PLOS ONE

RESEARCH ARTICLE

A tradeoff between the losses caused by computer viruses and the risk of the manpower shortage

Jichao Bi[1], Lu-Xing Yang[2], Xiaofan Yang[1]*, Yingbo Wu[1], Yuan Yan Tang[3]

1 School of Software Engineering, Chongqing University, Chongqing, 400044, China, **2** Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, GA 2600, The Netherlands, **3** Department of Computer and Infomation Science, The University of Macau, Macau

* xfyang1964@gmail.com

Citation: Bi J, Yang L-X, Yang X, Wu Y, Tang YY (2018) A tradeoff between the losses caused by computer viruses and the risk of the manpower shortage. PLoS ONE 13(1): e0191101. https://doi.org/10.1371/journal.pone.0191101

Editor: Hua Wang, Victoria University, AUSTRALIA

Received: May 28, 2017

Accepted: October 14, 2017

Published: January 25, 2018

Data Availability Statement: All relevant data are within the paper.

Funding: This research is supported by the following funds: National Natural Science Foundation of China (Grant No. 61572006 to Xiaofan Yang), http://www.nsfc.gov.cn/; National Natural Science Foundation of China (Grant No. 71301177 to Yingbo Wu), http://www.nsfc.gov.cn/; National Sci-Tech Support Plan (Grant No. 2015BAF05B03 to Yingbo Wu), http://www.most.gov.cn/; Basic and Advanced Research Program of Chongqing (Grant No. cstc2013jcyjA1658 to Yingbo Wu), http://www.cstc.gov.cn/; and

Abstract

This article addresses the tradeoff between the losses caused by a new virus and the size of the team for developing an antivirus against the virus. First, an individual-level virus spreading model is proposed to capture the spreading process of the virus before the appearance of its natural enemy. On this basis, the tradeoff problem is modeled as a discrete optimization problem. Next, the influences of different factors, including the infection force, the infection function, the available manpower, the alarm threshold, the antivirus development effort and the network topology, on the optimal team size are examined through computer simulations. This work takes the first step toward the tradeoff problem, and the findings are instructive to the decision makers of network security companies.

1 Introduction

Computer networks and online social networks provide us with a fast channel of acquiring information and communicating ideas. Meanwhile, computer viruses can also spread rapidly through these networks, inflicting enormous economic losses [1]. For the loss estimation, see Refs. [2–6]. When a new computer virus emerges, there is often no ready-made antivirus that is capable of detecting and eliminating it. As a result, before an antivirus targeting the virus is released, the virus is able to spread itself freely through networks, infecting a significant fraction of the hosts.

Consider a network security company that is dedicated to developing antiviruses. Suppose that when the fraction of the victims of a new virus exceeds a presupposed alarm threshold, the company will initiate a project of developing an antivirus against the virus. First, the amount of effort needed for the project, which is typically measured by persons years or persons months, is estimated [7–10]. When the effort is determined, the company will organize a team for the project. At this point, the decision maker of the company must make a decision on the size of the team. Definitely, the losses inflicted by the virus should be minimized. For this purpose, the development cycle for the project should be minimized or, equivalently, the number of the team members should be maximized. However, if too many manpower resources are

Fundamental Research Funds for the Central Universities (Grant No. 106112014CDJZR008823 to Yingbo Wu), http://www.cqu.edu.cn/v1/. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing interests: The authors have declared that no competing interests exist.

injected into the project, the company will take the risk of having no enough manpower to undertake other projects. Therefore, a deliberate tradeoff must be made between the two conflicting demands of reducing the losses caused by the virus and reducing the team size. In our opinion, the tradeoff problem is worthy of deep-going study. To our knowledge, to date this problem has not been addressed mathematically.

The key to solving the tradeoff problem is to accurately estimate the speed and extent of virus infections. Computer virus spreading dynamics as an emerging interdiscipline is devoted to gaining insight into the consequence of computer viruses through modeling and analyzing their spreading process. Since the seminal work by Kephart and White [11, 12], large numbers of computer virus spreading models, ranging from the population-level spreading models [13–17] and the network-level spreading models [18–22] to the individual-level spreading models [23–30], have been proposed. In particular, a special type of spreading models known as the Susceptible-Infected (SI) models [31, 32] are especially suited to capturing the spreading process of a new digital virus before the relevant antivirus is released.

This article addresses the above-mentioned tradeoff problem. First, an individual-level virus spreading model, which is known as the individual-level SI model, is proposed to capture the spreading process of the virus before the appearance of its natural enemy, which is then utilized to assess the expected losses caused by the virus during the development period of an antivirus aiming at the virus. Then, the tradeoff problem is modeled as a discrete optimization problem. On this basis, the influences of different factors, including the infection force, the infection function, the available manpower, the alarm threshold, the antivirus development effort and the network topology, on the optimal team size are examined through computer simulations. This work takes the first step toward the tradeoff problem, and the findings are instructive to the decision makers of network security companies.

The subsequent materials of this work are organized as follows. Section 2 presents the individual-level SI model, and models the tradeoff problem. Section 3 experimentally examines the influences of different factors on the optimal team size. Finally, this work is summarized by Section 4.

2 The modeling of the tradeoff problem

Imagine that a network security company prepares to develop the antivirus aiming at a new computer virus. From the company's perspective, the losses inflicted by the virus should be minimized, and the manpower allocated for the development project should be minimized so that there is enough manpower to undertake other projects. Therefore, the decision maker of the company must make a tradeoff between the two conflicting demands. This section is dedicated to modeling the tradeoff problem. For this purpose, the virus spreading process must first be modeled.

2.1 The modeling of the virus spreading process

Suppose the new virus appears at time $t = 0$ and then spreads through a network $G = (V, E)$ connecting N hosts labelled $1, 2, \cdots N$. Let $\mathbf{A} = (a_{ij})_{N\times N}$ denote the adjacency matrix of the network. Before the release of the relevant antivirus, the virus is able to spread freely through the network, and every host in the network is either *susceptible* or *infected*. Let $X_i(t) = 0$ and 1 denote the event that at time t, host i is susceptible and infected, respectively. Let $S_i(t)$ and $I_i(t)$ denote the probability of host i being susceptible and infected at time t, respectively.

$$S_i(t) = \Pr\{X_i(t) = 0\}, \quad I_i(t) = \Pr\{X_i(t) = 1\}.$$

Let θ denote the presupposed alarm threshold for the virus, τ the time at which the expected fraction of the infected hosts in the network exceeds θ.

$$\tau = \inf\left\{t : \frac{1}{N}\sum_{i=1}^{N} I_i(t) \geq \theta\right\}. \tag{1}$$

At this time, the security company will initiate the development project of the antivirus against the virus. Let W denote the effort of the project, n the number of the team members assigned to the project. Then the development period for the project is $\frac{W}{n}$.

