Research on virus diffusion prevention method for computer singularity in complex sensor networks

Lei Ma, Ying Jian Kang and Hua Han

Beijing Polytechnic,
No. 9 Liangshuihe Street,
Beijing Economic and Technological Development Zone,
Beijing 100000, China
Email: dkymalei@163.com
Email: kyj12346@163.com
Email: yybbccww@126.com

Gihong Min*

Paichai University,
155-40 Baejae-ro (Doma-Dong),
Seo-Gu, Daejeon 302735, South Korea
Email: ming@pcu.ac.kr
*Corresponding author

Abstract: In current virus propagation defence methods, immunisation failures, as well as combination influence of infectious vector and propagation delay in propagation are not considered. Therefore, propagation of computer singularity virus is hard to control. A new SIS propagation model is proposed based on mean field theory with infectious vector and propagation delay. The influence of computer virus in complex sensor networks on the propagation property is analysed. A new cellular automata model is built to simulate computer virus propagation. With abstraction layer from computer singularity virus detection model based on immunisation principle, a fusion method for singularity virus detection is proposed. Through fusion of different antigen presentation gene library, ability of defence of computer singularity virus propagation is improved. Experimental results show that target immune network connectivity factor ratio of our method is only 0.18, lower than 0.37 multiples of nearest neighbour immunity.

Keywords: complex sensor network; computer singularity; virus propagation defence; internet manufacturing; internet services.

Reference to this paper should be made as follows: Ma, L., Kang, Y.J., Han, H. and Min, G. (2020) 'Research on virus diffusion prevention method for computer singularity in complex sensor networks', *Int. J. Internet Manufacturing and Services*, Vol. 7, Nos. 1/2, pp.64–82.

Biographical notes: Lei Ma is currently an Assistant Professor in Beijing Polytechnic. Her research interests include computer security and big data. Bachelor degree graduated from Agricultural University of China computer major in July 2002, graduated from Beijing University of Aeronautics and Astronautics computer Application Engineering Master in 2008. In 2015, Lei she was named Associate Professor. For many years, she has been engaged in the teaching and scientific research of computer major and has taught

professional core courses such as ‘C Language’, ‘Discussion on Database Design’, ‘WEB Front End’, ‘Dynamic Web Design’ and so on. In recent years, more than 10 projects have been completed and studied, and many Chinese core and SCI papers have been published.

Ying Jian Kang is currently an Assistant Professor in Beijing Polytechnic. Her research interests include computer software and big data. In July 1994, she graduated from the Department of Mathematics, Capital normal University, majoring in computer science, and in 2010, she graduated with the Master’s of Engineering in Electronics and Communications Engineering, Tianjin University. She was a Senior Lecturer in 2004, and transferred to Associate Professor in 2014. For many years, she has been engaged in the teaching and scientific research of computer major and has taught professional core courses such as ‘C Language’, ‘JAVA Language’, ‘WEB Front End’, ‘Dynamic Web Design’ and so on. In recent years, more than ten projects have been completed and studied, and many Chinese core and SCI papers have been published.

Hua Han is currently a Senior Accountant in Beijing Polytechnic. Her research interest is financial data management. She has been engaged in financial management since 2000, and has rich practical experience and strong scientific research ability. She has published ten papers in the provincial-level and above official publications, participated in the writing of the book *Higher Vocational College Governance – Internal Control* and edited a textbook. As an expert, she has been invited to participate in the financial policy research of higher vocational colleges, primary and secondary schools, off-campus activities and other fields organised by the Ministry of Education. As a project leader, she has been entrusted with a project entrusted by the Ministry of Education funds Supervision Center. Participate in three projects of the Ministry of Education Finance Department commissioned.

Gihong Min is currently a Lecturer in Department of Game Engineering, Paichai University. His research interest is data management and processing, big data processing. He has been engaged in programming management over ten years, and has rich practical experience and strong scientific research ability. He has published more than ten papers in the provincial-level and above official publications. As an expert, he has been invited to act as reviewers for many respected journals, including *The Journal of Supercomputing*, *Multimedia Tools and Applications*, *Computer and Electrical Engineering*, *IET Image Processing*, and so on. As a project leader, he has been entrusted with many projects entrusted by the government’s funds.

1 Introduction

With the rapid development of the internet, the network has penetrated into every corner of society and has become an indispensable part of people’s lives. It has also become an important force for promoting social and economic development (Yang and Yang, 2015; Liu et al., 2013b; Hermance and Thangamani, 2015). However, the ensuing network security problems have become increasingly serious. The resulting economic losses have been rising rapidly year by year. At the same time, the problems of privacy leakage and theft of property have caused hidden dangers to the stability of the society (Casteel et al., 2015). According to relevant literature statistics, the proportion of computer viruses that have spread through storage devices has been decreasing in recent years. However, the number of viruses transmitted and destroyed mainly through complex web browsing and downloading has increased significantly (Hanawal et al., 2016). At the same time, the relevant literature points out that the types of virus and the mode of transmission are increasingly diversified. The number of viruses infected computers is increasing. The most widely spread and most harmful computer virus is a virus with strange characteristics. The harm is particularly serious. The propagation speed is getting faster and faster. The detection and prevention of viruses with computer singularity characteristics has become one of the hot research directions in complex network security (Wu et al., 2015; Bien et al., 2016; Liu et al., 2013a). Since the birth of the strange characteristic virus, the spread and destruction of malicious code represented by strange characteristic viruses has caused tremendous troubles and losses to the computer world and human society. Through analysing and studying the internal structure, propagation mechanism, destruction and attack behaviours, and abnormalities caused by strange-looking viruses, researchers have proposed various methods for detecting known viruses and finding unknown viruses (Oliveira et al., 2015; D'Alba and Shawkey, 2015). Cao and Ma (2017) used the differential equations to propose a virus propagation model in computer networks for the problem of virus propagation on computer networks, and analysed the existence and stability of equilibrium points for the constructed differential equation system. They came up with thresholds and extinction conditions for virus transmission, and further studied the effects of node speed, communication radius, immune success rate, and immune failure rate on the spread of viruses in computer networks. Liu et al. (2016) proposed a defence strategy model and an improved binary particle swarm optimisation algorithm based on this model for network security assessment and active defence. In the initial stage of virus transmission, a set of weighted defence strategies is constructed based on each computer virus intrusion action in the attack graph, aiming to highlight the defence cost. In order to prevent network virus intrusion at the minimum cost, binary particle swarm optimisation algorithm was introduced to improve the minimum key strategy set of the attack graph. The inadequacies of the existing network virus transmission defence methods mainly manifest in the following aspects:

1 Only the infection vector or propagation is analysed. The types of viruses in complex sensor networks are not well understood and the vigilance of singularity virus is low.

