Network Threat Ratings in Conventional DREAD Model Using Fuzzy Logic

Ak. Ashakumar Singh[1], K.Surchandra Singh[2]

[1]Department of Computer Science, Thoubal College, Manipur University, Manipur-795138, India.

[2] Department of Computer Science, CMJ University, Shillong, Meghalaya, India.

Abstract

One of the most popular techniques to deal with ever growing risks associated with security threats is DREAD model. It is used for rating risk of network threats identified in the abuser stories. In this model network threats needs to be defined by sharp cutoffs. However, such precise distribution is not suitable for risk categorization as risks are vague in nature and deals with high level of uncertainty. In view of these risk factors, the paper proposes a novel fuzzy approach using DREAD model for computing risk level that ensures better evaluation of imprecise concepts. Thus, it provides the capacity to include subjectivity and uncertainty during risk ranking. These threat parameters need to be frequently updated based on feedbacks from implementation of previous parameters. These feedbacks are always stated in the form of ordinal ratings, e.g. "high speed", "average performance", "good condition". Different people can describe different values to these ordinal ratings without a clear-cut reason or scientific basis. There is need for a way or means to transform vague ordinal ratings to more appreciable and precise numerical estimates. The paper transforms the ordinal performance ratings of some system performance parameters to numerical ratings using Fuzzy Logic.

Keywords**:** *Fuzzy logic, threat rating, Transformation,* DREAD *Model.*

1. Introduction

The computer network security remains a problem of great concern within information technology research area. Increase of network scale, development of advanced information technologies, and other factors enhance the number of possible targets for attacks against computer networks. These factors negatively influence upon the efficiency of the existing computer networks security systems and enable research and development of *new protection models and technologies* [1].

[2]System security is one of the most significant issues in today's software society. Several security threats arise during software development process. Software failures, due to various vulnerabilities present in software, suggest essential presence of security in every phase of software development method. Microsoft's DREAD model is a popular approach for computing risk level of threats but it allows only crisp values [3]. Virtually every risk element can be characterized using two metrics, "Low, Medium, and High," or through "Ordinal Ranking". Therefore, most appropriate approach for defining risk level is using fuzzy logic. In this truth or validity of any statement becomes its degree of belongingness or membership.

This degree corresponds to a value to which an object is similar or compatible with the concept represented by fuzzy set. Truthfulness of a statement can be of various degrees which ranges from completely true, to partially true and then to completely false [4]. Moreover, fuzzy logic has linguistic values taken as words which can represent natural language for human reasoning during fuzzy rules construction. This means that these ratings have some elements of uncertainty, ambiguity or fuzziness.

When humans are the basis for an analysis, there must be a way to assign some rational value to intuitive assessments of individual elements of a fuzzy set. There is need to translate from human fuzziness to numbers that can be used by a computer.

Lofti A Zadeh introduced Fuzzy Set Theory (FST) in the early 1960's as a means of modeling the uncertainty, vagueness, and imprecision of human natural language. It was built on the basis that as the complexity of a system increases, it becomes more difficult and eventually impossible to make a precise statement about its behavior, eventually

arriving at a point of complexity where the fuzzy logic method born in humans is the only way to get at the problem.

[5] Described *Fuzzy Set Theory (FST)* as the extension of classical set theory. The basic idea is that the membership of a value to a set cannot only assume the two values "yes" or "no", but can be expressed by gradual membership function within a range from zero to normally "1" in case of full membership degree. Membership function can assume several forms, and in practice triangular or trapezium forms are often used (Figure 1).

2. Problem Defined

The linguistics variables parameters of conventional DREAD Model viz. Damage potential (DP) of threat, Reproducibility (R) of the attack works, Exploitability (E) of threat, Affected User (A), and Discoverability(D) of the attacker are imprecise or fuzzy. The network threat parameters involved in the paper are respectively categorized as (1) Blind SQL Injection, (2) Login page SQL Injection, (3) Unencrypted login request, (4) Application error, (5) Inadequate account lockout, (5) Permanent cookie contains sensitive session information, (6) Session information not updated, (7) Unencrypted password parameter, and (8) Unencrypted view state parameter.

