Available online at www.scholarsresearchlibrary.com

Scholars Research Library

ISSN:0975-508X

Archives of Applied Science Research, 2020, 12 (3):1-7

(http://scholarsresearchlibrary.com/archive.html)

Artificial intelligence approach to cyber security

Jerome M Gumpy [1*], Ibrahim Goni [2], Murtala Mohammad [3]

[1] Department of computer science Federal University Gashua, Nigeria

[2,3] Department of Computer Science, Adamawa State University Mubi, Nigeria

[*]Corresponding Author: Jerome M Gumpy, Department of computer science Federal University Gashua, Nigeria; E-mail: algonis1414@gmaail.com

ABSTRACT

Cyber security is a major concern of developed and developing countries due to the high rate of attack and threat to the cyber space. The purpose of this research work was to developed a fuzzy logic system for cyber security. Four inputs were used and three outputs were produced with their associated linguistic variables, Triangular angular membership function was used to implement the system. Fuzzy logic controller is behaving best on the linguistic variables used in the research that is special control, physical control, and denial of service, virus, and special software Trojan horse logic bomb and so on as applied to this research. These are the variables used in this work were rules are derived best on the cyber experts reasoning to cater the intruders.

Keywords: *Cybersecurity, Fuzzy logic, Membership function, Linguistic variables.*

INTRODUCTION

The advancement in cloud computing, mobile computing, mechatronics, net centric computing, wireless sensor network, nanotechnology and internet of things has led to the conjunction in the cyber space and even leading to the creation of fog computing. Moreover, this cyberspace is a platform where business security system, financial systems, education system, industries, power plants among others. The combination of this technology and systems has improved the functionalities of cyber space and leading to vulnerability to the cyber-attack [1]. In the recent time a lot of framework and systems are published based on the application of artificial intelligence techniques to cyber security and digital forensics. The research of [2] applied deep learning technique to design a framework for cyber forensics. [3] Uses data mining techniques in anti-cybercrime. In [4] deep learning neural network and fuzzy logic was used for abnormal traffic control in a network using CICIDS 2017 data sets. In [5] applied deep learning techniques in DOS attack and [6] applied fuzzy logic technique to protect car for cyber-attack. [7] Combined Neuro-fuzzy and genetic algorithm to implement intrusion detection system.

METHOD

The methods of data collection used in this research work are questionnaires administered to the cyber experts, network administrators and system administrators. The data obtained are related linguistic variables used in this work. Best on these linguistic variables this study evaluates cyber terrorists who might attack the systems which can be any form of systems be it communication system, oil and gas system, financial system security system among others.

System architecture

Inputs and outputs analysis

The fuzzification and defuzzification of inputs and outputs in this experiment was implemented using triangular membership function as shown in the figure below.

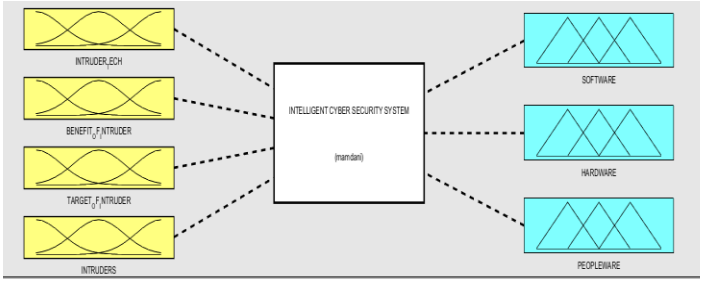


Figure 1: System Architecture

Intruder’s techniques

The major technique used by the intruders are the one that would favor him after studying the weaknesses of the system based on this we have identified the techniques they might use in table 1 below.

Sl no.	Intruder’s Technique	Abbreviation
1	Network attack	NA
2	Denial of service	DoS
3	Virus	V
4	E-mail Virus	EV
5	Logic Bomb	LB
6	Trojan horse	TH
7	Social engineering	SE
8	Malware	M

Table 1: Intruder techniques and their abbreviation.

The above table 1 was used to plot a membership function for intruder’s.

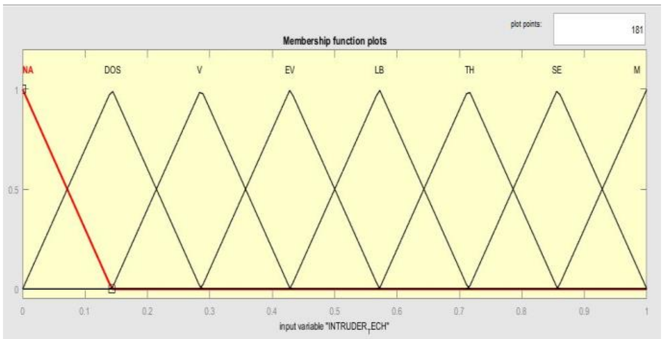


Figure 2: Intruder Techniques Membership.