2 The influence of the variety of complex sensor network environment on virus infection rate is ignored. In the existing virus propagation models, the virus infection rate is considered as a value between 0 and 1 with fixed probability. However, the propagation of singularity virus in networks is affected by the network connectivity, network bandwidth, and immunisation.

3 There is not enough understanding of the immunisation status of the virus. The current research on virus immunity is almost assumed that in the early stage of virus propagation, the virus invasion action in networks is selected to carry out immunisation (Jia et al., 2014). In fact, the immunity of the virus is lagging behind. Users who have not yet been infected with the virus may install appropriate countermeasures after hearing about the dangers of certain viruses. Infected users are also immunised after they have cleared the virus and become subjectively immunised (Fan et al., 2016).

Aiming at the problems of detection and defence of computer virus in complex sensor networks which is not solved by the current methods, the technology of singularity virus detection and defence in complex sensor networks is researched in this paper. The influence of computer virus infectious vector and propagation delay in complex sensor networks on the propagation property is analysed. A new cellular automata model is built to simulate the whole process of computer virus propagation. Therefore, it not only ensures the normal propagation of harmless data in complex sensor networks, but also can effectively prevent the large spreading and propagation of singularity virus in complex sensor networks.

2 Transmission immunity analysis of computer virus under complex networks

In order to obtain the topological information of a large-scale practical network, the classic computer virus propagation model is used to understand the influence of the topological structure of the complex network on viral transmission behaviour. In order to facilitate the analysis of this effect, people usually define individuals in the population as nodes in the network. The abstraction of an interaction or connection between individuals exists as the edge between nodes. According to the characteristics of spread of network computer virus (Pythoud et al., 2015), different immunisation strategies are given for different network topologies (Neto et al., 2016). The specific descriptions are as follows.

2.1 Construction of computer virus propagation model under complex network

In the three traditional propagation models of SIS, SIR, and SI (Wong et al., 2015), each individual in the population is in one of three states of the susceptible state *S*, infection state *I*, and removed state *R*. The susceptible state represents the individual is not infectious, but may be infected. The infection state represents the individual has been infected and infectious. The removed state represents the individual has been cured and acquired the immune capacity, not infectious, and will not be infected again. Assume the infection probability in unit time step is denoted by β, the probability of the infected individual transformed into the removed state is denoted by γ, $s(t)$, $i(t)$, and $r(t)$ denote the density of *S*, *R*, and *I* kind of nodes at the *t* time, respectively, that is, the proportion. In the classic SIR propagation model, the process of the propagation of viruses is expressed by equation (1)

$$\frac{ds}{dt} = -\beta, \quad \frac{di}{dt} = \beta - \gamma, \quad \frac{dr}{dt} = \gamma \tag{1}$$

where *ds*, *dr*, and *di* are propagation rate of the infected individual in the SIS, SIR and SI model, *dt* is the current state of the individual. For some viruses such as influenza, the patients cannot obtain immunity after cured. In this case, SIS propagation model should be adopted. The only difference between this model and other models is that the infected individuals can automatically return to the susceptible state after being cured. For classic SIS propagation model, the propagation mechanism of the virus is depicted by equation (2).

$$\frac{ds}{dt} = -\beta + \gamma, \quad \frac{di}{dt} = \beta - \gamma, \tag{2}$$

In addition, people usually use the SI model to study the dynamical behaviour of the virus in the early stages of the virus outbreak. Because the virus can be controlled at this stage to obtain better results, the corresponding differential equations for the SI model are defined by equation (3).

$$\frac{d\rho(t)}{dt} = -\rho(t) + \lambda\langle k\rangle \rho(t)\left(1-\rho(t)\right) \tag{3}$$

Due to the distribution of node degrees of uniform networks such as ER stochastic network (Varanda et al., 2015) and WS small-world network (Musso, 2015), there is a peak at the network average degree $\langle k\rangle$, and it rapidly declines exponentially at $k \ll \langle k\rangle$ and $k \gg \langle k\rangle$. Therefore, when the average field theory is used to study the propagation dynamics of the SIS model over a homogeneous network, $\langle k\rangle$ can be used to approximate the network node degree k. Ignore the degree of correlation between nodes and the changes in birth and natural death of nodes within the virus propagation cycle. Let $\rho(t)$ be the density of infected nodes in the network, and the SIS propagation model response equation for a uniform network is defined by equation (4).

$$\rho(t)\left[-1 + \lambda\langle k\rangle\left(1-\rho(t)\right)\right] = 0 \tag{4}$$

The first consideration in the above equation is that the infected node is recovered as an easy-to-sweep node at a unit rate, and the second consideration is the average density of newly infected nodes generated by a single infected node. It is proportional to the effective transmission rate of the virus λ, the average node degree of the network $\langle k\rangle$, and the probability of being connected to the healthy node $1 - \rho(t)$. Convention ρ is the density of infected nodes at $\rho(t)$ steady state, and is derived from steady-state condition $d\,\rho(t)/d(t) = 0$. We can obtain equation (5).

$$\rho(t) - \left[-1 + \lambda\langle k\rangle\left(1-\rho(t)\right)\right] = 0 \tag{5}$$

Solving the above formula can obtain a uniform network with a propagation threshold of $\lambda_e = 1/\langle k\rangle$. This shows that there is a propagation threshold value λ_e greater than zero in a homogeneous network. When the effective transmission rate is $\lambda > \lambda_e$, the virus can spread in the network and will exist for a long time. If $\lambda < \lambda_e$, the virus will die out at an exponential rate.

According to the above steps, computer virus propagation model under complex networks is constructed. Based on our proposed model, immunity strategy of computer virus is proposed and analysed.

