Hindawi
Security and Communication Networks
Volume 2017, Article ID 2910310, 8 pages
https://doi.org/10.1155/2017/2910310

Research Article

Malware Propagation and Prevention Model for Time-Varying Community Networks within Software Defined Networks

Lan Liu,[1,2] Ryan K. L. Ko,[2] Guangming Ren,[1] and Xiaoping Xu[1]

[1] *School of Electronics & Information, Guangdong Polytechnic Normal University, Guangzhou 510665, China*
[2] *Cyber Security Lab, Department of Computer Science, University of Waikato, Hamilton, New Zealand*

Correspondence should be addressed to Lan Liu; hust_ll@126.com

Received 10 December 2016; Revised 18 February 2017; Accepted 5 March 2017; Published 28 March 2017

Academic Editor: Ángel Martín Del Rey

As the adoption of Software Defined Networks (SDNs) grows, the security of SDN still has several unaddressed limitations. A key network security research area is in the study of malware propagation across the SDN-enabled networks. To analyze the spreading processes of network malware (e.g., viruses) in SDN, we propose a dynamic model with a time-varying community network, inspired by research models on the spread of epidemics in complex networks across communities. We assume subnets of the network as communities and links that are dense in subnets but sparse between subnets. Using numerical simulation and theoretical analysis, we find that the efficiency of network malware propagation in this model depends on the mobility rate q of the nodes between subnets. We also find that there exists a mobility rate threshold qc. The network malware will spread in the SDN when the mobility rate $q > qc$. The malware will survive when $q > qc$ and perish when $q < qc$. The results showed that our model is effective, and the results may help to decide the SDN control strategy to defend against network malware and provide a theoretical basis to reduce and prevent network security incidents.

1. Introduction

With separate control and data planes for computer networking [1], Software Defined Networks (SDNs) are considered by many to be a promising network platform as it empowers programmability and flexible configuration—paving the way for more powerful network control and traffic data analysis. However, the SDN architecture also introduces complexity and increased risks to network security. With the continuous development of SDN security applications, we need to anticipate issues that might arise throughout the implementation of SDN-based security applications.

At their core, SDN computer networks are complex systems [2]. The research content of computer networks includes network topology, network traffic characteristics, and the influence of the network behavior on the whole network. The spread and prevention of network malware are key technologies studied in SDN and have been one of the most prolific fields in complex network dynamics research. Through our research, we found that some characteristics of computer network virus propagation are similar to real world epidemic spread.

Compared to past computer network architectures (where it is not easy to control the whole network from the global level), SDNs are considered by many to be a promising network platform as it empowers programmability and flexible configuration—enabling powerful network control and traffic data analysis. As such, the study of the transition probability for malware within SDN makes not just an interesting endeavor but also an important research area considering upcoming trends in computer networking. Hence, in this research, we present a simple network model with a time-varying community network and investigate network malware spreading processes within this model. In terms of scope, this paper does not consider the source and the specific types of the malware.

The remainder of the paper is organized as follows. Section 2 discusses the background and related work. In Section 3, a model with a time-varying community network of malware propagation in SDN is proposed. Then, in Section 4, we implement a numerical simulation to evaluate the influences of the mobility rate on the dynamic behavior of SDN, and the theoretical analysis of this model is performed. In Section 5, the possible applications of our research are presented. Finally, we conclude and offer prospective areas for future research in Section 6.

2. Background and Related Work

2.1. Industry Trends. This research paves the way for practical implementations using SDN as a platform for malware propagation control. In the industry, Google has already deployed SDN for data center backbone traffic. Major commercial switch vendors including Cisco, IBM, HP, Dell, and Juniper Networks have announced intent to support or have already launched switching products that support SDN. We see a lot of potential in applying our research into similar environments.

The market research company IDC predicts that the market for SDN applications will reach $37 billion by 2016 [3]. It is also realistic to expect malware (e.g., network viruses, Botnets) to continue to be a threat for future SDN deployments. Specifically, we witness a recent surge in malware (e.g., Mirai) specifically designed for launching Distributed Denial-of-Service (DDOS) attacks to network-connected assets. To assure Internet security, effective detection malwares are indispensable. Our research addresses these issues directly.

2.2. Research Trends and Gaps. Research on the network security of SDN raised concern in recent years. Most prior studies have looked at the development and analysis of SDN security applications [4]. However, few solutions provide an effective defense mechanism against the threat of attacks in SDNs because all types of open applications make the end-hosts and switches the target of attacks, which is a threat to the entire network [5]. In all types of security incidents, network malware usually spreads quickly and has a strong influence on availability, making network malware the most important issue to resolve in Internet security.

The control plane of SDN will have direct control over the data plane elements [6]. Network administrators of SDNs often use programmable soft switches to provide network virtualization. Modifying routing rules in traditional networks is difficult but easier in SDNs, which will help address problems in traditional networks and is advantageous to adjust the route strategy of the entire network. The logical centralization of network intelligence presents exciting challenges and opportunities to enhance security in such networks, including new ways to prevent, detect, and react to threats, as well as innovative security services and applications that are built upon SDN capabilities. Malicious code detection and prevention under the new architecture need further study [7–14].

