Global Journals LATEX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Artificial Intelligence Approach to Cyber Security

Ibrahim Goni

Received: 30 March 2020 Accepted: 21 April 2020 Published: 6 May 2020

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.

Index terms—

1 I. Introduction

he 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.

2 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.

3 T III. 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;

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

4 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

5 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 **??**.

6 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.

8

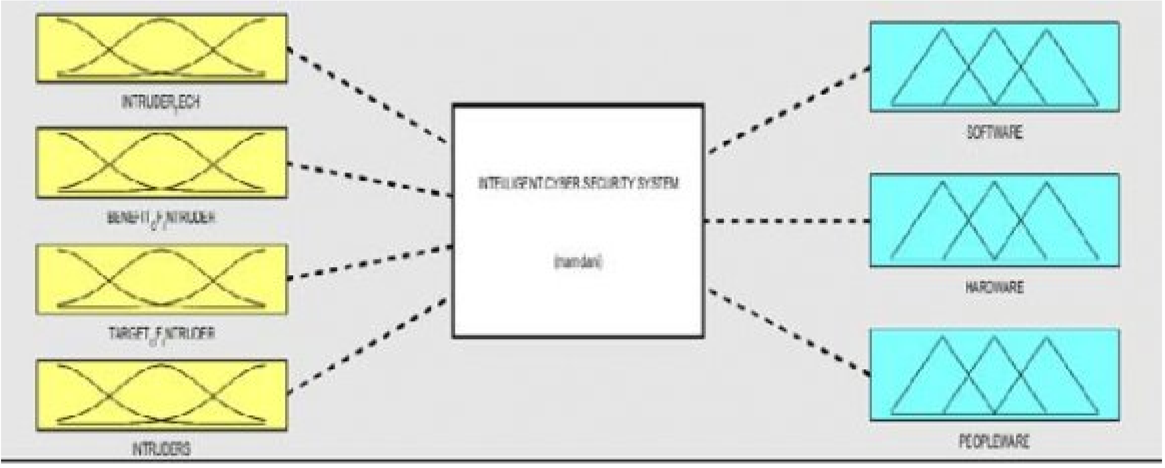

Figure 1: Figure 8 :

6

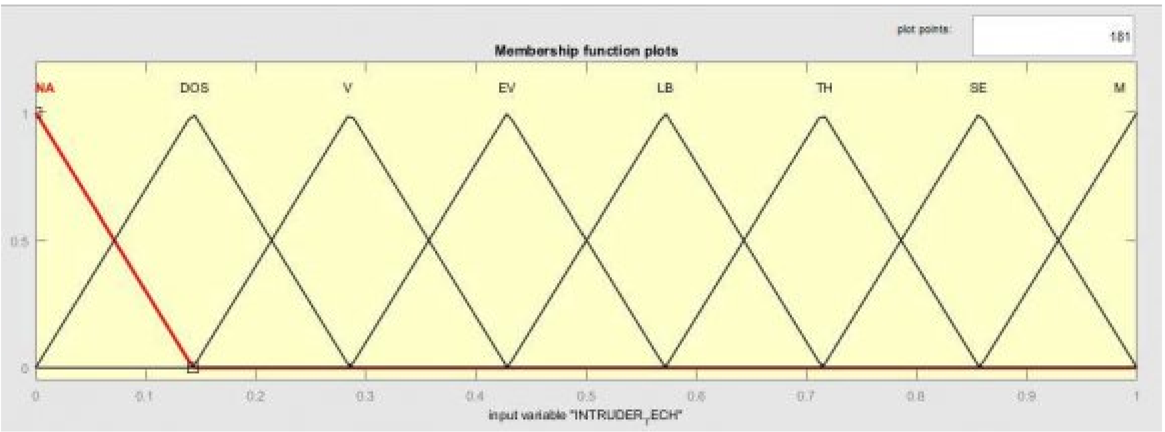

Figure 2: Figure 6 :

