ScieRxiv

NOT PEER-REVIEWED

Research Article

An Improved SIR Epidemic Model with Security Hierarchy Protection for Malware Propagation Analysis

Liping Feng*, Yaojun Hao, Peng Wei

Computer Science Department, Xinzhou Normal University, Xinzhou, Shanxi, 034000, China.

***Correspondence to**: Liping Feng, Computer Science Department, Xinzhou Normal University, Xinzhou, Shanxi, 034000, China. E-mail: fenglp@yeah.net

Received: 27 March 2025 | Approved: 03 June 2025 | Online: 03 June 2025

Abstract

With the fast development of the Internet, the issues of cyber security are becoming more and more severe. Malware is one of important factors to cause cybersecurity accidents. In this paper, an improved Susceptible-Infected-Recovery (i-SIR) epidemic model is proposed to portray the characteristic of malware propagation. And the security hierarchy protection measure is considered in this model, which means that the nodes in S state are devided into S_H (susceptible with high security level) and S_L (susceptible with low security level) two parts . Then, using function theory, equilibria

DOI: 10.20517/scierxiv202506.0168.v1 https://www.scierxiv.com/

of the model are obtained. Specially, the stability of malware-free equilibrium is proved by the stability theory. Finally, numerical analysis and simulation experiments validate that theoretical analysis are correct. Simulated results indicate that security hierarchy protection measures can defend effectively the prevalence of malware in the network. The conclusions of this paper can contribute to a better theoretical basis for understanding feasibility of hierarchy protection system.

Keywords: Network security, malware propagation model, security hierarchical protection, dynamical model, stability theory

INTRODUCTION

A MALWARE (milicious software) is a computer virus which aims to violate computer systems' security policy. In today's networks and systems, malwares are still a severe threat to critical applications like education, hospitals, banking, and so on [1,2]. For instance, in 2007, a notorious ransomware named Wanna Decryptor swept the globe, resulting in massive computer paralysis and causing huge economic losses [3,4]. Therefore, it has always been significant and urgent to take effective coutermeasures to control the propagation of malware in networks.

To the goal, many epidemic models have been proposed by cyber security researchers to study propagation law of malware on Internet, duo to similarity between the prevalence of malware on Internet and diffusion of human epidemic disease in the population. Pioneering work is that Kephart and White [5,6] constructed computer virus propagation models which combined traditional biological methods and network topology. These researches laid the foundation for understanding and predicting virus propagation on Internet. And then, lots of researchers proposed the propagation models of malware

considering different anti-virus measures [7-12]. Dong *et al* [13] put forward the fractional SIRS malware propagation model based on fractional interconnected Takagi-Sugeno (T-S) fuzzy systems and point out some qualitative properties on the model. Hosseini *et al*.[14] raised a discrete-time SEIRS model to investigate the dynamical characteristic of malware propagation in scale-free networks by considering software diversity. In view of the effect of communication radius and distribution density of wireless sensor network nodes on worm prevalence, Feng *et al*.[15] came up with an improved SIRS epidemic model to evaluate the impact of communication radius and distribution density in wireless sensor networks on worm diffusion. And they analyzed the stability of worm spread through solving the equilibriums of the model. In view of the fact that the anti-virus measures may lead to time lag, Yao and Nithya *et al*. [16 - 19] proposed time delay dynamic models to obtained the critical view of time delay when Hopf bifurcation arised. Based on the optimal control theory applied widely to human epidemics [20-23], some scholars constructed the propagation models of malware with optimal control function and investigated optimal control strategies of malware [24-28].

The above mentioned literatures provide theoretical insights for controlling the propagation of malware in computer networks. We notice that these works all assume all nodes in computer networks are protected by the same intensive anti-virus measures. However, there is the fact in reality that the importance of different nodes is also diverse in computer networks. So, considering cost-effectiveness, anti-virus measures should be distinct intensity. In fact, the hierarchy protection measures are used widely to control the propagation of malware in real network security managments. Hence, in this paper, we put forward our dynamical model with hierarchy protection measures and examine the effectiveness of this strategy by comparing it with current models without hierarchy protection measures usig computer simulations.

DOI: 10.20517/scierxiv202506.0168.v1 https://www.scierxiv.com/

The rest of this artical is outlined as below. In Section 2, we present the improved Susceptible-Infected-Recovered (i-SIR) model with hierachy protection measures. Section 3 analyze the stability of virus-free equilibrium. In section 4, we carry out numerical simulations and simulation experiments to confirm that the theoretical analysis are correct. Section 5 concludes the paper and presents the future research.

THE I-SIR MALWARE PROPAGATION MODEL

Network security protection will consume system resources, and the defender will pay the cost. Hence, the best strategy for the defender is to take appropriate security measures based on the importance of system resources. In reality, different information network systems have different functions, and benefit loss is also different when a cyber security incident occurs. for example, some information systems are designed for sensitive information such as ID cards and bank card numbers, and some information systems are related to critical infrastructures or enterprise core business. Thus, these systems must be protected strongly when security defense measures are taken. In contrast, some information systems that carry general business can take less strong security protection measures.

