Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 | Print ISSN: 0975-4350 |

Artificial Intelligence Approach to Cyber Security

By Murtala Mohammad & Ibrahim Goni
Adamawa State University

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 aim of this research work was to develop a fuzzy logic system for cyber security. Four inputs were used and three outputs was produced with their associated linguistic variables, Triangular angular membership function was used to implement the system. Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle.

GJCST- B Classification: *I.2*

Artificial Intelligence Approach to Cyber Security

Murtala Mohammad [α] & Ibrahim Goni [σ]

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 aim of this research work was to develop a fuzzy logic system for cyber security. Four inputs were used and three outputs was produced with their associated linguistic variables, Triangular angular membership function was used to implement the system. Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle.

I. 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.

II. Method

The data used for this work have been extracted from a series of questionnaires collected from cyber experts and system administrators. The obtained data are related especially with the headlines given below; Denial of Service (Dos) attacks, virus, malware, logic bomb, social engineering and Trojan horse and Out of service, seizing web page, attacks for protesting, seize critical systems, capture confidential information and take system control. This study evaluates cyber terrorists who might attack communications systems, financial centers, power plants, emergency services, transportation, water supply, oil and natural gas distribution stations. People capable of cyber terrorism such as dedicated special staff, hackers, cyber activists and opponents of the state are evaluated in the proposed cyber security system.

III. System Architecture

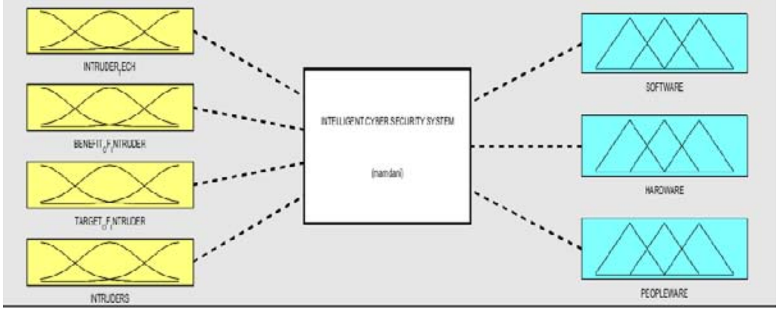


Figure 1: System Architecture

a) Inputs and Outputs Analysis

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

b) 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;

Author α σ: Department of Computer Science, Adamawa State University, Mubi. e-mail: algonis1414@gmaail.com

Table 1: Intruder Techniques and their Abbreviation

S/N	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

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

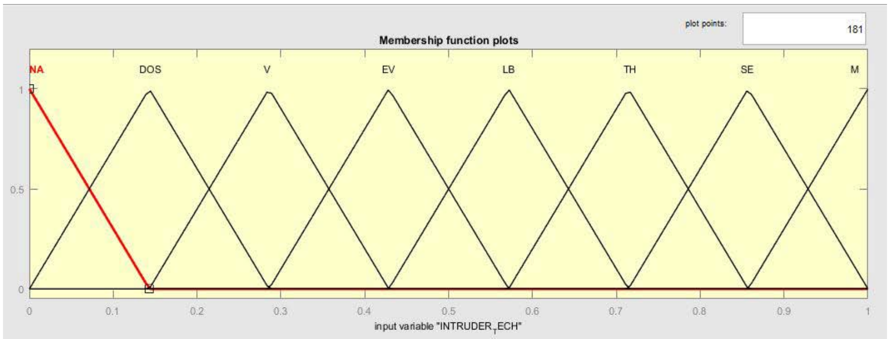


Figure 2: Intruder Techniques Membership

c) *Benefit of Intruders*

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

Table 3: Benefit of Intruders and its Abbreviation

S/N	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

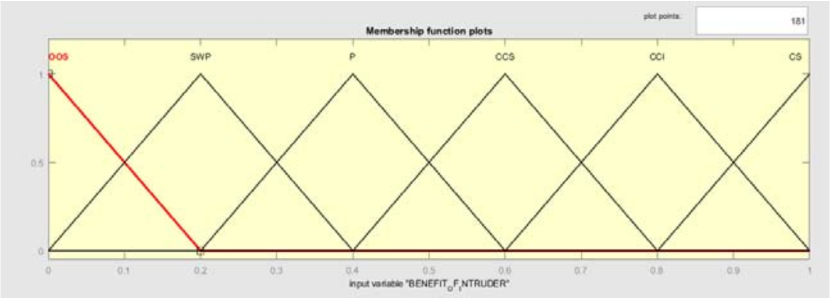


Figure 3: Benefit of Intruders

d) *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 4.