It is assumed that due to the infections by neighboring infected hosts, at time $t \in \left[0, \tau + \frac{W}{n}\right)$ susceptible host i gets infected at rate $\beta f\left(\sum_{j=1}^{N} a_{ij} I_j(t)\right)$, where the parameter $\beta > 0$ is referred to as the *infection force*, the function f is referred to as the *infection function*, which is strictly increasing and concave, $f(0) = 0, f(x) \leq x, x \geq 0$. For the rationality of the assumption, see Ref. [30]. According to the assumption, the spreading process of the virus is modeled as the following dynamical system.

$$\frac{dI_i(t)}{dt} = \beta[1 - I_i(t)]f\left(\sum_{j=1}^{N} a_{ij} I_j(t)\right), \quad 0 \leq t < \tau + \frac{W}{n}, 1 \leq i \leq N. \tag{2}$$

We refer to the model as the *individual-level SI model*.

2.2 The modeling of the tradeoff problem

Suppose the losses per unit time led by an infected host are one unit. Then the overall losses caused by the virus in the time interval $\left[\tau, \tau + \frac{W}{n}\right)$ are expected to be

$$L(n) = \sum_{i=1}^{N} \int_{\tau}^{\tau + \frac{W}{n}} I_i(t)dt. \tag{3}$$

Definitely, this expected loss should be minimized, which implies that n should be maximized. However, with the increase of n, the company will take a higher risk of having no enough manpower to undertake other projects. To reduce the risk, n should be minimized. To the extreme, it is best to assign only a single person for the project. Therefore, the decision maker of the company must make a deliberate tradeoff between the two conflicting demands. Let $\bar{n}$ be the number of currently available programmers of the company. Let us measure the tradeoff with

$$J(n) = kn + L(n) = kn + \sum_{i=1}^{N} \int_{\tau}^{\tau + \frac{W}{n}} I_i(t)dt, \tag{4}$$

where $k > 0$ stands for the relative weight of the two parts in the tradeoff; a larger k value means an emphasis on the reduction of the risk of manpower shortage, whereas a smaller k value implies that a lower loss is pursued. The tradeoff problem is then reduced to solving the following discrete optimization problem.

$$\text{Minimize}_{\ 1 \leq n \leq \bar{n}} J(n) = kn + \sum_{i=1}^{N} \int_{\tau}^{\tau + \frac{W}{n}} I_i(t)dt. \tag{5}$$

An optimal solution to the optimization problem stands for a better choice of the team size from the company's respective.

3 The determination of the factors involved in the optimization problem

The optimal team size, i.e., the optimal solution to the optimization problem (5), involves six factors: the network G, the infection force β, the infection function f, the alarm threshold θ, the antivirus development effort W, and the available manpower $\bar{n}$. Before solving the problem, these factors must be determined.

The available manpower $\bar{n}$ is at hand, the alarm threshold θ can be set flexibly by the company, the development effort can be estimated with the software cost estimation techniques given in Refs. [7–10], and the topological structure of the network G is obtainable using the network crawler described in Ref. [33].

The infection function f can be approached by applying the deep learning techniques presented in Refs. [34, 35] to the massive synthetic infection data. This is what we are going after.

The infection force β can be estimated by applying the time series analysis techniques exhibited in Ref. [36] to the successively monitored fraction of the infected hosts. See Refs. [37, 38]. This is what we will figure out.

When these factors are all determined, the optimization problem can be solved numerically.

Consider three instances of the optimization problem (5), where $k \in \{1, 3, 5\}$, $\beta = 0.001$, $f(x) = \frac{x}{1+x}$, $\theta = 0.01$, $W = 100$, $\bar{n} = 100$, and a Facebook sub-network with 2000 nodes given in Ref. [39] is taken as the virus-spreading network, denoted G_0. The team size vs. the tradeoff is shown in Fig 1. It can be seen that with the increase of the team size, the tradeoff first goes sharply down then goes slowly up, and the respective optimal team sizes are 47, 27 and 21 for $k = 1$, 3 and 5.

4 The influence of different factors on the optimal team size

The optimal team size is dependent upon six factors: the infection force β, the infection function f, the available manpower $\bar{n}$, the alarm threshold θ, the development effort W, and the network G. This section is devoted to exploring the influence of each of these factors on the optimal team size.

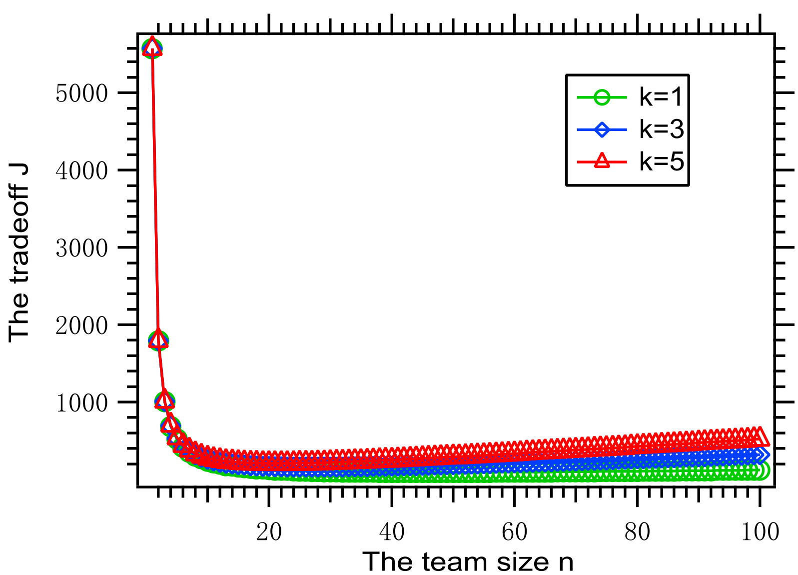

Fig 1. The team size vs. the tradeoff for the above parameters.

https://doi.org/10.1371/journal.pone.0191101.g001

In the following five experiments, $G = G_0$, the infection function $f \in \{f_i : f_i(x) = \frac{x}{1+ix}, 1 \le i \le 5\}$.

4.1 The influence of the infection force

To understand the influence of the infection force on the optimal team size, we present Fig 2, where each data point is obtained by solving the optimization problem (5) with a given set of parameters.