2.2 Immunisation strategy analysis of computer virus based on virus propagation model

Based on virus propagation model, an effective immunisation strategy of computer virus is proposed. Random immunisation is the simplest kind of immunisation strategy. The strategy is characterised by completely randomly selecting a part of nodes from the network to implement immunity, and ignoring the differences existing between the nodes in the network. That is to say, equal-heavy nodes and small nodes, although the higher the node's risk of being infected by viruses, the higher. The immune density of the appointed node is g, and the immune critical value corresponding to random immune in the uniform network is defined by equation (6).

$$g_e = 1 - \frac{\lambda_e}{\lambda} \tag{6}$$

From equation (6), in the uniform network, only if λ λ_e, the virus can spread in the network and then immunisation strategy is implemented. The critical value of immunisation after random immunisation in the scale-free network is given by equation (7).

$$g_e = 1 - \langle k \rangle / \lambda \langle k^2 \rangle \tag{7}$$

When the scale of the scale-free network is infinite, $\langle k^2 \rangle \to \infty$, and then $g_e \to 1$. It explains that in the process of random immunisation in the scale-free network, if the number of nodes in the network is more, all of the nodes are needed to completely prevent the virus breaking out in the network. It is unrealistic for many complex system with large-scale. Therefore, the effect of immunisation with the random immunisation strategy is good for the uniform network, but not suitable for the scale-free network.

As the poor effect of immunisation for the scale-free network, the effective immunisation strategy should be designed according to the network's own characteristics. In the scale-free network, the degree of most of nodes is small, while the degree of little nodes is relatively large. If these nodes with large degree are immunised, it can be very good to suppress the propagation of the virus and obtain the better immunisation effect. Using the non-uniformity of scale-free networks, we can select the nodes with largest degree in the network to immunise. When these nodes are immunised, the nodes connecting with them can be removed from the network, which drastically reduces the possible route of the virus propagation. The critical value in the scale-free network after immunisation is given by equation (8).

$$g_e \propto e^{-\frac{2}{m\lambda}} \tag{8}$$

From equation (8), it explains that no matter how the effective propagation rate changes, the critical value of propagation is always small. Therefore, compared with the random immunisation strategy, when the immunisation strategy is implemented in the scale-free network, the critical value of propagation is small. Only using a little part of nodes can achieve good immunisation effect, which means it is suitable for the scale-free network. According to the characteristics of the target immunisation, the immunisation effect of the network with heterogeneous topology is better, which explains that the topology structure of network plays an important role in the virus propagation dynamics.

3 Singularity virus propagation with consideration of infection vector and propagation delay

In view of the presence of vectors and propagation delays in the spread of viruses on computers under complex networks, a new SIS propagation model is proposed based on the theory of mean fields (Pan et al., 2017). It analyses the influence of computer virus vectors and propagation delays in complex networks on the impact of virus propagation on the network. Uniform networks and scale-free networks are used to describe the contact between different individuals in a population. From the overall point of view, a new cellular automata model was established to simulate the whole process of computer virus transmission. We also consider the impact of individual movement and individual distribution heterogeneity on the computer virus propagation behaviour, and build the basis of cellular automata update rules is the probabilistic characteristics of virus propagation process.

3.1 Propagation behaviour of the proposed SIS model in the uniform network

In the uniform network, the degree of each individual is approximately equal to the average $\langle k \rangle$ degree. Define the densities of the healthy individual and the infected individual of N individuals H at t time are $s(t)'$ and $\rho(t)'$ with $s(t) + \rho(t) = 1$. The density of the infected individual of Ω individuals M is $v(t)$. When the time t approaches infinity, the steady densities of the infected individuals H and M is ρ and v. Ignore the correlation of the degree between different individuals H, the reaction equations of $\rho(t)'$ and $v(t)$ obtained with the dynamic mean field method are given by equation (9).

$$\begin{cases} \partial_t s(t)' = \rho_T(t) - \lambda\langle k\rangle s(t)'\rho(t)' - \gamma_2 s(t)'\vartheta(t) \\ \partial_r \rho_0(t)' = -\rho_0(t) + \lambda\langle k\rangle s(t)'\rho(t)' + \gamma_2 s(t)'\vartheta(t) \\ \qquad\qquad\vdots \\ \partial_t \rho_T(t)' = -\rho_T(t) + \rho_{T-1}(t) \\ \partial_t \vartheta(t) = -\vartheta(t) + \gamma_1\left[1 - \vartheta(t)\right]\vartheta(t) \end{cases} \tag{9}$$

In the first equation, the first item on the right side considers the density of the infected individual H which return to the susceptible state at the unit speed after propagation delay T, the second item considers the average density of the new infected individual at t time which is directly proportional to the effective propagation rate λ, the degree of nodes, and the probability of contact with healthy individuals $s(t)'$, and the last item considers the average density of the infected state from the susceptible state caused by bite by the individual M with virus, healthy individual H, and infection probability γ_2. The second to $T + 2$ equations represent the conversion relationship of the infection densities $\rho_T(t)$ and $\rho_{T-1}(t)$of the individual H. In the last equation, he first item on the right side considers the death of the infected individual M at the unit speed, the second item considers the average density of the infected state from the susceptible state caused by the diseased individual H, the individual M, and infection probability γ_1. In the infection vector, the infection density $\vartheta(t)$ of the individual M is closely related with the steady infection density ρ of the individual H. $\vartheta(t)$ monotonically increases with the increasing of ρ. For the steady infection density ρ of the individual H, the propagation critical value of the uniform network is given by equation (10).

$$\lambda_e = \left(1/(t+1) - \gamma_1\gamma_2/\langle k\rangle\right) \tag{10}$$

From equation (10), in the proposed model, the propagation critical value λ_e is the function of T, γ_1, and γ_2, which is different from the SIS model. Compared with the cases of only considering the influence of propagation delay and infection vector, which are the conditions pf $\lambda_e = 1/((T + 1)\ \langle k \rangle)$ and $\lambda_e = 1/(\gamma_1\gamma_2)/\langle k \rangle$. Both of them significantly reduce the propagation critical value of the uniform network and thus increase the risk of the singularity virus outbreak. In the above equation, if let $T = \gamma_1 = \gamma_2 = 0$, $\lambda_e = 1/\langle k \rangle$ is obtained. Therefore, in the case of not considering the influence of propagation delay and infection vector, the propagation critical value will be too large, which obviously affect the defence of the virus propagation.

