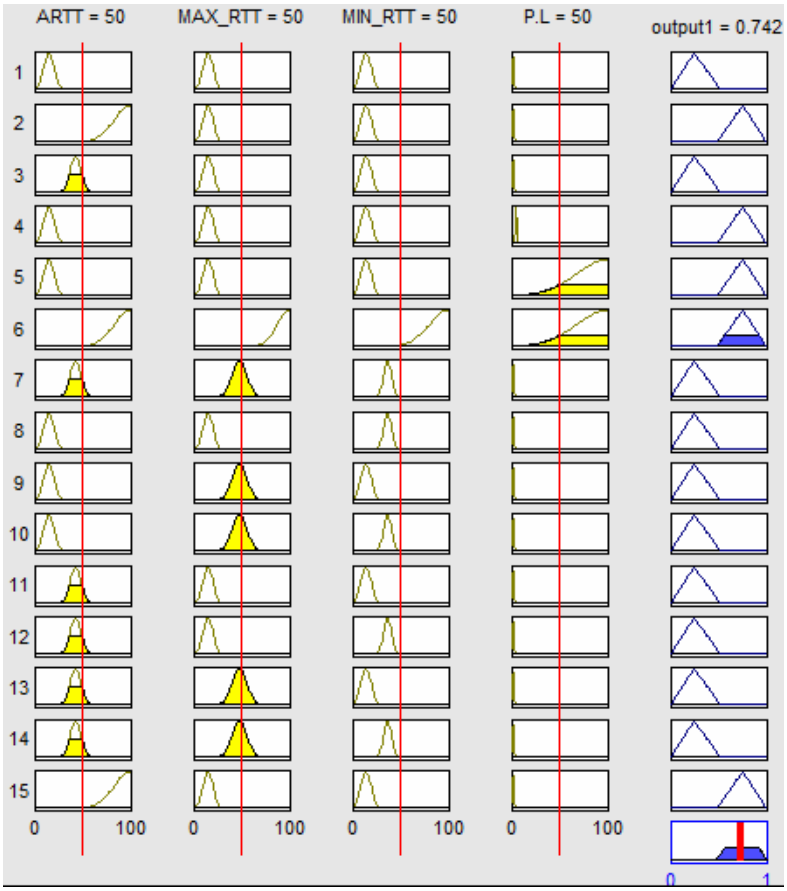

Fig. 9 Fuzzy simulation on progress

4. RESULTS

The proposed system is simulated in Matlab Simulink using PingER data set. In order to compare the results, the same data set is simulated in WEKA environment using NaiveBayes and Decision tree (J48) machine learning techniques. The performance of each simulation is evaluated using accuracy rate and misclassification rate. The following formulas are used:

$$\text{Accuracy rates} = \frac{\text{Number of correctly classified instances}}{\text{Total number of instances}} \quad (1)$$

$$\text{MisClassification rate} = 1 - \frac{\text{Number of correctly classified instances}}{\text{Total number of instances}} \quad (2)$$

Table [3] presents the evaluation of the proposed system, NaiveBayes and Decision tree results in terms of Accuracy and Misclassification rates. In Table 3 very high accuracy for Decision Tree (J48) should be noted.

Table 3 Experimental Results

	Naive Bayes	Decision Tree (J48)	Proposed System (DFLC)
Data Split Training set (%)	30	30	0
Accuracy rate (%)	92.163	99.0593	95.614
Misclassification rate (%)	7.837	0.9404	4.386

5. DISCUSSION AND CONCLUSION

Conclusively, the proposed Dynamic Fuzzy Logic Controller has proved to be an optimal approach to detecting anomalies in networks. With PingER dataset, simulation results prefer DFLC compared to NaiveBayes but not to Decision tree in terms of accuracy and misclassification rates. The study shows that processing time is not a setback, as it is only a single system integrated with the monitoring host. Yet it is recommended that the monitoring host should have enough computing resources and power as huge datasets need to be processed by the system.