The ratings are in rough (imprecise, inexact or fuzzy) ranges, reflecting the variability in how each strategy could be implemented and the uncertainties involved in projecting the impacts of the strategies. For a meaningful numerical research, as stated in the introduction, these ordinal ratings need to be transformed to numerical ratings and this forms the thrust of the paper. That is, to transform opinion held by human beings, which would be "fuzzy" (e.g. low, mid-high performance) to being very precise (e.g. 15%, 80% performance), that is not "fuzzy" using fuzzy set theory [5], [6].

3. Theoretical Foundations

A fuzzy system is a system whose variable(s) range over states that are approximate. The fuzzy set is usually an interval of real number and the associated variables are linguistic variable such as "most likely", "about", etc. [5]. Appropriate quantization, whose coarseness reflects the limited measurement resolution, is inevitable whenever a variable represents a real-world attribute. Fuzzy logic consists of Fuzzy Operators such as "IF/THEN rules", "AND, OR, and NOT" called the *Zadeh operators* [6].

The Membership Function is a graphical representation of the magnitude of participation of each input. It associates a weighting with each of the inputs that are processed, define functional overlap between inputs, and ultimately determines an output response. Once the functions are inferred, scaled, and combined, they are defuzzified into a crisp output which drives the system. There are different memberships functions associated with each input and output response. Some features of different membership functions are: SHAPE - triangular is common, but bell, trapezoidal, haversine and, exponential have been used also; HEIGHT or magnitude (usually normalized to 1); WIDTH (of the base of function); SHOULDERING; CENTER points (centre of the member and OVERLAP (Figure 1) [9].

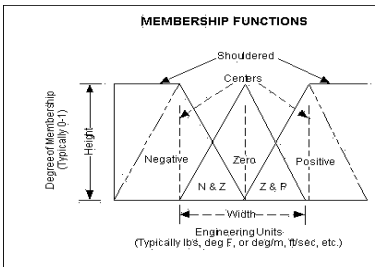


Fig. 1 Triangular membership function

The degree of fuzziness of a system analysis rule can vary between being very precise, that is not "fuzzy", to being based on an opinion held by a human, which would be "fuzzy." Being fuzzy or not fuzzy, therefore, has to do with the degree of precision of a system analysis rule.

The Degree of Membership (DOM) is the placement in the transition from 0 to 1 of conditions within a fuzzy set. The degree of membership is determined by plugging the selected input parameters into the horizontal axis and projecting vertically to the upper boundary of the Membership function(s) [9]. Fuzzy Variable includes words like red, blue, good and sweet are fuzzy and can have many shades and tints. A Fuzzy Algorithm is a procedure, usually a computer program, made up of statements relating linguistic variables. A Fuzzy Logic Control System-measures an input against a given situation and the system takes action automatically.

4. Methodology

The relative effectiveness of these threat ratings is summarizes as shown in Table 1 in terms of conventional five basic criteria: [2] (1)Damage Potential (DP) of threat, (2)Reproducibility (R) of the attack works, (3)Exploitability (E) of threat, (4)Affected User (A), and (5)Discoverability(D) of the attacker. In the table, the system performs between ***medium to high*** on practical reduction effectiveness, ***high*** in terms of economic efficiency, ***medium to high*** on economic equity for the poor and ***medium to high*** on immediate access flexibility.

5. Notations

a Blind SQL Injection
b Login page SQL Injection
c Unencrypted login request
d Application error
e Inadequate account lockout
f Permanent cookie contains sensitive session information
g Session information not updated
h Unencrypted password parameter
i Unencrypted view state parameter
me medium
hi high
lo low
min Minimun
Max Maximum
Avg Average
Temp Temperature
Conc Concentration
THR Threat

Table 1: Threat parameters ratings

Multi-objective Evaluation of the system					
Threat parameters	Ratings on Objectives (high = best)				
	DP	R	E	A	D
(a)	me-hi	hi	me-hi	me-hi	me
(b)	me-hi	me-hi	me-hi	me-hi	hi
(c)	lo-me	lo-me	me	hi	me-hi
(d)	lo-me	lo	me	hi	lo
(e)	lo-me	lo	me	me	lo-me
(f)	lo	me	hi	lo-me	lo
(g)	me	hi	lo-me	me-hi	me
(h)	me-hi	lo	me	lo	me-hi
(i)	hi	me	lo-me	me-hi	lo

6. Fuzzy Variables

In the paper, the adjectives describing the fuzzy variables and the range of threat are shown in Table 2. The Range of threat for the individual fuzzy variables is substituted in Table 1 to obtain Table 3.

