Designing a Fuzzy Rule Based Expert System for Cyber Security

Kerim Göztepe

War Colleges Command, Army War College, Dept. of Combat Tactics.

Yenilevent-34330, İstanbul, Turkey. Tel: +90 212 398-0100, e-mail: kerimgoztepe@yahoo.com

Abstract- The topic of cyber security has been subject to more attention and interest outside the community of computer security experts. Cyber security is not a single problem, but rather it is a group of highly different problems involving different sets of threats. Fuzzy Rule based system for cyber security is a system that consists of a rule depository and a mechanism for accessing and running the rules. The depository is usually constructed with a collection of related rule sets. The aim of this study is to develop a fuzzy rule based technical indicator for cyber security with the use of an expert system which is named FRBCES (Fuzzy Rule Based Cyber Expert System). Rule based systems employ fuzzy rule to automate complex processes. Common cyber threats assumed for cyber experts are used as linguistic variables in this paper.

Keywords- Cyber security, cyber terrorism, fuzzy logic, fuzzy rules, Fuzzy Rule Based Cyber Expert System (FRBCES).

1. Introduction

The development of internet and communication systems started the cyber movement into the new era. People, governments, and firms now rely on the use of the internet for their business, activities and personnel affair. The integration of information technology into today's systems and functions has improved efficiency and led to significant change in daily life, but this reliance on integrated information technology system has also led to greater risk from cyber threats menacing the economic stability of many developed nations. Increased use of technology and interconnectivity means that the vital components of various countries' critical infrastructures – those areas necessary to perform the government and economy – are exposed to cyber attack [1],[2]. Moreover, protecting critical infrastructures has become a more difficult issue for the system administrator and the users. In order to control this vast cyber space, governments need to use intelligent cyber defence systems for detecting a wide range of threats and attacks.

Focusing on cyber protection of critical government systems from cyber terrorists and providing their needs is one of best ways to increase security. When any system administrator wants to increase the system's robustness, he has to consider several parameters affecting this circumstance.

The objective of this study is to provide critical system administrators for protecting systems, with the aid of the developed fuzzy rule based expert system. The expert system's role in defending network is to meet critical data needs against cyber terrorist attack and to develop appropriate solutions.

The paper is organized as follows. Section 2 illustrates the background of the models used in this research and the related literature. Section 3 describes the proposed research method in relation to the fuzzy logic. Section 4 expresses the proposed method how it is implemented as an expert system. Two scenarios were given in this implementation. Finally, the work is concluded in Section 5.

2. Literature Review

The three key elements of this research are cyber security/cyber terrorism, fuzzy set and number, and fuzzy rule based expert system. These elements are described below in regard to the relevant literature.

2.1. Cyber Security/Cyber Terrorism

Security of computer and networking systems have been an issue since computer networks became widespread. Today internet is changing social life. Sophisticated computer systems are deployed worldwide in many critical infrastructures ranging from business centres, nuclear power plants, and government agencies to transportation systems. Cyber threat puts serious threats to the integrity, confidentiality and availability of data for the whole internet and intranet users [3].

Cyber security and intrusion detection has emerged as a significant field of research, because it is not theoretically possible to set up a complete system with no fault [4]. Intrusion incidents to computer systems are increasing because of the widespread usage of the internet and local networks [5]. It is known that different machine learning algorithms, for example support vector machine [6], genetic algorithm [7], neural network [8], data mining [9], fuzzy logic [3],[10] and some others have been extensively applied to detect intrusion activities.

There are some emerging definitions for cyber terrorism. Terrorism is defined as intentional, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The term "international terrorism" means terrorism involving citizens or territory of more than one country. The term "terrorist group" means any group practicing, or has significant subgroups that practice, international terrorism [11].

Persistent computer security vulnerabilities may expose the government's critical infrastructure and government's network systems to cyber attack by terrorists, possibly affecting the economy or other areas of the national security at large [12]. Furnel and Warren [13] discussed the problems posed by cyber terrorists. They considered the nature of the responses necessary to protect the future security of society. By the rising threat of cyber attacks, some researchers tried to describe cyber threat and made attempts for finding a solution to their studies [14]-[17].

So far, many studies have been done on cyber security, but these are mostly focused on prevention of cyber intrusion, [18]-[21], effects of cyber attacks or on different machine learning applications [5],[6],[8]-[10]. Although there are some studies using fuzzy rules [22]-[24], fuzzy expert systems' effectiveness are totally different analysis. In this paper, apart existing literature, a new approach has been developed to prevent cyber attacks using a fuzzy expert system. The proposed fuzzy expert system in this study gives valuable information to system administrators to improve the achievement of the cyber security. This work contributes to the system in a general manner and it can be adapted to different cyber security scenarios.

2.2. Fuzzy sets and fuzzy number

The fuzzy set theory was introduced by Zadeh [25]. Fuzzy logic is a multi-value logic which permits intermediate values to be defined between conventional ones like true/false, low/high, good/bad etc. In a classical set theory, an element may either belong to set or not. In fuzzy set theory, an element has a degree of membership. A degree of membership function can be described as an interval [0, 1].

In this paper, triangular fuzzy number (TFN) was used for cyber threat computational efficiency. A TFN is shown simply as (l, m, u). "l, m, u" parameter represents the smallest possible value (lower bound), mean value, the largest possible value (upper bound) respectively [26]. $\mu_{\tilde{M}}$ is a membership function (Fig. 1.).

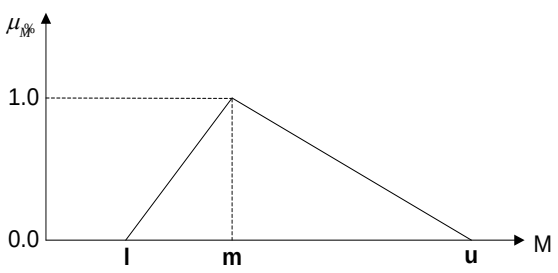

Fig.1: A triangular fuzzy number $\tilde{M}$.