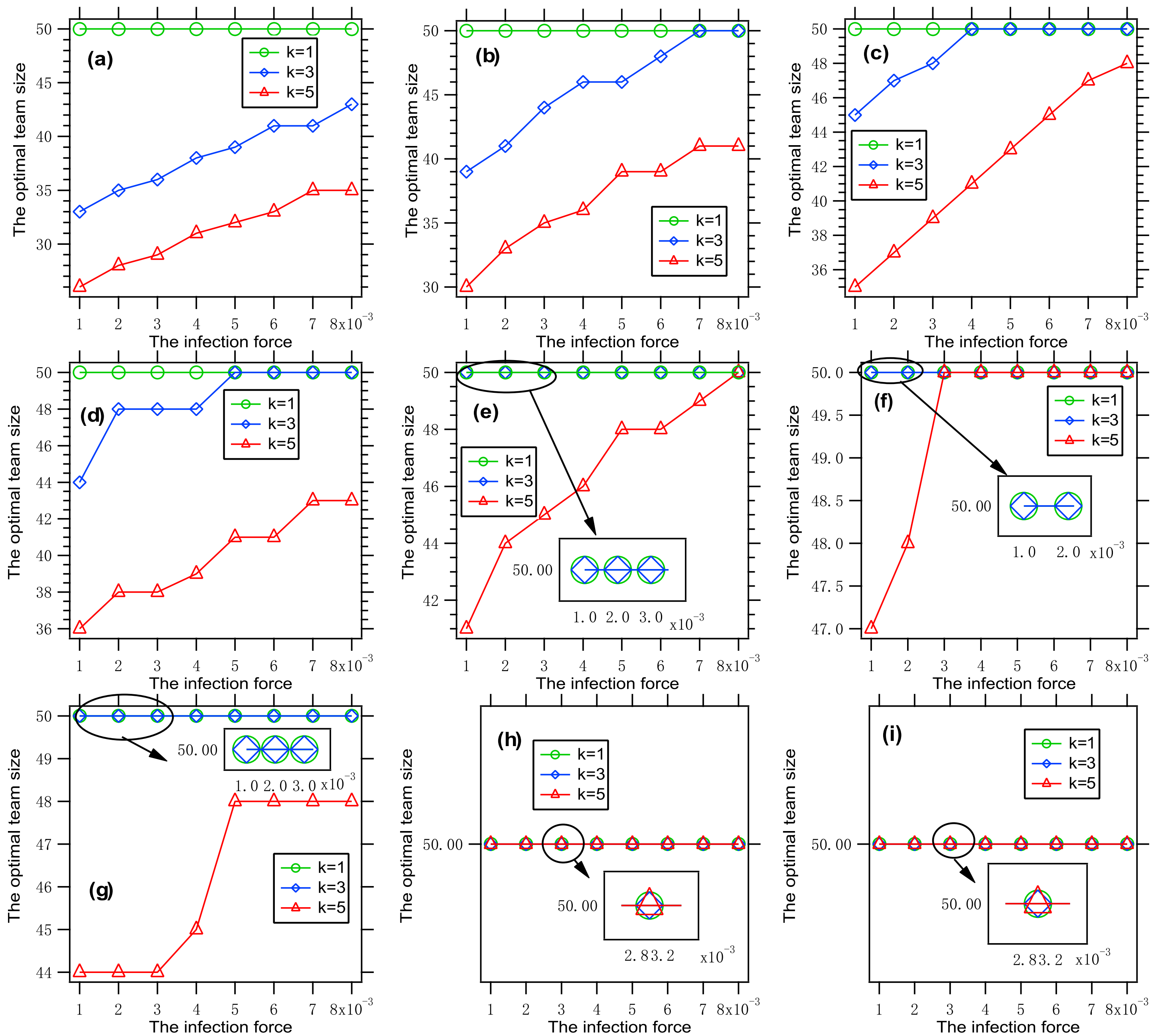

Fig 2. The optimal team size vs. the infection force. Each data point is obtained by solving the optimization problem (5) with $\beta \in \{a \cdot 10^{-3}: a = 1, \cdots, 8\}$, $k \in \{1, 3, 5\}$, $G = G_0$, $f = f_1$, $\bar{n} = 50$, (a) $\theta = 0.01$, $W = 150$; (b) $\theta = 0.01$, $W = 200$; (c) $\theta = 0.01$, $W = 250$; (d) $\theta = 0.02$, $W = 150$, (e) $\theta = 0.02$, $W = 200$; (f) $\theta = 0.02$, $W = 250$; (g) $\theta = 0.03$, $W = 150$; (h) $\theta = 0.03$, $W = 200$; (i) $\theta = 0.03$, $W = 250$. It can be seen that the optimal team size is increasing with the infection force.