REFERENCES

1. Feizolah, A., Anuar, N.B., Salleh, R., Mat Kiah, K.L., 2013, *Anomaly Detection Using Cooperative Fuzzy Logic Controller*, Intelligent Robotics Systems: Inspiring the NEXT, 376, pp. 220-231.
2. Lim, H.H., Qiu, B., 2001, *Fuzzy logic traffic control in broadband communication networks*, The 10th IEEE International Conference on Fuzzy Systems, 1(5), pp. 99-102.
3. Zadeh, L., 2008, *Is there a need for fuzzy logic?*, Annual Meeting of the North American Fuzzy Information Processing Society – NAFIPS, 8(9), pp. 1-3.
4. Giannini, J.A., Kilgus, C., 1997, *A fuzzy logic technique for correcting climatological ionospheric models*, IEEE Transactions on Geoscience and Remote Sensing, 35(2), pp. 470-474.
5. Cottrell, W.M., Matthews, W., 2000, T*he PingER Project: Active Internet Performance Monitoring for the HENP Community*, IEEE Communications Magazine, 38(5), pp. 130-136.
6. Postel, J., 1981, *Internet Control Message Protocol*, RFC Editor, United States.
7. Mathis M., 1997, *The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm*, Computer Communication Review, 27(3), pp. 67-82.
8. Petković, D., Issa, M., Pavlović, D. N., Zentner L., 2013, *Intelligent Rotational Direction Control of Passive Robotic Joint with Embedded Sensors*, Expert Systems with Applications, 40(4), pp. 1265-1273.
9. Shamshirband, S., Petković, D., Ćojbašić, Ž., Nikolić, V., Anuar, N.B., Mohd Shuib, N.L., Mat Kiah, M.L., Akib, S., 2014, *Adaptive neuro-fuzzy optimization of wind farm project net profit*, Energy Conversion and Management, 80(4), pp. 229–237.
10. Zakaria, R., Sheng, O.Y., Wern, K., Shamshirband, S., Petković, D., Pavlović, T.N., 2014, *Adaptive neuro-fuzzy evaluation of the tapered plastic multimode fiber based sensor performance with and without silver thin film for different concentrations of calcium hypochlorite*, IEEE Sensors Journal, DOI: 10.1109/JSEN.2014.2329333.

11. Shamshirband, S., Petković, D., Anuar, N.B., Mat Kiah, M.L., Akib, S., Gani, A., Ćojbašić, Ž., Nikolić, V., 2014, *Adaptive neuro-fuzzy generalization of wind turbine wake added turbulence models*, Electrical Power and Energy Systems, 62, pp. 490–495.
12. Petković, D., Shamshirband, S., Iqbal, J., Anuar, N.B., Pavlović, D.N., Mat Kiah, M.L., 2014, *Adaptive neuro-fuzzy prediction of grasping object weight for passively compliant gripper*, Applied Soft Computing, 22, pp. 424–431.
13. Shamshirband, S., Petković, D., Anuar, N.B., Gani, A., 2014, *Adaptive neuro-fuzzy generalization of wind turbine wake added turbulence models*, Renewable and Sustainable Energy Reviews, 36, pp. 270–276.
14. Petković, D., Shamshirband, S., Ćojbašić, Ž., Nikolić, V., Anuar, N.B., Md Sabri, A.Q., Akib S., 2014, *Adaptive neuro-fuzzy estimation of building augmentation of wind turbine power*, Computers & Fluids, 97, pp. 188–194.

DFCL: DINAMIČKI FAZI KONTROLER ZA DETEKCIJU INTRUZIJE

Intruzije su problemi pri mrežnom prenosu koje dovode do pogrešne primene i abnormalnog ponašanja u pouzdanim opercijama mreže i servisa. U ovom radu, dinamički fazi kontroler (DFK) je predložen za detekciju anomalije u mreži, sa ciljem da se reši problem detekcije brzine napada i proces bržeg reagovanja. Podaci su skupljeni u okviru projekta PingER. Reč je o projektu koji aktivno meri performanse do krajnih korisnika svetske internet mreže. Pokriva više od 168 zemalja u celom svetu. PingER koristi univerzalan Internet Ping kako bi izračunao parametar korisnih performansi. Pri svakom setu od 10 pinga između praćenog hosta i udaljenog hosta, karakteristike koje se računaju uključuju Minimum Round Trip Time (RTT), Jitter, Packet loss, Mean Opinion Score (MOS), Directness of Connection (Alpha), propusna moć, ping nepredvidljivost i ping dosezanja. Set od 10 pinga se šalje od praćenog čvora do udaljenog čvora svakih 30 minuta. Primljeni podaci prikazuju trenutnu karakteristiku i ponašanje mreže. Svaka promena u primljenim podacima ukazuje na primenu potencijalne pretnje ili abnormalnog ponašanja. DFK koristi kombinaciju parametara kao ulaz da detektuje bilo koje abnormalno ponašanje mreže. Predložen sistem je simuliran u Matlab-u. Rezultati simulacije pokazuju da sistem može da uhvati 95% anomalija sa mogućnošću da odvoji normalno i abnormalno ponašanje mreže.

Ključne reči: *detekcija intruzije, fazi sistemi, pinger, vreme cirkulacije (rtt), gubitak podataka.*