Membership function of TFN is presented as follows:

$$\mu_{\tilde{M}}(x)=\begin{cases}0 & x<l\\ \dfrac{x-l}{m-l} & l\le x\le m\\ \dfrac{u-x}{u-m} & m\le x\le u\\ 0 & x>l\end{cases} \quad (1)$$

Basic fuzzy set definitions are given below.

Definition 1: (Fuzzy set) Let X be a universal set. Then a fuzzy set A of X is defined by its membership function

$$\mu_{A}(x)\to[0,1],\ x\mapsto\mu_{A}(x)\in[0,1]. \quad (2)$$

The value of $\mu_A(x)$ represents the grade of membership of x in X, and is interpreted as the degree to which x belongs to A, therefore the closer the value of $\mu_A(x)$ is 1, the more belongs to A. A crisp or ordinary set A of X can also be viewed as a fuzzy set in X with a membership function as its characteristic function, i.e.,

$$\mu_{\tilde{A}}(x)=\begin{cases}1 & x\in A\\ 0 & x\notin A\end{cases} \quad (3)$$

A fuzzy set A can be characterized as a set of ordered pairs of elements x and grade $\mu_A(x)$ is noted

$$\tilde{A}=\{(x,\mu_A(x))\mid x\in X\} \quad (4)$$

where each pair $(x,\mu_A(x))$ is called a singleton. When x is a countable or finite set, a fuzzy set A on x is expressed as

$$\tilde{A}=\sum_{x_i\in X}\mu(x_i)/x_i \quad (5)$$

When X is a finite set whose elements are $x_1, x_2, ..., x_n$, a fuzzy set A on x is expressed as

$$\tilde{A}=\{(x_1,\mu_A(x_1)),(x_2,\mu_A(x_2)),....(x_n,\mu_A(x_n))\} \quad (6)$$

When X is an infinite and uncountable set, a fuzzy set A on X is expressed as [27]

$$\tilde{A}=\int_x \mu(x)/x \quad (7)$$

Definition 2: (Support of a fuzzy set) Let $\tilde{A}$ be a fuzzy set on X. Then the *support* of $\tilde{A}$ denoted by supp $(\tilde{A})$, is the crisp set given by [27]

$$\text{supp}(\tilde{A})=\{x\in X\mid \mu_{\tilde{A}}(x)>0\} \quad (8)$$

Definition 3: (Normal fuzzy set) Let A be a fuzzy set on X. The height of A, denoted by hgt (A), is defined as [27]

$$hgt(\tilde{A})=\sup_{x\in X}\mu_{\tilde{A}}(x) \quad (9)$$

If $hgt(\tilde{A})=1$, then the fuzzy set A is called a *normal fuzzy set* otherwise; it is called *subnormal*.

Definition 4: (Empty fuzzy set) A fuzzy set $\tilde{A}$ is empty, denoted by $\varnothing$,

if $\mu_{\tilde{A}}(x)=0$ for all $x\in X$ (10)

Definition 5: (Some operations) Let $\tilde{A}, \tilde{B}$ and $\tilde{C}$ be fuzzy sets on X. We have [27]

- $\varnothing\subset\tilde{A}\subset X$; (11)
- Reflexive law : $\tilde{A}\subset\tilde{A}$; (12)
- Transferability: If $\tilde{A}\subset\tilde{B}$ and $\tilde{B}\subset\tilde{C}$, then $\tilde{A}\subset\tilde{C}$; (13)
- Commutativity law: $\tilde{A}\cup\tilde{B}=\tilde{B}\cup\tilde{A}$ and $\tilde{A}\cap\tilde{B}=\tilde{B}\cap\tilde{A}$; (14)
- Associativity law: $(\tilde{A}\cup\tilde{B})\cup\tilde{C}=\tilde{A}\cup(\tilde{B}\cup\tilde{C})$ and $(\tilde{A}\cap\tilde{B})\cap\tilde{C}=\tilde{A}\cap(\tilde{B}\cap\tilde{C})$ (15)

2.3. Fuzzy Rule Based Expert Systems

An expert system is the computer program that emulates the behavior of human experts in a well-specified manner [28]. Expert systems are in a wide area family of research known as artificial

intelligence (AI). AI is the study of developing computer programs, which indicates human-like intelligence. Early AI researchers focused on such problems as game theory, robotic control, and vision systems [29]. A fuzzy expert system is simply an expert system that uses a variety of fuzzy membership functions and rules, instead of Boolean logic, to reason about data [30]. The rules in a fuzzy expert system are usually in a form of the following:

If A is low and B is high then X= medium

where A and B are input variables, (16)

X is an output variable.

In this paper, the expert system roles have been designed to capture the details of cyber attacks. After that the system can use them and offer recommendations for system administrator.

3. Designing a Fuzzy Rule Based Expert System for Cyber Security

The designing stages include defining cyber security expert system variables, data collection for cyber threats, system design and implementation. These stages are described in the following subsections.

3.1. Stage 1: Defining Cyber Security Expert System Variables

The first step in the proposed model is the establishment of input and output variables [31]. This task is usually done by studying the problem domain and by consultation with the cyber experts. There is infinite number of potential candidates which should be restricted to positive numbers. In this paper, the key variables were defined with reference to interviews with cyber security experts. Input and outputs of proposed model is given in Fig. 2.