10

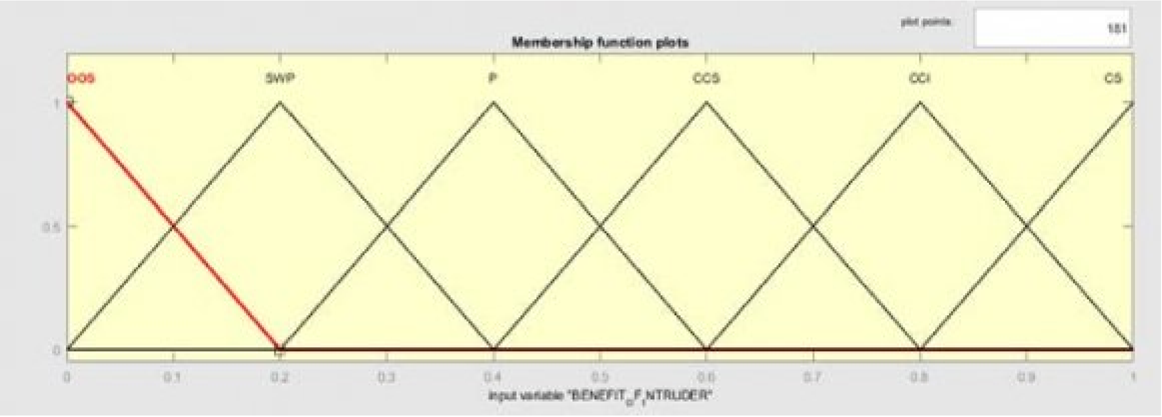
plot points: 181

Figure 3: Figure 10 :

11

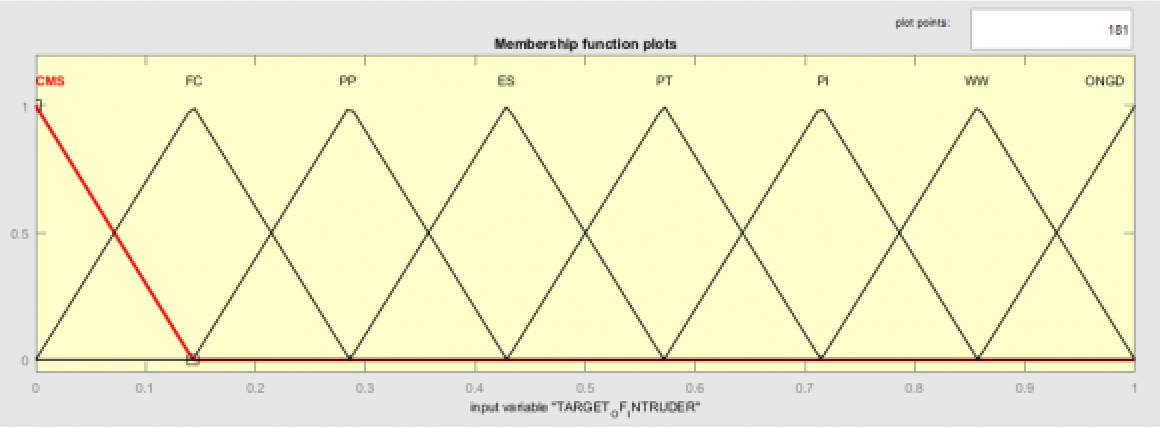
plot points: 181

Figure 4: Figure 11 :