At its core, the spread of network malware on the Internet is a dynamic complex network challenge. In complex network dynamics, if the network evolution speed is slower than the information transmission speed, it can be approximately regarded as a static network. This assumption is set up in many cases, such as computer malware spreading on the Internet. Therefore, we consider that the community structures in complex network models have considerable influence on the spreading of network malware in SDN.

In recent years, many studies have indicated that time-varying networks play an important role in the investigation of the network malware spreading that occurs in complex networks [15]. In computer networks, we can assume subnets as "communities" and "links" that are dense in a subnet but sparse between subnets. Network malware spreading is rapid in the subnets but slow between subnets. Because different subnets are disparate, it is impossible for individuals to propagate malware to different subnets at the same time even if these individuals have connections with many different subnets in a static network. Thus, there are no links among subnets at each time step in a time-varying network, but individuals can move among subnets because of the centralized control of SDN [16].

Toutonji and Yoo proposed a model Passive Worm Dynamic Quarantine (PWDQ) to enable network malware detection and protection [17]. When a node is listed as a suspicious node, the PWDQ model departs from previous models in that infected nodes will be recovered either by passive benign worms or by quarantine measures. Computer simulations show that this method may decrease the number of infectious nodes and reduce the speed of network malware propagation.

Omote and Shimoyama found a method for preventing the spread of network malware [18]. An estimating unit calculates the expected number of infected nodes when the malware transmits a predetermined number of packets, based on the infectivity calculated by the infectivity calculating unit.

Bradley et al. [19] and other studies have shown that the network topology has an impact on network malware spreading: the closer to the "center" of the network the malware is, the faster the malware spreads and the higher the probability of repeated infection is.

Gourdin et al. found that the effect of network malware spreading in a telecommunication network [20], where a certain curing strategy is deployed, can be captured by epidemic models. In their model, the probability of each node being infected depends on the curing and infection rate of its neighbors.

Tang and Li investigated malware spread in Wireless Sensor Networks (WSNs) through Susceptible-Infective (SI) epidemic models [21] and proposed two adaptive network protection schemes for securing WSNs against malware attacks.

Abaid et al. [22] proposed elastically partitioning network traffic to enable distributing detection load across a range of detectors and making a centralized SDN controller, which allows for network-wide threat correlation as well as quick control of malicious flows.

Ichiro et al. mentioned that, in security incident response, the isolation of network virus-infected nodes and investigation of the damage situation of network virus activity are needed [23]. They proposed a method to isolate virus-infected nodes while avoiding being detected by malware by changing network quickly and partially using SDN.

Hosseini et al. [24, 25] proposed a dynamic model of malware propagation in scale-free networks (SFNs) based on a rumor spreading model. The model considers the impact of software diversity to halt the outbreak of malware in networks. Their research stated that the simulation results demonstrate that the model is more effective than other existing models of malware propagation, in terms of reducing the density of infected node.

These research efforts provide several new approaches for studying network malware spreading and prevention in the SDN environment. In terms of our approach, we believe that since an SDN controller can manage and quarantine nodes in the entries network, when new network malware breaks out in a subnet, this controller may change the flow table strategy according to network status and prevent the spreading of the malware to other subnets. As such, we designed a network malware propagation model of SDN to effectively defend against the spreading of network malware.

3. Modeling Network Malware Spreading in an SDN Environment

As the spread of network malware in SDN is similar to the spread of diseases, we can use similar models to study the spread of network malware. This type of model has two assumptions: (1) the state of a network node at any moment t is limited; the states include *"susceptible"; "infected"; "recovery"; "isolation"*. We can choose different sets of states according to the characteristics of the network malware and modeling purposes. (2) The infected nodes have a certain probability of infecting other nodes in the network.

Our mathematical model of computer malware spread is mostly based on the Susceptible-Infected-Recovery (SIR) model or the simple Susceptible-Infected-Susceptible (SIS) model [26]. To simplify our research, we adopted the SIS model, where each node belongs to one of two states: susceptible or infected [27, 28]. Mathematical analysis on such a model has revealed the importance of topology for propagation dynamics. Particularly, we found that the time-varying community network model is suitable for networks with small numbers of susceptible nodes, and we assumed that the network evolves more slowly than the diffusion process.

3.1. Model Assumptions. Different nodes belong to different subnets in a computer network. In our study, we use logical subnets to classify the community network; network malware spreads more quickly within the subnet and spreads slowly between different subnets. To simplify the complex model, we assume that the network malware cannot spread between different subnets in normal conditions. Because the SDN may change its routing strategy, when one infected node moves from one subnet to another logical subnet, it probably makes the network malware spread between subnets.

To study the effects of network malware spreading when an infected node changes from one subnet to another in SDN, we establish some simple model assumptions.

(1) Consider a total population of N nodes in the model, which means that no new nodes enter or leave the system at any time.

(2) In the model, nodes only have two possible states: susceptible (S) and infected (I). A node must be in one of the two states, and an infected node cannot be infected again. We define the initial infected nodes as $X(0) = I_0$.

(3) The network malware cannot spread between different subnets in normal conditions, which means that there are no infection paths between different subnets.