3.2 Propagation behaviour of the proposed SIS model in the scale-free network

In the scale-free network, the degree of each node is different, that is, the number of arbitrary individual *H* connected with others *H** is not equal. Therefore, in the discussion of the propagation characteristics of the proposed model in the scale-free network, the assumption of uniformity of the network must be dropped. Consider the steady value of the relative density $\rho_h(t)$ of the infected individual *H* with degree *k* is ρ_h, the propagation of the virus between the individual *H* and *M*′ is uniform and decided by the infection probability γ_1 and γ_2. The dynamic mean field reaction equations of the propagation behaviour of the proposed SIS model are given by equation (11).

$$\begin{cases} \partial_t \rho_h(t) = -\rho_{h,T}(t) + \lambda k\left[1-\rho_h(t)\right]\theta\left(\rho(t)'\right)\theta(t) + \gamma_2\left[1-\rho_h(t)\right] \\ \partial_t \theta(t) = -\theta(t) + \gamma_1\left[1-\theta(t)\right]\theta\left(\rho(t)'\right) \end{cases} \tag{11}$$

where $\rho_{h,T}(t)$ is the relative density of the infected individual *H* with degree *k* at time $t - T$. $\theta(\rho(t)')$ is the probability of arbitrary given edge connected to an infected individual *H* and the steady value is θ. The non-uniformity of the scale-free network must be considered in the computation of $\theta(\rho(t)')$.

$$\theta\left(\rho(t)'\right) = \sum_k \frac{\partial_t \rho_h(t) P(k) \rho_h}{\sum_o \vartheta P(s')} \tag{12}$$

Here, 1 is the degree distribution function of the individual 2 in the scale-free network, and the average density of all infected individuals 3 in the scale-free network can be expressed as equation (13).

$$\rho(t)' = P(k)\rho_h \tag{13}$$

According to the steady conditions $\partial_t \rho_h(t) = 0$ and $\partial_t \theta(t) = 0$, equation (14) is obtained.

$$\begin{cases} -\rho_{h,T} + \lambda k\left(1-\rho_h\right)\theta + \gamma_2\left(1-\rho(t)'\right)\vartheta = 0 \\ -\vartheta + \gamma_1\left(1-\vartheta\right)\vartheta = 0 \end{cases} \tag{14}$$

From the above equations, when the system described in equation (11) is in the steady state, the relative density ρ_h of the infected individual *H* is the function of *T*, γ_1, and γ_2. Then ϑ is the implicit function of *T*, γ_1, γ_2 and *T*. The propagation critical value of the scale-free network is given by equation (15).

$$\lambda_e' = \left[\left(1-\gamma_1\gamma_2\right)\langle k \rangle\right] \big/ \left[(T+1)\langle k^2 \rangle\right] \tag{15}$$

where $\langle k^2 \rangle = \sum_k k^2 P(k)$. When $T = \gamma_1 = \gamma_2 = 0$, $\lambda_e = \langle k \rangle / \langle k^2 \rangle$ is obtained in the condition of not considering the influence of propagation delay and infection vector. Both of them significantly reduce the propagation critical value.

3.3 Cellular automata SIS propagation model with consideration of propagation delay

The complex sensor network can be denoted by the form of $G = (N, E)$, where N' is the set of all of nodes in the network and E' is the set of edges between all nodes. Each edge in E' is corresponding to a pair of nodes in N' and the corresponding relationship is contained in the adjacency matrix of the network A. Each node in the network is considered as a cell, and then the network with N' nodes is considered as cellular automata with N' cells. The N' cells construct a one dimensional cell space C. In the proposed SIS model, the states of the cell c include the susceptible state and the infected state and denoted by 0 and 1. Then the state set $Q = \{0, 1\}$ is obtained. Assume $Z_e(t)(Z_e(t \in Q))$ denotes the state variable of the cell c at the time t, then equation (16) is obtained.

$$Z_{e,t} = \begin{cases} 0, & (c \text{ is susceptible at time } t) \\ 1, & (c \text{ is infected at time } t) \end{cases} \tag{16}$$

As the adjacency matrix A can reflect the topology information of network, A denotes the relationship among the cell neighbours in the cellular space. The neighbour V_e of the cell c is the set of all of elements with the value 1 in the row c', that is, $V_e = \{j | a_{cj} \in A, a_{cj} = 1\}$ $(c, j = 1, 2, \ldots, N)$, where a_{cj} 1 is the edge of the cells of c and j and $a_{cc} = a_{jj} = 0$. In the SIS model, any cell in the cellular space is only infected by its neighbours. In the SIS propagation model proposed in this paper, any healthy cell in the cell space may only be infected by its neighbour nodes. Similar to the classic SIS model, cell t that is in an infected state at time c will infect its healthy neighbour cells with probability. The difference from the classic SIS model is that after the propagation delay T, the infected cell c will return to health at the $t + 1 + T^{\text{th}}$ hour. From this, it can be seen that the state $Z_{c,t}$ of the cell c at time t depends not only on the state $Z_{c,t-1-T}$ of the cell itself at the $t - 1 - T$ time, but also on the state $Z_{V_c,t-1}$ of its neighbour at the $t - 1$ time. Based on this, the evolution rules for cell state $Z_{c,t}$ are given by equation (17).

$$\begin{cases} Z_{c,t-j} = Z_{c,t-j-1} + Z_{c,t-j-1} f(r_\lambda), & \text{if } 1 \le j \le T \\ Z_{c,t-j} = \overline{Z_{c,t-j}} \left(Z_{c,t-1} + \overline{Z_{c,t-1}} f(r_{gl}) \right), & \text{if } j = T + 1 \end{cases} \tag{17}$$

Here, $\overline{(\cdot)}$ represents a negation operation, and r_λ is a random number satisfying a uniform distribution between 0 and 1. $f(x)$ is defined in equation (18).

$$f(x) = \begin{cases} 0, & \text{if } x \ge 1 - (1-\lambda)^{m_{c,n}} \\ 1, & \text{if } x < 1 - (1-\lambda)^{m_{c,n}} \end{cases} \tag{18}$$

The formula above shows the result of a contact between a healthy cell c and an infected cell at time t and results in a state transition after a time step: when $r_\lambda < 1 - (1-\lambda)^{m_{c,n}}$ o'clock, cell c is infected, and when $r_\lambda \ge 1 - (1-\lambda)^{m_{c,n}}$ o'clock, cell c maintains its original health state, where $m_{c,t}$ is the number of infected states in the neighbourhood of Cell c at the t^{th} time, and its expression is defined by equation (19).