Based on the above, in this section, we will discuss a malware diffusion dynamical model called i-SIR, which is an improvement of the SIR model by considering security defense measures of different strengths. In this way, the i-SIR model furnishes an insight for us to understand the scientific significance of hierarchical protection measures, and this is very vital for management and control of malware prevalence.

DOI: 10.20517/scierxiv202506.0168.v1

For the i-SIR model, there are four states: S_H (Susceptible state with high security level), S_L (Susceptible state with low security level), I (infected state), and R (recovered state). In reality, apart from the most basic state transition among S_H (S_L)-I-R, users can often immune their computers by anti-virus measures in state S_H (S_L), or state I, owing to their cost-benefit anslysis when a security emergency occurs. These anti-virus measures may lead to the following three new state transition paths.

- $S_H \rightarrow R$, employing real-time anti-virus measures;
- $S_L \rightarrow R$, employing real-time anti-virus measures;
- $I \rightarrow R$, employing anti-virus measures after computers are infected.

According to the above statement, a novel SIR model, i.e. i-SIR model is shown in Figure 1, where μ is the removal rate of old nodes; β_H and β_L represent infection rate of susceptible nodes S_H and S_L, respectively; δ is the curative rate from I to R; ω and γ describe the impact of implementing real-time immunization; N_H and N_L represent new number of S_H and S_L, respectively, and N is total number of nodes.

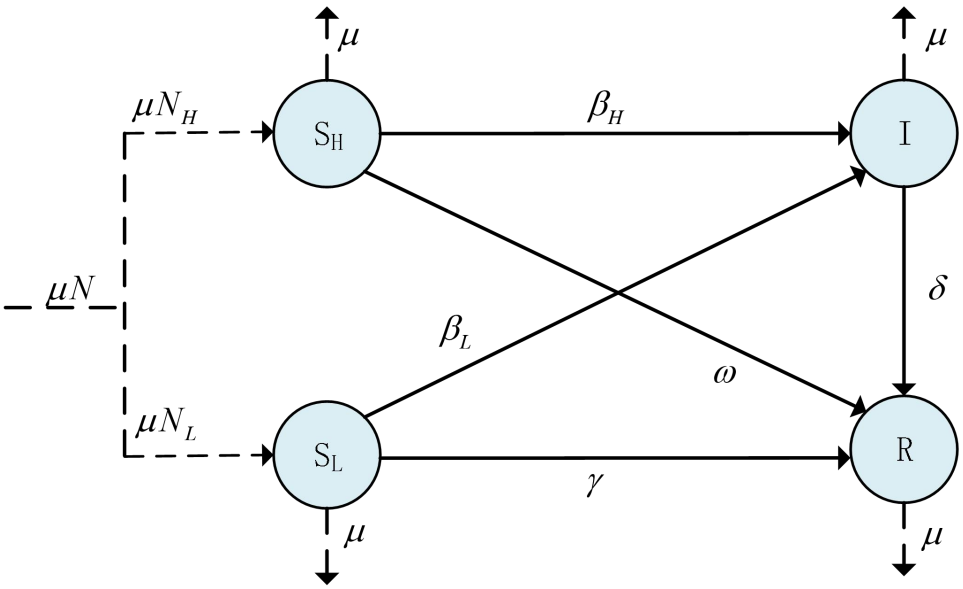

Figure 1. The i-SIR model.

DOI: 10.20517/scierxiv202506.0168.v1

There we presume the number of nodes in a information network is relatively steady. Let $S_H(t)$, $S_I(t)$, $I(t)$ and $R(t)$ be the number of nodes at time t in states S_H, S_I, I and R, respectively, then we can get

$$S_H(t)+S_L(t)+I(t)+R(t)=N. \tag{1}$$

The i-SIR dynamical model can be formulated by the following differential equations.

$$\begin{cases} \dfrac{dS_H(t)}{dt}=\mu N_H-\beta_H S_H(t)I(t)-(\mu+\omega)S_H(t), \\ \dfrac{dS_L(t)}{dt}=\mu N_L-\beta_L S_L(t)I(t)-(\mu+\gamma)S_L(t), \\ \dfrac{dI(t)}{dt}=(\beta_H S_H(t)+\beta_L S_L(t))I(t)-(\mu+\delta)I(t), \\ \dfrac{dR(t)}{dt}=\omega S_H(t)+\gamma S_L(t)+\delta I(t). \end{cases} \tag{2}$$

We note that the fourth equation do not affect the first three equations in system (2), and hence, the fourth equation can be omitted without losing its generalization. So, system (2) can be rewritten as

$$\begin{cases} \dfrac{dS_H(t)}{dt}=\mu N_H-\beta_H S_H(t)I(t)-(\mu+\omega)S_H(t), \\ \dfrac{dS_L(t)}{dt}=\mu N_L-\beta_L S_L(t)I(t)-(\mu+\gamma)S_L(t), \\ \dfrac{dI(t)}{dt}=(\beta_H S_H(t)+\beta_L S_L(t))I(t)-(\mu+\delta)I(t). \end{cases} \tag{3}$$

MODEL ANALYSIS

Now, we analyze the dynamical characteristic of system (3) by solving its equilibrium. equilibrium states of system (3) meet the following equations:

$$\begin{cases} \dfrac{dS_H(t)}{dt}=0, \\ \dfrac{dS_L(t)}{dt}=0, \\ \dfrac{dI(t)}{dt}=0. \end{cases} \tag{4}$$

DOI: 10.20517/scierxiv202506.0168.v1

Let $dI(t)/dt = 0$, we can get $I^* = 0$, or $I^* = \left(\beta_H S_H^* + \beta_L S_L^*\right)/(\mu + \delta)$.