3.2. Stage 2: Data Collection for Cyber Terrorism

The expert system models the knowledge of the human expert. It also provides explanations similar to the human expert. The system can describe various questions asked by the user. 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 topics given below [11],[32];

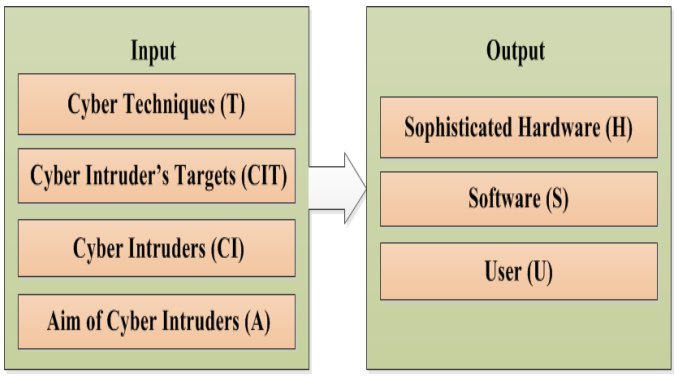

Fig.2: Inputs and outputs of proposed model.

- Denial of Service (Dos) attacks, virus, malware, logic bomb, social engineering, Trojan horse ,
- Out of service, seizing web page, attacks for protesting, seize critical systems, capture confidential information, system control (Fig.3).

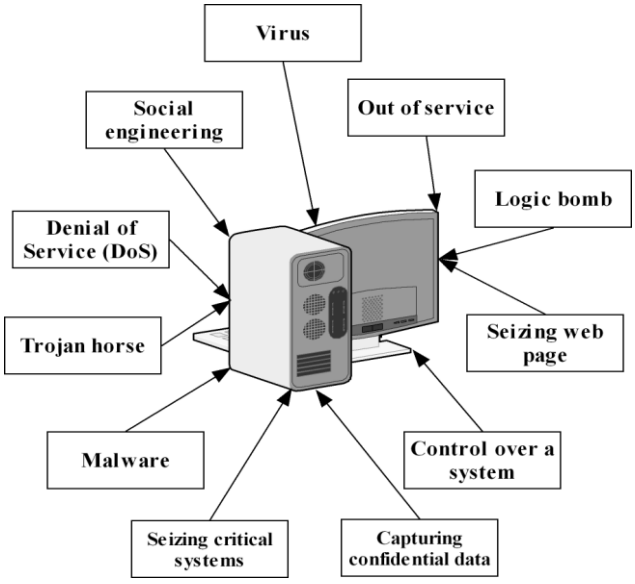

Fig.3: Potential cyber threats [11],[32],[33].

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 FRBCES model.

3.3. Stage 3: System Design

Expert systems may be forward or backward chaining. In forward chaining systems, we reason from antecedent truth to consequent truth; that is, we reason from facts in the rule antecedent that we know to be true to establish new facts whose truth is implied by the antecedent. Backward chaining reverses this; we attempt to find facts to establish the truth of some goal state. It is possible to emulate backward chaining with a forward chaining system [34].

Forward Chaining: An expert system rule may be formulated simply as "if A then B" where A is a set of conditions on data and B is a set of instructions to be carried out when the rule is fires. The rules are examined to see which rules are made firable by the data, that is, A is satisfied, and a rule or rules selected for executing. When the rule is executed, the set of instructions B is executed. Most rule-based expert systems works in this way [34]. Forward chaining is used in proposed FRBCES model.

Backward chaining: A different sequence is followed in backward chaining. In backward chaining, we specify what conclusion we would like to reach, that is, we specify B. We find a rule or rules that have the desired consequent, and look at the antecedent A to see what the data must be to satisfy A. Now we find out how those data can be established, and look for rules that have those data as a consequent, or input data from a user to see if the antecedent can be satisfied. In backward chaining we work backward from goals to data; in forward chaining we work forward from data to goals [34].

According to the theory of expert systems [35], the three main components are given below:

- User interface.
- Decision making inference engine.
- Database (storing the data and fuzzy rules).

The model that embraces the fuzzy expert system is given in Fig.4 [4], [36]. The cyber expert can interact with the expert system interface in order to ask and read the advice from the proposed model. The inference engine consists of the cyber data threats, cyber terrorist profiles, and cyber attack techniques. System administrator (or any user) interacts with FRBCES using Matlab Fuzzy module. Inference engine gets commands from user by interface and evaluates these with the help of database in which rules are deposited.

3.4. Stage 4:Fuzzy Rule Based Model

The general architecture for rule-based expert system and the components of a fuzzy rule based inference system are shown in Fig.4. The main modules of a fuzzy rule based system are fuzzification - or fuzzifier module - , fuzzy rules, inference engine and defuzzifier.

Step 1. Fuzzification module: It converts a crisp input of the domain of the input variable domain to a grade by fuzzy set. Constructing a fuzzy logic membership functions play a crucial role for fuzzy rule based models. Triangular membership function was used in many fuzzy logic based applications [37]-[42]. In this study triangular membership functions have been used.

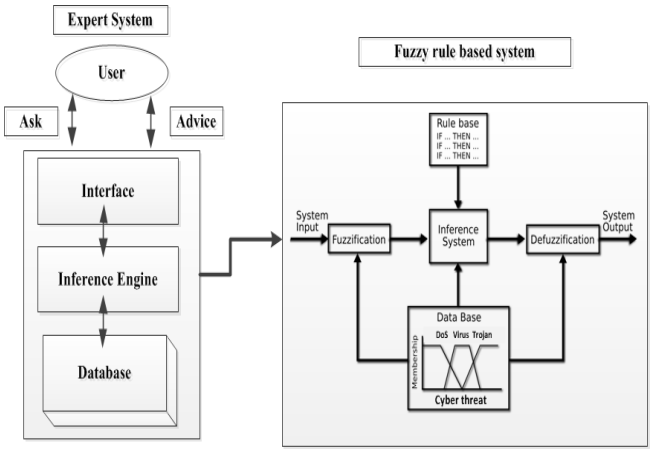

Fig.4: Fuzzy rule based expert system model

Step 2. Defining fuzzy rules: Fuzzy rules consist of antecedent and consequent in the form of IF-THEN statements. There are a number of rules, and they make a group which forms the basis for inference [43]. The following some fuzzy rules have been taken with the combination of linguistic

variable values. Input and output criteria of the model are "cyber techniques-(T)", "aim of cyber intruders-(A)", "cyber intruders (CI)- talented people capable of cyber terrorism", "cyber intruder's target-(CIT)", "sophisticated hardware-(H)", "software-(S)" and "user-(U)". Definitions of the criteria that is used in the FRBCES model and some of fuzzy rules for related criteria are given below:

