Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 3, June 2025, pp. 1698~1707
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i3.pp1698-1707

Adaptive mathematical modeling for predicting and analyzing malware

Gulzhanat Beketova[1], Ainur Manapova[2]
[1]Department of IT Engineering and Artificial Intelligence, Institute of Automation and Information Technology, Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
[2]Center for Scientific Research and Competence, Civil Aviation Academy, Almaty, Kazakhstan

Article Info

Article history:

Received Aug 28, 2024
Revised Nov 14, 2024
Accepted Nov 24, 2024

Keywords:

Cyber threat
Cybersecurity
Malware
Mathematical modeling
SIR model

ABSTRACT

In this paper, we propose and investigate an improved mathematical model of malware propagation in network structures based on a modification of the well-known raw-immune-response susceptible-infected-recovered (SIR) model. For detailed numerical analysis, our study introduces the fourth-order Runge-Kutta method, which provides higher accuracy in determining fundamental parameters such as infection, recovery and immunity loss coefficients of network nodes. The obtained simulation results demonstrate that the peak of the epidemic occurs when 34.7% of all nodes are infected, with a peak after 32.5-time units. The main contribution of this work is the in-depth understanding and quantification of cyber threats, which emphasizes the importance of prompt response, regular system software updates, and continuous monitoring of network activity. This research makes a significant contribution to cybersecurity applications by providing quantitative tools and strategies to help strengthen network defenses against malicious attacks. The identified patterns and their numerical interpretation can be integrated into processes for optimizing measures to prevent the widespread spread of malware, thereby enhancing the overall security and stability of networked systems.

Corresponding Author:

Gulzhanat Beketova
Department of IT Engineering and Artificial Intelligence
Institute of Automation and Information Technology
Almaty University of Power Engineering and Telecommunications
Almaty, 050013 Almaty, Kazakhstan
E-mail: g.beketova@aues.kz

1. INTRODUCTION

With the rapid growth and development of cyber threats, traditional security methods, which are often reactive in nature, are becoming less effective. There is an urgent need for advanced tools that can model and predict the spread of malware, which is critical for proactive protection and optimizing cybersecurity resources. One of the key challenges is the lack of in-depth understanding of how factors such as infection rates, the effectiveness of measures implemented and the potential for re-infection affect the dynamics of threat propagation in a networked environment. This limits the ability to make informed decisions when developing security strategies. Thus, the focus of this study is to develop a mathematical model that can accurately describe and predict the behavior of malware on networks. Such a model will be a powerful tool for analyzing risks and creating effective defense strategies, improving the overall resilience of networks in the face of cyber threats.

Mathematical modeling of malware propagation in networks has a long history. The fundamental basis for this was laid by [1], which first applied epidemiological models to describe the spread of computer viruses. Subsequently, various models have been developed that adapt to specific conditions and network types, including network saturation accounting [2] and node scanning [3]. Susceptible-infected-recovered (SIR) models and their modifications, such as susceptible-exposed-infected-recovered-susceptible (SEIRS) [4] and time-delay susceptible-infected-recovered-susceptible (SIRS) [5], have been widely used, offering methods for analyzing software propagation in wireless and other network environments. Current research shifts the focus to complex network structures [6], [7] and human factors [8], which makes the models more realistic and deeper in describing everyday network interactions. Also important is the direction of threat modeling related to risk assessment for cyber-physical systems [9].

Another important aspect of mathematical modeling in cybersecurity is the formulation of vulnerabilities and threats into a single system. An example of this approach is the ICAR model proposed by [10], which uses category theory to establish mathematical relationships. Traditional defense mechanisms have not kept pace with the rapidly changing tactics of cyber adversaries, who use advanced techniques such as machine learning and deep learning to avoid detection. In response, researchers are exploring the application of machine learning and game theory to develop more effective cybersecurity solutions [11], [12]. Commercial antivirus products remain one of the primary defenses for computer security. Many researchers [13]-[18] have proposed the use of deep learning for malware classification as a key component of next-generation malware defense systems.

Many authors have focused on adversarial learning-based attacks, but few have proposed defenses [19] offering adverse pattern learning; in [20] proposed a defense against distillation-based attacks based on adverse learning. More recently, several authors have proposed ensemble-based defense against unfavorable patterns [21]-[24]. Bellamy [25], potentially unfavorable patterns are identified by measuring the difference between a new pattern and the original pattern with the unwanted input features removed. An extrusion system was proposed.