When $I^* = 0$, there has the virus-free equilibrium

$$Q^0 = \left(S_H^0, S_L^0, I^0\right) = \left(\frac{\mu}{\mu+\omega} N_H, \frac{\mu}{\mu+\omega} N_L, 0\right). \tag{5}$$

When $I^* > 0$, there has the virus-endemic equilibrium

$$Q^* = \left(S_H^*, S_L^*, I^*\right) = \left(S_H^*, S_L^*, \frac{\beta_H S_H^* + \beta_L S_L^*}{\mu+\delta}\right). \tag{6}$$

Following, we analyze the local and global stability of the virus-free equilibrium. According to Eq.(5), we can obtain the following characteristic equation of system (3) at Q^0:

$$\det\begin{pmatrix} -(\mu+\omega)-\lambda & 0 & -\beta_H S_H^0 \\ 0 & -(\mu+\gamma)-\lambda & -\beta_L S_L^0 \\ 0 & 0 & \beta_H S_H^0 + \beta_L S_L^0 - (\mu+\delta) - \lambda \end{pmatrix} = 0, \tag{7}$$

which is equivalent to

$$\beta_H S_H^0 + \mu + \gamma + \lambda = 0. \tag{8}$$

According to Eq.(8), obviously that characteristic root $\lambda < 0$. Therefore, the following lemma can be obtained.

Lemma 1. The system (3) has always the virus-free equilibrium Q^0, and Q^0 is locally asymptotically stable.

Define

$$R_0 = \frac{\beta_H S_H^0 + \beta_L S_L^0}{\mu+\delta}. \tag{9}$$

Further, the Theorem 1 can be obtained.

Theorem 1. The system (3) has always the virus-free equilibrium Q^0, and Q^0 is globally asymptotically stable when $R_0 < 1$.

Proof. We can have from the first equation of system (3)

$S_H'(t) \le \mu N_H - (\mu+\omega) S_H$.

Thus

DOI: 10.20517/scierxiv202506.0168.v1

$$S_H(t) \le \frac{\mu N_H}{\mu+\omega} + \left(S_H(0) - \frac{\mu N_H}{\mu+\omega}\right)\exp\left[-(\mu+\omega)t\right],$$

when $t \to \infty$, it can be obtained

$$S_H(t) \le \frac{\mu N_H}{\mu+\omega}.$$

In a similar way, we can obtain

$$S_L(t) \le \frac{\mu N_L}{\mu+\gamma}.$$

Define

$$K(t) = I(t).$$

Then, we can get the time derivative of $K(t)$ along the system (3).

$$\dot{K}(t) = \left(\beta_H S_H(t) + \beta_L S_L(t)\right) I(t) - (\mu+\delta) I(t) \le \left[\beta_H \frac{\mu N_H}{\mu+\omega} + \beta_L \frac{\mu N_L}{\mu+\gamma} - (\mu+\delta)\right] I(t)$$
$$= \frac{1}{\mu+\delta}(R_0 - 1) I(t) \le 0.$$

So, the Theorem 1 is proved. □

NUMERICAL SIMULATIONS AND SIMULATION EXPERIMENTS

Numerical simulations

To test the Theorem proposed in this paper, we will carry out numerical experiments in this section.

Firstly, we introduce the numerical experiment parameters. Parameters of the i-SIR model are devided into two types: system parameters and state transition parameters[26]. In general, system parameters are fixed if we don't clearly point out the alterations. In these parameters, t_I is the vital one that is related to user behaviors, defender's response time and the malware characteristics. In this paper, we fixed t_I=14(day), and the value of δ is computed as $\delta = 1/t_I - \mu$. The values of other parameters are depicted in Table 1. In

addition, the values of $S_H(0)$, $S_L(0)$, $I(0)$ and $R(0)$ has an important influence on malware prevalence. According to the real situation, $I(0)$ is small.

Now, we verify the validity of theories analysis by numerical simulations. Set initial values of state S_H, S_I, I and R are $S_H(0)=50000$, $S_L(0)=49990$, $I(0)=10$ and $R(0)=0$, $I(0)=10$ and $R(0)=0$, respectively. State conversion rate $\omega=0.0008$, $\gamma=0.0005$, and δ can be computed by t_I shown in Table 1. Then we can get malware control parameters: $R(0)=0.0102<1$. The simulation result is depicted in Figure.2. From Figure.2, we can see that the system attained the stable virus-free equilibrium over time after malware infection outbreaks occurred. The conclusion agrees with Theorem 1.

