A Model for Assessing the Level of Multi-Parameter Threats Using the Mamdani Fuzzy Logic Algorithm

Petrenko Olha Yevhenivna[1]
Petrenko Oleksii Serhiiovych[2],
Ostrovskyi Zakhar Nazarovych[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail olha.petrenko@nure.ua*
[2] *Ivan Kozhedub Kharkiv National Air Force University 77/79 Sumska Str., Kharkiv UA-61023, Ukraine, e-mail alexwgs78@gmail.com*
[2] *Ivan Kozhedub Kharkiv National Air Force University 77/79 Sumska Str., Kharkiv UA-61023, Ukraine, e-mail ostrovskiyzakhar1@gmail.com*

Abstract. *This paper introduces a model for assessing threats and prioritizing them on a scale from 0 to 1 by utilizing fuzzy logic methods, which ensure high accuracy of results. The model is developed using the first type Mamdani algorithm. The proposed threat assessment model has been tested in both static and dynamic real-time attack scenarios. The implementation relies on fuzzy logic methods, with system modeling carried out using the MATLAB Fuzzy Logic Toolbox. This toolbox provides tools for designing systems based on fuzzy logic principles. The introduced threat prioritization procedure, constructed on the fuzzy set model, significantly enhances functionality by enabling accurate determination of threat levels. This procedure forms a solid foundation for making well-informed decisions regarding measures to counter these threats.*

Keywords: *model; fuzzy logic; membership function; threat assessment; threat prioritization; decision support; uncertainty; linguistic variables; fuzzy inference.*

I. Introduction and Problem statement

Fuzzy logic originated in the mid-1960s of the 20th century through the contributions of Lotfi Zadeh, an American mathematician and logician who introduced the concept. Over time, its theoretical foundations and models have undergone significant development, making it one of the most commonly applied methods today. The practical application of fuzzy set theory took off in 1975 with E. Mamdani's creation of the first fuzzy controller [1]. Fuzzy logic techniques are extensively utilized across diverse control systems, especially in areas such as managing nonlinear processes, developing self-learning systems, assessing risks and critical situations, pattern recognition, conducting financial analysis, examining corporate warehouse data, optimizing management strategies, and coordinating activities [2, 3].

In the modern era, the swift advancement of information technology and the intricate nature of decision-making processes highlight the importance of methods that address uncertainty and incomplete data. In this regard, fuzzy logic-based approaches are gaining prominence, as they enable the modeling and analysis of complex systems where conventional methods prove less effective. Fuzzy set methods prove highly valuable in cases where constructing a precise mathematical model of a system's behavior is unfeasible. By leveraging the principles of fuzzy set theory, it becomes feasible to incorporate vague and subjective expert insights from the relevant field to guide decision-making, eliminating the need to express these insights through conventional mathematical models.

Thus, the application of fuzzy logic methods to evaluate threat levels and prioritize them for timely and well-balanced countermeasures represents a pressing scientific task.

The purpose of research is to create and evaluate a fuzzy model designed to assess threats and establish priorities, enabling the determination of the sequence of counteractions needed to address these threats effectively.

II. Problem solution and Results

Fuzzy logic stands out as a flexible and straightforward methodology for addressing problems, facilitating its efficient application in systems for data control and analysis. Additionally, it incorporates human intuition and leverages operator expertise in the process [4, 5].

Fuzzy inference involves applying a set of rules to assess the activated membership functions. Within this framework, these rules are collectively referred to as a rule base or knowledge base specific to a given subject area. Utilizing a rule set enhances the coverage of the reference space, while also improving the reliability of the conclusions reached [6].

Based on the set of rules, a fuzzy inference system is built, as shown in Fig. 1

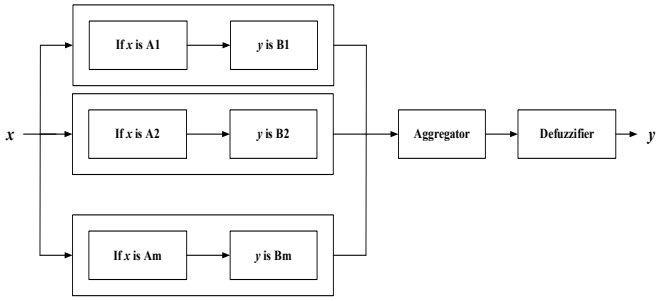

Figure 1. Block diagram of the fuzzy inference system

Fuzzy inference, grounded in the theory of fuzzy sets, utilizes fuzzy logic to establish a mapping between an input signal and an output result. This mapping forms the foundation for decision-making or pattern recognition. The process incorporates essential components such as membership functions, logical operations, and if-then rules [7]. This article introduces an enhanced algorithm based on fuzzy inference rules, specifically employing the Mamdani algorithm to evaluate threat levels. The algorithm analyzes multiple input data arrays to calculate the initial threat level.

