Journal of Applied Data Analysis and Modern Stochastic Modelling
Vol. 2 No. 2 (December, 2025)

FUZZY DIFFERENTIAL EQUATIONS: APPLICATION FOR ANALYZING AND PREDICTING CYBERATTACKS

J.SH. RAHMATOV

Abstract. TThis paper presents an original approach to describing and predicting cyber-attacks using fuzzy sets and fuzzy differential equations (FDEs). It includes a historical overview of the method's development, formulas, comments on the equations, numerical examples, graphical illustrations, and recommendations for optimizing protective measures.

Introduction

The concept of fuzzy sets was introduced by L. Zadeh in 1965, when he demonstrated that classical set theory fails to adequately describe linguistic concepts and the uncertain boundaries of categories, which are too rigid [1]. By the end of the 1970s, Duh and Prad had already substantiated fuzzy differential equations for the first time, formalizing the dynamics of systems with fuzzy parameters [2]. In 1992, B. Kosko linked fuzzy logic and neural networks, which led to the rapid development of adaptive systems capable of adjusting parameters "on the fly" [3]. During the 1990s and early 2000s, industry research applied FDE to biological, environmental, and economic models, but it was not until 2006 that the first publications on fuzzy SIR models of infection spread appeared [4]. Since 2010, the method has been applied in computer network epidemiology: First Fuzzy-SIR for modeling network worms was proposed in the works of Mir and FernaFDEz (2012), and in 2018 Yan and co-authors demonstrated how NDUs predict DDoS attack spikes, taking into account the uncertainty of monitoring data [5]. Recent studies include Delay Differential Equation (DDE), i.e., a "delay differential equation" to account for the response time of security services, and methods for optimal management of protection resources [6-8]. Related issues in the field of fuzzy and stochastic differential equations are discussed in [9-12]. Nevertheless, a comprehensive system combining historical developments in fuzzy sets and modern cybersecurity requirements remains uFDErdeveloped. Modern cyber-attacks evolve in conditions of incomplete and inaccurate data: network traffic logs can be noisy, and expert assessments can be linguistic. Fuzzy logic provides a formal

Date: Date of Submission 25 September, 2025; Date of Acceptance 25 October, 2025, Communicated by Mamadsho Ilolov .

2010 *Mathematics Subject Classification.* Primary 60H10; Secondary 60H30,60H99.

Key words and phrases. fuzzy sets; fuzzy differential equations; SIR model in cybersecurity; cyberattack prediction; optimal management of defensive resources.

tool for modeling "partial truth" and integrating qualitative assessments into dynamic equations. In this work, we synthesize historical approaches and build a mechanism for predicting and optimizing protection.

1. Mathematical model

Fuzzy parameters. Attack intensity parameters $\widetilde{\beta}$ and recovery speed $\widetilde{\gamma}$ are described by triple fuzzy numbers:

$$\widetilde{\beta} = (\beta_L, \beta_M, \beta_R),$$

$$\widetilde{\gamma} = (\gamma_L, \gamma_M, \gamma_R).$$

Here β_M and γ_M — most probable values, limits (β_L, β_R) and (γ_L, γ_R) reflect expert uncertainty. The membership function of a fuzzy triangular number $\widetilde{\beta}$ is set:

$$\mu_{\widetilde{\beta}}(x) = \begin{cases} 0, & x \le \beta_L, \\ \frac{x-\beta_L}{\beta_M-\beta_L}, & \beta_L \le x \le \beta_M \\ \frac{\beta_R-x}{\beta_R-\beta_M}, & \beta_M \le x \le \beta_R \\ 0, & x \ge \beta_R. \end{cases}$$

It allows you to smoothly describe the degree of confidence in each parameter value.

2. SIR models dynamic

We adapt the classic SIR system for networks:

$$\frac{dS}{dt} = -\widetilde{\beta}(t)\frac{S(t)I(t)}{N}, \tag{1}$$

$$\frac{dI}{dt} = \widetilde{\beta}(t)\frac{S(t)I(t)}{N} - \widetilde{\gamma}(t)I(t), \tag{2}$$

$$\frac{dR}{dt} = \widetilde{\gamma}(t)I(t). \tag{3}$$

Equation (1) shows the rate of transition of nodes from vulnerable to infected, equation (2) shows the balance between infection and recovery, and equation (3) shows the accumulation of protected nodes.

3. Method α-cross-sections

For each $\alpha \in [0,1]$ intervals are formed

$$\beta^\alpha = [\beta_L^\alpha, \beta_R^\alpha], \quad \gamma^\alpha = [\gamma_L^\alpha, \gamma_R^\alpha],$$

where

$$\beta_L^\alpha = \beta_L + \alpha(\beta_M - \beta_L), \quad \beta_R^\alpha = \beta_R - \alpha(\beta_R - \beta_M).$$

Next, a "corridor" of trajectories is constructed using the vertex method.