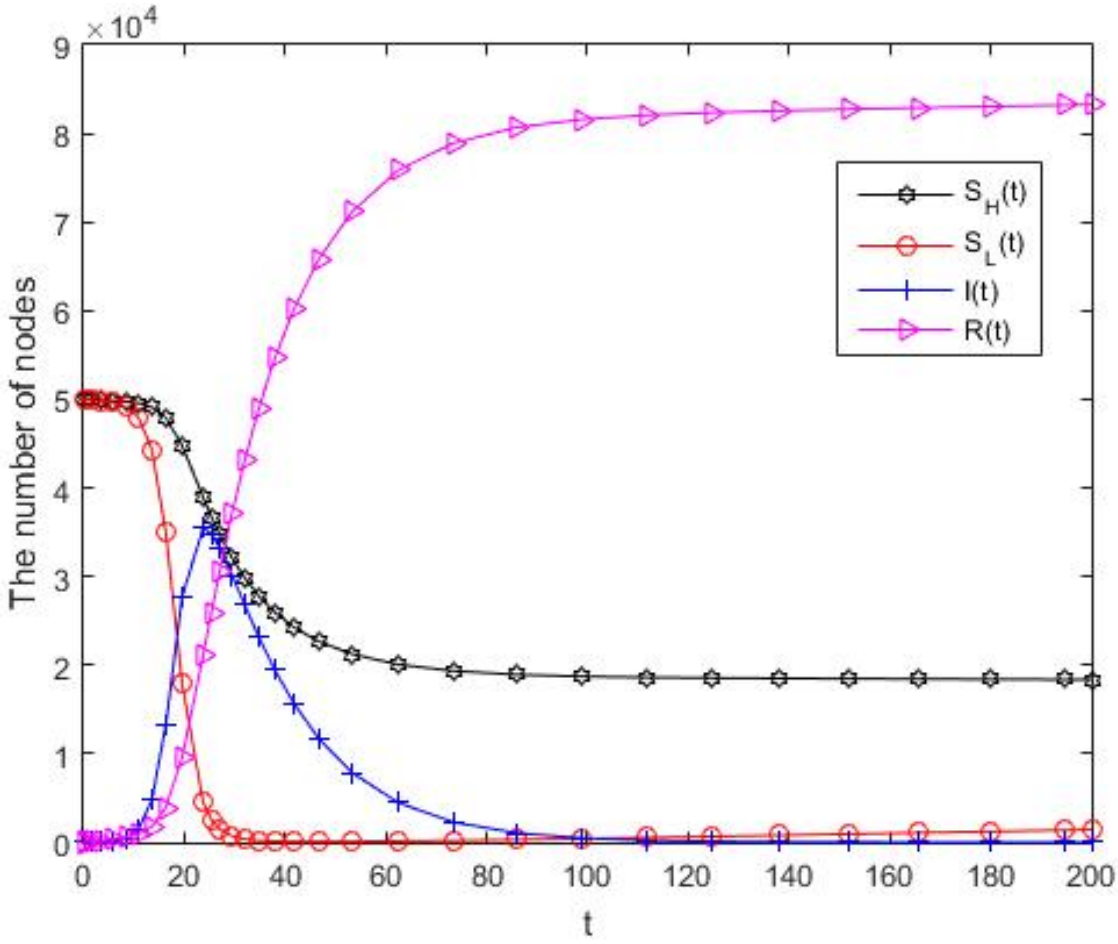

Figure 2. Malware propagation result with $R(0)=0.0102<1$.

DOI: 10.20517/scierxiv202506.0168.v1

Table 1. The parameters and the values in numerical experiments

parameters	Values	notes
N	100,000	Total number of nodes in the network
μ	1/4380	The removment rate of nodes (about
$S_H(0)$	Unfixed	The beginning amount of nodes in
$S_I(0)$	Unfixed	The beginning amount of nodes in
$I(0)$	Unfixed	The beginning amount of nodes in
$R(0)$	$N-S_H(0)-S_I(0)-I(0)$	The beginning amount of nodes in
ω	Unfixed	State conversion rate from S_H to R
γ	Unfixed	State conversion rate from S_I to R
t_I	12	The average time in state I
δ	$1/t_I-\mu$	State conversion rate from I to R

Considering that S_H and S_L have great impact on malware propagation, we simulate the trajectory of malware propagation with different S_H and S_L. Simulated result is depicted in Figure 3. From Figure 3, we can see that the values of S_H and S_L not only take great impact on the scale of malware propagation, but also have great influence on the propagation speed, which is the smaller value of S_H, the greater scale of malware propagation. When $S_H = 10000$ and $S_L = 89990$, malware can infect about 65% nodes on Internet in less than a day, and then the spread of malware slows down rapidly. In contrast, when $S_H = 90000$ and $S_L = 9990$, the scale and speed of malware propagation significantly decrease. The maximum scale of node infection on Internet is about 10%, and it takes about 5 days to reach the this peak. This is because the nodes in the state S_H in network information systems carry more important information, and the defender will take strong protection measures for these nodes, and the probability of the attack's successful attack is greatly reduced.