Mamdani fuzzy inference was initially introduced to create control systems that utilize the synthesis of linguistic rules crafted by experienced specialists. With their intuitive nature and streamlined rule base structure, Mamdani systems are particularly well-suited for expert systems where the rules derive from the knowledge and experience of experts.

The Mamdani algorithm operates through the following steps:

- for each input parameter, the degree of its belonging to the corresponding fuzzy set is determined;
- on the basis of each fuzzy logical rule, the degree of compliance of the rules with the received data is estimated;
- the degree of belonging of each conclusion that follows from fuzzy logical rules is calculated;
- calculations are performed to determine the values of the conclusions.

The outcomes are expressed as fuzzy values, representing the results of a logical analysis. To convert these into precise values, a defuzzification process is applied. The derivation procedure for the Mamdani system is outlined in Fig. 2.

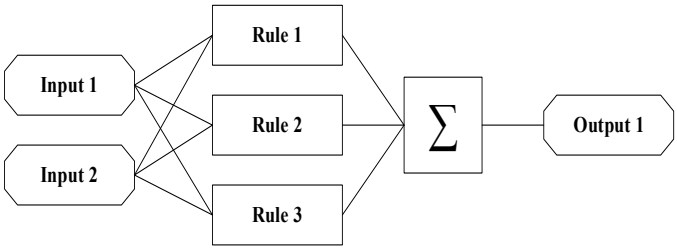

Figure 2. Fuzzy inference process for the Mamdani system

For modeling the system, the MATLAB Fuzzy Logic Toolbox and Simulink have been used. To represent the membership functions the triangular shapes were selected. The graphical interface of the membership function editor with defined input variables is shown in Fig. 3.

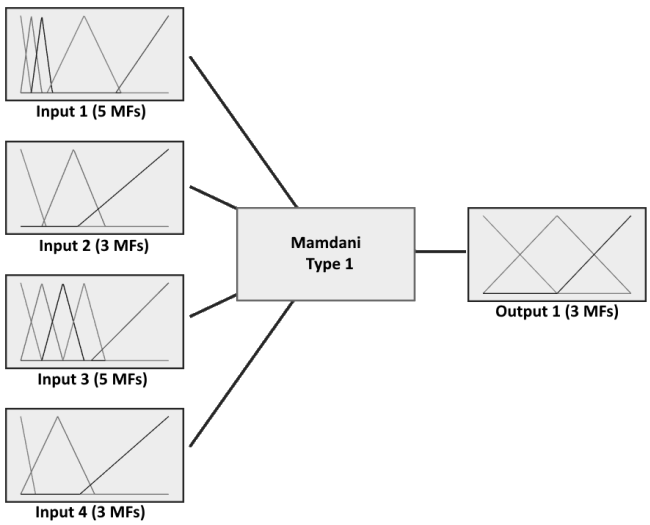

Figure 3. The graphical interface of the membership function editor

In the process, based on available standard data and expert comments on the relationship between input and output parameters, it is necessary to define fuzzy inference rules. Primary rules were formulated and evaluated by the reliability criterion both in static conditions and in a real-time scenario.

By utilizing the input data, the priority of threats can be adjusted in accordance with the formulated rules. The model produced a total of 226 rules, showcasing its robustness and efficiency. An in-depth explanation of the specific fuzzy inference rules employed are provided in Tab. 1.

Table 1. Basic fuzzy inference rules used in the model

Rule	Description
Rule 1 (low priority)	IF (Input1 is mf1) AND (Input2 is mf3) AND (Input3 is mf5) AND (Input4 is mf1) THEN (Output1 is mf1) (Weight: 1)
Rule 2 (low priority)	IF (Input1 is mf2) AND (Input2 is mf2) AND (Input3 is mf4) AND (Input4 is mf2) THEN (Output1 is mf1) (Weight: 1)
Rule 3 (low priority)	IF (Input1 is mf3) AND (Input2 is mf3) AND (Input3 is mf3) AND (Input4 is mf3) THEN (Output1 is mf1) (Weight: 1)
Rule 4 (medium priority)	IF (Input1 is mf4) AND (Input2 is mf2) AND (Input3 is mf3) AND (Input4 is mf3) THEN (Output1 is mf2) (Weight: 1)
Rule 5 (medium priority)	IF (Input1 is mf4) AND (Input2 is mf2) AND (Input3 is mf3) AND (Input4 is mf2) THEN (Output1 is mf1) (Weight: 1)
Rule 6 (high priority)	IF (Input1 is mf5) AND (Input2 is mf1) AND (Input3 is mf1) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)
Rule 7 (high priority)	IF (Input1 is mf5) AND (Input2 is mf2) AND (Input3 is mf1) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)
Rule 8 (high priority)	IF (Input1 is mf5) AND (Input2 is mf1) AND (Input3 is mf2) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)

Fig. 7 illustrates the block diagram of the fuzzy model designed for a static threat assessment scenario, implemented with using MATLAB. In this case, the input parameters are treated as fixed data points at each moment in time. The core fuzzy inference system evaluates the threat level based on each set of input parameters.