Methods include statistical and advanced machine learning approaches, such as Fisher-Boshloo exact criterion and polynomial vector learning, which demonstrate high accuracy in threat classification. In the area of reinforcement learning, a method for malware classification using multinomial connected latent latent modular dual Q-learning has been presented, demonstrating the potential of applying complex algorithms in cybersecurity tasks. Research in Android malware detection has a long history. Early works included the application of neural network with back propagation of error [26]. Machine learning techniques continue to evolve, including the use of deep networks to improve data security [27] and the comparison of different algorithms, which contributes to the selection of effective cyber defense strategies.

The main objective of the research is to develop an effective mathematical model that can accurately describe and predict the behavior of malware in computer networks. This aims to create a tool that will assist information security professionals in developing more effective defense and risk management strategies. The objectives of the research are to investigate current approaches to modeling malware propagation to identify their strengths and weaknesses, create an improved model that takes into account the unique characteristics of today's cyber threats and network infrastructure, based on the findings, propose specific recommendations to improve existing and develop new strategies to defend against cyber threats.

2. METHOD

2.1. Mathematical model

Consider a mathematical model of malware propagation in a network using a modified SIR model:

$$\begin{cases} \frac{dS}{dt} = -\beta SI + \gamma R \\ \frac{dI}{dt} = \beta SI - \delta I \\ \frac{dR}{dt} = \delta I - \gamma R \end{cases} \quad (1)$$

where S is the number of vulnerable nodes, I is the number of infected nodes, R is the number of protected nodes, β is the infection rate, δ is the recovery rate, and γ is the rate of immunity loss. Vulnerable nodes S can be infected with a probability proportional to the number of infected nodes I. Infected nodes I can be recovered at a certain rate. Recovered nodes R may become vulnerable again over time.

2.2. Numerical model

The application of the 4th order Runge-Kutta method for the SIR model (1) begins with defining a function for each equation of the system:

$$\begin{cases} f_1(t,S,I,R) = -\beta SI + \gamma R \\ f_2(t,S,I,R) = \beta SI - \delta I \\ f_3(t,S,I,R) = \delta I - \gamma R \end{cases} \quad (2)$$

The required parameters S, I, R are expressed as follows:

$$S_{n+1} = S_n + \frac{h}{6} \cdot (k_{1,1} + 2k_{2,1} + 2k_{3,1} + k_{4,1})$$

$$I_{n+1} = I_n + \frac{h}{6} \cdot (k_{1,2} + 2k_{2,2} + 2k_{3,2} + k_{4,2})$$

$$R_{n+1} = R_n + \frac{h}{6} \cdot (k_{1,3} + 2k_{2,3} + 2k_{3,3} + k_{4,3})$$

$$t_{n+1} = t_n + h$$

here where $h = \frac{b-a}{N}$ is step length. $k_{1,1}$, $k_{1,2}$, $k_{1,3}$, $k_{2,1}$, $k_{2,2}$, $k_{2,3}$ $k_{3,1}$, $k_{3,2}$, $k_{3,3}$ $k_{4,1}$, $k_{4,2}$, $k_{4,3}$ are defined as follows:

$$k_{1,i} = f_i(x_n,\ S_n, I_n, R_n)$$

$$k_{2,i} = f_i\left(t_n + \frac{h}{2}, S_n + \frac{h}{2}k_{1,1}, I_n + \frac{h}{2}k_{1,2}, R_n + \frac{h}{2}k_{1,3}\right)$$

$$k_{3,i} = f_i\left(t_n + \frac{h}{2}, S_n + \frac{h}{2}k_{2,1}, I_n + \frac{h}{2}k_{2,2}, R_n + \frac{h}{2}k_{2,3}\right)$$

$$k_{4,i} = f_i\left(t_n + h, S_n + hk_{3,1}, I_n + hk_{3,2}, R_n + hk_{3,3}\right)$$

here $i = 1,2,3$ for S, I, R respectively.