Benefit of Intruders

A cyber intruder normally has the reason his attack the table 2 below summarize the possible benefit of the intruder.

Sl no.	Benefit of intruders	Abbreviation

1	Out of service	OOS
2	Seizing web page	SWP
3	Protesting	P
4	Control of critical system	CCS
5	Capture confidential info.	CCI
6	Control system	CS

Table 2: Benefit of intruders and its abbreviation.

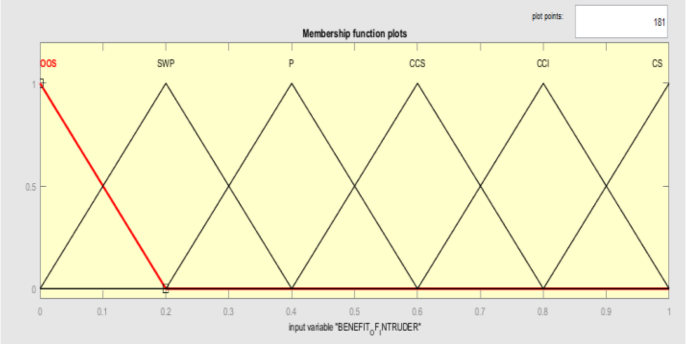


Figure 3: Benefit of Intruders.

Target of Intruders

Target is a critical term for a cyber-intruder. According to target, a cyber-intruder may use one or more different cyber techniques. A cyber intruder's target may be as in Table 3.

Sl no.	Target of intruders	Abbreviation
1	Communication system	CS
2	Financial center	FC
3	Power plant	PP
4	Emergency source	ES
5	Public transportation	PT
6	Public institution	PI
7	Water works	WW
8	Oil and natural gas distribution	ONGD

Table 3: Target of Intruder's.

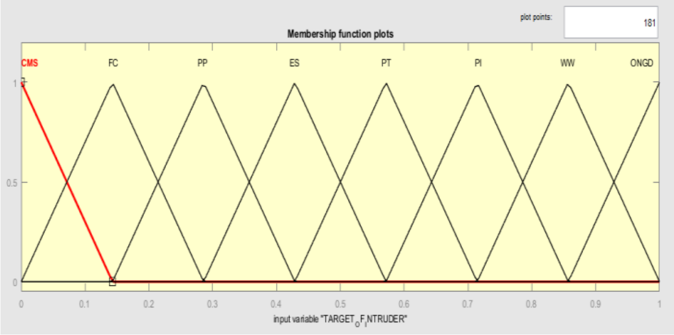


Figure 4: Target of intruders membership.

Intruders

Intruders are person or group of persons responsible for the unauthorized access to the system. They are summarized in the table 4 below.

Sl no.	Intruders	Abbreviation
1	Special staff	SPS
2	Computer Hacker	CH
3	Enemy of the system	EOS
4	Cyber activist	CA

Table 4: Intruders and its abbreviation.

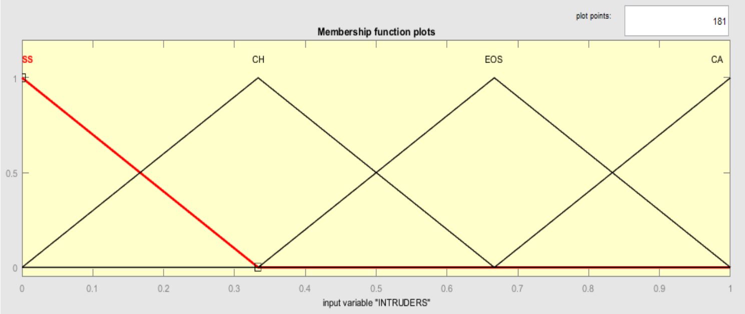


Figure 5: Intruders membership

Hardware

In some situations network administrators has a software device to prevent attack as summarized in the table 5 below.

Sl no.	Hardware	Abbreviation
1	Physical control	PC
2	Special control	SC
3	Technical control	TC

Table 5: Hardware and its abbreviation.