https://doi.org/10.1371/journal.pone.0191101.g002

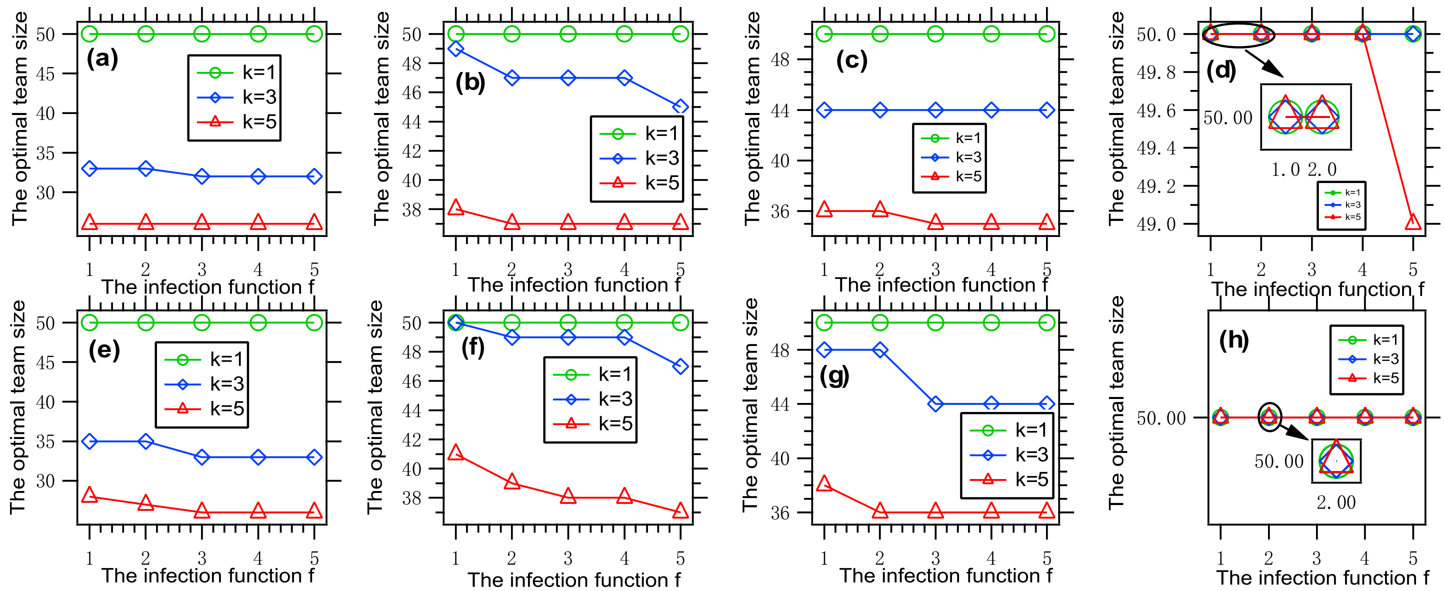

Fig 3. The optimal team size vs. the infection function. Each data point is obtained by solving an optimization problem with $f \in \{f_i: 1 \leq i \leq 5\}$, $k \in \{1, 3, 5\}$, $G = G_0$, $\bar{n} = 50$, (a) $\beta = 0.001$, $\theta = 0.01$, $W = 150$; (b) $\beta = 0.001$, $\theta = 0.01$, $W = 300$; (c) $\beta = 0.001$, $\theta = 0.02$, $W = 150$; (d) $\beta = 0.001$, $\theta = 0.02$, $W = 300$, (e) $\beta = 0.002$, $\theta = 0.01$, $W = 150$; (f) $\beta = 0.002$, $\theta = 0.01$, $W = 300$; (g) $\beta = 0.002$, $\theta = 0.02$, $W = 150$; (h) $\beta = 0.002$, $\theta = 0.02$, $W = 300$. It can be seen that the optimal team size is increasing with the infection function.

https://doi.org/10.1371/journal.pone.0191101.g003

It is concluded from the figure that the optimal team size is increasing with the infection force. This phenomenon can be explained as follows. The loss part in the tradeoff is increasing with the infection force. To better balance the two parts in the tradeoff, the team size must be increased properly.

4.2 The influence of the infection function

To understand the influence of the infection function *f* on the optimal team size, we present Fig 3, where each data point is obtained by solving an optimization problem (5) with a given set of parameters.

It is concluded from the figure that the optimal team size is increasing with the infection function. The explanation of this phenomenon is similar to that of the previous one.

4.3 The influence of the available manpower

To understand the influence of the available manpower on the optimal team size, we present Fig 4, where each data point is obtained by solving the optimization problem (5) with a set of given parameters.

It is concluded from the figure that the optimal team size is increasing and tends to saturation with the available manpower. This phenomenon can be explained as follows. When there is a small available manpower, the balance between the two parts in the tradeoff would lead to an optimal team size that is equal to the available manpower. With the increase of the available manpower, the balance would lead to an optimal team size that is increasing less rapidly than the available manpower and finally tends to saturation.

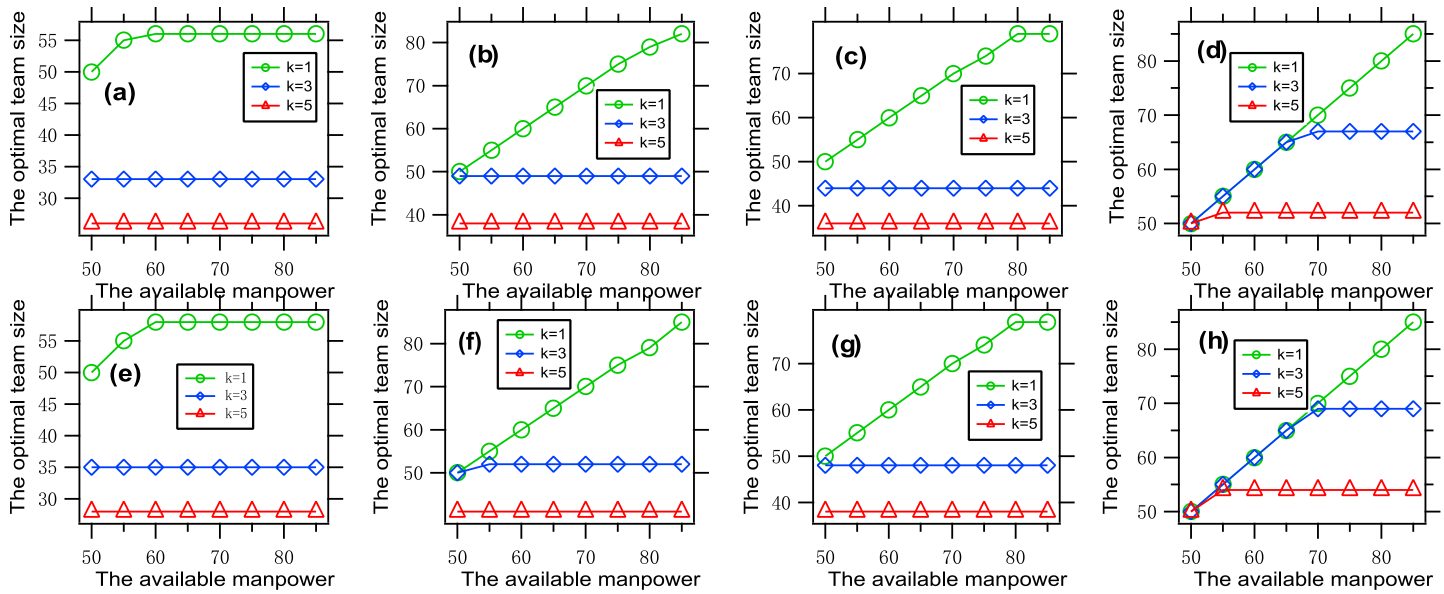

Fig 4. The available manpower vs. the optimal team size. Each data point is obtained by solving the optimization problem (5) $\bar{n} \in \{50, 55, 60, 65, 70, 75, 80, 85\}$, $k \in \{1, 3, 5\}$, with $f = f_1$, $G = G_0$, (a) $\beta = 0.001$, $\theta = 0.01$, $W = 150$; (b) $\beta = 0.001$, $\theta = 0.01$, $W = 300$; (c) $\beta = 0.001$, $\theta = 0.02$, $W = 150$; (d) $\beta = 0.001$, $\theta = 0.02$, $W = 300$, (e) $\beta = 0.002$, $\theta = 0.01$, $W = 150$; (f) $\beta = 0.002$, $\theta = 0.01$, $W = 300$; (g) $\beta = 0.002$, $\theta = 0.02$, $W = 150$; (h) $\beta = 0.002$, $\theta = 0.02$, $W = 300$. It can be seen that the optimal team size is increasing and tends to saturation with the available manpower.

https://doi.org/10.1371/journal.pone.0191101.g004

4.4 The influence of the alarm threshold

To understand the influence of the alarm threshold on the optimal team size, we present Fig 5, where each data point is obtained by solving the optimization problem (5) with a given set of parameters.