Table 2: Fuzzy Variables and their ranges.

Fuzzy Variables	Range of threat %
High (hi)	75 – 100
Med-High (me-hi)	55 - 80
Med (Medium)(me)	35 - 60
Low-Med (lo-me)	15 - 40
Low (lo)	0 - 20

Table 3**:** Fuzzy Range of Performance for the individual fuzzy variables.

Multi-objective Evaluation of the system					
Threat parameters	Ratings on Objectives (high = best)				
	DP	R	E	A	D
(a)	55 - 80	75 – 100	55 - 80	55 - 80	35-60
(b)	55 - 80	55 - 80	55 - 80	55 - 80	75-100
(c)	15 - 40	15 - 40	35 - 60	75 – 100	55-80
(d)	15 - 40	0 - 20	35 - 60	75 – 100	0-20
(e)	15 - 40	0 - 20	35 - 60	35 - 60	15-40
(f)	0-20	35-60	75-100	15-40	0-20
(g)	35-60	75-100	15-40	55-80	35-60
(h)	55-80	0-20	35-60	0-20	55-80
(i)	75-100	35-60	15-40	55-80	0-20

7. Fuzzy Mapping

The fuzzy variables in Table 1, were transformed to numerical ratings using *Fuzzy Set Theory* as shown in Figures 2–6.

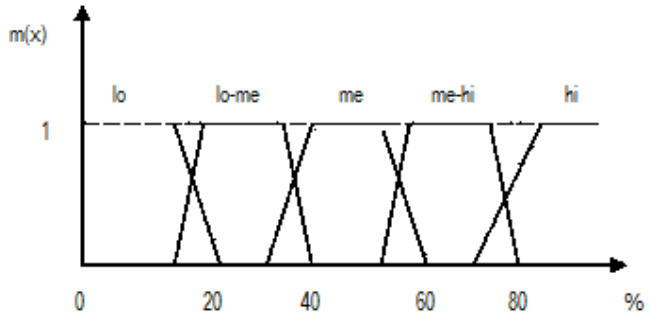


Fig. 2: Trapezoidal membership function

8. Aggregation of Fuzzy Scores

Using Figure 3, for each System parameters (SP) *i* and each criterion (CRIT) *j*,

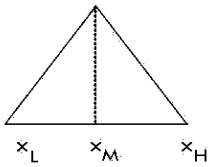


Fig. 3: Aggregation of Fuzzy Scores.

i = 1, 2, 3, ...,9 . and j = 1, 2, 3, 4, 5.

For CRIT (j) when SP(i, j) = x_L THEN SPTHR (i, j) = L

For CRIT (j) when SP(i, j) = x_M THEN SPTHR (i, j) = M

For CRIT (j) when SP(i, j) = x_H THEN SPTHR (i, j) = H

Where, CRIT (j) ≡ Criterion j (j = 1, 2, 3, 4, 5)

SP (i, j) ≡ System parameters i under Criterion j
SPTHR(i, j) ≡ System Threat parameters i under Criterion j
Performance:

$$\text{SPTHRSCORE(i)} = \sum_{j} \frac{\text{SP(i, j)}}{5} \qquad (1)$$

9. Membership Functions of the Fuzzy Sets

Using Aggregation methods for the fuzzy sets to reduce it to a triangular shape for the membership function, overlapping adjacent fuzzy sets were considered with the membership values shown in Figure 4.