Assume that each susceptible neighbor of an infected node has a probability λ of being infected and a susceptible node has k_{inf} infected neighbors at time T in the model. At $T+1$ step, this susceptible node will become infected with probability $1-(1-\lambda)^{k_{\text{inf}}}$. At the same time, the infected node may become susceptible at rate μ through network malware killing and patching.

3.2. Model with Time-Varying Community Network. Although various studies have shown that a computer network is a "scale-free" network, to simplify the model, we begin our analysis with the simple time-varying community network.

Based on the model assumption, we construct a time-varying community network with network malware spreading.

(1) Consider a total population of N nodes that is divided into m subnets with random n_i $(i = 1, 2, \ldots, m)$ nodes in each subnet, and let them satisfy

$$\sum_{i=1}^{m} n_i = N. \tag{1}$$

(2) For each subnet i, we use probability p_i to add a link between each two nodes and let them satisfy

$$\sum_{i=1}^{m} p_i \cdot \frac{1}{2} n_i \left(n_i - 1\right) = \frac{N \cdot \langle k \rangle}{2}. \tag{2}$$

In addition, $\langle k \rangle$ is the average degree of the entire network.

(3) When an infected node jumps from one subnet into another subnet, it will spread the network malware. We assume that every node j $(j = 1, 2, \ldots, N)$ has probability q to jump to another subnet, which is chosen randomly. In order to simulate malware spreading caused by node jump, we add links between different subnet with probability q. During each time step, break all of the links between different subnet connected at last time step. Then connect nodes in the different subnet with probability q again. The most important value is a threshold λ_c. The network malware spreads and becomes infected for $\lambda > \lambda_c$ and perishes for $\lambda < \lambda_c$. In this model, we have a network malware threshold λ_c. The network malware spreads and becomes infected when $\lambda > \lambda_c$. From the theory of probability [29], we have $\lambda_c = \mu / \langle k \rangle$ in the time-varying community network model. For a specific community i, when the mobility rate $q = 0$, its network malware subthreshold is defined as

$$\lambda_c^i = \frac{\mu}{\langle k_i \rangle} = \frac{\mu}{p_i \left(n_i - 1\right)}. \tag{3}$$

The network malware in the specific community i will survive when $\lambda > \lambda_c^i$ and die for $\lambda < \lambda_c^i$. We assume that there is only one seed at the beginning, which means $X(0) = 1$. The network malware will spread within the subnet where the seed is chosen and will not affect other subnets.

Because of the regular changes in the routing strategy in SDN, network nodes including mobile devices, network devices, and hosts can be redirected, which means that the node mobility rate between subnets satisfies $q > 0$. When $\lambda > \lambda_c^i$ $(i = 1, 2, \ldots, m)$, even if there is only one seed at the beginning, the network malware may spread into all of the subnets. We discover that the time of the network malware outbreak in the subnets is dependent on the mobility rate q. When $\lambda < \lambda_c^i$ $(i = 1, 2, \ldots, n;\ n < m)$, a mobility rate threshold q_c is considered. The network malware in subnet is i where $\lambda < \lambda_c^i$ can survive when $q > q_c$ because of the jump of infected nodes.

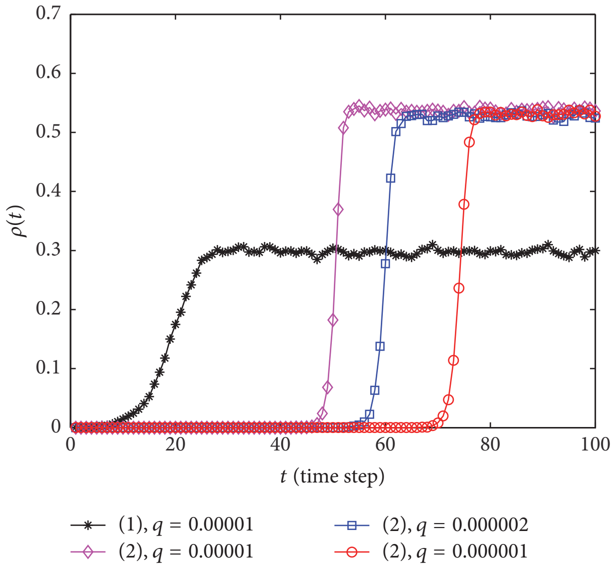


Figure 1: Density of infected nodes $\rho(t)$ in two subnets with different mobility rates q. The symbol (1) denotes the first subnet, and the symbol (2) denotes the second subnet.

4. Simulation and Evaluation

To simulate the network malware spreading, we use a similar experimental environment. To be brief we set $m = 2$ and analyze the network malware spreading in two cases. At the beginning, there is only one infected node, $X(0) = 1$, and we set $N = 3000$, $n_1 = 1200$, $n_2 = 1800$, $\langle k \rangle = 20$, $p_1 = 0.0069$, and $p_2 = 0.0155$. These parameters satisfy (1) and (2).

(A) $\lambda > \lambda_c^i$ $(i = 1, 2)$. Let us set $\mu = 0.1$. We can obtain $\lambda_c^1 = 0.0121$ and $\lambda_c^2 = 0.0036$ from (3). We set $\lambda = 0.02 > \lambda_c^i$ $(i = 1, 2)$.