DOI: 10.20517/scierxiv202506.0168.v1

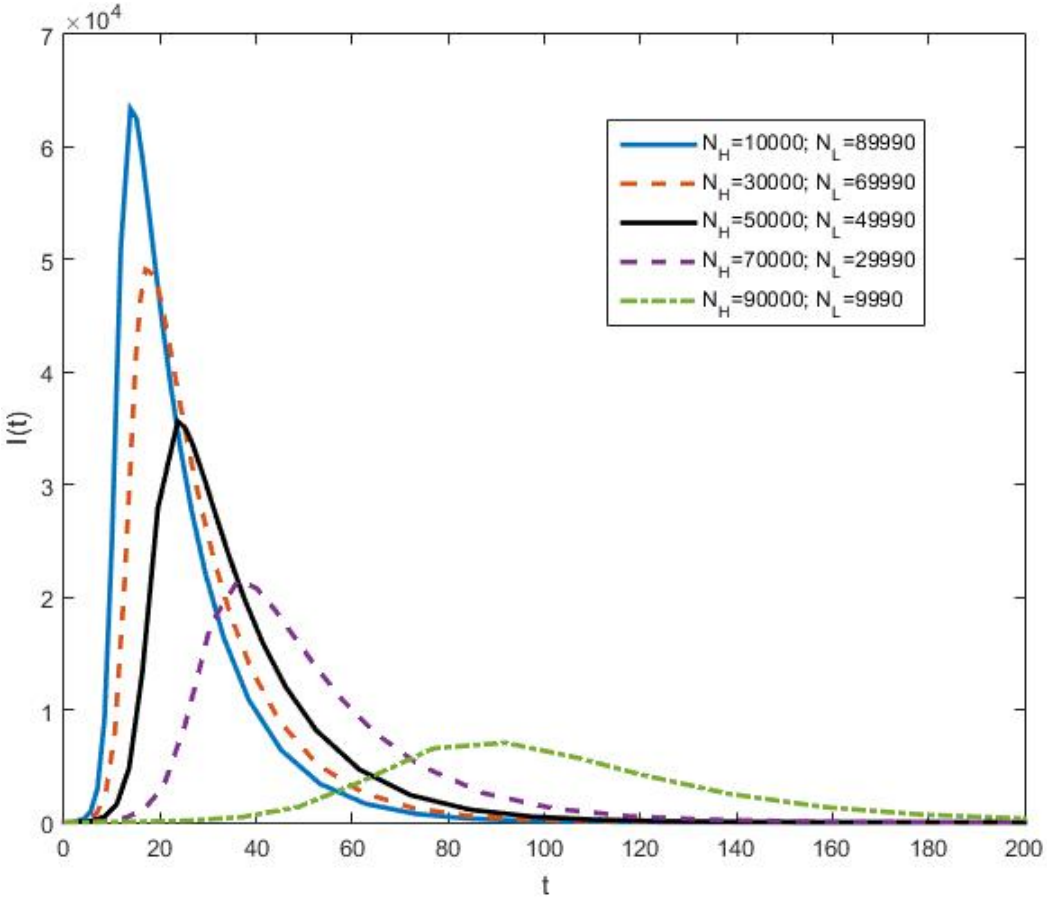

Figure 3. Malware propagation results with different S_H and S_L

Next, we observe the situation without security classification protection. There are two kinds of situations: (i) all nodes take strong protection measures, i.e. $S_H = 99990$ and $S_L = 0$; (ii) all nodes take weak protection measures, i.e. $S_H = 0$ and $S_L = 99990$. Numerical simulation results are shown in Figure 4. Obviously, strong protection measures can effectively prevent large-scale malware infection, and weak protection will lead to the heavy network security accident. However, due to cost, cyber security pursues the optimal defense rather than the strongest defense. Simulation results show that it is reasonable to take security defense measures of different intensities according to the importance of information systems,