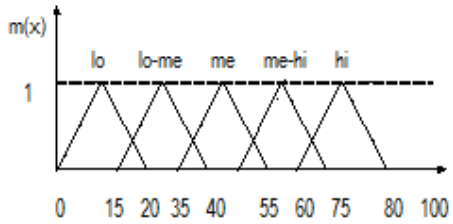
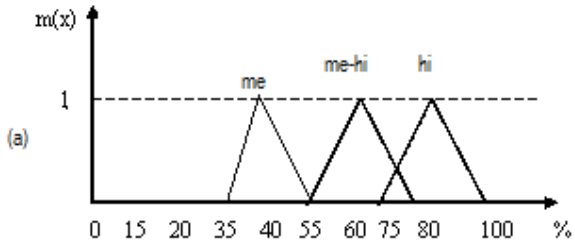
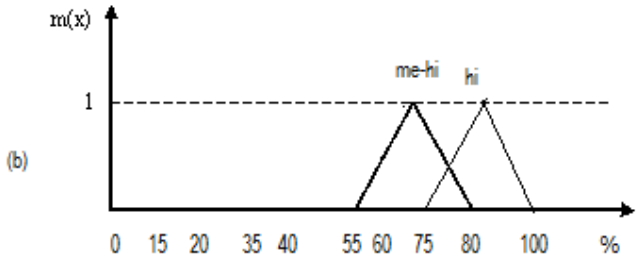


Fig. 4: Derived Triangular membership function

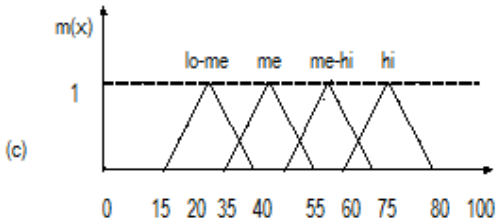
For the strategies and their performances, the membership functions shown in Figure 5 of the fuzzy sets were assigned.



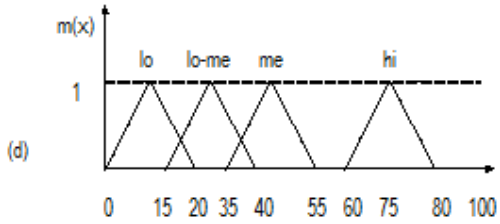
Criteria: (DP, E, A = med-hi; R = hi; D=me)



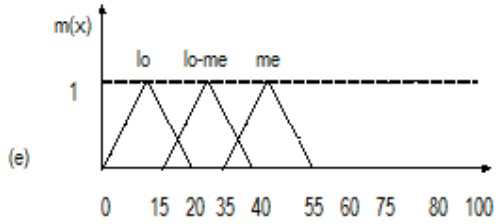
Criteria: (DP, R,E,A = me-hi; D=hi)



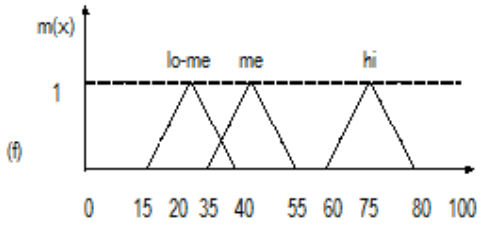
Criteria: (DP, R = lo-me; E = me; A = hi; D=me-hi)



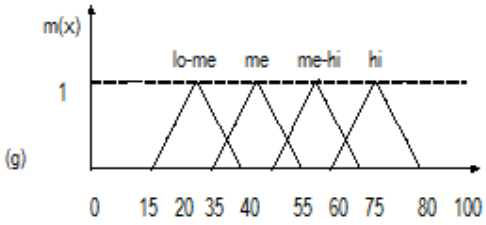
Criteria: (DP = lo-me; R, D = lo; E = me; A = hi)



Criteria: (DP, D = lo-me; R = lo; E, A = me)



Criteria: (DP, D,A = lo-me; R = me; E=hi)

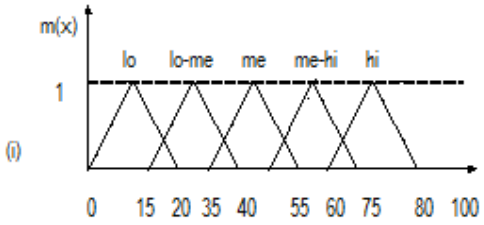


Criteria: (DP, D=me; R =hi; E= lo-me; A = me-hi)

Criteria: (DP, D=me-hi; R,A=lo; E = me)

Criteria: (DP=hi; R=me; E=lo-me; A=me-hi; D =lo)

Fig. 5: Derived triangular membership functions for the System parameters.



The ranges in figure 4 and figure 5 were aggregated to singletons. For the average performance of all the strategies, we have the fuzzy scaled rating as shown in figure 6.