It is concluded from this figure that the optimal team size is increasing with the alarm threshold. This phenomenon can be explained as follows. The loss part in the tradeoff is increasing with the alarm threshold. To better balance the two parts in the tradeoff, the team size must be increased properly.

4.5 The influence of the antivirus development effort

To understand the influence of the antivirus development effort on the optimal team size, we present Fig 6, where each data point is obtained by solving an optimization problem with a given set of parameters.

It is concluded from this figure that the optimal team size is increasing with the antivirus development effort. This phenomenon can be explained as follows. The loss part in the tradeoff is increasing with the effort. To better balance the two parts in the tradeoff, the team size must be increased properly.

4.6 The influence of the network heterogeneity

To understand the influence of the network heterogeneity on the optimal team size, the following experiment assumes $G \in \{G_i: 1 \leq i \leq 5\}$, where G_i are scale-free networks with 100 nodes, 109 edges, and a power exponent of 2.7, 2.8, 2.9, 3.0, and 3.1, respectively [40]. See Fig 7.

We present Fig 8, where each data point is obtained by solving the optimization problem (5) with a given set of parameters.

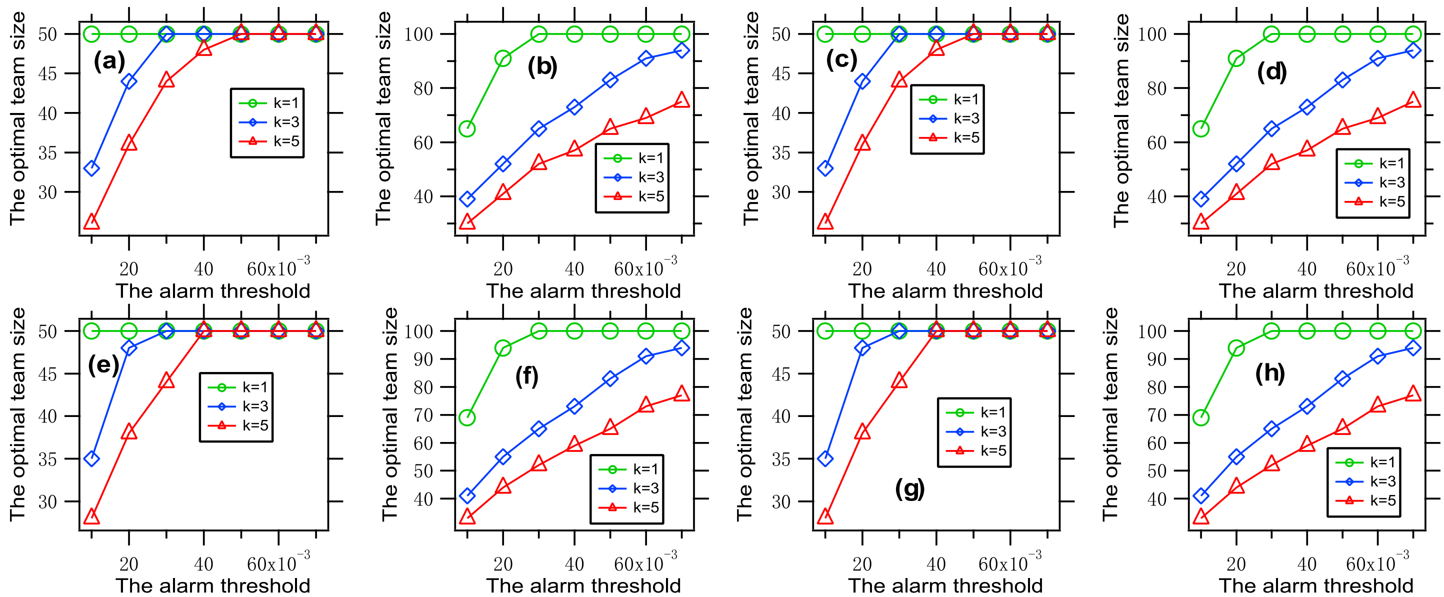

Fig 5. The optimal team size vs. the alarm threshold. Each data point is obtained by solving the optimization problem (5) with $\theta \in \{a \cdot 10^{-2}: a = 1, \cdots, 7\}$, $k \in \{1, 3, 5\}$, $f = f_1$, $G = G_0$, (a) $\beta = 0.001$, $\bar{n} = 50$, $W = 150$; (b) $\beta = 0.001$, $\bar{n} = 100$, $W = 200$; (c) $\beta = 0.001$, $\bar{n} = 50$, $W = 150$; (d) $\beta = 0.001$, $\bar{n} = 100$, $W = 200$, (e) $\beta = 0.002$, $\bar{n} = 50$, $W = 150$; (f) $\beta = 0.002$, $\bar{n} = 100$, $W = 200$; (g) $\beta = 0.002$, $\bar{n} = 50$, $W = 150$; (h) $\beta = 0.002$, $\bar{n} = 100$, $W = 200$. It can be seen that the optimal team size is increasing with the alarm threshold.

https://doi.org/10.1371/journal.pone.0191101.g005

It is concluded from this figure that the optimal team size is increasing with the network heterogeneity. This phenomenon can be explained as follows. The loss part in the tradeoff is increasing with the effort, because malware spreads more rapidly in a more heterogeneous network than in a more homogeneous network. To better balance the two parts in the tradeoff, the team size must be increased properly.