Input 1. Cyber techniques (T): This criteria describes techniques that cyber attackers can use for an intrusion or any cyber crime. Common techniques used by cyber intruders are;

- Network attack (N-A),
- Denial of Service (DoS),
- Virus (V),
- E-mail virus (E-V),
- Logic bomb (L-B),
- Trojan horse (T-H),
- Social engineering (S-E),
- Malware (M).

Cyber Techniques (T) Rules

1R: If (T is N-A) and (A is OoS) and (CIT is CC) then (H is TC) (1)
2R: If (T is E-V) then (S is SpS)(H is SpC)(U is UT) (1)
3R: If (T is N-A) and (A is S-W-P) and (CIT is Kl) and (CI is CI) then (S is SpS)(H is TC) (1)
4R: If (T is M) and (A is CS) and (CIT is Kl) and (CI is SS) then (S is SpS)(H is SpC)(U is UT) (1)
5R: If (T is S-E) and (A is CS) and (CIT is CC) and (CI is CH) then (S is SU) (1)
6R: If (T is DoS) and (A is OoS) and (CIT is WW) and (CI is CH) then (S is NDB)(H is TC) (1)
7R: If (T is S-E) and (A is CCI) and (CIT is FC) and (CI is CH) then (U is UT) (1)
8R: If (T is S-E) and (A is CCI) and (CIT is Kl) and (CI is CI) then (U is UT) (1)

Input 2. Aim of Cyber Intruders (A): A cyber intruder usualy has purpose for cyber attack. This criteria defines various intention of cyber intruders. Aims of cyber intruders are;

- Out of service (OoS),
- Seizing web page (S-W-P),
- Protesting (P),
- Control of critical systems (CoCS),
- Capture confidental information (CCI),
- Control system (CS).

Aim of Cyber Intruders (A) Rules

9R: If (A is S-W-P) and (CIT is CC) and (CI is CI) then (S is SU) (1)
10R: If (A is P) and (CIT is Kl) and (CI is SS) then (S is SpS)(H is TC) (0.8)
11R: If (A is P) and (CIT is TR) and (CI is SS) then (S is SpS)(H is TC) (1)
12R: If (A is P) and (CIT is CC) and (CI is ES) then (S is SU)(U is AW) (1)
13R: If (A is CS) and (CIT is Kl) and (CI is SS) then (H is PC) (1)
14R: If (A is CS) and (CIT is Kl) and (CI is CI) then (S is SpS)(H is SpC)(U is UT) (1)
15R: If (A is CCI) and (CIT is FC) and (CI is CH) then (S is SU)(H is TC)(U is UsC) (1)

Input 3. Cyber Intruders (CI): A cyber intruder is a group or a person who violates network deficiencies. Different cyber intruders have been described as membership function in FRBCES model. They are;

- Special staff (SS),
- Computer hacker (CH),
- Enemy of the system (ES),
- Cyber activist (CA).

Cyber Intruders (CI) Rules

16R: If (CI is Kl) and (CI is SS) then (S is SpS)(H is SpC)(U is UT) (1)
17R: If (CI is Kl) and (CI is ES) then (S is SpS)(H is SpC)(U is UT) (1)
18R: If (CI is Kl) and (CI is CI) then (S is SpS)(H is SpC)(U is UT) (1)
19R: If (CI is Kl) and (CI is CH) then (S is SpS)(H is SpC)(U is UT) (1)
20R: If (CI is FC) and (CI is SS) then (S is SU)(H is TC)(U is UsC) (1)
21R: If (CI is FO and (CI is CHI then (S is SU)(H is TC)(U is UsO (1)
22R: If (CI is TR) and (CI is SS) then (S is SpS)(H is SpC)(U is AW) (1)

23R: If (CI is ES) and (CI is SS) then (S is SpS)(H is SpC)(U is AW) (1)

Input 4. Cyber Intruder's Target (CIT): 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;

- Communication systems (CC),
- Finance centers (FC),
- Power plants (PP),
- Emergency services (ES),
- Public transportation (PT),
- Public instituions (PI),
- Water works (WW),
- Oil and natural gas distributions (OND).

Cyber Intruder's Target-(CIT) Rules

24R: If (CIT is Kl) and (T is L-B) and (CI is CH) then (S is SpS)(H is SpC)(U is UT) (1)
25R: If (CIT is CC) and (T is L-B) and (CI is ES) then (S is SU)(H is TC)(U is AW) (1)
26R: If (CIT is Kl) and (CI is SS) then (S is SpS)(H is SpC)(U is UT) (1)
27R: If (CIT is Kl) and (CI is ES) then (S is SpS)(H is SpC)(U is UT) (1)
28R: If (CIT is Kl) and (CI is CI) then (S is SpS)(H is SpC)(U is UT) (1)
29R: If (CIT is Kl) and (CI is CH) then (S is SpS)(H is SpC)(U is UT) (1)

Output 1. Sophisticated hardware (H): System administrators should use special hardware in order to prevent cyber attacks. Sophisticated hardware criteria includes;

- Physical control (PC),
- Special computers (SC),
- Technical support (TS).