12

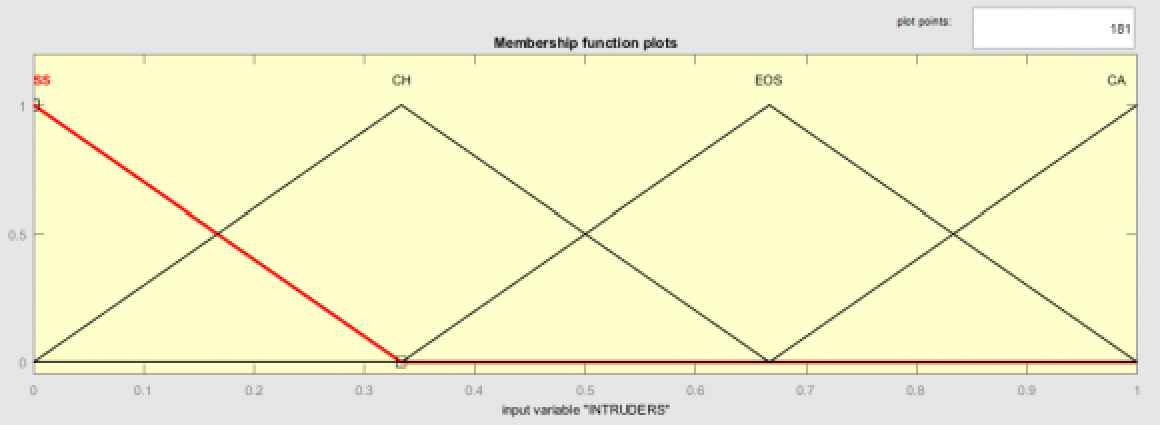
plot points: 181

Figure 5: Figure 12 :

14

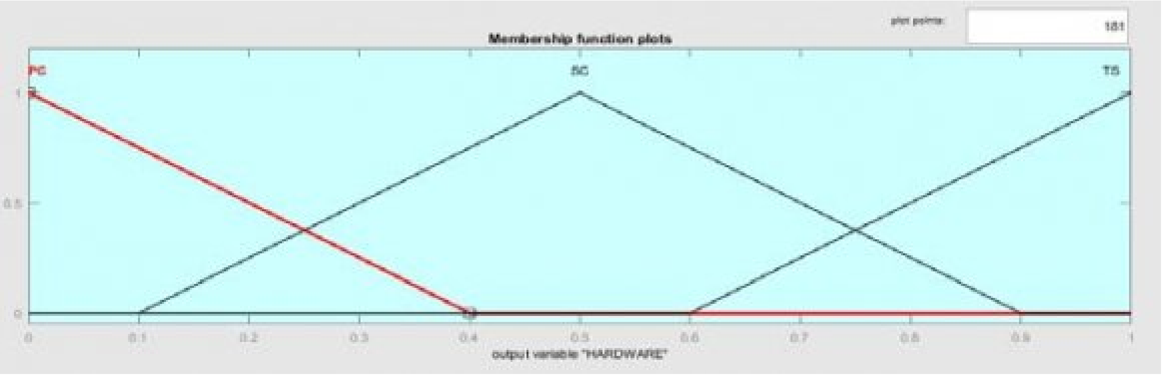

Figure 6: Figure 14 :

15

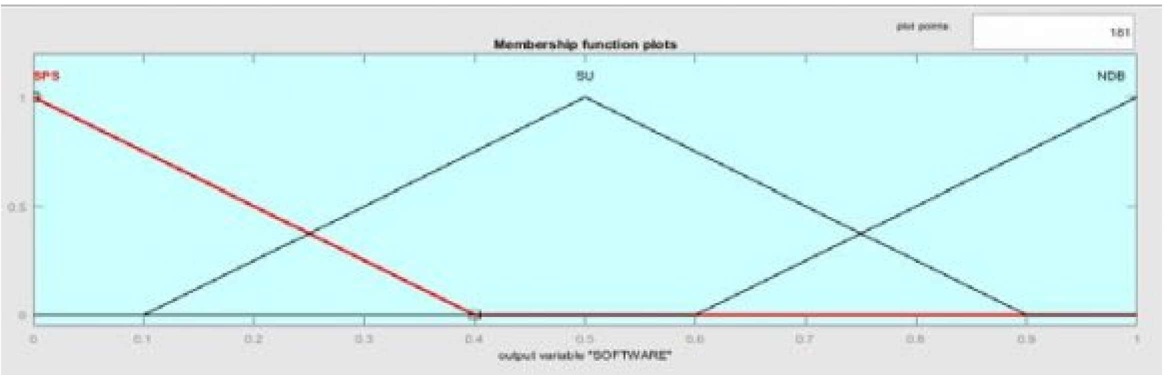

Figure 7: Figure 15 :