DOI: 10.20517/scierxiv202506.0168.v1

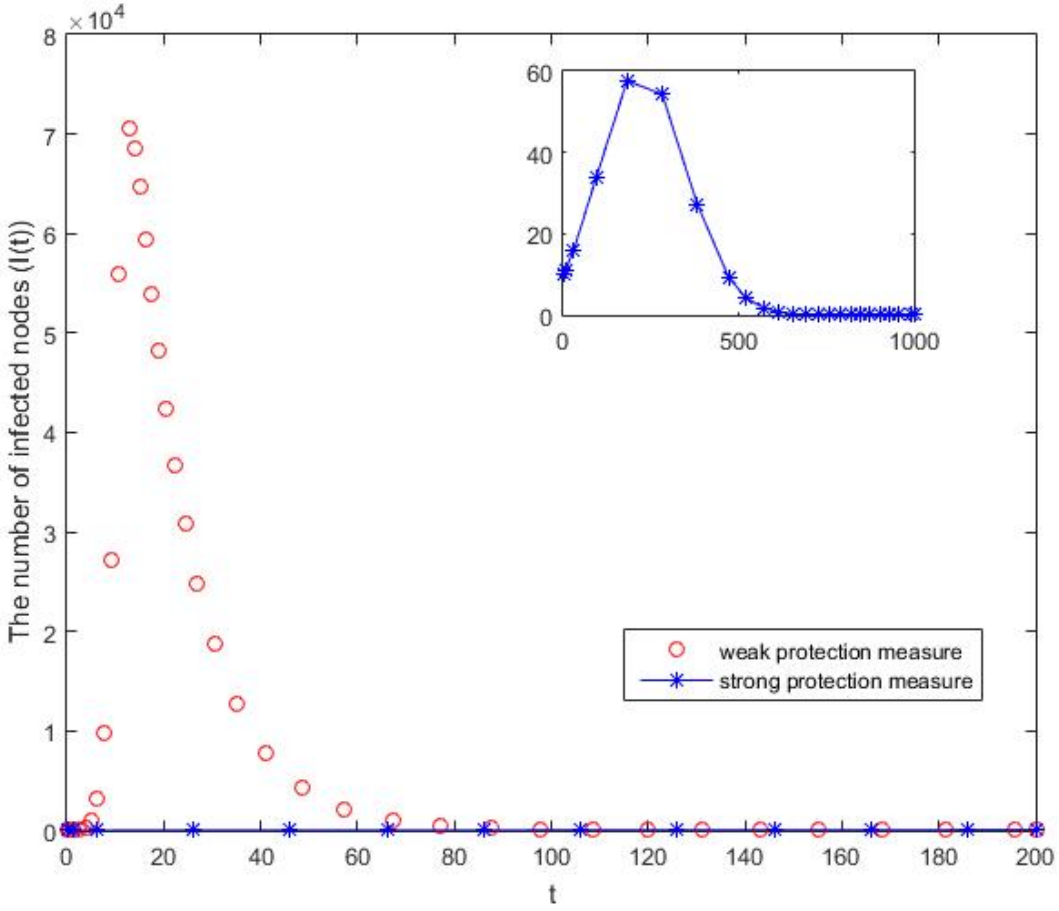

Figure 4. The tragetory of malware infection without security classification protection

Simulation experiments

For the sake of simulating the practical behavior of malware prevalence and the validity of theoretical and numerical analysis, we execute discreate-time simulation experiments. Simulation experiments are devoted to reflecting malware propagation in the real network. In our simulations, we assume that there are 100000 nodes in the network. We choose randomly 10 nodes to be infectious nodes, i.e. $I(0)=10,$ and then we verify the correctness of theoretical and numerical analysis with different values of S_H and S_L. To enhance the precision of discreate-time simulations, we set 0.5 second as the discrease time unit. The implimentation of transition rate of malware prevalence relies on probability. Fig. 5 presents the comparisons between numerical analysis and simulation

DOI: 10.20517/scierxiv202506.0168.v1

experients with different S_H and S_L. We can see that the simulation results are almost coincident with numerical results.