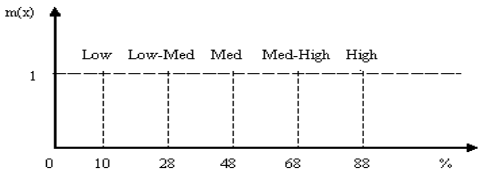


Fig. 6: Singleton aggregation of the ratings in table 1.

From Figs. 2–6, the Membership Values assigned to each set of Universe of Discourse can be tabulated as shown in Table 4.

Table 4: Fuzzy threat ratings of Membership Values assigned to each set of Universe of Discourse.

Threat parameters	Criteria									
	DP		R		E		A		D	
(a)	Me-hi		hi		Me-hi		Me-hi		me	
	X	Y	X	Y	X	Y	X	Y	X	Y
	55	0	75	0	55	0	55	0	35	0
	68	1	88	1	68	1	68	1	48	1
	80	0	100	0	80	0	80	0	60	0
(b)	Me-hi		Med-hi		Me-hi		Me-hi		hi	
	X	Y	X	Y	X	Y	X	Y	X	Y
	55	0	55	0	55	0	55	0	75	0
	68	1	68	1	68	1	68	1	88	1
	80	0	80	0	80	0	80	0	100	0
(c)	Lo-me		Lo-me		me		hi		Me-hi	
	X	Y	X	Y	X	Y	X	Y	X	Y
	15	0	15	0	35	0	75	0	55	0

	28	1	28	1	48	1	88	1	68	1
	40	0	40	0	60	0	100	0	80	0
(d)	Lo-me		lo		me		hi		Lo	
	X	Y	X	Y	X	Y	X	Y	X	Y
	15	0	0	0	35	0	75	0	0	0
	28	1	10	1	48	1	88	1	10	1
	40	0	20	0	60	0	100	0	20	0
(e)	Lo-me		lo		me		me		Lo-me	
	X	Y	X	Y	X	Y	X	Y	X	Y
	15	0	0	0	35	0	35	0	15	0
	28	1	10	1	48	1	48	1	28	1
	40	0	20	0	60	0	60	0	40	0
(f)	Lo-me		lo		me		Lo-me		Lo	
	X	Y	X	Y	X	Y	X	Y	X	Y
	15	0	0	0	35	0	15	0	0	0
	28	1	10	1	48	1	28	1	10	1
	40	0	20	0	60	0	40	0	20	0
(g)	me		hi		Lo-me		Me-hi		me	
	X	Y	X	Y	X	Y	X	Y	X	Y
	35	0	75	0	15	0	55	0	35	0
	48	1	88	1	28	1	68	1	48	1
	60	0	100	0	40	0	80	0	60	0
(h)	Me-hi		lo		me		lo		Me-hi	
	X	Y	X	Y	X	Y	X	Y	X	Y
	55	0	0	0	35	0	0	0	55	0
	68	1	10	1	48	1	10	1	68	1
	80	0	20	0	60	0	20	0	80	0
(i)	hi		me		Lo-me		Me-hi		lo	
	X	Y	X	Y	X	Y	X	Y	X	Y
	75	0	35	0	15	0	55	0	0	0
	88	1	48	1	28	1	68	1	10	1
	100	0	60	0	40	0	80	0	20	0

10.Results

From the above figure 3, it is shown that x_L , x_M and x_H are referred to as the Minimum performance, Average performance and Maximum Performance. Using equation (1), we can calculate the Average Scores of different LAN performance strategies for all the four criteria in respect of x_L referring to as the Minimum Performance (as shown in Table 5), in respect of x_M referring to as the Average Performance (as shown in Table 6), and in respect of x_H referring to as the Maximum performance (as shown in Table 7).

Table 5: Numerical transformation of Threat parameters for Minimum threat using fuzzy set theory.

Multi-objective Evaluation of the System						
Threat parameters	Ratings on Objectives (high = best)					
	DP	R	E	A	D	Avg. Score
(a)	55	75	55	55	35	55
(b)	55	55	55	55	75	59
(c)	15	15	35	75	55	39
(d)	15	0	35	75	0	25
(e)	15	0	35	35	15	20
(f)	15	0	35	15	0	13
(g)	35	75	15	55	35	43
(h)	55	0	35	0	55	29
(i)	75	35	15	55	0	36

Table 6: Numerical transformation of Threat parameters for Medium Threat using fuzzy set theory.