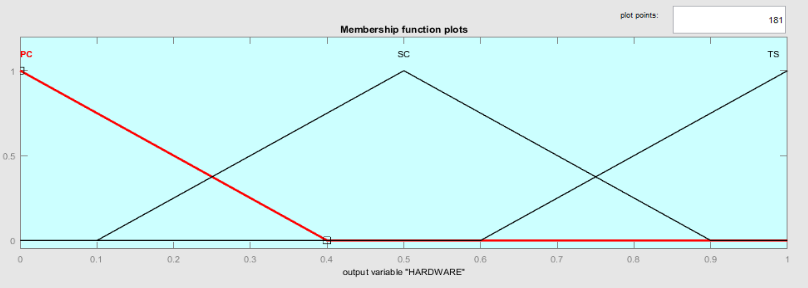


Figure 6: Hardware membership

Software

Sometime it is possible to use software to combat intruders as summarized in the table 6 below.

Sl no.	Software	Abbreviation
1	Special software	SPC
2	System update	SU
3	National data bank	NDB

Table 6: software and its abbreviation.

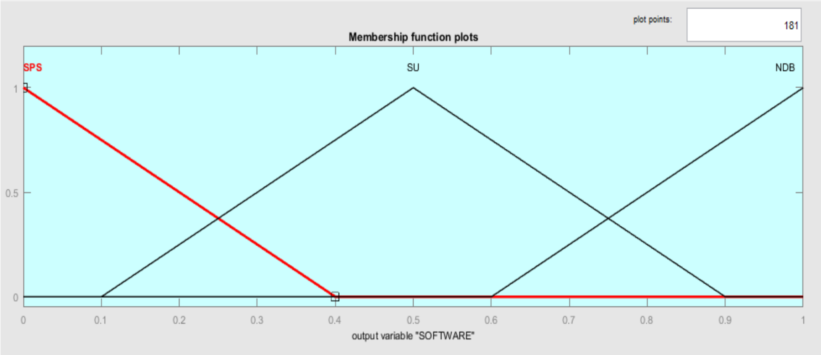


Figure 7: Software membership

People ware

Users can play a vital role in combating cyber-attack if they have technical knowhow of attacks as it summarized in the table 7 below.

Sl no.	People ware	Abbreviation
1	User training	UT

2	Awareness	A
3	User control	UC

Table 7: People ware and its abbreviation.

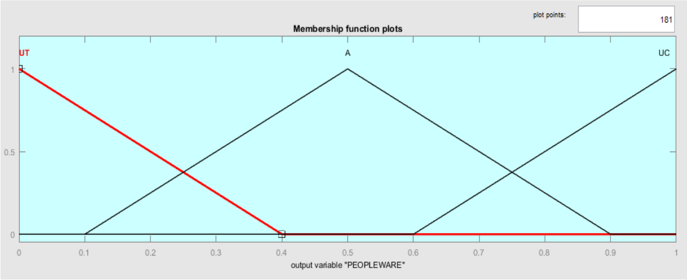
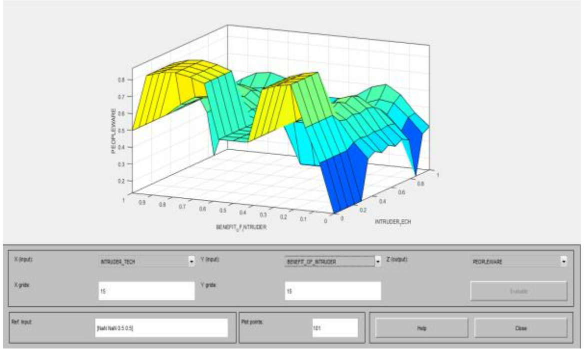


Figure 8: People ware membership.

RESULTS

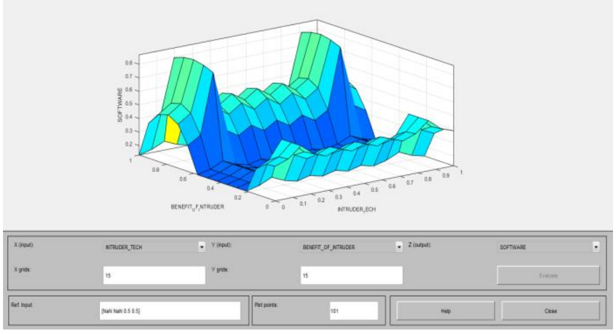
The input variable Intruder techniques (IT) is not a fixed value they are fuzzy variables as network attack, virus, Trojan horse, malware etc. Similarly for input variable benefit of intruders (BI) has the fuzzy variables out of service, protesting, control system etc. and output variable People ware has the fuzzy variables user training, awareness and user control. Depending on the inputs the outputs take different fuzzy variables value. It can be seen that Intruder techniques (IT) criteria is in x axis, benefit of intruders (BI) criteria is in y axis, and solution criteria People ware (P) is in z axis as shown in Figure 1.