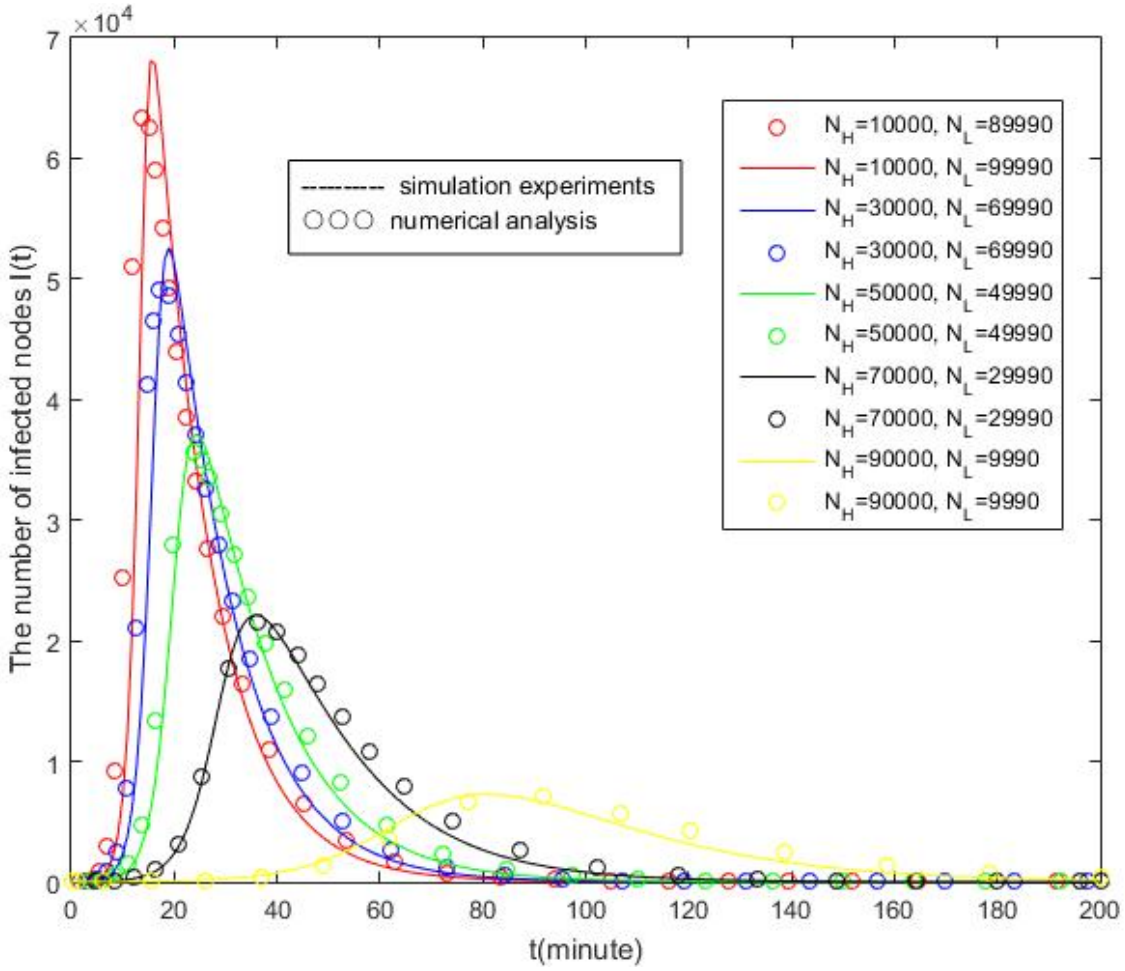

Figure 5. Comparisons between numerical solutions and simulations with different S_H and S_L

CONCLUSIONS

In this paper, we come up with an i-SIR model with different strengths of security defense measures for different information systems. Then the stability of the virus-free equilibrium is analyzed. Through theoretical analysis, meaningful conclusions are acquired. In the meanwhile, theoretical results are verified by the numerical analysis and simulation experiments. We can gain the following scientific results by our study:

DOI: 10.20517/scierxiv202506.0168.v1

(1) The malware prevalence will be restrainted over time when $R_0 < 1$. according to this conclusion, we can forecast the diffusion of malware, and malwares can be controlled to a low level or be eliminated finally.

(2) According to the importance of different information systems, adopting security defense measures of different intensities can greatly reduce the spread of malware in terms of scale and speed.

This work is contributed to understanding the effect of hierarchical security protection measures on controlling malware propagation. In future studies, we will consider the topology of networks and investigate its effect on malware spread further.

DECLARATIONS

Acknowledgments

This work was supported by Fundamental Research Program of Shanxi Province (202203021211116).

Authors'contributions

Liping FENG drafted the entire manuscript， Yaojun HAO developed the theoretical framework and Peng WEI conducted Numerical Simulations.

Data Availability

All the data used to support the findings of this study are available from the corresponding author upon request.

Financial support and sponsorship

Science and Technology Department of Shanxi Province

Conflicts of Interest

There is no conflicts of interest regarding the publication of this paper.

Ethical approval and consent to participate

The paper does not involve ethical issues

Consent for publication

Written informed consent was obtained from all participants

Copyright

REFERENCES

1. Shahid N, Aziz-ur Rehman M, Khalid A, et al. Mathematical analysis and numerical investigation of advection-reaction-diffusion computer virus model. *Results in Physics* 2021;26:104294.[DOI:10.1016/j.rinp.2021.104294]
2. Abijah Roseline S, Geetha S. A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering* 2021;92:107143.[DOI:10.1016/j.compeleceng.2021.107143]
3. S Mohurle, M Patil. A brief study of wannacry threat: Ransomware attack 2017, International Journal of Applied Mathematics and Computer Science, 8(2017). Available from: https://www.ijarcs.info/index.php/Ijarcs/article/view/4021[Last accessed on 19 May 2025]

4. Mansfield-devine S. Leaks and ransoms – the key threats to healthcare organisations. *Network Security* 2017;2017:14-9.[DOI:10.1016/s1353-4858(17)30062-4]
5. JO Kephart, SR White. Directed-graph epidemiological models of computer viruses, in: IEEE Symposium on Security and Privacy, 1991, pp. 343–361. [DOI:10.1109/risp.1991.130801]
6. JO Kephart, SR White. Measuring and modeling computer virus prevalence, in: IEEE Computer Security Symposium on Research in Security and Privacy, IEEE, 1993, pp. 2–15.[DOI:10.1109/risp.1993.287647]
7. Mishra BK, Saini DK. SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics and Computation* 2007;188:1476-82.[DOI:10.1016/j.amc.2006.11.012]
8. C C Zou, W Gong, D Towsley. Code red worm propagation modeling and analysis, in: Proceedings of the 9th ACM Conference on Computer and Communications, Security, 2002, pp 138–147.[DOI:10.1145/586110.586130]
9. Zou CC, Towsley D, Gong W. Modeling and Simulation Study of the Propagation and Defense of Internet E-mail Worms. *IEEE Trans Dependable and Secure Comput* 2007;4:105-18.[DOI:10.1109/tdsc.2007.1001]
10. Feng L, Liao X, Li H, Han Q. Hopf bifurcation analysis of a delayed viral infection model in computer networks. *Mathematical and Computer Modelling* 2012;56:167-79.[DOI:10.1016/j.mcm.2011.12.010]
11. Feng L, Liao X, Han Q, Li H. Dynamical analysis and control strategies on malware propagation model. *Applied Mathematical Modelling* 2013;37:8225-36.[DOI:10.1016/j.apm.2013.03.051]