Output 2. Software (S): Cyber intruders may exploit software insufficiency. Users should apply;

- Special software (SS),
- System update (SU),
- National data bank (NDB).

Output 3. User (U): Users have awareness of cyber threats. They should take cyber security courses for improving their cyber ability. This criteria includes,

- User traning (UT),
- Awareness (AW),
- User control (UC).

Overview of the FRBCES model data is given in Table 1.

Step 3. Defuzzification: It acts as the interface between the fuzzy logic control and the inference system, by providing the crisp output. Regular defuzzification methods are centroid, bisector, mean value of maximum values, smallest value of maximum values and largest value of maximum [44],[26]. The conversion of a fuzzy set to a single crisp value is called defuzzification and reverse process is fuzzification [26]. Mamdani defuzzification method (centroid of the area) is used in the model. To find the defuzzification value the formula (Eq.17) has been used as:

$$z^* = \frac{\int \mu_C(z).z\ dz}{\int \mu_C(z)dz} \qquad (17)$$

where $\int$ denotes an algebraic integration.

4. Implementation

In this study, MATLAB® fuzzy logic toolbox is used for fuzzy rule based cyber expert system. The study is structured on as 4 input and 3 output criteria as depicted in Fig.2. Fuzzy Rule Based Cyber Expert System (FRBCES) against cyber terrorism has been implemented. The implementation has been performed with the help of the fuzzy rule with the minimum and maximum norm. The FRBCES has been developed with a view to taking the criteria "cyber techniques (T)", "aim of cyber intruders (A)", "cyber intruders (CI)", "cyber intruder's target-(CIT)", as input. "Sophisticated hardware (H)", "software (S)" and "user (U) criteria are designed as output. A membership function value for both input and output criteria is contributed using MATLAB®. Eighty-three fuzzy rules have been found in the

combination of the model. Different cyber terrorism activities have been recorded for the inputs (T, A, CIT, CI). One can state that based on FRBCES, precautions against cyber terror may be predicted. It is possible to use many MATLAB® commands in order to get detailed data concerning the proposed model. A sample symbolic output of MATLAB® fuzzy tool "getfis" and "showrule" command is given in following.

```
>>getfis (model_FRBCES)
    Name      = model_FRBCES
    Type      = mamdani
    NumInputs = 4
    InLabels  =
        T
        A
        CIT
        CI
    NumOutputs = 3
    OutLabels =
        S
        H
        U
    NumRules = 83
    AndMethod = min
    OrMethod = max
    ImpMethod = min
    AggMethod = max
    DefuzzMethod = centroid
ans =
model_FRBCES
```

Table 1. Model overview.

Overview	Overview FRBCES Model Data	Input	Input Membership Function Labels	Output	Output Membership Function Labels
Type	mamdani	Cyber Techniques (T)	N-A	Sophisticated Software (S)	SpS
Inputs/Outputs	[4 3]		DoS		SU
NumInputMFs	[8 6 8 4]		V		NDB
NumOutputMFs	[3 3 3]		E-V	Hardware (H)	PC
NumRules	83		T-H		SpC
AndMethod	min		S-E		TC
OrMethod	max		M	User (U)	UT
ImpMethod	min		L-B		AW
AggMethod	max	Aim of Cyber Intruders (A)	OoS		UsC
DefuzzMethod	centroid		S-W-P		
Input Labels	T		P		
	A		CCI		
	CIT		CoCS		
	CI		CS		
Output Labels	S	Cyber Intruders Target (CIT)	CC		
	H		FC		
	U		PP		
Input Range	[0 1]		OND		
	[0 1]		WW		
	[0 1]		TR		
	[0 1]		ES		
Output Range	[0 1]		KI		
	[0 1]	Cyber Intruders (CI)	CH		
	[0 1]		CA		
			ES		
			SS		

```
>>showrule (a,[3 1], 'symbolic')

ans =

3. (T==N-A) & (A==S-W-P) & (CIT==KI) &
(CI==CA) => (S=SpS)(H=TC) (1)

1. (T==N-A) & (A==OoS) & (CIT==CC) => (H=TC)
(1)
```

4.1. FRBCES Simulation Sample

Simulation: A special staff (SS) intents to deploy cyber attack to finance centers (FC) using denial of service (DoS) technique. His aim is to control of system (CS). According to the proposed model, a sample solution is given in Fig.5 when CI(SS)=0.15; CIT(FC)=0.32; T(DoS)=0.17; A(CS)=0.92. Here, model outputs are S=0.392; H=0.719 and U=0.57. Solution area is shown in red line.

It can be seen that cyber techniques (T) criteria is in y axis, cyber intruder's target (CIT) criteria is in x axis, and solution criteria (sophisticated software, S) is in z axis (Fig.6).

Output of S=0.392 means that system needs update (SU); H=0.719 means that system needs technical support (TS); U=0.57 means that users awareness (AW) is important. MATLAB® images of the solution set for output criteria S when CIT=0.32, T=0.17 and T=0.17, A=0.92 is given in Figs. 6 and 7.

5. Conclusions

In this paper, an expert system for cyber security based on fuzzy rule was presented. After consultation with cyber experts and system administrators, the inputs and output of the system were determined. Mamdani fuzzy inference system was selected. The inference of the fuzzy rules was carried out using the 'min' and 'max' operators for fuzzy intersection and union. A series of 83 fuzzy if-then rules were designed for the knowledge base. Input space was divided into multidimensional partitions in order to formulate the initial rule base. Actions were then assigned to each of the partitions.