For particular SIR system (2), the coefficients $k_{1,i}$, $k_{2,i}$, $k_{3,i}$, $k_{4,i}$ will be calculated as follows:

$$k_{1,1} = -\beta S_n I_n + \gamma R_n$$

$$k_{1,2} = \beta S_n I_n - \delta I_n$$

$$k_{1,3} = \delta I_n - \gamma R_n$$

$$k_{2,1} = -\beta\left(S_n + \frac{h}{2}k_{1,1}\right)\left(I_n + \frac{h}{2}k_{1,2}\right) + \gamma\left(R_n + \frac{h}{2}k_{1,3}\right)$$

$$k_{2,2} = \beta\left(S_n + \frac{h}{2}k_{1,1}\right)\left(I_n + \frac{h}{2}k_{1,2}\right) - \delta\left(I_n + \frac{h}{2}k_{1,2}\right)$$

$$k_{2,3} = \delta\left(I_n + \frac{h}{2}k_{1,2}\right) - \gamma\left(R_n + \frac{h}{2}k_{1,3}\right)$$

$$k_{3,1} = -\beta\left(S_n + \frac{h}{2}k_{2,1}\right)\left(I_n + \frac{h}{2}k_{2,2}\right) + \gamma\left(R_n + \frac{h}{2}k_{2,3}\right)$$

$$k_{3,2} = \beta\left(S_n + \frac{h}{2}k_{2,1}\right)\left(I_n + \frac{h}{2}k_{2,2}\right) - \delta\left(I_n + \frac{h}{2}k_{2,2}\right)$$

$$k_{3,3} = \delta\left(I_n + \frac{h}{2}k_{2,2}\right) - \gamma\left(R_n + \frac{h}{2}k_{2,3}\right)$$

$$k_{4,1} = -\beta\left(S_n + hk_{3,1}\right)\left(I_n + hk_{3,2}\right) + \gamma\left(R_n + hk_{3,3}\right)$$

$$k_{4,2} = \beta\left(S_n + hk_{3,1}\right)\left(I_n + hk_{3,2}\right) - \delta\left(I_n + hk_{3,2}\right)$$

$$k_{4,3} = \delta\left(I_n + hk_{3,2}\right) - \gamma\left(R_n + hk_{3,3}\right)$$

This method allows to numerically solve the system of differential equations of the SIR model with high accuracy, taking into account the nonlinearity of interactions between different groups (susceptible, infected and recovered) in the process of malware distribution in the network. For the numerical implementation of the SIR model, the values of the coefficients of the system of (1) and the initial conditions of the sought variables from Table 1 will be used.

The values of $\beta = 0{,}3$, $\delta = 0{,}1$, $\gamma = 0{,}05$ are based on an analysis of modern malware and its ability to spread quickly. These values take into account the average propagation rate for different types of malware, from relatively slow worms to fast botnets, both automatic defenses and manual intervention by administrators, the cycle of security updates and the emergence of new malware versions. These parameters were selected based on analysis of real-world malware propagation data and consultation with cybersecurity experts. They provide a realistic representation of malware propagation dynamics in modern network environments, taking into account both the technical aspects of virus propagation and organizational factors that affect response and recovery rates.

Table 1. Simulation parameters

Determination	Value
Infection rate, β	0.3
Recovery rate, δ	0.1
The rate of immune loss, γ	0.05
Initial number of nodes in the network, N	1,000
Initial number of vulnerable nodes, S	995
Initial number of infected nodes, I	5
Number of protected nodes, R	0

3. RESULTS AND DISCUSSION

Figure 1 shows the spread of malware in the network. There is a rapid increase in the number of infected nodes, then a peak is reached, after which the number of infected nodes begins to decrease. The maximum number of infected nodes reaches ~347, which is about 34.7% of the entire network. This occurs about 32.5 time units after the start of propagation. By the end of the simulated period (100 time units), about 442 nodes, 44.2% of the network, are in a state of recovery.

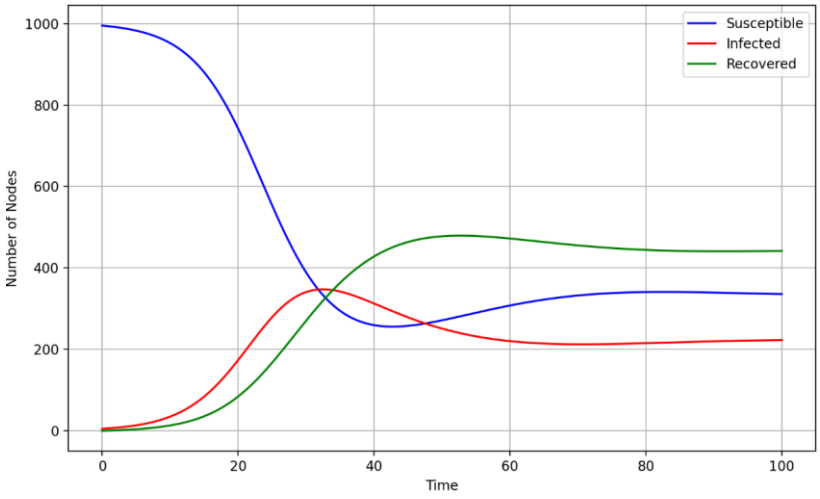

Figure 1. Results of the SIR model

The model shows that even after a long period, infected nodes remain in the network, which can pose a persistent threat. The initial malware propagation rate is high, emphasizing the importance of rapid threat response. The recovery rate δ plays a key role in deterring malware propagation. Increasing this parameter can significantly reduce the infection peak. The presence of immunity loss rate γ indicates that the network may be vulnerable to repeated attacks or new malware variants.

Early detection and rapid response systems should be in place to minimize the initial spread of malware. Regular updates and patches can increase the recovery rate δ and reduce network vulnerability.

After the main wave of infection subsides, monitoring should continue as there may still be infected nodes in the network. Increasing user awareness can reduce the infection rate β and increase the overall resilience of the network. Given the possibility of loss of immunity γ, it is important to continuously adapt defense measures to new threats.

Figure 2 shows how quickly malware spreads across the network over time, reaching a peak infection rate and then declining. The peak infection rate indicates the point at which the virus spreads most intensely. After this point, containment and remediation measures begin to have a significant impact.

Figure 3 of the recovery rate illustrates the effectiveness of the infection removal measures, it shows how quickly nodes recover from infection. As the number of infected nodes increases, the recovery rate also increases, reaching a peak and then decreases as the number of infected nodes decreases. The peak of the recovery rate coincides with the peak of the number of infected nodes, indicating the effective application of recovery measures.

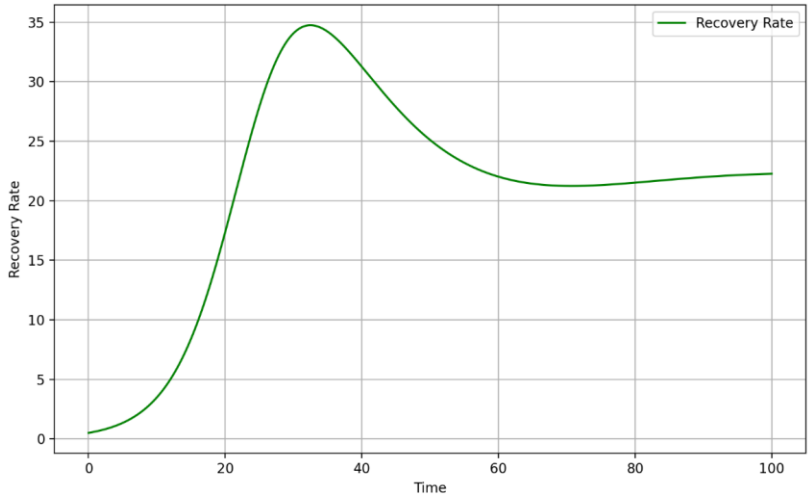

Figure 2. Time dependence of the rate of infection

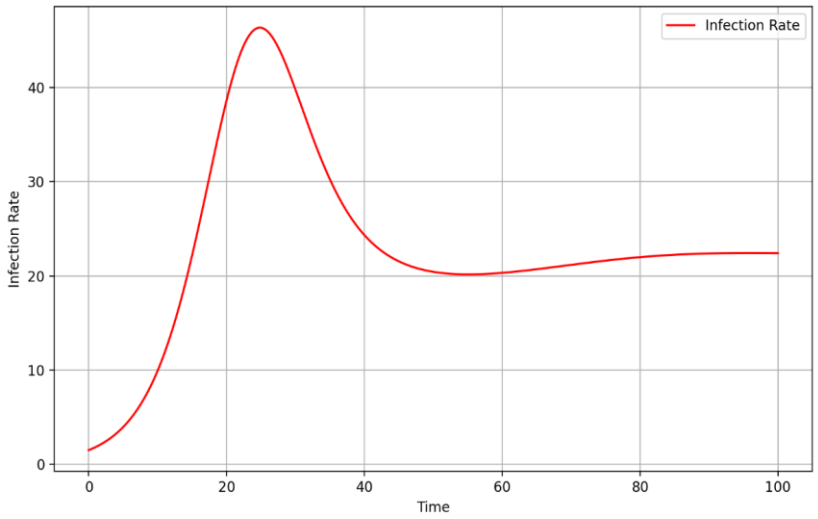

Figure 3. Dependence of recovery rate on time

Figure 4 of the state distribution of nodes at the end of the simulation gives a clear picture of the final state of the network after the infection wave has passed. A high percentage of recovered nodes indicates that the threat was successfully contained and eliminated. A low number of infected nodes at the end of the period indicates that the infection has been almost completely suppressed.

The model exhibits typical infestation behavior, where the initial phase is characterized by a rapid increase in infestation followed by a recovery phase. The effectiveness of recovery and threat containment measures is evidenced by the high percentage of nodes recovered. It is important to continue monitoring and maintaining security measures to prevent repeat attacks or new threats.

The phase portrait in Figure 5 shows the trajectories of the changing states of the system S, I, R in phase space. The graph shows how the system moves from an initial state where most nodes are susceptible S to a state where most nodes are recovered R. The trajectories show that as the number of infected nodes I increases, the number of susceptible nodes S decreases and the number of recovered nodes R increases. The phase portrait demonstrates that the system tends towards a state where the number of infected nodes is minimized and most nodes are either susceptible or recovered. This indicates a natural attenuation of the epidemic in the absence of new infections.

Figure 6 shows the value of the base reproductive number $R0$, which in this case is 3. This means that each infected node on average infects 3 other nodes in a fully susceptible population. A value of $R0 > 1$ indicates that the infection can spread in the network, causing an epidemic. This emphasizes the importance of measures to reduce $R0$, such as reducing the infection rate β or increasing the recovery rate δ.

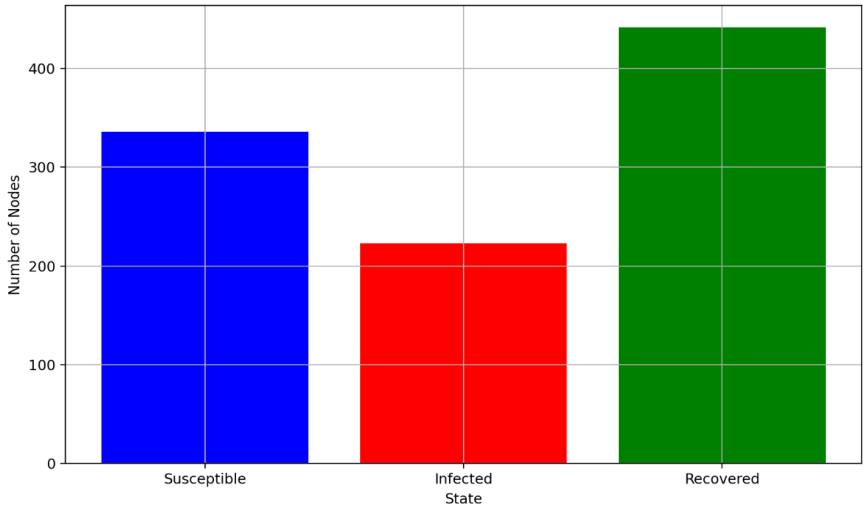

Figure 4. State distributions of nodes at the end of the simulation

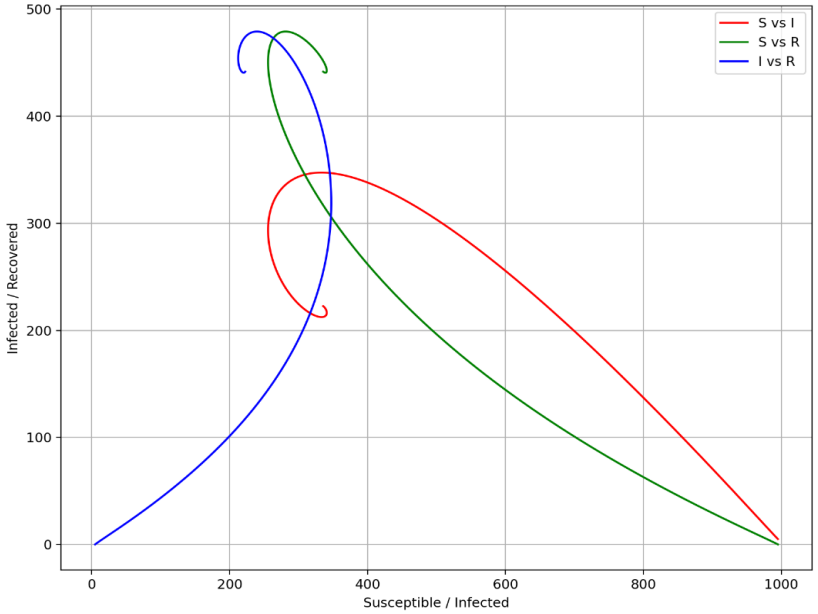

Figure 5. Phase portrait of the SIR model

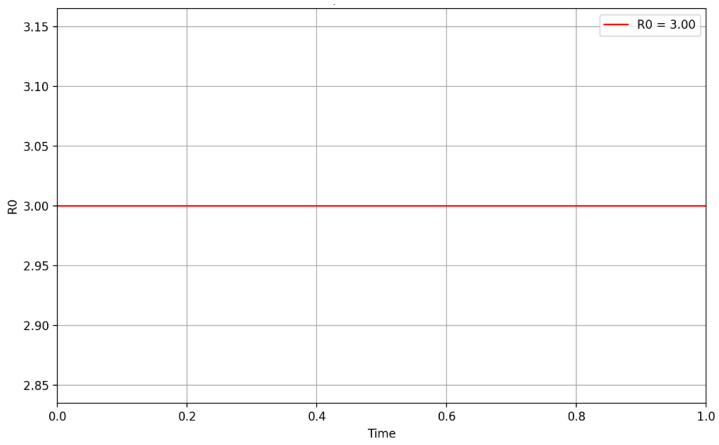

Figure 6. Basic reproductive number $R0$

Figure 7 shows that increasing the infection rate β leads to faster and more intense spread of infection, while increasing the recovery rate δ reduces the peak infection and speeds up recovery. The scenarios show that measures to increase the recovery rate more. Figure 8 shows the total number of nodes that have been infected since the start of the simulation. A high cumulative number of infections indicates the severity of the threat and the need for preventive measures to reduce the initial spread of infection.

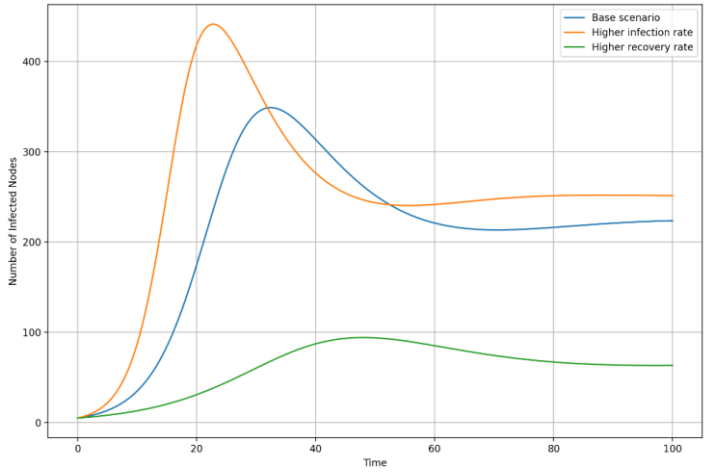

Figure 7. Comparative analysis of different scenarios

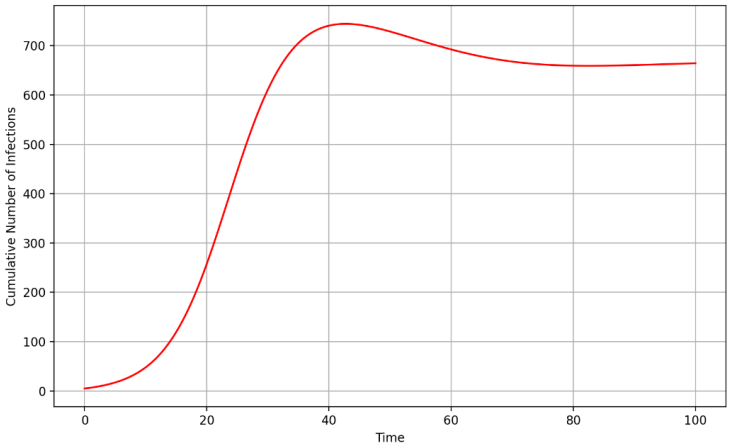

Figure 8. Cumulative infections over time

Figure 9 shows how the vulnerability of the network changes over time. At the beginning of the simulation, the vulnerability decreases rapidly but then starts to increase slowly due to the loss of immunity $\gamma > 0$. The increase in network vulnerability over the long term indicates the need for continuous monitoring and updating of defense measures to prevent reoccurring attacks or new threats.

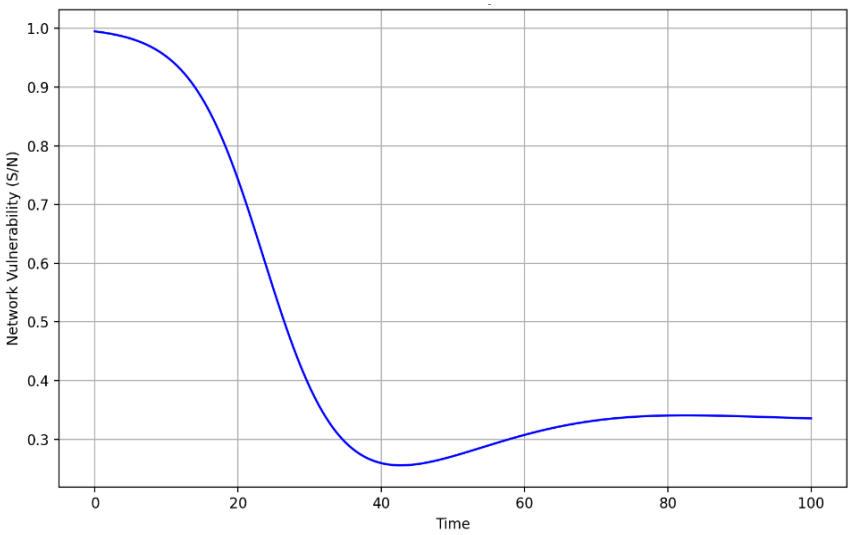

Figure 9. Network vulnerability over time

The phase portrait and $R0$ plot emphasise the importance of understanding the dynamics of the system and the key parameters affecting the spread of infection. Our study demonstrates that effective management of SIR model parameters can significantly affect the dynamics of malware propagation in networks. Without timely intervention and network updates, the peak of infection can be significant, emphasizing the need for rapid response and strategies to improve security. The baseline reproductive number $R0$ shows the potential for rapid infection spread, requiring measures to reduce infection rates and increase recovery rates. Increasing the recovery rate δ has proven effective in reducing the peak of infection and shielding the network from prolonged malicious attacks. The immunity loss parameter γ indicates the need for continuous adaptation of defense measures and updates for resilience to new threats. These results emphasize the need for preventive measures and continuous monitoring in real-world scenarios, which can help protect the network from cyber threats. These results emphasize the importance of dynamic adaptation and management of model parameters to improve cybersecurity and network resilience.

4. CONCLUSION

The paper provides a comprehensive analysis of the use of a modified SIR model to model and understand malware propagation in network infrastructures. The findings emphasize the importance of: clearly understanding and managing infection, recovery, and immunity loss rates are key components in developing effective strategies to counter cyber threats. The simulations highlight the critical role of operational responses, such as updating network security protocols and user education, in reducing infection peaks and protecting the network. The data shows that even after the main wave of infection has subsided, the network can remain vulnerable, emphasizing the need for continuous monitoring and adaptation of security measures. The results of the study can be practically applied to strengthen cybersecurity in various sectors, including corporate networks and government information systems. The utilization of the identified strategies helps to increase the resilience of the system to new types of threats. Thus, this study makes a meaningful contribution to understanding the dynamics of malware propagation and presents relevant solutions for enhancing the cybersecurity of modern networks.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gulzhanat Beketova	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ainur Manapova	✓	✓	✓	✓		✓	✓		✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article.

REFERENCES

[1] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the Symposium on Security and Privacy*, 1991, pp. 343–358, doi: 10.1142/9789812812438_0004.

[2] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proceedings of the ACM Conference on Computer and Communications Security*, Nov. 2002, pp. 138–147, doi: 10.1145/586110.586130.

[3] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 105–118, Apr. 2007, doi: 10.1109/TDSC.2007.1001.

[4] B. K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, no. 3, pp. 710–715, Mar. 2010, doi: 10.1016/j.apm.2009.06.011.

[5] L. X. Yang and X. Yang, "A new epidemic model of computer viruses," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1935–1944, 2014, doi: 10.1016/j.cnsns.2013.09.038.

[6] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, Apr. 2001, doi: 10.1103/PhysRevLett.86.3200.

[7] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 942–960, 2014, doi: 10.1109/SURV.2013.100913.00195.

[8] P. Wang, M. C. González, C. A. Hidalgo, and A. L. Barabasi, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 324, no. 5930, pp. 1071–1076, May 2009, doi: 10.1126/science.1167053.

[9] A. Shostack, *Threat modeling: designing for security. Indianapolis*. John Wiley & Sons, Inc., 2014.

[10] A. Valence, "ICAR, a categorical framework to connect vulnerability, threat and asset managements," *arXiv preprint arXiv:2306.12240*, 2023, doi: 10.48550/arXiv.2306.12240.

[11] J. W. Stokes, D. Wang, M. Marinescu, M. Marino, and B. Bussone, "Attack and Defense of dynamic analysis-based, adversarial neural malware classification models," *arXiv preprint 1712.05919*, pp. 1–8, Dec. 2017, doi: 10.1109/MILCOM.2018.8599855.

[12] A. Wolsey, "The state-of-the-art in AI-based malware detection techniques: a review," *arXiv preprint 2210.11239*, Oct. 2022, doi: 10.48550/arXiv.2210.11239.

[13] G. E. Dahl, J. W. Stokes, L. Deng, and D. Yu, "Large-scale malware classification using random projections and neural networks," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, May 2013, pp. 3422–3426, doi: 10.1109/ICASSP.2013.6638293.

[14] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, "Malware classification with recurrent networks," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, Apr. 2015, vol. 2015-August, pp. 1916–1920, doi: 10.1109/ICASSP.2015.7178304.

[15] W. Huang and J. W. Stokes, "MtNet: a multi-task neural network for dynamic malware classification," in *Detection of Intrusions and Malware, and Vulnerability Assessment: 13th International Conference, DIMVA*, vol. 9721, Springer International Publishing, 2016, pp. 399–418.

[16] B. Athiwaratkun and J. W. Stokes, "Malware classification with LSTM and GRU language models and a character-level CNN," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, Mar. 2017, pp. 2482–2486, doi: 10.1109/ICASSP.2017.7952603.

[17] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in *Advances in Artificial Intelligence: 29th Australasian Joint Conference*, 2016, pp. 137–149, doi: 10.1007/978-3-319-50127-7_11.

[18] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv*, 2014.

[19] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *2016 IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 582–597, doi: 10.1109/SP.2016.41.

[20] A. Kantchelian, J. D. Tygar, and A. D. Joseph, "Evasion and hardening of tree ensemble classifiers," in *International conference on machine learning*, 2016, vol. 5, pp. 2387–2396.

[21] F. Tramer, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *25th USENIX security symposium (USENIX Security 16)*, 2016, pp. 601–618.

[22] J. Feng, T. Zahavy, B. Kang, H. Xu, and S. Mannor, "Ensemble robustness of deep learning algorithms," *arXiv preprint 1602.02389*, pp. 1–19, 2016, [Online]. Available: http://arxiv.org/abs/1602.02389.

[23] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, "Ensemble adversarial training: attacks and defenses," *arXiv preprint 1705.07204*, May 2017, [Online]. Available: http://arxiv.org/abs/1705.07204.
[24] W. Xu, D. Evans, and Y. Qi, "Feature squeezing: detecting adversarial examples in deep neural networks," 2018, doi: 10.14722/ndss.2018.23198.
[25] J. Bellamy, *Computer telephony integration*. New York: Wiley, 2010.
[26] A. Mahindru *et al.*, "PermDroid a framework developed using proposed feature selection approach and machine learning techniques for Android malware detection," *Scientific Reports*, vol. 14, no. 1, May 2024, doi: 10.1038/s41598-024-60982-y.
[27] N. Papernot, P. McDaniel, X. Wu, S. Jha and A. Swami, "Distillation as a Defense to adversarial perturbations against deep neural networks," *IEEE Symposium on Security and Privacy (SP)*, pp. 582-597, 2016, doi: 10.1109/SP.2016.41.

BIOGRAPHIES OF AUTHORS

Gulzhanat Beketova received a master's degree in computer science from Korkyt Ata Kyzylorda State University in 2008. In 2019, she received a Ph.D. in computer science and software from Satpayev University. She currently works as an associate professor at the IT Engineering (ITE) Department at Almaty University of Power Engineering and Telecommunications. She is the author or co-author of more than 40 publications. Her research interests are informational systems and cybersecurity. She can be contacted at email: g.beketova@aues.kz.

Ainur Manapova received her master's degree in mathematical and computer modeling/applied mathematics and computer science in 2018. She is currently working at the Civil Aviation Academy. She is the author and co-author of more than 15 publications. Her research interests are CFD, numerical simulation, modeling. She can be contacted at email: manapova.a.k.math@gmail.com.