Multi-objective Evaluation of The System						
Threat parameters	Ratings on Objectives (high = best)					
	DP	R	E	A	D	Avg. Score
(a)	68	88	68	68	48	68
(b)	68	68	68	68	88	72
(c)	28	28	48	88	68	52
(d)	28	10	48	88	10	37
(e)	28	10	48	48	28	32
(f)	28	10	48	28	10	25
(g)	48	88	28	68	48	56
(h)	68	10	48	10	68	41
(i)	88	48	28	68	10	48

Table 7: Numerical transformation of the Threat parameters for Maximum Threat using fuzzy set theory.

Multi-objective Evaluation of System						
Threat parameters	Ratings on Objectives (high = best)					
	DP	R	E	A	D	Avg. Score
(a)	80	100	80	80	60	80
(b)	80	80	80	80	100	84
(c)	40	40	60	100	80	64
(d)	40	20	60	100	20	48
(e)	40	20	60	60	40	44
(f)	40	20	60	40	20	36
(g)	60	100	40	80	60	68
(h)	80	20	60	20	80	52
(i)	100	60	40	80	20	60

Table 8: Comparison between the ordinal fuzzy ratings and the transformed ratings on various criteria of LAN performance.

Ordinal (Fuzzy Ratings)	System parameters	Min Thr	Avg Thr	Max Thr
m-h	(a)	55	68	80
m-h	(b)	55	68	80
m-h	(c)	15	28	40

Similarly, for other fuzzy ratings of different System criteria, their comparisons can be found out.

Hence, their threat ratings can be shown such as $x_L < x_M < x_H$.

11. Conclusion

Fuzzy logic was used to transform ordinal System parameters of computer network threat ratings that are imprecise and fuzzy in nature to precise and defuzzified numerical ratings used in the analysis of threat ratings of different optimized threat parameters. The Technique used is the only way for solving any highly complex problem. The optimized system parameters will surely save the search time for technologies involved in the analysis of computer network threats.

Reference:

[1] Vladimir Gorodetski, Igor Kotenko and Oleg Karsaev, Multi-Agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning, *International Journal of Computer Systems Science and Engineering*, *18*(4), 2003, 191-200.

[2] Sonia, Archana Singhal and Banati, Fuzzy Logic Approach for threat prioritization in Agile Security Framework using DREAD Model, *International Journal of Computer Science Issues*, *8*(4), July 2011, 182-190.

[3] Howard M., and Leblanc D., Writing Secure Code, Second Edition, Microsoft Press, December 2002.

[4] System Vulnerability Mitigation, The SANS Institute, Dec-2003,www.sans.org/system-vulnerability-mitigation _339-United States.

[5] L.A. Zadeh, Fuzzy sets, *Information and Control*, 1965, *8*, 338 – 353.

[6] L.A. Zadeh, Toward a theory of fuzzy information granulation and its Centrality in human reasoning and Fuzzy logic, *International Journal of Soft Computing and Intelligence*, *90*(2), 1997, 111 – 127.

[7] T.Sowell,*Fuzzy-Logic*,http://www.fuzzy logic.com/ ch3. Htm, (2005).

[8] S.D. Kaehler, *Fuzzy Logic*, http://www.seattlerobotics.org/encoder/mar98/fuz /flindex.html (1998)

[9] M.Kantrowitz,*Fuzzy-logic/part1*.[Online], 1997.

Biography:

Ak. Ashakumar Singh graduated in Mathematics from Manipur University, Imphal and passed MCA in the year 2000 from the same varsity. He was awarded Ph.D. in the area of Computer Science from the Dept. of Mathematics of the same varsity in the year 2008. Then produced eight M.Phil scholars in Computer Science and now supervising three scholars leading to Ph.D. in Computer Science. The area of research is on Soft computing and related applications of computer science.

K.Surchandra Singh completed his Master of Computer Application (MCA) from Manipur University in the year 2000. Currently, he is a research scholar in the Department of Computer Science, CMJ University-India. He was working as faculty in the Institute of Cooperative Management, Imphal (India) since 2001 upto 2011, which has been conducting Post Graduate Diploma in Computer Application (PGDCA) affiliated to Manipur University, Canchipur (India). His research interest is in low cost network activities using Fuzzy logic principles.