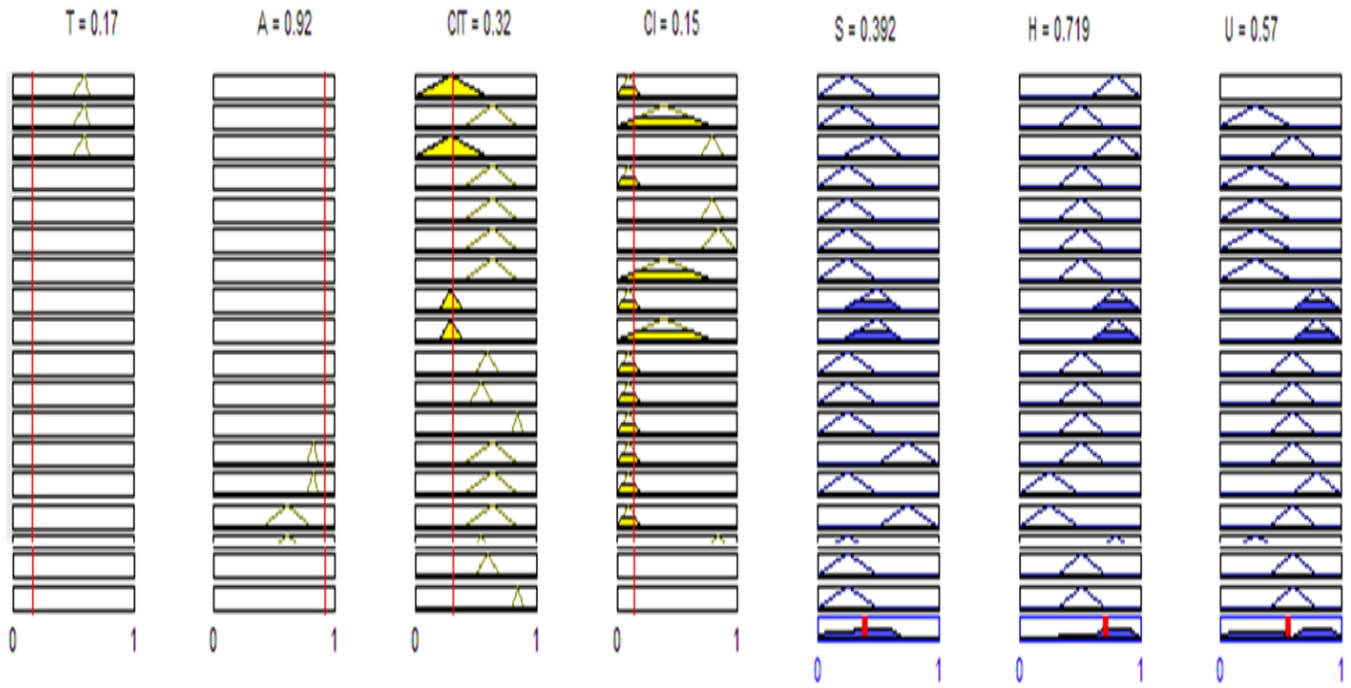

Fig.5: Sample solution area of simulation.

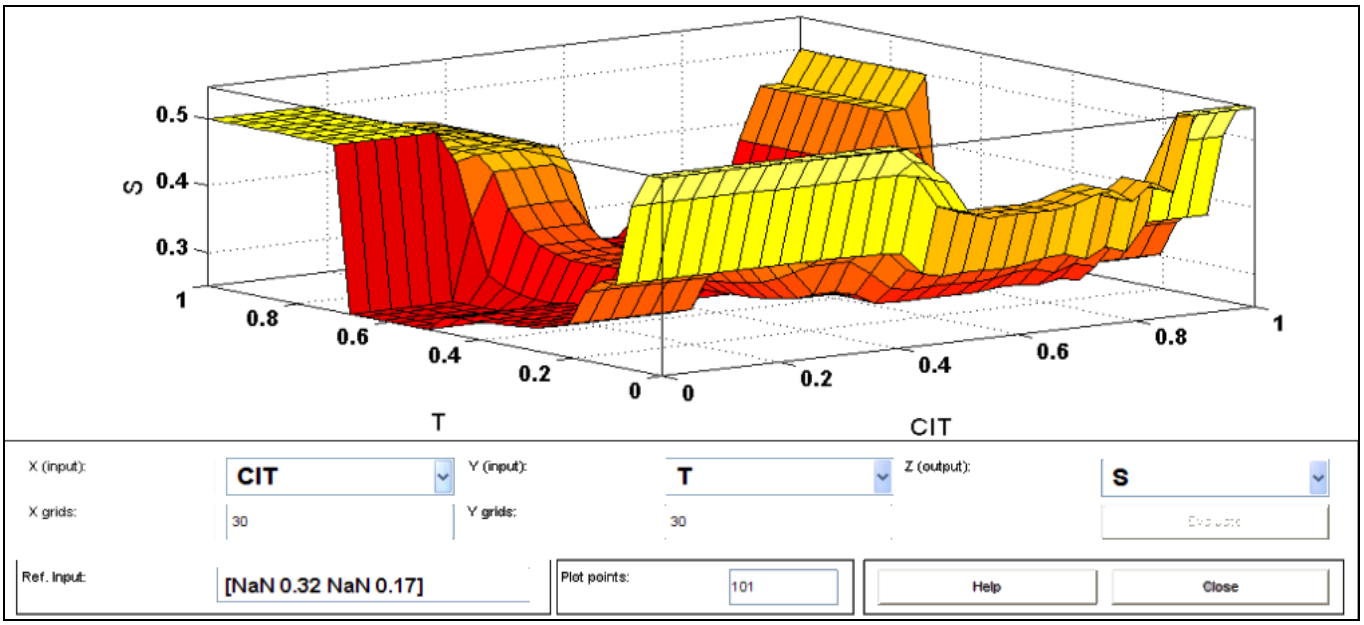

Fig.6: Sample solution set for "CIT-T- S"