$$m_{c,t} = \sum_{j=1}^{N} a_{cj} Z_{j,t} \tag{19}$$

The first fraction in the formula indicates that within the propagation delay T, if the cell c has been infected, the original infection state is maintained, whereas if the cell c is in the susceptible state, it will be infected with a probability of $1-(1-\lambda)^{m_{c,t}}$. The second fraction shows that if cell c is infected at $t - 1 - T$, it will be cured after T discrete times. On the other hand, if the cell c is in an easy-to-stain state at the $t - 1 - T^{\text{th}}$ instant, it is infected at the t^{th} instant or with a probability of $1-(1-\lambda)^{m_{c,t}}$, or maintains its infection state. Agreement $\mathrm{y}_{\wp}$ is the level of network virus infection at steady state. The statistical result is defined by equation (20).

$$y_{\wp} = \frac{1}{N} \sum_{c=1}^{M'} Z_{c,\wp} \tag{20}$$

The number of convention system implementations is M', $\mathrm{y}_{\wp,j}$ is the level of virus infection at the third implementation. When the virus broke out at the j^{th} time when it was implemented at $\mathrm{y}_{\wp,j} > 0$ o'clock. If the number of virus outbreaks in the M'^{th} system implementations is M_1', then the virus outbreak rate R is defined as equation (21).

$$R = M_1'/M \tag{21}$$

Among them, the expression of the density of infected nodes in the network at time t is y_t, which is defined by equation (22).

$$y_t = \frac{1}{N} \sum_{c=1}^{N} Z_{c,t} \tag{22}$$

In summary, based on analysis of virus propagation behaviour under uniform network and scale-free network, cellular automaton SIS propagation model is constructed. Experimental results show that our model can effectively count characteristics virus of propagation in the network, calculate the probabilistic characteristics of virus propagation and detect strange characteristic virus according to probability characteristics and propagation characteristics of virus.

4 Singularity virus detection based on immunisation and DS evidence theory

The in-depth analysis of the computer virus characteristic immune system under the complex network and proposes an antigen presentation strategy. The obtained program features a binary string of a specific length. Based on the information of the abstraction layer output by the computer virus singularity characteristic virus detection model based on the immune principle, a fusion method for virus detection is proposed. By merging the detection results of different antigen presentation gene banks, the ability to detect computer-based singularity virus detection models based on the principle of immunity can be improved.

Computer singularity virus in the complex sensor network is detected with the immunisation principle. Antigen presentation of the biological immunisation system is simulated, which is to obtain the antigen feature. The antigen is defined as a program in a computer system. Feature extraction of program is carried out by an antigen presenting gene library with specific length to obtain the feature of antigen (program) which is antigenic determinant, that is program eigenvector. The feature set of computer program F is defined by equation (23).

$$F = \left\{ \langle x_1, \ldots, x_n \rangle \middle| x_i \in (0, 1) \right\}, \quad p \in P, x_i = f_c\left(p, agl, l\right) \tag{23}$$

where x_i is the feature information of program $p \in P$ from the gene agl in the antigen presenting gene library, n is the dimension of eigenvector of singularity virus which is the same as the antigen presenting gene library, l is the size of gene fragments in agl, the function $f_c(p, agl, l)$ is the operation of feature extraction, and the function $f_c(p, j, l)$ is the antigen presenting gene with length l exacted from the program. The procedural information of the program is obtained based on whether or not the antigen presenting genes of length l extracted from the program $p \in P$ appear in the corresponding antigen-presenting gene bank. Function $f_c(p, j, l)$ is to extract a length of l antigen presenting genes from the program. The feature extraction of the program was performed using the selected antigen presentation gene bank (n' genes in the simulated biological immune system were used for feature extraction) to obtain the n''dimensional feature information of the program, thereby constituting a program feature vector.

$$f_c(p, agl, l) = \begin{cases} 1 & \text{if} \quad f_c(p, j, l) \in agl \\ 0 & \text{if} \quad f_c(p, j, l) \notin agl \end{cases} \tag{24}$$

The process of antigen presentation is to extract a length l antigen-presenting gene string from the program $p \in P$ of the features to be extracted. It was obtained by calculating whether the extracted antigen-presenting gene string appeared in the antigen-presenting gene bank agl, which appeared as 1 and did not appear as 0. Each dimension value x_i in program state vector $(x_1, \ldots, x_{n'})$ of program $x_i(x_i \in \{0, 1\})$ is available. After antigen presentation, the program obtained is characterised by a binary string of length of the gene bank. Define a self-contained normal program file that is free of viruses in computer systems under complex networks. Define non-self as a virus program in a computer system, or a program file that is infected with a virus. Combining the antigen presentation algorithm given above, the self-collection Q and the non-self collection N' is defined by equation (25).

$$\begin{cases} Q = \left\{ a \middle| a \in F, b \subset B, |a| = k, a = APC(b) \right\} \\ N' = \left\{ a \middle| a \in F, v \subset V, |a| = k, a = APC(v) \right\} \end{cases} \tag{25}$$

In equation (25), k is the size of the selected antigen presentation gene bank, B is the collection of normal programs, V is the collection of virus programs, and APC is the presentation of antigens, i.e., program state vectors extracted from the program. The feature information extracted from the normal program reflects the characteristics of the normal program, thus establishing a normal system state model of the system. The normal procedural state model was used to generate detectors to cover the virus program space. To efficiently generate detectors, the concept of a gene bank was introduced. The detector gene bank is defined as equation (26).

$$G = \left\{ x \middle| x \in \{0,1\}^m, \quad m \le k, m \in \dot{M}, k \in \dot{N} \right\} \tag{26}$$

In equation (26), $\dot{N}$ is a natural number, *k* is the size of the selected antigen presentation gene bank. That is, *G* is a set of binary strings whose length is smaller than that of the self. The detector gene bank is mainly used to generate immature detectors more efficiently. Corresponding to the biological rabbit disease system, the detector set *D* is defined as equation (27).

$$D = \left\{ \langle d_1, d_2, \ldots, dn \rangle \middle| d_i \in \{0,1\} \right\} \tag{27}$$

The detector is further divided into immature detector set *I* and mature detector set *M*. Immature detector *I* refers to a detector that has not yet passed autotolerance. Its generation methods mainly include:

1 Recombination or mutation generation of gene fragments in the detector gene library *G*.

2 Randomly generate a binary string of length k to generate. The maturation detector $\dot{M}$ refers to a self-tolerant detector, and the auto tolerance process is shown in equation (10).

$$I = \left\{ x \middle| x \in D \right\} \tag{28}$$

$$M = \left\{ x \middle| x \in D, \forall s \in S'', d_d(s, x) \ne 1 \right\} \tag{29}$$

$$f_d(s, x) = \begin{cases} 1 & f_r(x, y) \ge \beta \\ 0 & \text{otherwise} \end{cases} \tag{30}$$

The detector is generated as follows: An immature detector $d \in I$ is generated. If the immature detector *d* self-tolerates successfully (i.e., it is less than β with *r* consecutive bit distances from any element in the normal program state vector set *s*, the resulting detector *d* is not in the normal program space). Then the immature detector *d* becomes a legitimate mature detector, which is added to the mature detector set.