Table 4: Target of Intruder's

S/N	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

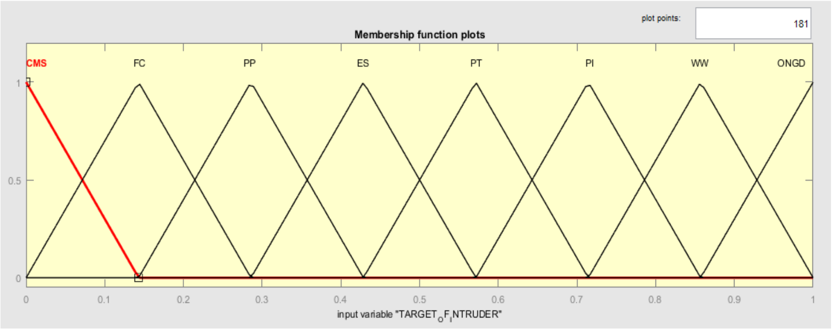


Figure 4: Target of Intruders Membership

e) Intruders

Intruders are person or group of persons responsible for the unauthorized access to the system. They are summarized in the table 5 below;

Table 5: Intruders and its Abbreviation

S/N	Intruders	Abbreviation
1.	Special staff	SPS
2.	Computer Hacker	CH
3.	Enemy of the system	EOS
4.	Cyber activist	CA

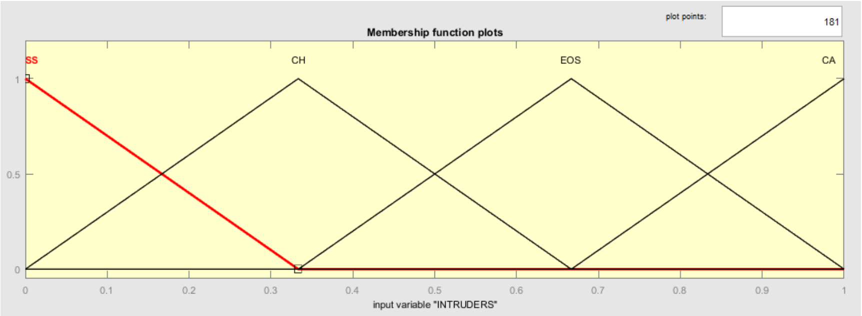


Figure 5: Intruders Membership

f) Hardware

In some situations network administrators has a software device to prevent attack as summarized in the table 6 below;

Table 6: Hardware and its Abbreviation

S/N	Hardware	Abbreviation
1.	Physical control	PC
2.	Special control	SC
3.	Technical control	TC

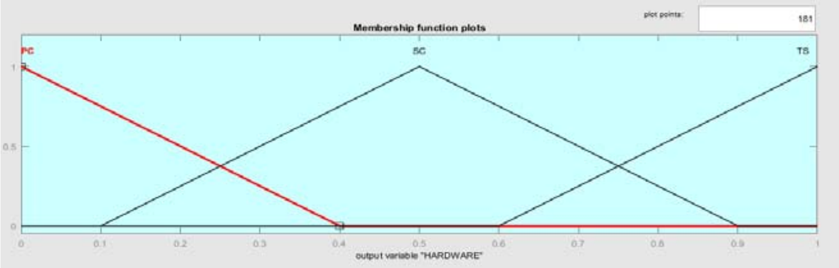


Figure 6: Hardware Membership

i. *Software*

Sometime it is possible to use software to combat intruders as summarized in the table 7 below;

Table 7: Software and its Abbreviation

S/N	Software	Abbreviation
1.	Special software	SPC
2.	System update	SU
3.	National data bank	NDB

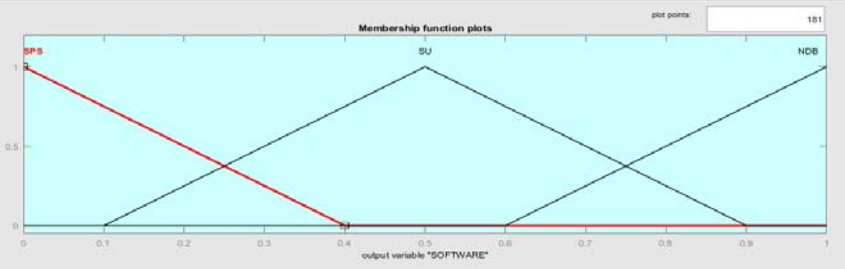


Figure 7: Software Membership

ii. *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 8 below

Table 8: People Ware and its Abbreviation

S/N	People ware	Abbreviation
1.	User training	UT
2.	Awareness	A
3.	User control	UC