X (input): INTRUDER_TECH
Y (input): BENEFIT_OF_INTRUDER
Z (output): PEOPLEWARE
X grids: 15
Y grids: 15
Ref. Input: [NaN NaN 0.5 0.5]
Plot points: 101

Figure 9: Input variables Intruder Techniques (IT), Benefit of Intruders (BI) vs. output variable People ware (P).

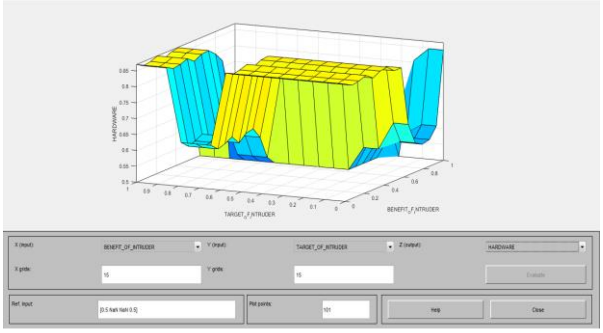
As shown in Figure 10 Intruder techniques (IT) criteria is in x axis, benefit of intruders (BI) criteria is in y axis, and solution criteria software (S) is in z axis.



X (input): INTRUDER_TECH
Y (input): BENEFIT_OF_INTRUDER
Z (output): SOFTWARE
X grids: 15
Y grids: 15
Ref. Input: [NaN NaN 0.5 0.5]
Plot points: 101

Figure 10: Input variables Intruder Techniques (IT), Benefit of Intruders (BI) vs. output variable Software (S).

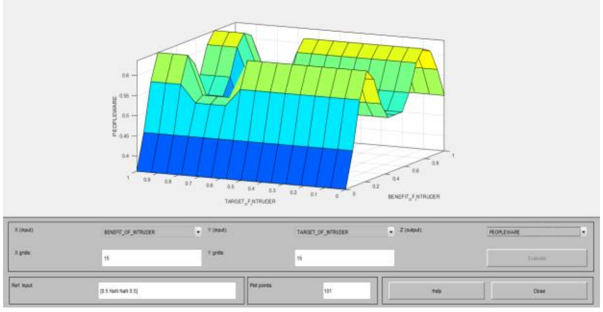
As shown in Figure 11 Benefit of intruders (BI) criteria is in x axis, and Target of Intruders (TI) criteria is in y axis, and solution criteria hardware (H) is in z axis.



X (input): BENEFIT_OF_INTRUDER
Y (input): TARGET_OF_INTRUDER
Z (output): HARDWARE
X grids: 15
Y grids: 15
Ref. Input: [0.5 NaN NaN 0.5]
Plot points: 101

Figure 11: Benefit of intruders (BI) criteria is in x axis, and Target of Intruders (TI) criteria are in y axis, and solution criteria hardware (H) is in z axis.

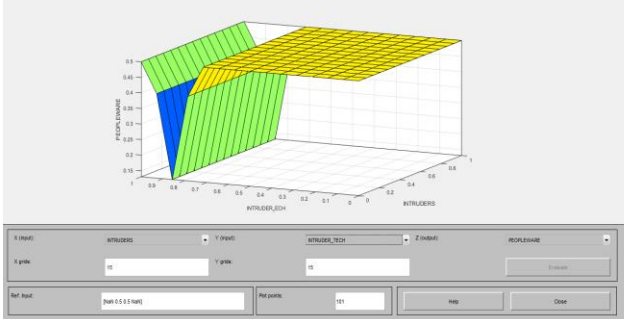
As shown Figure 12 benefits of intruders (BI) criteria is in x axis, and Target of Intruder (TI) criteria is in y axis, and solution criteria People ware (P) is in z axis.



X (input): BENEFIT_OF_INTRUDER
Y (input): TARGET_OF_INTRUDER
Z (output): PEOPLEWARE
X grids: 15
Y grids: 15
Ref. Input: [0.5 NaN NaN 0.5]
Plot points: 101

Figure 12: Input variables Benefit of Intruders (BI), Target of Intruder (TI), vs. output variable People ware (p).