12. Cao H, Peng D, Yu D. Modeling and controlling spatiotemporal malware propagation in mobile Internet of Things. *Applied Mathematical Modelling* 2025;144:116042.[DOI:10.1016/j.apm.2025.116042]
13. Dong NP, Giang NL, Long HV. Interconnected Takagi-Sugeno system and fractional SIRS malware propagation model for stabilization of Wireless Sensor Networks. *Information Sciences* 2024;670:120620.[DOI:10.1016/j.ins.2024.120620]
14. Hosseini S, Azgomi MA, Rahmani AT. Malware propagation modeling considering software diversity and immunization. *Journal of Computational Science* 2016;13:49-67.[DOI:10.1016/j.jocs.2016.01.002]
15. Feng L, Song L, Zhao Q, Wang H. Modeling and Stability Analysis of Worm Propagation in Wireless Sensor Network. *Mathematical Problems in Engineering* 2015;2015:1-8.[DOI:10.1155/2015/129598]
16. Yao Y, Xie X, Guo H, Yu G, Gao F, Tong X. Hopf bifurcation in an Internet worm propagation model with time delay in quarantine. *Mathematical and Computer Modelling* 2013;57:2635-46.[DOI:10.1016/j.mcm.2011.06.044]
17. Yao Y, Xiang W, Qu A, Yu G, Gao F, Mishra BK. Hopf Bifurcation in an SEIDQV Worm Propagation Model with Quarantine Strategy. *Discrete Dynamics in Nature and Society* 2012;2012:304868.[DOI:10.1155/2012/304868]
18. Yao Y, Feng X, Yang W, Xiang W, Gao F, Karimi HR. Analysis of a Delayed Internet Worm Propagation Model with Impulsive Quarantine Strategy. *Mathematical Problems in Engineering* 2014;2014:369360.[DOI:10.1155/2014/369360]
19. Nithya D, Madhusudanan V, Murthy B, et al. Delayed dynamics analysis of SEI2RS malware propagation models in cyber–Physical systems. *Computer Networks* 2024;248:110481.[DOI:10.1016/j.comnet.2024.110481]

20. Chen L, Sun J. Optimal vaccination and treatment of an epidemic network model. *Physics Letters A* 2014;378:3028-36.[DOI:10.1016/j.physleta.2014.09.002]

21. Zaman G, Kang YH, Cho G, Jung IH. Optimal strategy of vaccination & treatment in an SIR epidemic model. *Mathematics and Computers in Simulation* 2017;136:63-77.[DOI:10.1016/j.matcom.2016.11.010] Caution!

22. Jajarmi A, Yusuf A, Baleanu D, Inc M. A new fractional HRSV model and its optimal control: A non-singular operator approach. *Physica A: Statistical Mechanics and its Applications* 2020;547:123860.[DOI:10.1016/j.physa.2019.123860]

23. Abdullahi Baba I, Ahmad Nasidi B, Baleanu D. Optimal Control Model for the Transmission of Novel COVID-19. *Computers, Materials & Continua* 2021;66:3089-106.[DOI:10.32604/cmc.2021.012301]

24. Zhu Q, Yang X, Yang L, Zhang C. Optimal control of computer virus under a delayed model. *Applied Mathematics and Computation* 2012;218:11613-9.[DOI:10.1016/j.amc.2012.04.092]

25. Sayed Ahmed A, Ahmed HM, Nofal TA, Darwish A, Omar OA. Hilfer-Katugampola fractional epidemic model for malware propagation with optimal control. *Ain Shams Engineering Journal* 2024;15:102945.[DOI:10.1016/j.asej.2024.102945]

26. Yang L, Li P, Yang X, Xiang Y, Tang YY. Simultaneous Benefit Maximization of Conflicting Opinions: Modeling and Analysis. *IEEE Systems Journal* 2020;14:1623-34.[DOI:10.1109/jsyst.2020.2964004]

27. Jafar MT, Yang L, Li G, Zhu Q, Gan C, Yang X. Malware containment with immediate response in IoT networks: An optimal control approach. *Computer Communications* 2024;228:107951.[DOI:10.1016/j.comcom.2024.107951]

28. Liu G, Chen J, Liang Z, Peng Z, Li J. Dynamical Analysis and Optimal Control for a SEIR Model Based on Virus Mutation in WSNs. *Mathematics* 2021;9:929.[DOI:10.3390/math9090929]