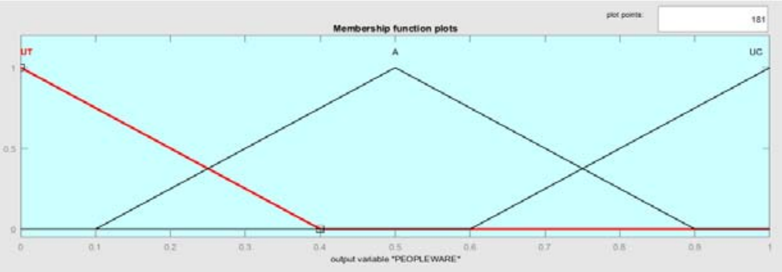
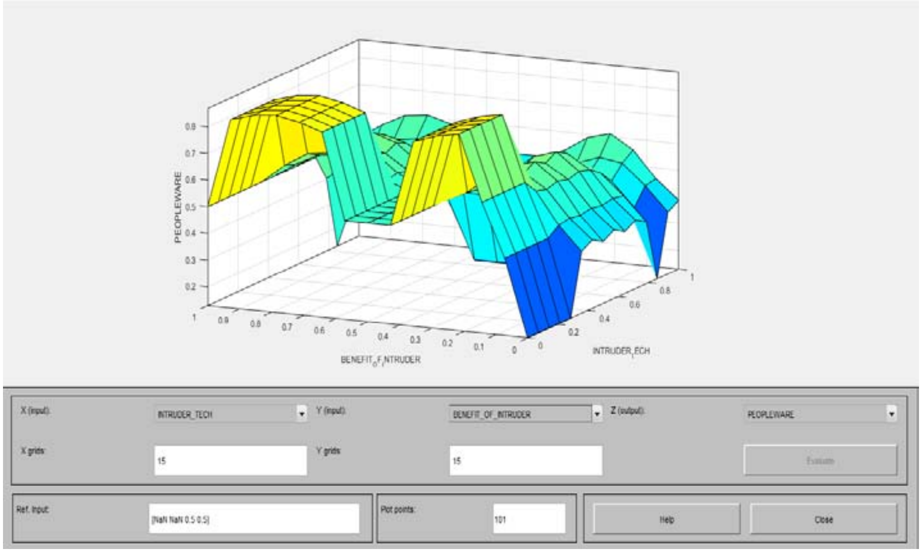


Figure 8: Peopleware Membership

IV. Result

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

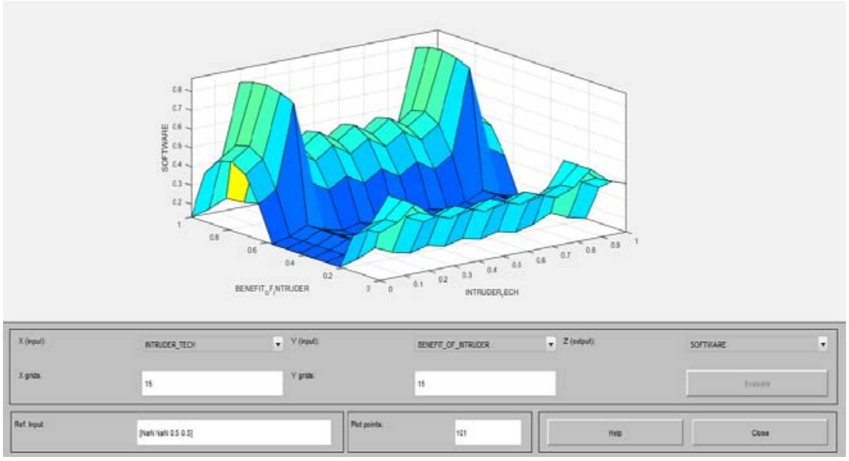
Y grids: 15

Ref. input: [NaN NaN 0.5 0.5]