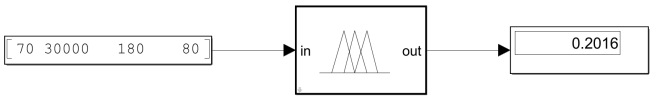

Figure 7. Static model of fuzzy logic for threat assessment in MATLAB

A threat assigned a higher priority level represents a more perilous combination of input parameters. The priority value of the threat plays a pivotal role in decision-making regarding the executing of protection measures to mitigate it. The results from the simulation, conducted under a static test scenario across eight time points for three input parameters (P_1, P_2, P_3), are presented in Tab. 2.

Table 2. Simulation results in a static test scenario with an 8-cycle sequence

№	P_1	P_2	P_3	Threat
1	70	45000	250	0.202
2	187	38000	220	0.5
3	295	33700	150	0.4963
4	450	27700	100	0.5
5	792	17000	70	0.5
6	955	10200	45	0.7661
7	1110	7690	30	0.7942
8	1224	5960	20	0.8085

The results of testing this model with the parameters given in Tab. 2 are shown in Fig. 8.

Evaluating the threat level in static scenario is crucial for maintaining the security and reliability of a system. This process enables the identification of potential risks, uncovers vulnerabilities within the architecture or code, and anticipates potential damage scenarios. Thorough and well-executed testing minimizes the occurrence of critical issues, lowers the risk of system failures, and supports making more informed decisions to safeguard assets such as information or data.

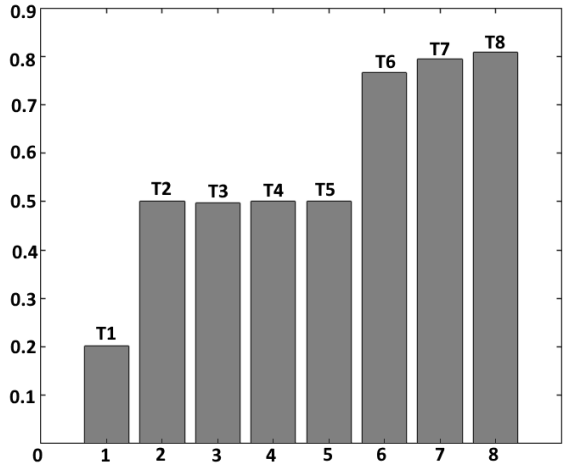

Figure 8. Threat level values when testing a static scenario

Fig. 9 illustrates a dynamic scenario designed to adaptively evaluate input parameters, utilizing them as critical data to address evolving real-world challenges. The flowchart representing this scenario was created within the MATLAB software platform.

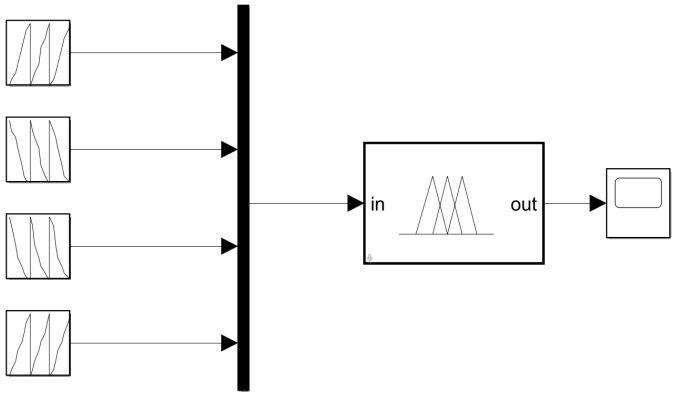

Figure 9. Dynamic model of fuzzy logic for threat assessment in MATLAB

In this scenario, the input data for the fuzzy model is formed as a set of input parameters that are received in real time. Each parameter evolves over time with specific patterns.

For instance, parameter P_1 exhibits an increasing trend, with its variable values at eight consecutive time points being [70, 187, 295, 450, 792, 955, 1110, 1224]. Conversely, parameter P_2 demonstrates a decreasing trend, with its values at the same intervals recorded as [45000, 38000, 33700, 27700, 17000, 10200, 7690, 5960]. Additionally, parameters P_3 and P_4 also show a declining pattern. Their respective values across the eight time intervals are [250, 220, 150, 100, 70, 45, 30, 20] for P_3 and [200, 170, 140, 110, 80, 50, 20, 10] for P_4. The temporal variations of the parameters P_1 (a) and P_2 (b) are visually represented in Fig. 10.

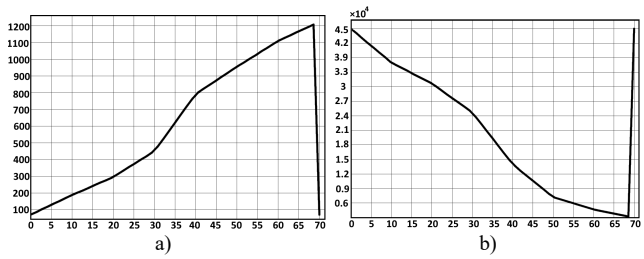

Figure 10. Dependence of input parameters on time

Fig. 11 illustrates the outcomes of the fuzzy system's threat assessment. It is evident that the threat level rises considerably as the P_1 parameter increases, meanwhile the remaining three parameters exhibit a declining pattern. The final threat value is 0.8014, which indicates its rather high level.

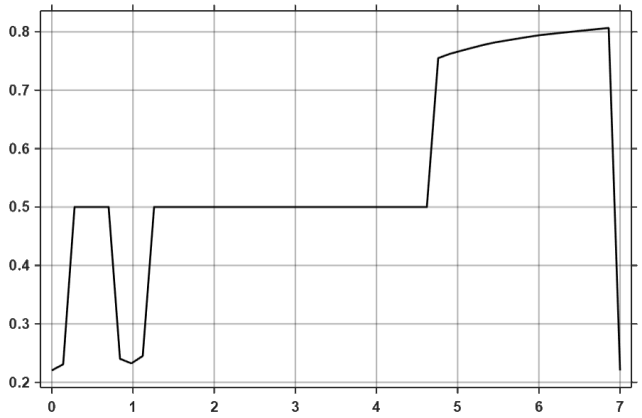

Figure 11. Output of the fuzzy logic threat assessment model for a dynamic scenario

Thus, the possibility of using fuzzy logical expressions and fuzzy logic operations for a formalized description of expert criteria for prioritizing threats is validated. This approach enables the derivation of numerical evaluations for threats based on defined input parameters, enhancing precision and flexibility within the analysis framework.

III. Conclusions

An algorithm utilizing a fuzzy logic system to rate threats on a scale from 0 to 1 has been proposed, offering a high level of accuracy. The developed threat assessment model was evaluated under both static and dynamic attack scenarios. A comparison between the outcomes of static and the dynamic threat modeling scenarios showed strong accuracy, reliability, and a minimal error rate in the model. This indicates its effectiveness and potential for use in various conditions.

The threat prioritization procedure developed with using the fuzzy set model significantly enhances functionality and allows determining the levels of threats. Consequently, it creates the basis for making well-informed decisions regarding the implementation of countermeasures.

REFERENCES

[1] Mamdani, E.H., and S. Assilian. An experiment in linguistic synthesis with a fuzzy logic controller / International Journal of Man-Machine Studies 7, no. 1 (January 1975): P. 1–13.

[2] Chen, G. (Guanrong) Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems / Guanrong Chen, Trung Tat Pham. - Boca Raton, London, New York: CRC Press LLC, 2001. – 316 p.

[3] I Espinosa J. Fuzzy Logic, Identification and Predictive Control / Jairo Espinosa, Joos Vandewalle, Vincent Wertz. – USA: Springer-Verlag London Limited, 2005. – 263 p.

[4] Kecman Vojislav Learning and soft computing. support vector machines, neural networks, and fuzzy logic models / Vojislav Kecman. – Massachusetts: Massachusetts Institute of Technology, 2001. – 541 p.

[5] Ross, Timothy J. Fuzzy logic with engineering applications / Timothy J. Ross. – England: John Wiley & Sons Ltd., 2004. – 628 p.

[6] Shubin I. Y. Fuzzy sets and fuzzy logic as a tool for formalizing requirements / O. Ashurova, I. Shubin // Information systems and technologies: materials of the 9th International Scientific and Technical Conference, November 17-20, 2020 - Kharkiv: Madrid, 2020. - P. 64-68.

[7] Y. Liang, A fuzzy knowledge-based system in situation and threat assessment, Journal of Systems Science & Information, 4, P.791–802, 2006.