In the simulation, we chose an infected node in the first subnet randomly, and the other nodes in the two subnets were susceptible. We simulate the step with mobility rate $q = 0.000001$ to 0.00001 between the subnets, and the result is shown in Figure 1. The curve with black asterisks represents the density of infected nodes in the first subnet as a function of time with mobility rate $q = 0.00001$ and the other curves represent the evolution of infected nodes in the second subnet with different mobility rates from 0.00001 to 0.000001.

As can be observed from the diagram, the network malware first broke out in the first subnet and then propagated into the second subnet. The time of network malware outbreak in the second subnet decreased with the increase in the mobility rate q.

We have not plotted the curve of the other mobility rate in the first subnet because the network malware spreading in the first subnet has less of a relationship with q. The values of mobility rate q applied above were chosen based on experiment and by experience. A deep understanding of the detailed time evolution of network malware spreading is a prerequisite to finding optimal strategies to prevent network malware outbreaks. Thus, we analyzed it in detail.

From the simulation, we knew that when $\lambda > \lambda_c^2$, the network malware would have an outbreak in the second subnet only if there was one node that was infected by the nodes and had moved from the first subnet.

At each time step, the number of infected nodes that move from the first subnet can be calculated as $n_1 q \rho_1(t)$, where $\rho_1(t)$ represents the density of the infected nodes in the first subnet at time t, q is the mobility rate between subnets, and n_1 is the total number of nodes of the first subnet.

In the time-varying network model, small world model, and scale-free model, these theories are based on mean field theory. According to mean field theory, $\rho_1(t)$ satisfies equation $\dot{\rho}_1(t) = -\mu\rho_1(t) + \lambda\langle k_1\rangle\rho_1(t)(1 - \rho_1(t))$.

In this equation, $\rho_1(t)$ represents the density of the infected nodes in the first subnet and each infected node will become susceptible at rate μ. λ is the probability that each susceptible node linked by an infected node will be infected. On the right side of the equation, $-\mu\rho_1(t)$ shows the reduced number of infected nodes, $(1 - \rho_1(t))$ is the density of susceptible nodes, and $\langle k_1\rangle\rho_1(t)$ presents the number of infected nodes around a susceptible node. According to the multiplication rule, $\lambda\langle k_1\rangle\rho_1(t)(1 - \rho_1(t))$ presents the increased number of infected nodes in the entire network. The simplified formula is

$$\rho_1(t) = \frac{a/b}{1 + ce^{-at}}, \tag{4}$$

where $a = \lambda\langle k_1\rangle - \mu$, $b = \lambda\langle k_1\rangle$, and

$$c = \frac{a - \rho_1(0)\, b}{\rho_1(0)\, b}. \tag{5}$$

$\rho_1(0)$ shows the density of infected nodes at time $t = 0$, and, in this simple example, we obtain $\rho_1(0) = 1/n_1$. At time step t, there are $n_1\rho_1(t)$ infected nodes in the first subnet. According to model, the nodes between subnets connect with probability q. So, in the second subnet, there are $n_1\rho_1(t)n_2 q$ nodes connected with the infected nodes in the first subnet, which have a probability λ of being infected. So, at each time step t, the probability of the node in the second subnet being infected is $n_1\rho_1(t)n_2q\lambda$. Supposing that the probability of the node in the second subnet being infected at t_c time step is 100%, we can write the formula as

$$\int_0^{t_c} n_1\rho_1(t)\,n_2q\lambda\,dt = 1. \tag{6}$$

Then, we can obtain

$$t_c = \frac{\ln\left(e^{\ln(1+c)+b/(\lambda n_1 n_2 q)} - c\right)}{a}. \tag{7}$$

We can obtain the outbreak time of the network malware in the second subnet by

$$T_c = t_c + t_0 = \frac{\ln\left(e^{\ln(1+c)+b/(\lambda n_1 n_2 q)} - c\right)}{a} + \frac{\ln c}{a}. \tag{8}$$

In this formula, $t_0 = \ln c/a$ is the time for the number of infected nodes in the second subnet to increase from one to half of the stabilized value. To check the above theoretical analysis, we simulate experiments to obtain test data. We make numerical experiments and determine T_c by checking the number of infected nodes of the second subnet, which reaches half of the stabilized value at time step T_c. We build the time-varying network with the same parameters as shown in Figure 1 and set $\lambda = 0.02$ and $\lambda = 0.08$. We simulate the experiment many times and take the average result of several experiments. When we change the mobility rate q from 0.000001 to 0.00001, we obtain two curves, as shown in Figure 2. The circles and asterisks denote the results from two different λ values by experiment, and the two lines represent the results calculated from (8), where $\lambda = 0.02$ and $\lambda = 0.08$. As we can see, the numerical simulations and theoretical conclusion are consistent.