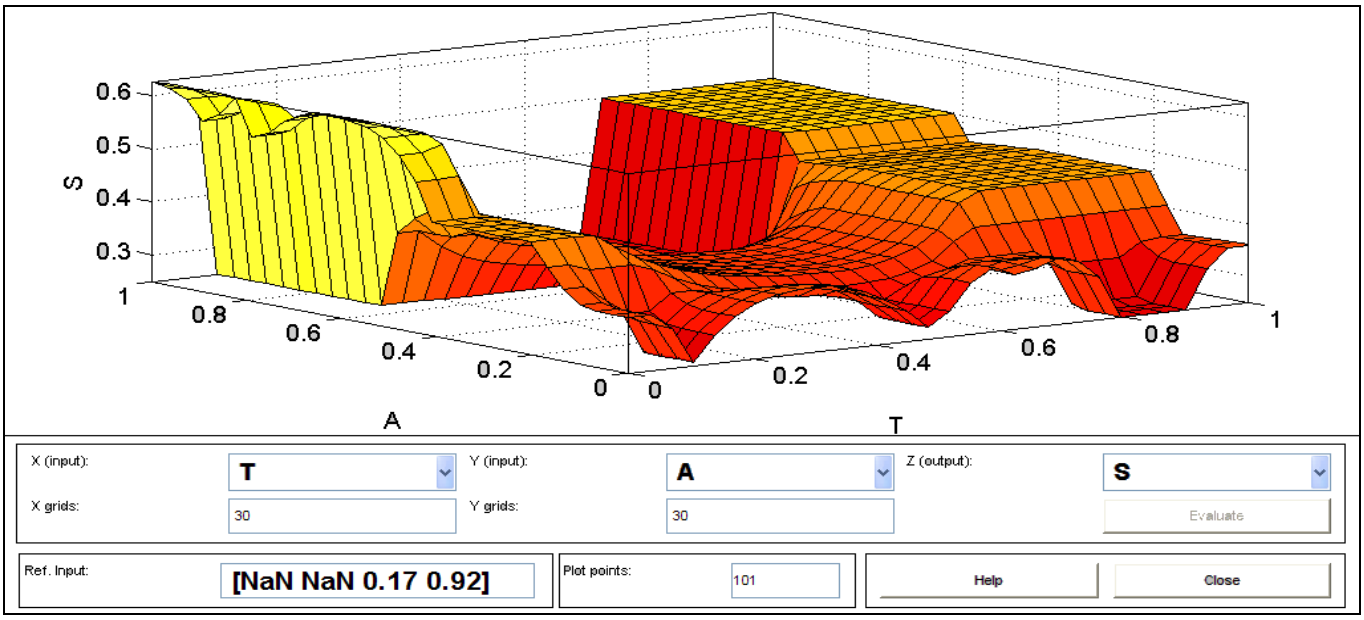

Fig.7: Sample solution set for "T-A-S"

This study proposes a fuzzy rule based cyber indicator that warns system administrators for expected cyber threats. It has been found that a system works well when applied with a given cyber threat scenario (please see the simulation results). This facilitates some warning signals generated by the rules. The model's goal is not to protect a system; however it aims at warning the system administrator for expected cyber threats. The proposed model shows its superiority in the areas of development flexibility and fast response for cyber threats. The model can be used by system administrators in order to determine the nature of cyber threat triggered by cyber terrorists. Also, it can be used by commercial firms or government institutions to form a more secured knowledge environment.

It could be attractive to the researchers to

compare the performance of fuzzy rule based expert system with other meta-heuristics (e.g. Artificial Neural Network, Genetic Algorithm, Fuzzy Neural Networks) or regular statistical methods (Linear/Nonlinear Regression). A special interest would be on testing whether fuzzy rule based approach has any advantage in dealing with the cyber security threats.

ACKNOWLEDGEMENT

I thank to Prof.Dr. Cengiz Kahraman for his valuable contribution.

REFERENCES

[1] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, S. Shenoi, "Security strategies for SCADA networks," in: Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, Mar. 19-21, 2007.

[2] N. Fovino, M. Masera, "Through the description of attacks: a multidimensional view", in: Proceeding of the 25th International Conference on Computer Safety, Reliability and Security, Gdansk, Poland, Sep. 26-29, 2006.

[3] R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), vol.2, 1, pp. 101-111, 2011.

[4] S. M. Bridges, and R. B.Vaughn, "Fuzzy Data Mining And Genetic Algorithms Applied to Intrusion Detection", In Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, 2000, pp.16-19.

[5] J.T. Yao, S.L. Zhao, and L.V. Saxton, "A Study On Fuzzy Intrusion Detection", In Proceedings of the Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, SPIE, Vol. 5812, Orlando, Florida, USA, 2005, pp. 23-30.

[6] S. Mukkamala, G. Janoski, A. Sung, "Intrusion detection: support vector machines and neural networks." In: Proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE), St. Louis, MO, 2002, pp. 1702-1707.

[7] Y. Yu, and H. Hao, "An Ensemble Approach to Intrusion Detection Based on Improved Multi-Objective Genetic Algorithm", Journal of Software, Vol.18, No.6, pp.1369-1378, June 2007.

[8] J. Cannady, "Artificial Neural Networks for Misuse Detection", in Proceedings of the '98 National Information System Security Conference (NISSC'98), 1998, pp. 443-456.

[9] W. Lee, S. Stolfo, and K. Mok, "A Data Mining Framework for Building Intrusion Detection Model", In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, 1999, pp. 120-132.