Plot points: 101

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

As shown in Figure 11. 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

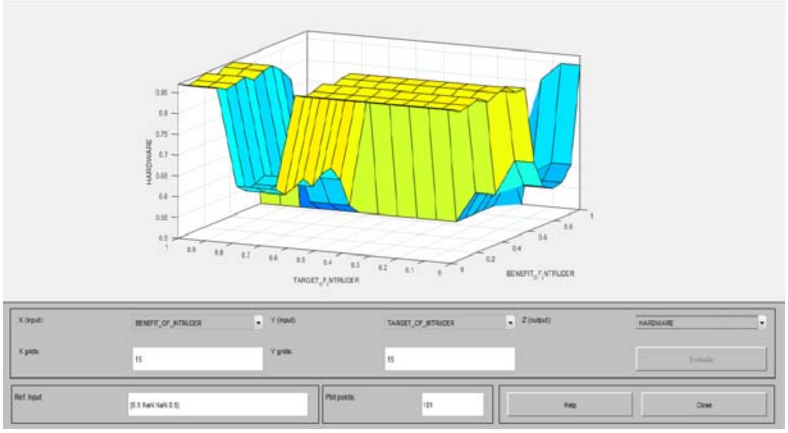
Ref. input: [NaN NaN 0.5 0.5]

Plot points: 101

Figure 11: Input variables Intruder Techniques (IT), Benefit of Intruders (BI) vs. output variable Software (S).

Benefit of Intruders (BI) vs. output variable Software (S).

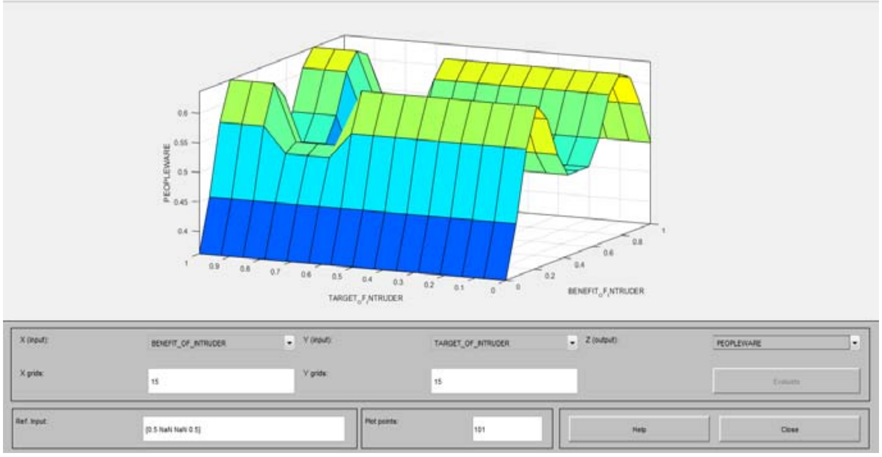
As shown in Figure 12 Benefit of intruders (BI) criteria is in x axis, and Target of Intruders (TI) criteria is in y axis, and solution criteria hardware (H) is in z axis.



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 12: 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

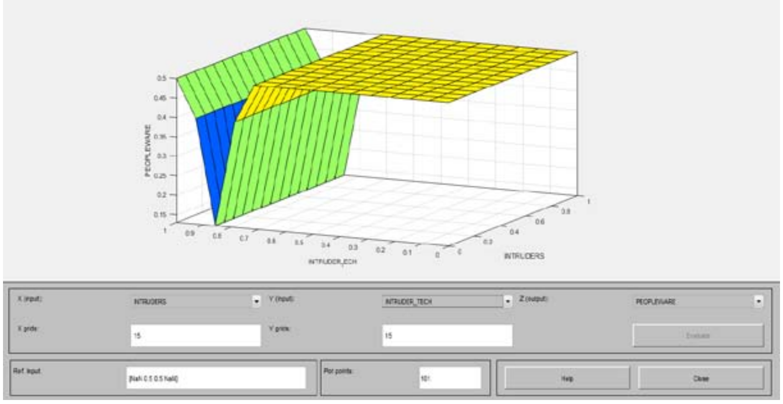
As shown Figure 13 benefits of intruders (BI) criteria is in x axis, and Target of Intruder (TI) criteria is in y axis, and solution criteria People ware (P) is in z axis.



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 13: Input variables Benefit of Intruders (BI), Target of Intruder (TI), vs. output variable Peopleware (P)

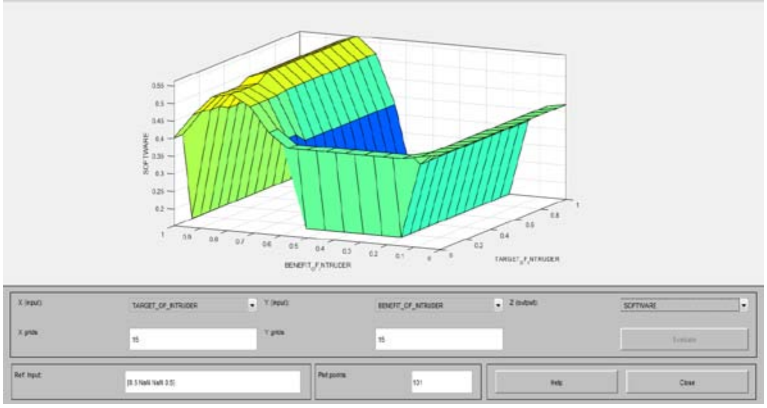
As shown Figure 14 Intruders (I) criteria is in x axis, and Intruder techniques (IT) criteria is in y axis, and solution criteria Peopleware (P) is in z axis.



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 14: Input variables Intruders (I), Intruder Techniques (IT) vs. output variable Peopleware

As shoswn Figure 15 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

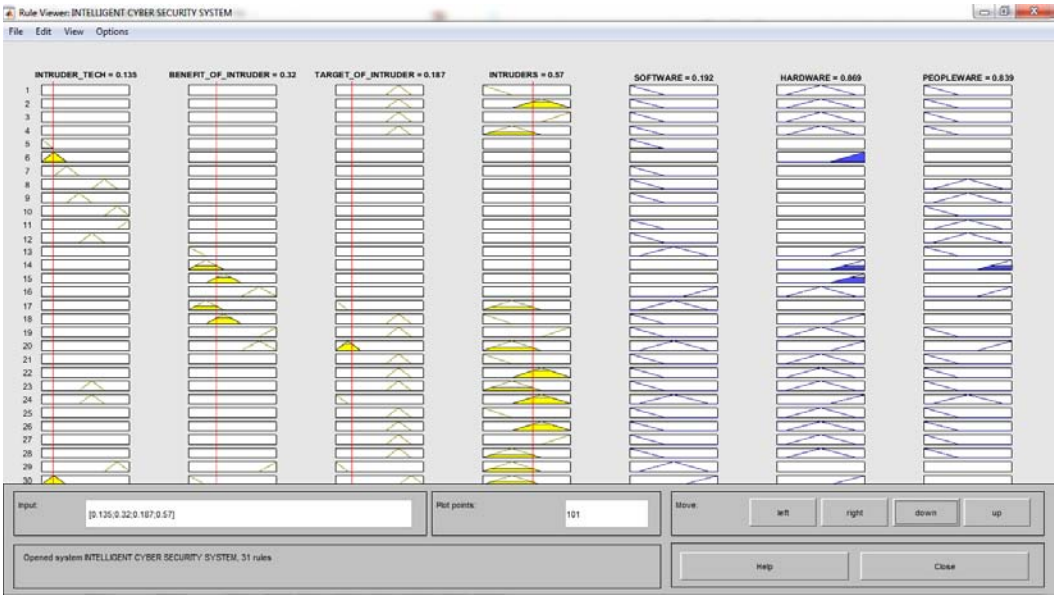
Y grids: 15

Ref. Input: [0.5 NaN NaN 0.5]

Plot points: 101

Figure 15: Input variables Target of Intruders (I), Benefit of Intruder (BI) vs. output variable Software (S)

In Figure 16 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;0.187;0.57]

Plot points: 101

Opened system INTELLIGENT CYBER SECURITY SYSTEM, 31 rules

Figure 16: Fuzzy Rule viewer for intelligent cyber security system

V. Conclusion

Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle. After an intelligent cyber security system was carefully designed, we test the system and discuss the impact of the input variables on the output variables as shown on the rules viewers and the surface viewers.

References Références Referencias

1. Thanh T. N. and Vijay J.R. (2019) Deep Reinforcement learning for cyber security [CsCR] arxiv: 1906.05799 vol. I
2. Nickson M.K., Victor R.K. and Venter H.S. (2019) Diverging deep learning cognitive computing techniques into cyber forensics.Forensics science international library.Science Direct Vol. 1, 61-67.
3. Khan M. A., S.K., Pradham H., and Fatima M. (2017) Applying data mining techniques in cybercrimes: in anti-cybercrime (ICACC) 2017 2nd International conference on IEEE pp. 213-216.
4. Amosov O.S., Ivanov Y.S. and Amosova G. (2019) Recognition of abnormal traffic using deep learning neural network and fuzzy logic IEEE 2019 international multi-conference on industrial engineering and modern technologies

5. Yuan X. and Li X. (2017) deep defense Identify DDOS attack via deep learning IEEE international conference on smart computing 29-31, may, 2017
6. Fabio M., Fransesco M., Victoria N. and Antonella S. (2017) Car hacking identification through fuzzy logic algorithm IEEE 2017.
7. Goni & Ahmed L. Propose Neuro-Fuzzy-Genetic Intrusion Detection System. International Journal of Computer Applications115(8): 1-5 (2015)