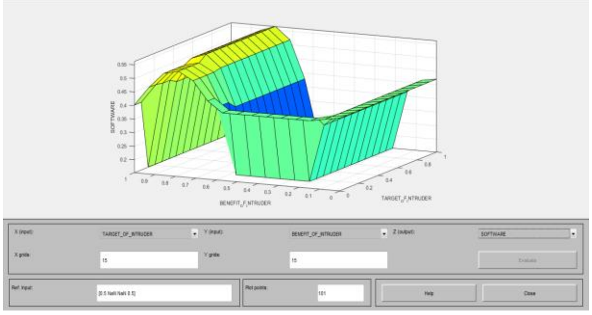
As shown Figure 13 Intruders (I) criteria is in x axis, and Intruder techniques (IT) criteria is in y axis, and solution criteria Peopleware (P) is in z axis.



X (input): INTRUDERS
Y (input): INTRUDER_TECH
Z (output): PEOPLEWARE
X grids: 15
Y grids: 15
Ref. Input: [NaN 0.5 0.5 NaN]
Plot points: 101

Figure 13: Input variables Intruders (I), Intruder Techniques (IT) vs. output variable People ware (P).

As shown Figure 14 Target of Intruders (TI) criteria is in x axis and benefit of Intruder (BI) criteria is in y axis and solution criteria Software (S) is in z axis.

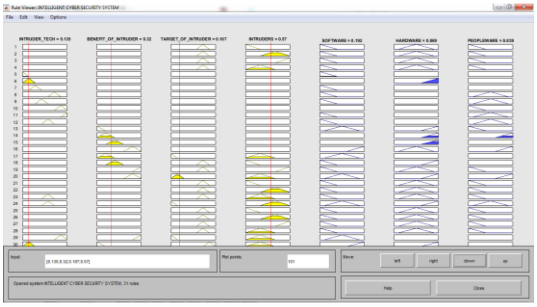


X (input): TARGET_OF_INTRUDER
Y (input): BENEFIT_OF_INTRUDER
Z (output): SOFTWARE
X grids: 15
Y grids: 15
Ref. Input: [0.5 NaN NaN 0.5]
Plot points: 101

Figure 14: Input variables Target of Intruders (I), Benefit of Intruder (BI) vs. output variable Software (S).

In Figure 15 of fuzzy rule viewer for Intelligent cyber security system is shown using MATLAB. According to the proposed model, a sample solution is given in Figure 16 when IT=0.135; BI=0.32; TI=0.187; I=0.57. Here, model outputs are

S=0.192; H=0.869 and P=0.839. Output of S=0.192 means that system Software Update (SU); H=0.571 means that system needs Technical support (TS); P=0.839 means that user needs User Control (UC) is important.



Input: [0.135,0.32,0.167,0.57]

Plot points: 101

Opened system INTELLIGENT CYBER SECURITY SYSTEM, 31 rules

Figure 15: Fuzzy Rule viewer for intelligent cyber security system.

CONCLUSION

In this work Fuzzy logic methodology are applied to cybersecurity. From the Inputs variables used triangular membership was used moreover, linguistic variables derived from the inputs and rules were extracted best on this linguistic variable and the system used them to evaluate the cyber-attack. The concept used in this work can be used to modeled the cyber security system.

REFERENCE

[1] Thanh, T. N., and Vijay, J.R., Deep Reinforcement learning for cyber security. Veins Publications, 2019. 1(2): p.12-15.

[2] Nickson, M.K., Victor, R.K., and Venter, H.S., Diverging deep learning cognitive computing techniques into cyber forensics. Forensics Sci Int Lib, 2019. 1(8): p.61-67.

[3] Khan, M. A., Pradhan, S.K., and Fatima, M., Applying data mining techniques in cybercrimes: in anti-cybercrime (ICACC) 2017 2nd Int Conf IEEE, 2017. 2(3): p. 213-216.

[4] Amosov, O.S., Ivanov, Y.S., and Amosova, G., Recognition of abnormal traffic using deep learning neural network and fuzzy logic IEEE 2019 Int Multi-Conf Industr Eng Moder Technol, 2019. 10(2): p. 14-17.

[5] Yuan, X., and Li, X., Deep defense Identify DDOS attack via deep learning IEEE Int Conf Smart Comput, 2017. 106(2): p. 29-31.

[6] Fabio, M., Fransesco, M., Victoria, N., and Antonella, S., Car hacking identification through fuzzy logic algorithm IEEE 2017. 11(2): p. 1-3.

[7] Goni, I., and Ahmed, L., Propose Neuro-Fuzzy-Genetic Intrusion Detection System. Int J Comput Appl, 2015. 115(8): 1-5.