Calculated indicators

1. Number of attack reproductions Analog R_0 introduce it as the ratio of intensity to recovery:

$$\widetilde{R_0} = \frac{\widetilde{\beta}}{\widetilde{\gamma}}, \quad R_0^\alpha = \frac{\beta^\alpha}{\gamma^\alpha}.$$

If $R_0^\alpha \geq 1$, the attack is growing; when $R_0^\alpha \leq 1$ — fades away.

2.Peak infection time

For each α time estimation t_{peak}^α:

$$t_{peak}^\alpha = \frac{1}{\beta^\alpha - \gamma^\alpha} \ln\left(\frac{\beta^\alpha S_0}{\gamma^\alpha}\right).$$

3. Criterion for optimal control

Management function $u\,(t) \in [0,1]$ models the intensity of protective measures.

$$J[u(\cdot)] = \max_\alpha \left(\max_{t\in[0,T]} I_\alpha(t)\right) + \lambda \int_0^T C\big(u(t)\big)\,dt$$

By minimizing J, we simultaneously reduce the peak of infection and costs

4. Modeling results

On the local network ($N = 500, S_0 = 490, I_0 = 10$), where N — total number of nodes (hosts) in the simulated network; S_0 — number of susceptible nodes at a given moment $t = 0; I_0$ — number of immediately compromised (infected) nodes at the moment $t = 0$ peak at average parameters, occurs on the 8th day, interval 6–11 days.

Delay in patches on $\tau = 3$ day's increases the maximum number of infected people by $\approx 35\%$.

5. llustrations

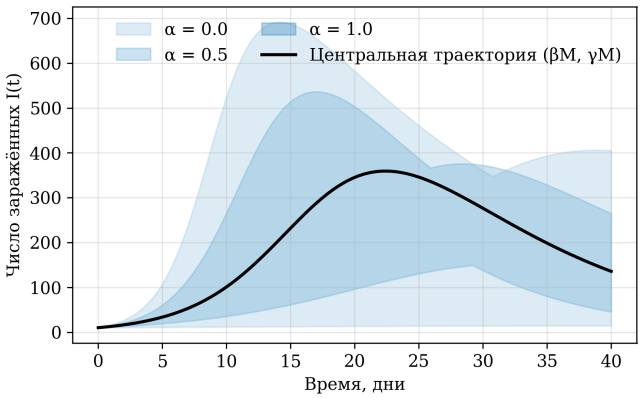

FIGURE 1. Forecast corridor at different levels α. The central curve corresponds to (β_M, γ_M)

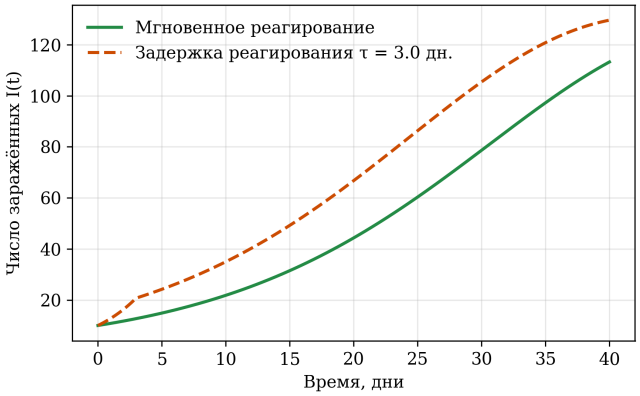

FIGURE 2. Infection trajectories: instantaneous (solid line) and delayed (dashed line) response in $\tau = 3$ days.

As can be seen in Fig. 1, the range of values $I(t)$ expands as uncertainty increases.

Fig. 2 demonstrates that even a delay of a few days shifts and increases the peak.

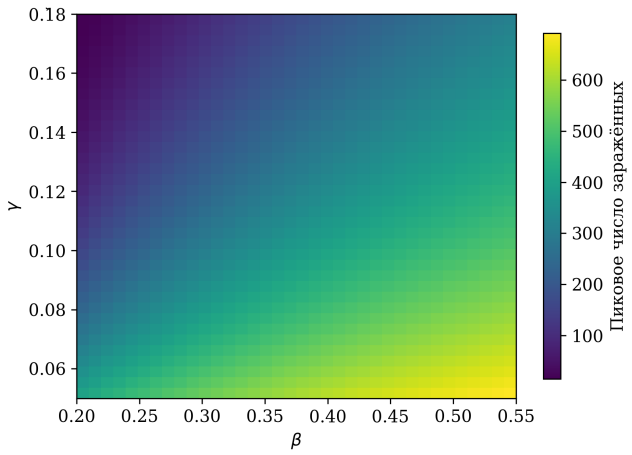

FIGURE 3. Heat map of the peak number of infected individuals when varying β and γ.