Mature detectors with self-tolerance have been used to detect computer strange properties of viruses. The feature vector of the program is obtained after the antigen is presented. Then calculate the distance between the program feature vector and the maturity detector. If *r* consecutive bit match is greater than the set threshold then it indicates that the program is a virus program, otherwise it is a normal program.

The advantages and disadvantages of different nodes in a complex network are different, and the relationships and interactions between complex network nodes are characterised by weights. The size and distribution of weights will have an important impact on the nature and function of the network. Since the weighted network can better portray the details of interactions between nodes in the network, the weighted network model is closer to the real complex network. Weights and their distribution will have an important impact on the spread of viruses in complex networks. The SIS propagation model is used to study complex networks. The virus's weird characteristic of an early outbreak of virus transmission. The weights between the edges of the nodes are considered to be the tightness of the connections between the nodes. The difference in intimacy will affect the difference in virus propagation speed between nodes. The speed at which a single signature virus spreads is defined as the rate of change of an infected.

$$v(t)' = \frac{dist(t)}{d(t)} \approx \frac{I(t) - I(t-1)}{\dddot{N}} \tag{31}$$

Among them: I is the number of strange characteristic virus infections in complex networks. $\dddot{N}$ represents the number of nodes in the entire complex network. Assuming that the weight of the edges between nodes i'' and j'' is $w_{i''j''}$, then the virus infection probability $\lambda_{i''j''}$ between them is defined as equation (32).

$$\lambda_{i''j''} = \left(\frac{w_{i''j''}}{w_{\dddot{M}}} \right)^{\alpha} \tag{32}$$

In equation (32), V' represents the maximum value of edge weight in the network. α is an adjustable parameter.

Vaccinations are given to nodes in the network, which not only can prevent the vaccinated nodes infected with the virus, and can prevent infection by the node to others. So nodes to be vaccinated can be seen as removed from the complex sensor network. The best singularity virus control strategy is to prevent the spreading virus in the condition of the immunisation network with the least nodes. Use the shortest path of the complex sensor network and the connectivity of the network to define the antivirus capability of the network, called as connectivity coefficient C'', given by equation (33)

$$C' = \frac{1}{n''} \sum_{i''=1}^{V'} \sum_{j''=1}^{V'} \frac{1}{d_{i''j''}} \tag{33}$$

where $n'' = \frac{1}{2} V'(V'-1)$ denotes the probable maximum connecting edge in the complex sensor network, $d_{i''j''}$ is the shortest path from the node i'' to the node j''. If there is no path between the node i'' and the node j'', then $d_{i''j''}$ is considered as infinity. Connectivity coefficient C'' reflects the connectivity of the network. When the complex sensor network is fully connected network, $C'' = 1$ and the connectivity of the network is strongest. From any node, the virus can infect the entire network only through one step propagation. When all the nodes in the network are isolated nodes, there is no path between any two nodes, $C'' = 0$ and any node infected with the virus will not spread to other nodes, the connectivity is worst. It can be considered that the network has a strong antivirus ability. In other cases, $0 < C'' < 1$. Let $C'_{i\dddot{m}}$ denotes the connectivity value of the network without immunisation implementation, C'_{im} denotes the connectivity value of the network after immunisation implementation, and $\dddot{m}$ denotes the ratio of the connectivity coefficient after immunisation, that is, $\dddot{m} = C'_{i\dddot{m}} / C_0$. Obviously, $\dddot{m} < 1$, the smaller of m represents the strongest connectivity of network with the immunisation strategy and the better immunisation effect.

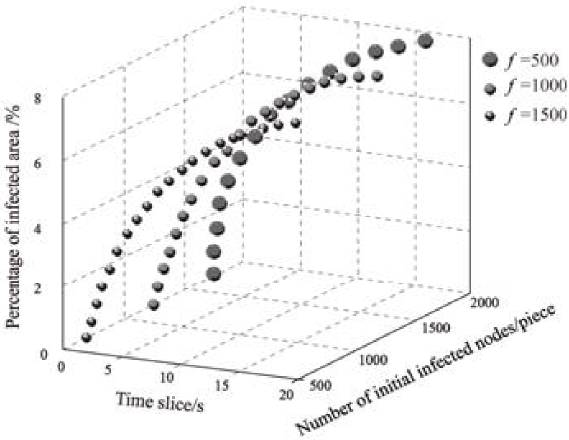
5 Experimental results and analysis

Using OPNET Modeler simulation software to simulate complex networks, Windows XP operating system, CPU frequency is dual-core 4.0GHz, 4GB of memory. After writing the relevant functions and setting the parameters, we will change the different experimental conditions to analyse the defensive effects of the defence methods proposed in this paper. This section will address the defences proposed in this paper from the impact of the size of the complex network, the impact of the virus infection ability of the unique characteristics, the impact of the initial infection rate, the change in the number of infected nodes, and the change in the ratio of connectivity factors with the immune rate. The method is tested and the defence method proposed in this paper is evaluated in full according to the results of the analysis. In addition, because the parameters of each experiment are different, the time represented by the time slices in each experiment is also different.

5.1 Impact of the scale size of the complex sensor network

The overall defence effect of the proposed defence methods may vary with the scale size of the complex sensor network. In the experiment, the initial infection node number is set to 5% of the whole complex sensor network size *f*, and the infection capability of the singularity virus is set to 3. The network size is set to 500, 1,000, and 1,500. The size of the infection area is observed and recorded. Experimental result is shown as Figure 1.

Figure 1 Impact of the scale size of the complex sensor network

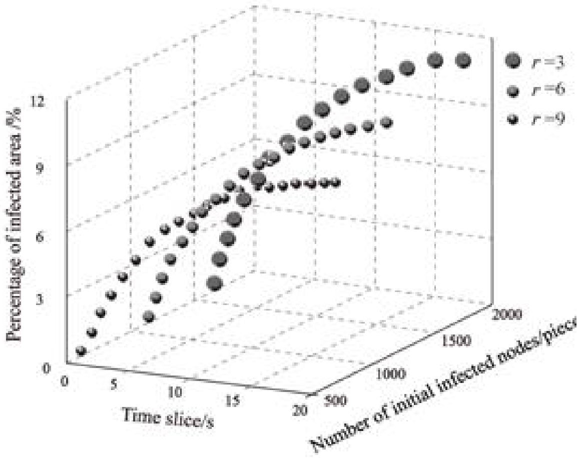


Through the impact of complex sensor network size on the defensive effect of singularity virus, it is found that, although the size of complex sensor network is different, the size of infection area is basically controlled within 8%. For different complex sensor network size, the defence effect of the proposed defence method doesn’t make much difference. It is important to point out that in the realistic complex sensor network, the infection ability of the complex sensor network is not large as the experiment, so the size of the infected area will not so large as the experiment shows.

5.2 Impact of the infection ability of the singularity virus

The infection ability *r* of the singularity virus may also directly affect the defence effect of the pro-posed method. In the experiment, the network size is set to 8,000 and the initial infection node number is set to 5% of the network size, that is, 400. The infection ability *r* of the singularity virus is set to 3, 6, and 9, respectively. The *K* value of the infection area is observed and recorded. Experimental result is shown as Figure 2.

Figure 2 Impact of the infection ability of the singularity virus

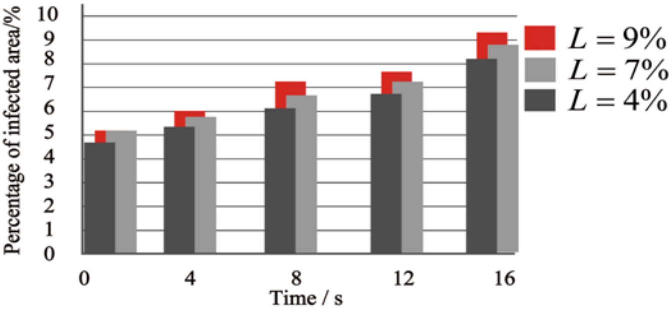


From the experimental results obtained with the set parameters, it can be seen that the size of the infection area is controlled below 12%. However, the singularity virus infection ability in the real network could not reach 6, less likely 9. This experiment is set to so high value only for the test of the defence capability of the proposed method in the high singularity virus infection. In the realistic complex sensor network, we can set some conditions to limit the infection ability of the singularity virus, while early warning information remains unchanged. In this case, the defence effect of the proposed method will be better.

5.3 Impact of the initial infection node ratio

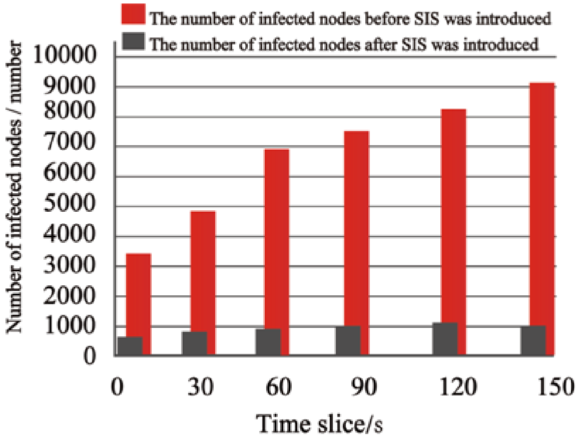
The number of nodes infected by the singularity virus in the initial stage of defence may affect the defence effect of the proposed defence method. In the experiment, the network size is set to 3,500 and the infection ability *r* of the singularity virus is set to 6, that is, infecting six neighbour nodes in a time section. The initial infection node ratio is set to 4%, 7%, and 9%, that is the number of the initial infected nodes is 140, 245, and 315. The *K* value of the infection area is observed and recorded. Experimental result is shown as Figure 3.

Figure 3 Impact of the initial infection node ratio (see online version for colours)



From the experimental results obtained with the set parameters, it can be seen that when the initial infection node ratio is 7%, the size of the infection area is only about 9%, but for the experiment, it is within acceptable value. In view of the limitation of this experiment, if the immunisation node density is adjusted, the target immunisation of complex sensor network can effectively suppress the propagation of the singularity virus and the defence effect is more ideal.

Figure 4 Variations of the number of infected nodes before and after the introduction of SIS model (see online version for colours)



In the complex sensor network, if there is no effective defence strategy, the singularity virus will make full use of the structure of the complex sensor network to quickly spread, and the number of infected nodes in the network will be more and more, finally lead to the whole network infection by singularity virus completely. However, after the introduction of SIS model, if the warning information can spread to other network nodes faster than the singularity virus attack (also understood as the propagation speed), then the singularity virus propagation in the complex sensor network will be suppressed to a certain limit and the case of large-scale singularity virus breakout is not appeared.

5.4 Variations of connectivity coefficient proportion with immunisation rate

Table 1 is the simulation results of defence with three kinds of immunisation methods of stochastic immunisation, acquaintance immunisation and node strength target immunisation in this paper. The immunisation rate is the ratio of the number of immunised nodes to the total number of nodes in the network. The connectivity coefficient is the ratio of the connectivity coefficient after and before immunisation. The unit is constant. Table 1 shows that target immunisation is better than the nearest neighbour immunisation and the nearest neighbour immunisation is better than random immunisation.

Table 1 Variations of connectivity coefficient proportion with immunisation rate

Immunisation rate /%	*Random immunisation*	*Nearest neighbour immunisation*	*Target immunisation*
2	0.78	0.68	0.45
4	0.69	0.57	0.35
6	0.57	0.45	0.26
8	0.43	0.37	0.18
10	0.37	0.18	0.09

As shown in Table 1, after 8% of nodes in the network are immunised, network connectivity factor ratio of our proposed method is only 0.18, lower than 0.37 multiples of nearest neighbour and 0.43 multiples of random immunisation. We can draw a conclusion that the target immunity using node intensity is more effective in breaking down the connectivity of the virus transmission network and blocking the virus transmission. Therefore, target immunity density based on node strength is the lowest.

6 Conclusions

In recent years, researches on the complex sensor network theory have attracted the attention of many researchers. The related researches show that the topology of the complex sensor network will affect the dynamic behaviour of the network to a great extent. As the deep researches on the propagation dynamics of the complex sensor network, it is found that the propagation behaviour of the virus will be affected by some specific factors, such as infection vector, propagation delay, and so on. In this paper, the influence of the above factors on the propagation dynamics of the complex sensor network and the related immunisation strategies are researched. The main works are as follows.

1 The basic concepts of infectious factors of infection vector and propagation delay are introduced. The research status of these factors affecting the process of viral propagation and some related immunisation strategies are summarised. Three classical virus propagation model of SIS, SIR, and SI are described, and the propagation dynamics of viruses on the uniform network and the scale-free network are discussed respectively on the basis of SIS model.

2 The propagation process of the virus is affected by the interaction between infection vector and propagation delay. The variation of the virus propagation characteristics is researched based on mean field theory in the case of coexistence of the two factors. It is found that coexistence of the two factors significantly accelerates the propagation of viruses in the complex sensor network and increases the number of infected nodes in the network. This explains the complexity of the dynamics behaviour of the virus propagation.

As the shortage of mean field theory in this research, in order to make the research more perfect, with the help of cellular automata to research the influence of propagation delay on the propagation behaviour of the singularity virus, a new cellular automata model is proposed in this paper. In the simulation research, the propagation delay is considered as the constant and related to the degree of node. It is found that propagation delay significantly enhances the infection intensity of the singularity virus, while reduces the critical propagation value. As the increase of propagation delay, the propagation rate and the explosion rate of the singularity virus will increase significantly. These results have important practical significance for further understanding the propagation behaviour of the singularity virus in the real network, and also provide some useful reference for the effective virus prevention and control.

References

Bien, K., Sobańska, Z. and Sokołowska, J. (2016) 'A lack of Fas/FasL signalling leads to disturbances in the antiviral response during ectromelia virus infection', *Archives of Virology*, Vol. 161, No. 4, pp.913–928.

Cao, Y. and Ma, J. (2017) 'Research on mobile ad hoc network virus propagation model based on differential equation', *Computer Engineering*, Vol. 43, No. 1, pp.172–177.

Casteel, C.L., De, A.M. and Bak, A. (2015) 'Disruption of ethylene responses by turnip mosaic virus mediates suppression of plant defense against the green peach aphid vector', *Plant Physiology*, Vol. 169, No. 1, pp.209–218.

D'Alba, L. and Shawkey, M.D. (2015) 'Mechanisms of antimicrobial defense in avian eggs', *Journal of Ornithology*, Vol. 156, No. 1, pp.1–10.

Fan, Y., Wang, X. and Li, G. (2016) 'Experimental demonstration of a tunable load-limited magnetically insulated transmission line oscillator', *IEEE Transactions on Electron Devices*, Vol. 63, No. 3, pp.1307–1311.

Hanawal, M., Abdelrahman, M. and Krunz, M. (2016) 'Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems', *IEEE Transactions on Mobile Computing*, Vol. 15, No. 9, pp.2247–2259.

Hermance, M.E. and Thangamani, S. (2015) 'Tick saliva enhances powassan virus transmission to the host, influencing its dissemination and the course of disease', *Journal of Virology*, Vol. 89, No. 15, pp.7852–7860.

Jia, B., Liu, S. and Yang, Y. (2014) 'Fractal cross-layer service with integration and interaction in internet of things', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 3, p.760248.

Liu, S., Fu, W. and Deng, H. (2013a) 'Distributional fractal creating algorithm in parallel environment', *International Journal of Distributed Sensor Networks*, Vol. 9, No. 9, p.281707.

Liu, S., Fu, W. and Zhao, W. (2013b) 'A novel fusion method by static and moving facial capture', *Mathematical Problems in Engineering*, No. 5, 497–504.

Liu, Y., LI, Q. and Wang, X. (2016) 'Improved PSO for network defense measures of weighted attack graph', *Computer Engineering and Applications*, Vol. 52, No. 8, pp.120–124.

Musso, D. (2015) 'Zika virus transmission from French Polynesia to Brazil', *Emerging Infectious Diseases*, Vol. 21, No. 10, pp.1887–1887.

Neto, L.P.S., Rossi, J.O. and Barroso, J.J. (2016) 'High-power rf generation from nonlinear transmission lines with barium titanate ceramic capacitors', *IEEE Transactions on Plasma Science*, Vol. 44, No. 12, pp.3424–3431.

Oliveira, V.C.D., Morgado, F.D.S. and Resende, RO. (2015) 'The silencing suppressor (NSs) protein of the plant virus Tomato spotted wilt virus enhances heterologous protein expression and baculovirus pathogenicity in cells and lepidopteran insects', *Archives of Virology*, Vol. 160, No. 11, pp.2873–2879.

Pan, Z., Liu, S. and Fu, W. (2017) 'A review of visual moving target tracking', *Multimedia Tools and Applications*, Vol. 76, No. 16, pp.16989–17018.

Pythoud, C., Rothenberger, S. and Martínezsobrido, L. (2015) 'Lymphocytic choriomeningitis virus differentially affects the virus-induced type i interferon response and mitochondrial apoptosis mediated by RIG-I MAVS', *Journal of Virology*, Vol. 89, No. 12, pp.6240–50.

Varanda, C.M.R, Santos, S. and Clara, M.I.E. (2015) 'Olive mild mosaic virus, transmission by Olpidium virulentus', *European Journal of Plant Pathology*, Vol. 142, No. 1, pp.1–5.

Wong, G., Qiu, X. and Richardson, J.S. (2015) 'Ebola virus transmission in guinea pigs', *Journal of Virology*, Vol. 89, No. 2, pp.1314–1323.

Wu, Z., Sinzger, C. and Reichel, J.J. (2015) 'Natural killer cells can inhibit the transmission of human cytomegalovirus in cell culture by using mechanisms from innate and adaptive immune responses', *Journal of Virology*, Vol. 89, No. 5, pp.2906–2917.

Yang, L.X. and Yang, X. (2015) 'The impact of nonlinear infection rate on the spread of computer virus', *Nonlinear Dynamics*, Vol. 82, Nos. 1–2, pp.85–95.