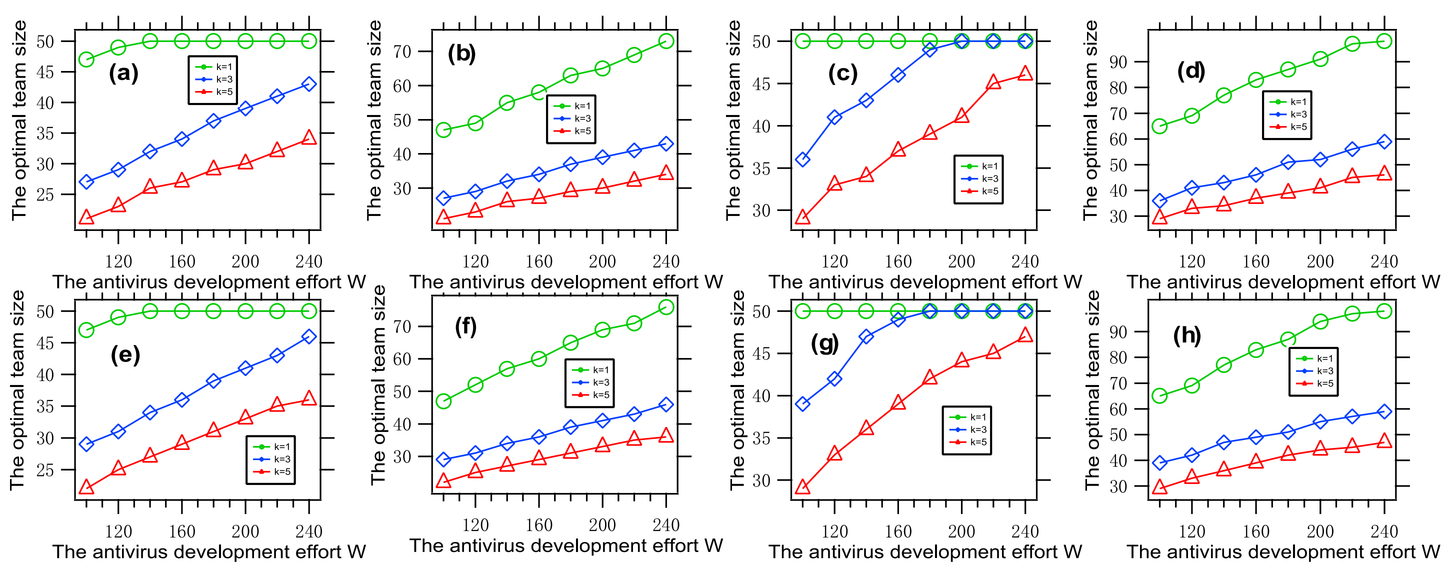

Fig 6. The optimal team size vs. the antivirus development effort. Each data point is obtained by solving the optimization problem (5) with $W \in \{80 + a \cdot 20: a = 1, \cdots, 8\}$, $k \in \{1, 3, 5\}$, $f = f_1$, $G = G_0$, (a) $\beta = 0.001$, $\theta = 0.01$, $\bar{n} = 50$; (b) $\beta = 0.001$, $\theta = 0.01$, $\bar{n} = 100$; (c) $\beta = 0.001$, $\theta = 0.02$, $\bar{n} = 50$; (d) $\beta = 0.001$, $\theta = 0.02$, $\bar{n} = 100$, (e) $\beta = 0.002$, $\theta = 0.01$, $\bar{n} = 50$; (f) $\beta = 0.002$, $\theta = 0.01$, $\bar{n} = 100$; (g) $\beta = 0.002$, $\theta = 0.02$, $\bar{n} = 50$; (h) $\beta = 0.002$, $\theta = 0.02$, $\bar{n} = 100$. It can be seen that the optimal team size is increasing with the antivirus development effort.

https://doi.org/10.1371/journal.pone.0191101.g006

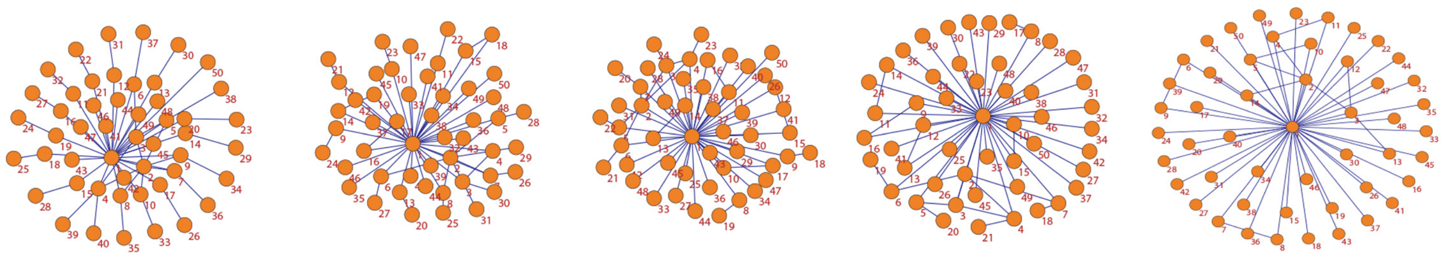

Fig 7. Five scale-free networks with 100 nodes, 109 edges, and a power exponent of 2.7, 2.8, 2.9, 3.0, and 3.1, respectively.