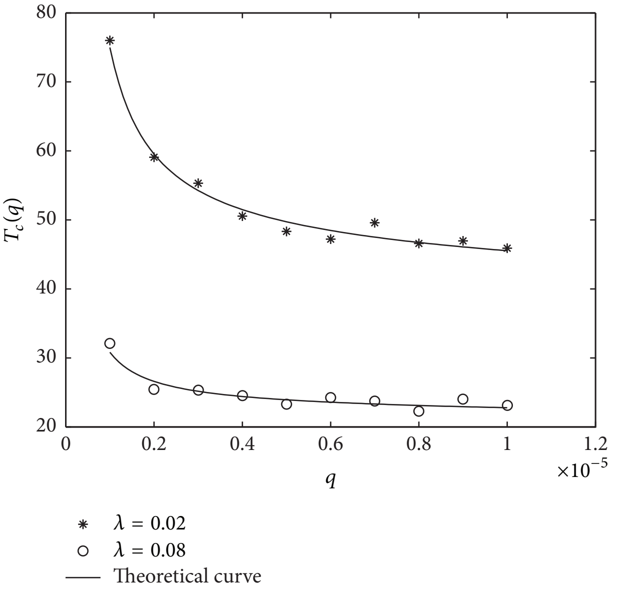


Figure 2: The network malware outbreak time T_c versus the mobility rate q. The symbols represent the results of numerical simulations, and the lines represent the results of theory.

(B) $\lambda_c^2 < \lambda < \lambda_c^1$. Through our analysis, we know that the network malware will perish in the first subnet, where the mobility rate q is too low. However, if the mobility rate is high enough, the network malware may also spread into the second subnet.

In the experiments, we select $\lambda = 0.008$ and use the same values of the other parameters of the time-varying network, as in Figure 1. The value conforms to $\lambda_c^2 < \lambda < \lambda_c^1$, and we use the initial value of infected nodes $X(0) = 100$, which is selected randomly from the first subnet. We get the values $\rho_1(0) = X(0)/n_1 = 0.083$, $\rho_2(0) = 0$, and $\rho(0) = X(0)/N = 0.033$, where $\rho_1(0)$, $\rho_2(0)$, and $\rho(0)$ represent the density of infected nodes in the first subnet, second subnet, and entire network, respectively.

Figures 3(a) and 3(b) show the evolution function curve of $\rho(t)$ in two subnets with the mobility rates $q = 0.0001$ and $q = 0.00001$. The black asterisks represent the density of infected nodes in the first subnet as a function of time, and the red circles represent the evolution of infected nodes in the second subnet. As indicated in Figure 3(a), the network malware broke out at $t = 70$ approximately for $q = 0.0001$ in the second subnet. However, for $q = 0.00001$, the number of infected nodes was reduced to zero slowly in the first subnet and the network malware did not break out at all in the second subnet, as shown in Figure 3(b).

We theoretically analyze how the mobility rate influences the spreading of network malware. Because $\lambda < \lambda_c^1$, there must be a time step t_1 when the network malware will perish when $t = t_1$ in the first subnet. The network malware can spread in the second subnet only if the infected nodes can move into the second subnet and at least one susceptible node in the second subnet is infected before $t = t_1$. According to (4), we know that when $a < 0$, $\rho_1(t)$ is reduced gradually to close to zero. We use $\rho_1(t_1) = 0.0001$ as a small number and solve (4) to obtain t_1:

$$t_1 = \frac{\ln((10000a - b)/bc)}{-a}. \tag{9}$$

From (7) and (9) and considering $t_1 = t$ when $q = q_c$, we define c as in (5) and obtain

$$q_c = \frac{b}{n_1 n_2 (\ln(bc/(10000a - b) + c) - \ln(1 + c))}. \tag{10}$$

To simulate the process better, we repeated the experiments several times and set $X(0) = 100$ to 200 and set $\lambda = 0.004$ to 0.01, and then the mobility rate q is gradually increased from 0. When the mobility rate q increases to the threshold q_c, the network malware will break out in the second subnet. For each set of $X(0)$ and λ, we conducted the experiment 100 times and averaged the test data. As shown in Figure 4, the circles and asterisks indicate the experiment results for $X(0) = 100$ and 200, respectively. The lines represent the theoretical value calculated from (10) and show that, for a specific λ, the mobility rate threshold q_c is approximately inversely proportional to $X(0)$, which is the initial number of infected nodes in the first subnet. However,