[10] J. Luo, and S. M. Bridges, "Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection", International Journal of Intelligent Systems, Vol. 15, No. 8, pp. 687-704, 2000.

[11] C. Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress, Oct. 17, 2003.

[12] N. Fovino, M. Masera, "A service oriented approach to the assessment of infrastructure security", in: Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, Mar. 19-21, 2007.

[13] S.M.Furnel and M.J.Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?", Computers & Security, vol.18, pp.28-34,1999.

[14] L. Pietre-Cambacedes, T. Kropp, J.Weiss, and R. Pellizzonni, "Cybersecurity standards for the electric power industry-A survival kit," in CIGRÉ Paris Session, 2008, D2-217.

[15] R. P. Evans, R. C. Hill, and J. G. Rodriquez, "A Comparison of CrossSector Cyber Security Standards Idaho National Laboratories", Idaho National Labs Rep. INL/EXT-05-00656, 2005.

[16] M. Ferris, "New Email Security Infrastructure", Proceeding of New security Paradigms Workshop, Aug. 3-5, 1994, pp. 20-27.

[17] M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, "Distributed network protocol security (DNPSec) security framework", in: Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, Arizona, Dec. 5-9, 2005.

[18] A. Abraham, C. Grosan, C. Martin-Vide, "Evolutionary design of intrusion detection programs." International Journal of Network Security, vol. 4(3), pp.328-339, 2007.

[19] W. Chimphlee, A.H. Abdullah, M.N. Sap, S. Srinoy, and S. Chimphlee, "Anomaly-based intrusion detection using fuzzy rough clustering." In Proceedings of the international conference on hybrid information technology (ICHIT'06), 2006, pp. 320-334.

[20] L. Khan, M. Awad, and B. Thuraisingham. "A new intrusion detection system using support vector machines and hierarchical clustering", The International Journal on Very Large Data Bases, vol. 16(4), pp.507–521, 2007.

[21] A.N. Toosi, M. Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Computer Communications, vol.30, pp. 2201-221, 2007.

[22] A. Tajbakhsh, M. Rahmati, A. Mirzaei, "Intrusion detection using fuzzy association rules", Applied Soft Computing, Vol: 9, No: 2, pp. 462-469, 2009.

[23] B. Shanmugam, N. B. Idris, "Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anamoly and Misuse Type of Attacks", in Proceedings of the International Conference of Soft Computing and Pattern Recognition, 2009, pp: 212-217.

[24] O. Cordon, F. Gomide, F. Herrera, F. Hoffmann, L. Magdalena, "Ten years of genetic fuzzy systems: current

framework and new trends", Fuzzy Sets and Systems, vol.141, no.1, pp. 5–31, 2004.
[25] L.A. Zadeh, "Fuzzy sets", Information Control, vol.8, pp.338-353,1965.
[26] E.H. Mamdani, and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller", Int. J. Man-Mach. Stud., vol.7, pp.1-13, 1975.
[27] J. Lu, G. Zhang, D. Ruan, "Multi-Objective Group Decision Making: Methods, Software and Applications with Fuzzy Set Techniques", Imperial College Press, London, 2007.
[28] J.C. Giarratano and G. Riley, "Expert systems principles and programming", MA, USA: PWS-KENT Publishing Company, 1989.
[29] N.J. Nilsson, "Principles of Artificial Intelligence", Palo Alto, CA. Tioga, 1980.
[30] M. Schneider, G. Langholz, A. Kandel, and G. Chew, "Fuzzy Expert System Tools", John Wiley & Sons, USA, 1996.
[31] J. J. Prichard and L. E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks", Journal of Information Technology Education, Vol. 3, 2004.
[32] J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification", CRS Report for Congress , Oct. 1, 2004.
[33] J. A. Chandler, Security in Cyberspace: Combatting Distributed Denial of Service Attacks, , University of Ottawa Law & Technology Journal, pp.231-261, 2004.
[34] W. Siler, J. J. Buckley, Fuzzy Expert Systems and Fuzzy Reasoning, New Jersey, 2005.
[35] L. Medsker, J. Liebowitz, "Design and development of expert systems and neural networks", NY, USA: McMillan College Publishing Company, 1994.
[36] A. Kengpol and W. Wangananon, "The expert system for assessing customer satisfaction on fragrance notes: Using artificial neural networks", Computer & Industrial Engineering, vol.51(4), pp.567-584, 2006.
[37] H. Hellendoorn, and C. Thomas, "Defuzzification in fuzzy controllers", Int. Fuzzy Syst., vol.1, pp.109-123, 1993.
[38] M. Fasanghari, F.H. Roudsari, "The fuzzy evaluation of e-commerce customer satisfaction", World Applied Sciences Journal, vol.4(2), pp.164-168, 2008.
[39] A.A. Gamil, R.S. El-fouly and N.M. Darwish, "Stock technical analysis using multi agent and fuzzy logic", Proceedings of the world congress on engineering. Vol I WCE 2007, Jul. 2-4, 2007.
[40] E. Giovanis, "Application of adaptive network-based fuzzy inference system in macroeconomic variables forecasting", World Acad. Sci. Eng. Technoh, vol.64, pp.660-667, 2010.
[41] H. Kwasnicka, and M. Ciosmak, "Intelligent techniques in stock analysis", Proceedings of Intelligent Information Systems. (IIS'02), Arnetminer, 2001, pp. 195-208.
[42] S. Önüt, S.S. Kara, and E. Işık, "Long term supplier selection using a combined fuzzy MCDM approach: A case study for a telecommunication company Industrial Engineering", Expert Systems with Applications, vol.36, pp. 3887-3895, 2009.
[43] M. Ganesh, "Introduction to Fuzzy Sets and Fuzzy Logic", Phi Learning, India, 2009.
[44] R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), vol.2, 1, pp. 101-111, 2011.