https://doi.org/10.1371/journal.pone.0191101.g007

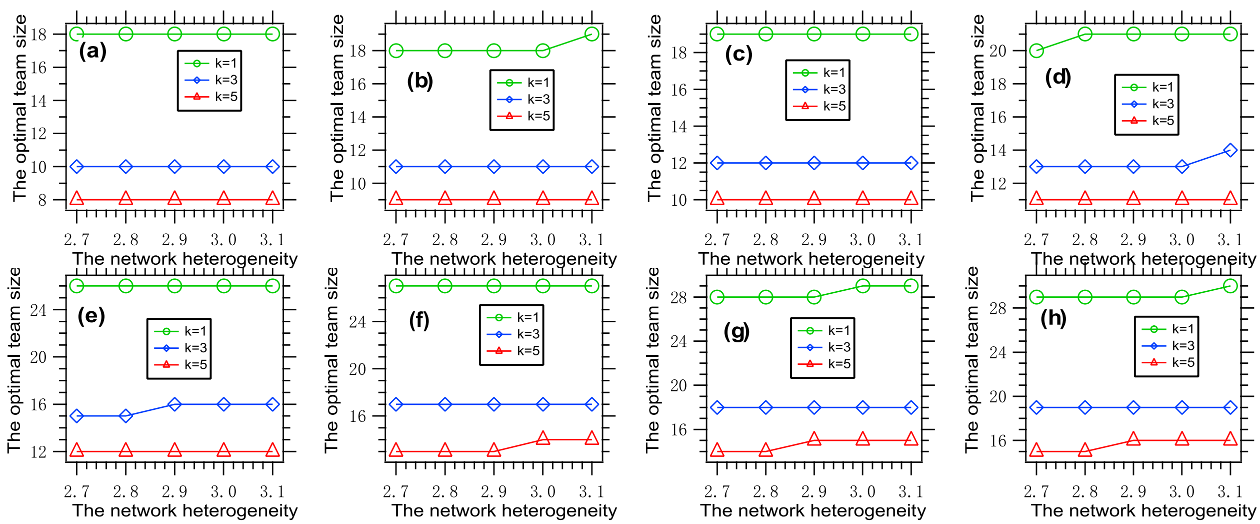

Fig 8. The optimal team size vs. the network heterogeneity. Each data point is obtained by solving the optimization problem (5) with $G \in \{G_i: 1 \leq i \leq 5\}$, $k \in \{1, 3, 5\}$, $f = f_1$, $W = 300$, $\bar{n} = 50$ (a) $\beta = 0.001$, $\theta = 0.01$; (b) $\beta = 0.003$, $\theta = 0.01$; (c) $\beta = 0.005$, $\theta = 0.01$; (d) $\beta = 0.007$, $\theta = 0.01$; (e) $\beta = 0.002$, $\theta = 0.02$; (f) $\beta = 0.004$, $\theta = 0.02$; (g) $\beta = 0.006$, $\theta = 0.02$; (h) $\beta = 0.008$, $\theta = 0.02$. It can be seen that the optimal team size is increasing with the network heterogeneity.

https://doi.org/10.1371/journal.pone.0191101.g008

5 Conclusions

This article has addressed the tradeoff between the losses caused by a new virus and the size of the team for developing an antivirus against the virus. First, an individual-level virus spreading model has been proposed to capture the spreading process of the virus before the appearance of its natural enemy. Then, the tradeoff problem is modeled as an optimization problem. Next, the influences of different factors, including the infection force, the infection function, the available manpower, the alarm threshold, the antivirus development effort and the network topology, on the optimal team size have been examined through computer simulations. The findings are instructive to the decision makers of network security companies.

Towards this direction, there are a number of problems that are worth study. As was indicated previously, the infection force and the infection function must be determined. The model should be extended to more sophisticated virus spreading models such as the impulsive spreading models [41–43], the stochastic spreading models [44–46], and the spreading models on time-varying networks [47–49].

Author Contributions

Funding acquisition: Xiaofan Yang, Yingbo Wu.

Investigation: Jichao Bi, Xiaofan Yang, Yingbo Wu.

Methodology: Xiaofan Yang.

Supervision: Lu-Xing Yang, Xiaofan Yang, Yuan Yan Tang.

Validation: Jichao Bi, Xiaofan Yang.

Visualization: Jichao Bi.

Writing – original draft: Jichao Bi, Lu-Xing Yang, Xiaofan Yang.

Writing – review & editing: Lu-Xing Yang, Xiaofan Yang, Yuan Yan Tang.

References

1. Szor P. The Art of Computer Virus Research and Defense. Addison-Wesley Education Publishers Inc; 2005.
2. Khouzani MHR, Sarkar S, Altman E. Optimal dissemination of security patches in mobile wireless networks. IEEE Transactions on Information Theory. 2012; 58: 4717–4732. https://doi.org/10.1109/TIT.2012.2195295
3. Eshghi S, Khouzani MHR, Sarkar S, Venkatesh S. Optimal patching in clustered malware epidemics. IEEE/ACM Transactions on Networking. 2016; 24: 283–298. https://doi.org/10.1109/TNET.2014.2364034
4. Yang LX, Draief M, Yang X. The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model. Physica A. 2016; 450: 403–415. https://doi.org/10.1016/j.physa.2016.01.026
5. Nowzari C, Preciado VM, Pappas GJ. Analysis and control of epidemics: A survey of spreading processes on complex networks. IEEE Control Systems. 2016; 36: 26–46. https://doi.org/10.1109/MCS.2015.2495000
6. Bi JC, Yang X, Wu Y, Xiong Q, Wen J, Tang YY. On the optimal dynamic control strategy of disruptive computer virus. Discrete Dynamics in Nature and Society. 2017; 2017: 8390784. https://doi.org/10.1155/2017/8390784
7. Heemstra FJ, Software cost estimation. Information and Software Technology. 1993; 34: 627–639.
8. Molkken K, Jrgensen M. A review of surveys on software effort estimation. Proceedings of the 2003 International Symposium on Empirical Software Engineering. 2003; 223.
9. Jorgensen M, Shepperd M. A systematic review of software development cost estimation studies. IEEE Transactions on Software Engineering. 2007; 33: 33–53. https://doi.org/10.1109/TSE.2007.256943
10. Usharani K, Ananth VV, Velmurugan D. A survey on software effort estimation. Proceedings of 2016 International Conference on Electrical, Electronics, and Optimization Techniques. 2016; 505-509.
11. Kephart JO, White SR. Directed-graph epidemiological models of computer viruses. IEEE Computer Society Symposium on Research in Security and Privacy. 1991; 343-359.
12. Kephart JO, White SR. Measuring and modeling computer virus prevalence. IEEE Computer Society Symposium on Research in Security and Privacy. 1991; 2-15.
13. Mishra BK, Pandey SK. Dynamical model of worms with vertical transmission in computer network. Applied Mathematics and Computation. 2011; 217: 8434–8446. https://doi.org/10.1016/j.amc.2011.03.041
14. Song LP, Han X, Liu DM, Jin Z. Adaptive human behavior in a two-worm interaction model. Discrete Dynamics in Nature and Society. 2012; 2012: 828246. https://doi.org/10.1155/2012/828246
15. Yang LX, Yang X. A novel virus-patch dynamic model. PloS ONE. 2015; 10: e0137858. https://doi.org/10.1371/journal.pone.0137858 PMID: 26368556
16. Ren J, Xu Y. A compartmental model for computer virus propagation with kill signals. Physica A: Statistical Mechanics and its Applications. 2017; 486: 446–454. https://doi.org/10.1016/j.physa.2017.05.038
17. Gan C, Yang M, Zhang Z, Liu W. Global dynamics and optimal control of a viral infection model with generic nonlinear infection rate. Discrete Dynamics in Nature and Society. 2017; 2017. https://doi.org/10.1155/2017/7571017

18. Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks. Physical Review Letters. 2001; 86: 3200–3203. https://doi.org/10.1103/PhysRevLett.86.3200 PMID: 11290142
19. Yang LX, Yang X. The spread of computer viruses over a reduced scale-free network. Physica A. 2014; 396: 173–184. https://doi.org/10.1016/j.physa.2013.11.026
20. Ren J, Liu J, Xu Y. Modeling the dynamics of a network-based model of virus attacks on targeted resources. Communications in Nonlinear Science and Numerical Simulation. 2016; 31: 1–10. https://doi.org/10.1016/j.cnsns.2015.06.018
21. Liu WP, Liu C, Yang Z, Liu XY, Zhang YH, Wei ZX. Modeling the propagation of mobile malware on complex networks. Communications in Nonlinear Science and Numerical Simulation. 2016; 37: 249–264. https://doi.org/10.1016/j.cnsns.2016.01.019
22. Yang LX. The effect of network topology on the spread of computer viruses: a modelling study. International Journal of Computer Mathematics.
23. Van Mieghem P, Omic JS, Kooij RE. Virus spread in networks. IEEE/ACM Transactions on Networking. 2009; 17: 1–14. https://doi.org/10.1109/TNET.2008.925623
24. Xu S, Lu W, Zhan Z. A stochastic model of multivirus dynamics. IEEE Transactions on Dependable and Secure Computing. 2012; 9: 30–45. https://doi.org/10.1109/TDSC.2011.33
25. Sahneh FD, Scoglio C, Van Mieghem P. Generalized epidemic mean-field mdel for spreading processes over multilayer complex networks. IEEE/ACM Transactions on Networking. 2013; 21: 1609–1620. https://doi.org/10.1109/TNET.2013.2239658
26. Xu S, Lu W, Xu L, Zhan Z. Adaptive epidemic dynamics in networks: Thresholds and control. ACM Transactions on Autonomous and Adaptive Systems. 2014; 8: 19. https://doi.org/10.1145/2555613
27. Yang LX, Draief M, Yang X. The impact of the network topology on the viral prevalence: a node-based approach. PloS ONE. 2015; 10: e0134507. https://doi.org/10.1371/journal.pone.0134507 PMID: 26222539
28. Yang LX, Draief M, Yang X. Heterogeneous virus propagation in networks: a theoretical study. Mathematical Methods in Applied Sciences. 2017; 40: 1396–1413. https://doi.org/10.1002/mma.4061
29. Yang LX, Yang X, Wu Y. The impact of patch forwarding on the prevalence of computer virus: A theoretical assessment approach. Applied Mathematical Modelling. 2017; 43: 110–125. https://doi.org/10.1016/j.apm.2016.10.028
30. Yang LX, Yang X, Tang YY. A bi-virus competing spreading model with generic infection rates. IEEE Transactions on Network Science and Engineering.
31. Zhou T, Liu JG, Bai WJ, Chen G, Wang BH. Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity. Physical Review E. 2006; 74: 056109. https://doi.org/10.1103/PhysRevE.74.056109
32. Bai WJ, Zhou T, Wang BH. Immunization of susceptible–infected model on scale-free networks. Physica A: Statistical Mechanics and its Applications. 2007; 384: 656–662. https://doi.org/10.1016/j.physa.2007.04.107
33. Ausiello G, Petreschi R (eds.). The Power of Algorithms: Inspiration and Examples in Everyday Life. Springer-Verlag Berlin Heidelberg; 2013
34. Goodfellow I, Bengio Y, Courville A. Deep Learning. MIT Press; 2016
35. Buduma N. Fundamentals of Deep Learning: Designing Next-Generation Machine Intelligence Algorithms. O'Reilly Media; 2017
36. Hamilton JD. Time Series Analysis. Princeton University Press; 1994
37. Tam CC, Tissera H, de Silva AM, De Silva AD, Margolis HS, Amarasinge A. Estimates of Dengue Force of Infection in Children in Colombo, Sri Lanka. PLoS Neglected Tropical Diseases. 2013; 7: e2259. https://doi.org/10.1371/journal.pntd.0002259 PMID: 23755315
38. Marmara V, Cook A, Kleczkowski A. Estimation of force of infection based on different epidemiological proxies: 2009/2010 Influenza epidemic in Malta. Epidemics. 2014; 9: 52–61. https://doi.org/10.1016/j.epidem.2014.09.010 PMID: 25480134
39. http://snap.stanford.edu/data/egonets-Facebook.html
40. Barabasi AL, Albert R. Emergence of scaling in random networks. Science. 1999; 286: 509–512. https://doi.org/10.1126/science.286.5439.509 PMID: 10521342
41. Yao Y, Guo L, Guo H, Yu G, Gao F, Tong X. Pulse quarantine strategy of internet worm propagation: Modeling and analysis. Computer and Electrical Engineering. 2012; 38: 1047–1061. https://doi.org/10.1016/j.compeleceng.2011.07.009
42. Yao Y, Feng X, Yang W, Xiang W, Gao F. Analysis of a delayed Internet worm propagation model with impulsive quarantine strategy. Mathematical Problems in Engineering. 2014; 2014: 369360. https://doi.org/10.1155/2014/369360

43. Yang LX, Yang X. The pulse treatment of computer viruses: a modeling study. Nonlinear Dynamics. 2014; 76: 1379–1393. https://doi.org/10.1007/s11071-013-1216-x

44. Britton T. Stochastic epidemic models: A survey. Mathematical Biosciences. 2010; 225: 24–35. https://doi.org/10.1016/j.mbs.2010.01.006 PMID: 20102724

45. Amador J, Artalejo JR. Stochastic modeling of computer virus spreading with warning signals. Journal of the Franklin Institute. 2013; 350: 1112–1138. https://doi.org/10.1016/j.jfranklin.2013.02.008

46. Amador J. The stochastic SIRA model for computer viruses. Applied Mathematics and Computation. 2014; 232: 1112–1124. https://doi.org/10.1016/j.amc.2014.01.125

47. Schwarzkopf Y, Rakos A, Mukamel D. Epidemic spreading in evolving networks. Physical Review E. 2010; 82: 336–354. https://doi.org/10.1103/PhysRevE.82.036112

48. Valdano E, Ferreri L, Poletto C, Colizza V. Analytical computation of the epidemic threshold on temporal networks. Physical Review X. 2015; 18: 503–512.

49. Ogura M, Preciado VM. Stability of spreading processes over time-varying large-scale networks. IEEE Transactions on Network Science & Engineering. 2016; 3: 44–57. https://doi.org/10.1109/TNSE.2016.2516346