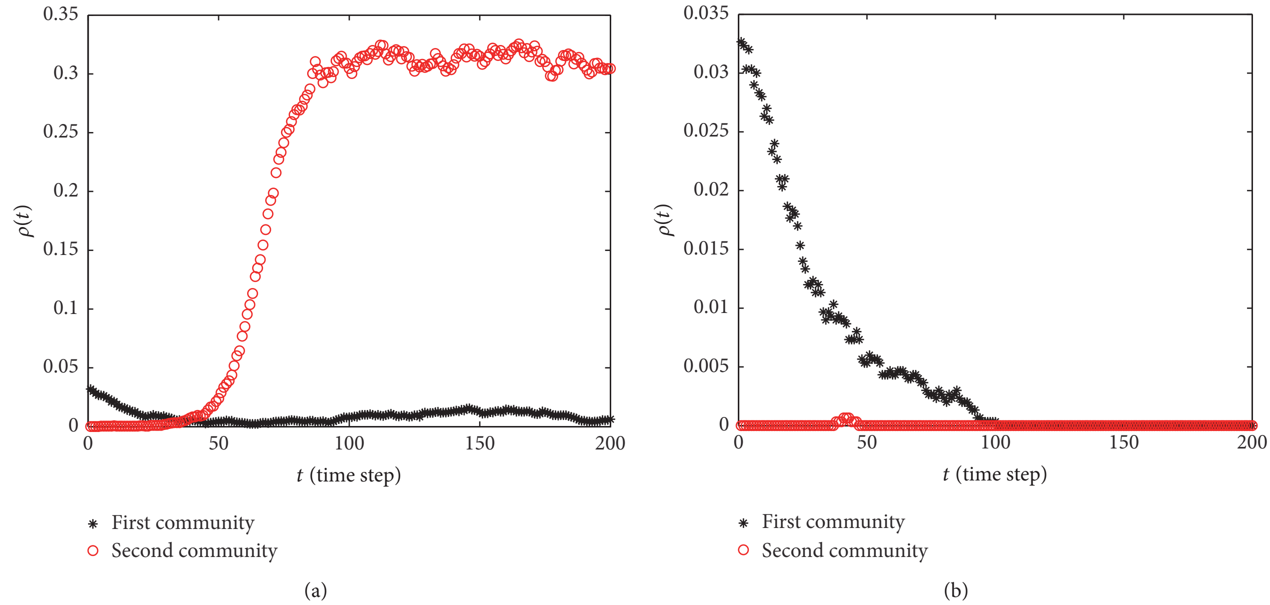


Figure 3: Density of infected nodes $\rho(t)$ as a function of t in two subnets with $\lambda = 0.008$. (a) $q = 0.0001$. (b) $q = 0.00001$.

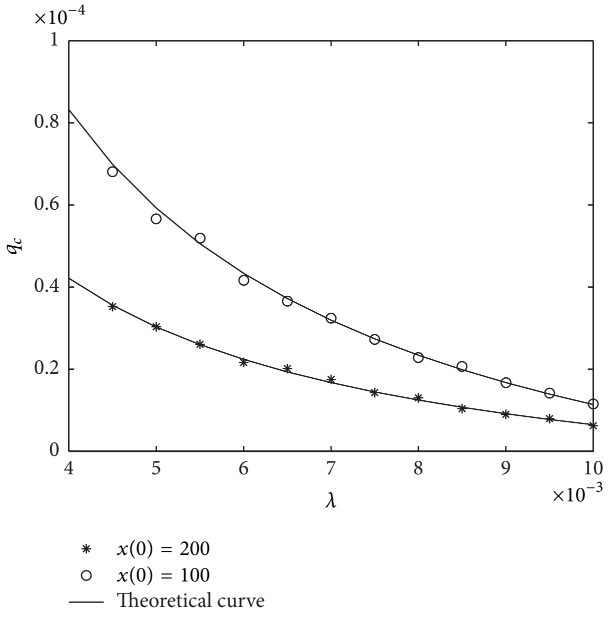


Figure 4: The mobility rate threshold q_c versus the infection rate λ with different initial numbers of infected nodes.

for a specific $X(0)$, q_c rapidly decreases with the increase in the infection rate λ. For example, when $X(0) = 100$, q_c decreases from $8.2 * 10^{-5}$ to 1.2×10^{-5} as λ increases from 0.004 to 0.01. The numerical simulation results confirm the theoretical formula in (10).

Some researchers [30, 31] have conducted studies on the impact of community structure on SIS epidemic spreading process and these research results provide us with a new idea of studying time-varying community structure of the field of network security. On the basis of the simulation experiments, we proved the effectiveness of our model to find the propagation threshold of network community. This may be helpful to evaluating the network malware outbreak time in SDN.

5. Possible Applications

With SDN redefining the traditional networking business model, customers can easily discover, learn, and get specific network applications and download them to their own environment. Conversely, malware will easily spread in the whole network. Specifically, our research may be useful at malware propagation and prevention within SDN in the following ways.

Firstly, by the analysis we can get the mobility rate threshold qc of the malware propagation and when there are some new and large-scale malware outbreaks, through some measures (such as firewall, access control), the respective national information security center (e.g., the national Computer Emergency Response Team (CERT)) may provide SDN-based network security for data centers and assets, detecting malware propagation and insider attacks at an early stage. The security center can decide the SDN control strategy to reduce the spread and the possibility of outbreak of the malware.

Secondly, in the face of a highly globalized business environment, many companies are eager to transform their network architectures into ones which are easy to control and adjust; SDN applications make this aspiration possible. Our model can help the companies' administrator(s) to modify the network routing policy to reduce and prevent the spread of the network malware.

Finally, a potential SDN-based "App" approach (recently introduced by HP and Huawei) offers a platform for customers to see real, high-value use cases of SDN that can benefit their organization. Customers can easily access and deploy innovative solutions to solve real business problems that legacy infrastructures cannot and gain the complete visibility and control only IP Address Management can provide. When they get the information of emerging malware, they can adjust their strategies to avoid their own resources by malware propagation.

6. Conclusion and Perspectives

This research proposes a network model with time-varying community structures in an SDN environment. A model was designed to analyze network malware spreading and prevention under SDN architecture. In our model, connections are static within subnets and are dynamic between subnets. The impact of the mobility rate q on network malware spreading is studied. It is found that when nodes infected with network malware move from the source subnet to the target subnet, the network malware would break out in the target subnet in which there exists no infected node initially, and the outbreak time decreases with increasing mobility rate.