16

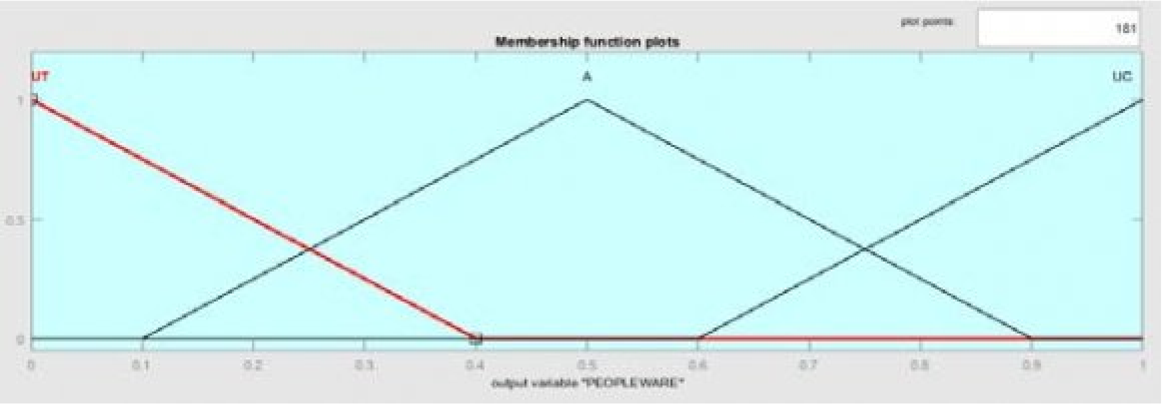

Figure 8: Figure 16 :

4

1.

[Note: c) Benefit of IntrudersA cyber intruder normally has the reason his attack the table 2. Below summarize the possible benefit of the intruder.Figure 3: Benefit of Intruders d) Target of IntrudersTarget 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]

Figure 9: Table 4 .

1

Figure 10: Table 1 :

3

Figure 2: Intruder Techniques Membership

[Note: Figure 4: Target of Intruders Membership e) IntrudersIntruders are person or group of persons responsible for the unauthorized access to the system. They are summarized in the table 5 below;Figure 5: Intruders Membership f) HardwareIn some situations network administrators has a software device to prevent attack as summarized in the table 6 below;Global Journal of Computer Science and TechnologyVolume XXII Issue I Version I]

Figure 11: Table 3 :

4

Figure 12: Table 4 :

5

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

i. Software

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

[Note: 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 8 below]

Figure 13: Table 5 :

6

Figure 14: Table 6 :

8

Figure 15: Table 8 :

6 V. CONCLUSION

7

[Note: and its Abbreviation Sometime it is possible to use software to combat intruders as summarized in the table 7 below;]

Figure 16: Table 7 :

[Khan and Pradham ()] 'Applying data mining techniques in cybercrimes'. M A Khan , S K Pradham , H , FatimaM . *anti-cybercrime (ICACC) 2017 2 nd International conference on IEEE*, 2017. p. .

[Thanh and Vijay ()] *Deep Reinforcement learning for cyber security*, T N Thanh , J R Vijay . arxiv: 1906.05799. 2019.

[Nickson et al. ()] 'Diverging deep learning cognitive computing techniques into cyber forensics.Forensics science international library'. M K Nickson , R K Victor , H S Venter . *Science Direct* 2019. 1 p. .

[Amosov et al. ()] *Recognition of abnormal traffic using deep learning neural network and fuzzy logic IEEE*, O S Amosov , Y S Ivanov , G Amosova . 2019. 2019.