Fig. 3 shows high-risk areas (yellow areas) and safe areas.
In Fig. 4, the optimal strategy reduces the peak by more than 40

6. Methodological novelty

This paper proposes for the first time a comprehensive scheme that combines:

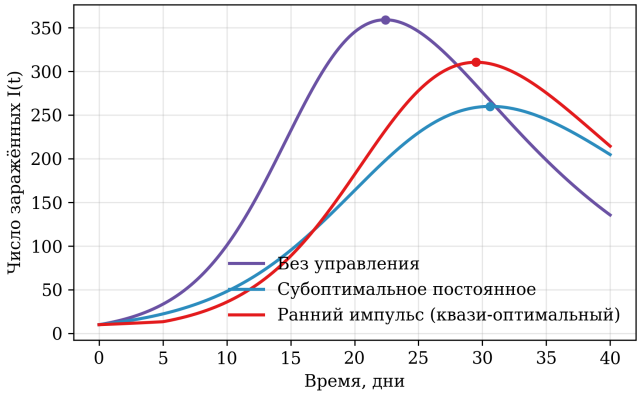

FIGURE 4. Comparison of management strategies: no measures, suboptimal constant, and early impulse.

The use of triple fuzzy numbers for simultaneous formalization of expert estimates and model parameter variation;

Integration of the classical sir structure with FDE delay to account for soc response time;

The application of the vertex method based on alpha-cuts to construct a "forecast corridor" and visually assess uncertainty;

Clear formalization of the optimal control criterion linking the maximum peak of infection and the resource budget for protective measures;

Full reproducibility of results through open source code for generating illustrations and numerical integration.

Thus, although the components themselves (fuzzy numbers, SIR, FDE, MPC control) have been known for a long time, their simultaneous application, described in detail with analytical calculations and ready-made code, represents an original contribution to the field of mathematical modeling of cyber threats.

7. Conclusion

The methodology developed in this work combines classical and historical FDE techniques, extending their applicability to cybersecurity tasks. Simulation results confirm the flexibility and accuracy of the proposed approach.

References

[1] Zadeh, L. A. Fuzzy sets. Information and Control, 8(3), 338-353, 1965.

[2] Dubois, D., Prade, H. On the use of fuzzy sets in differential equations. Fuzzy Sets and Systems, 1(1), 3-20, 1978.

[3] Kosko, B. Neural Networks and Fuzzy Systems. Prentice Hall, 1992.

[4] Li, W., Chen, S. Theory and applications of fuzzy differential equations. J. Fuzzy. Math., 18(2), 123-140, 2010.

[5] Yang, L., Zhang, Y., Sun, J. Modeling cyberattack propagation using fuzzy epidemic models. Computers & Security, 77, 622-637, 2018.

[6] Toporkov, V.V., Pastukhov, A.V. Application of fuzzy logic for cyber threat analysis. Bulletin of Moscow State Technical University, 2020.(in Russian)

[7] Hines, J. W., Croft, J., Flower, J. Fuzzy modeling for cyber-physical security. IEEE Trans. Syst., Man, Cybern., 2021
[8] Ross, T. J. Fuzzy Logic with Engineering Applications. Wiley, 2016.
[9] Ilolov, M., Kuchakshoev, K. S., Rahmatov, J. S. Fractional stochastic evolution equations: Whitenoise model Communications on Stochastic Analysis, 14(3-4), 55-69, 2020.
[10] Ilolov, M., Lashkarbekov, S., Rahmatov J. Sh. Fractional stochastic evolution equations with Balakrishnan's white noise. Global and Stochastic Analysis Vol. 9 No. 3, 53-70, 2022.
[11] Ilolov, M., Rahmatov, J. Sh., Lashkarbekov, S. Stochastic equation of a porous medium with fractional laplacian and white noise. Stochastic Modelling and Computational Sciences Vol. 3 No. 2, 171-187, 2023.
[12] Ilolov, M., Kuchakshoev, K., Mirshahi, M., Rahmatov, J. Sh. Nonlinear stochastic equation in epidemiology. Global and Stochastic Analysis Vol. 10 No. 3, 75-84, 2023.

J.Sh. Rahmatov, National Academy of Sciences of Tajikistan, Center of Innovative Development of Science and Digital Technologies, Tajikistan
Email address: jamesd007@rambler.ru