We have also found that there exists a mobility rate threshold q_c. The network malware breaks out when the mobility rate is larger than the threshold value and dies when the mobility rate is smaller than the threshold value in all of the subnets.

The control plane of SDNs enables us to adjust the management strategy of the entire network [32]. Our results may be helpful in evaluating the network malware outbreak time in a subnet that contacts other infected subnets from a global perspective. We can now isolate suspected infected nodes dynamically, control the mobility rate of subnets, and modify the network routing policy to reduce and prevent the spread of the network malware.

In terms of future work, we plan to analyze the network malware spreading and protection in a scale-free network model in an SDN environment because a scale-free network is more similar to a computer network. Increasingly, we find that emerging groups of researchers are starting to work on similar research areas, showing the validity and urgency of our work. Further improvements can be made, as our study is only beginning and its theoretical model is relatively simple; effort to make our study align closer to real-life network environments in large deployments is a critical direction. From a theoretical analysis viewpoint, the degree of nodes is different in scale-free networks, their mobility rate effects on the spread of computer malware are also different, and the mobility of center nodes will have more influence on the spread of computer malware. We will study the network malware spreading and protection in a scale-free network model and analyze the relationship between the node mobility rate and spread of network malware in this model. This model will be more complicated and our work will begin with simulation experiments.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is supported by the National Natural Science Foundation of China (no. 61571141), the Guangdong Province Teaching Quality Project ([2015] no. 133)-Network Engineering Comprehensive Reform, and the Guangdong Provincial Application Oriented Technical Research and Development Special Fund Project (2015B010131017). This research is also supported by the New Zealand Office of the Privacy Commissioner and STRATUS (https://stratus.org.nz).

References

[1] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with SDN: a feasibility study," *Computer Networks*, vol. 85, pp. 19–35, 2015.

[2] J. François, L. Dolberg, O. Festor, and T. Engel, "Network security through software defined networking: a survey," in *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm '14)*, pp. 1–8, ACM, Chicago, Ill, USA, 2014.

[3] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A survey of securing networks using software defined networking," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1086–1097, 2015.

[4] G. Carrozza, V. Manetti, A. Marotta et al., "Exploiting SDN approach to tackle cloud computing security issues in the ATC scenario," in *Dependable Computing*, pp. 54–60, Springer, Berlin, Germany, 2013.

[5] H. Zhou, C. Wu, M. Jiang et al., "Evolving defense mechanism for future network security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 45–51, 2015.

[6] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013.

[7] C. Fu, M. Li, Y. Zhang, D. Zou, and L. Han, "A hierarchical virus immunization method for community networks," *China Communications*, vol. 11, no. 9, pp. 148–159, 2014.

[8] T. Lu, K. Zheng, R. Fu, Y. Liu, B. Wu, and S. Guo, "A danger theory based mobile virus detection model and its application in inhibiting virus," *Journal of Networks*, vol. 7, no. 8, pp. 1227–1232, 2012.

[9] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 1, pp. 170–179, 2015.

[10] A. Hellal and L. Ben Romdhane, "Minimal contrast frequent pattern mining for malware detection," *Computers & Security*, vol. 62, pp. 19–32, 2016.

[11] N. Kheir and C. Wolley, "BotSuer: suing stealthy P2P Bots in network traffic through netflow analysis," in *Cryptology and Network Security*, vol. 8257 of *Lecture Notes in Computer Science*, pp. 162–178, Springer, Cham, Switzerland, 2013.

[12] M. Ali and A. B. M. Said, "Securing cloud infrastructure using bayesian predictive analysis against unrecognized malware," in *Proceedings of the 1st International Conference on Modern Communication & Computing Technologies*, 2014.

[13] H. Guo, H. K. Cheng, and K. Kelley, "Impact of network structure on malware propagation: a growth curve perspective," *Journal of Management Information Systems*, vol. 33, no. 1, pp. 296–325, 2016.

[14] L. Feng, X. Liao, Q. Han, and H. Li, "Dynamical analysis and control strategies on malware propagation model," *Applied Mathematical Modelling*, vol. 37, no. 16-17, pp. 8225–8236, 2013.

[15] M. Benaïm and J.-Y. Le Boudec, "A class of mean field interaction models for computer and communication systems," *Performance Evaluation*, vol. 65, no. 11-12, pp. 823–838, 2008.

[16] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security enhancement in wireless mobile networks," *Computer Networks*, vol. 66, pp. 94–101, 2014.

[17] O. Toutonji and S.-M. Yoo, "Passive benign worm propagation modeling with dynamic quarantine defense," *KSII Transactions on Internet and Information Systems*, vol. 3, no. 1, pp. 96–107, 2009.

[18] K. Omote and T. Shimoyama, "Anti-worm-measure parameter determining apparatus, number-of-nodes determining apparatus, number-of-nodes limiting system, and computer product," US, US7926110[P], 2011.

[19] J. T. Bradley, S. T. Gilmore, and J. Hillston, "Analysing distributed Internet worm attacks using continuous state-space approximation of process algebra models," *Journal of Computer and System Sciences*, vol. 74, no. 6, pp. 1013–1032, 2008.

[20] E. Gourdin, J. Omic, and P. Van Mieghem, "Optimization of network protection against virus spread," in *Proceedings of the 8th International Workshop on the Design of Reliable Communication Networks (DRCN '11)*, pp. 86–93, Krakow, Poland, October 2011.

[21] S. Tang and W. Li, "An epidemic model with adaptive virus spread control for Wireless Sensor Networks," *International Journal of Security and Networks*, vol. 6, no. 4, pp. 201–210, 2011.

[22] Z. Abaid, M. Rezvani, and S. Jha, "MalwareMonitor: an SDN-based framework for securing large networks ," in *Proceedings of the 2014 CoNEXT on Student Workshop (CoNEXT Student Workshop '14)*, pp. 40–42, Sydney, Australia, 2014.

[23] K. Ichiro, K. Satoshi, K. Takeyasu et al., "Method for network switching to support investigation of malware with SDN," *Ipsj Sig Technical Reports*, vol. 2014, pp. 1–8, 2014.

[24] S. Hosseini and M. A. Azgomi, "A model for malware propagation in scale-free networks based on rumor spreading process," *Computer Networks*, vol. 108, pp. 97–107, 2016.

[25] S. Hosseini, M. A. Azgomi, and A. T. Rahmani, "Malware propagation modeling considering software diversity and immunization," *Journal of Computational Science*, vol. 13, pp. 49–67, 2016.

[26] L. Pellis, F. Ball, S. Bansal et al., "Eight challenges for network epidemic models," *Epidemics*, vol. 10, pp. 58–62, 2015.

[27] R. M. Anderson and R. M. May, *Infectious Diseases in Humans*, Oxford University Press, Oxford, UK, 1992.

[28] J. C. Wierman and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics and Data Analysis*, vol. 45, no. 1, pp. 3–23, 2004.

[29] J. Marro and R. Dickman, *Nonequilibrium Phase Transitions in Lattice Models*, Cambridge University Press, Cambridge, UK, 1999.

[30] Z. Liu and B. Hu, "Epidemic spreading in community networks," *Europhysics Letters*, vol. 72, no. 2, pp. 315–321, 2005.

[31] J. Chen, H. Zhang, Z.-H. Guan, and T. Li, "Epidemic spreading on networks with overlapping community structure," *Physica A: Statistical Mechanics and Its Applications*, vol. 391, no. 4, pp. 1848–1854, 2012.

[32] Y. Sung, P. Sharma, E. Lopez, and J. Park, "FS-OpenSecurity: a taxonomic modeling of security threats in SDN for future sustainable computing," *Sustainability*, vol. 8, no. 9, article 919, 2016.

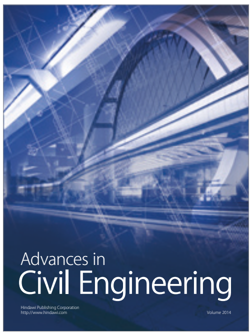
Journal of
Engineering

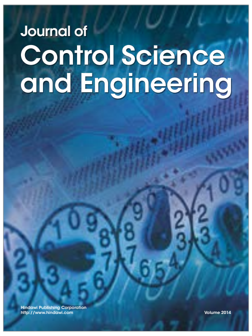
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

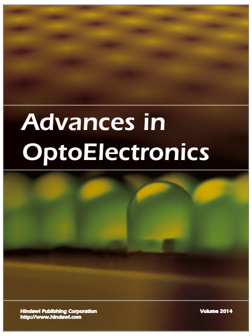
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

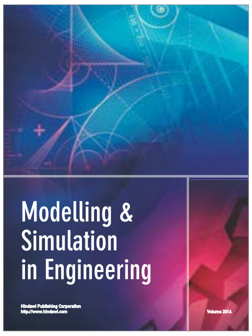
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

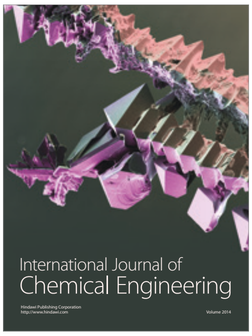

Advances in
OptoElectronics

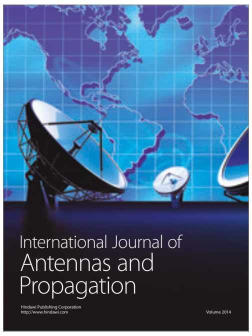
VLSI Design

International Journal of
Navigation and
Observation

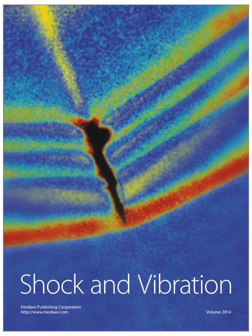

Modelling &
Simulation
in Engineering

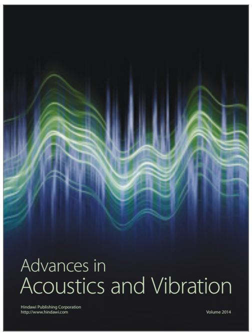
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration