ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201904.00028

Destructive Virus Propagation Model Based on Heterogeneous Mobile Networks (Postprint)

Authors: Liu Chao, Huang Shiwen, Huang Xianying, Liu Xiaoyang, Yang Hongyu

Date: 2019-04-01T00:00:00+00:00

Abstract

To address the problems that existing research has not considered the heterogeneity of mobile network nodes and has not constructed destructive virus propagation models, a destructive virus propagation model based on heterogeneous mobile networks is proposed. By considering the heterogeneity of mobile network nodes, the susceptible state is further divided into new system state and old system state, and combined with the latent and outbreak characteristics of destructive viruses, the infected state is divided into latent state and outbreak state. The equilibrium points and propagation threshold of the model are calculated, and it is pointed out that when the propagation threshold is greater than 1, the model is unstable at the positive equilibrium point; when the propagation threshold is less than 1, the model is locally asymptotically stable at the positive equilibrium point. Simulation comparative experiments are conducted on NW small-world networks and BA scale-free networks, and the simulation results show that the virus propagation speeds in the two networks are different, the NW network exhibits complete elimination of the virus, while the virus in the BA network cannot be completely eradicated.

Full Text

Preamble

Vol. 37 No. 5
Application Research of Computers

Destructive Virus Propagation Model Based on Heterogeneous Mobile Networks

Liu Chao, Huang Shiwen†, Huang Xianying, Liu Xiaoyang, Yang Hongyu

(College of Computer Science & Engineering, Chongqing University of Technology, Chongqing 400054, China)

Abstract: Existing research on mobile virus propagation has largely overlooked node heterogeneity in mobile networks and failed to construct models specifically for destructive viruses. To address these gaps, this paper proposes a destructive virus propagation model based on heterogeneous mobile networks. By accounting for node heterogeneity, the susceptible state is further divided into new-system and old-system states. Additionally, considering the latent and explosive characteristics of destructive viruses, the infected state is partitioned into latent and burst states. We derive the model' s equilibrium points and propagation threshold, demonstrating that the model is unstable at the positive equilibrium when the propagation threshold exceeds 1, and locally asymptotically stable when the threshold is below 1. Simulation experiments conducted on NW small-world and BA scale-free networks reveal distinct propagation speeds: the NW network can achieve complete virus elimination, whereas the BA network cannot.

Key words: heterogeneous mobile network; destructive virus; propagation model

0 Introduction

With the proliferation of mobile smart devices, viruses have increasingly targeted mobile terminals and networks. Various attack behaviors—including malicious billing, system destruction, data theft, and resource consumption—have inflicted substantial losses on mobile network users [**?**, **?**, **?**, **?**]. The continuous emergence of mobile viruses has drawn widespread societal attention and opened new research directions for network virus propagation modeling.

Researchers worldwide have conducted extensive studies on mobile virus propagation modeling, yielding fruitful results. For instance, Zhang et al. [**?**] investigated Hopf bifurcation in an SEIRS-V model with worm propagation in wireless sensor networks. Xiao et al. [**?**] proposed an SEIQR worm propagation model in Wi-Fi environments where infected nodes could be quarantined via Wi-Fi base stations to prevent worm diffusion. Nallusamy et al. [**?**] introduced a node-energy-based Bluetooth virus propagation model (NBV) to simulate and compare relationships among virus propagation, node energy, and network traffic.

Although these models effectively characterize virus propagation in mobile networks, most assume homogeneous mobile networks. However, studies have shown that real-world mobile networks exhibit heterogeneous characteristics [**?**]. In recent years, scholars have begun examining virus propagation models for heterogeneous mobile networks. Zhai et al. [**?**] considered file-download-based infection mechanisms and proposed a new model for HY worm analysis. Guo et

al. [?] incorporated factors such as connection probability, open probability, host defense, and CRC in heterogeneous networks to develop an H-worm simulation model. Huang et al. [?] considered Bluetooth network connectivity characteristics, heterogeneity, anti-virus strategies, and human behavior influences to propose a virus propagation model for heterogeneous Bluetooth communication networks.

Nevertheless, existing research on heterogeneous mobile networks suffers from two key limitations:

a) Neglect of node heterogeneity. In reality, uninfected nodes in mobile networks exhibit varying immunity levels due to security software differences [?, ?]. For example, Guo et al. [?] integrated the Internet and mobile communication networks as a heterogeneous structure and analyzed structural heterogeneity, but their model did not consider node heterogeneity. They categorized all virus-susceptible mobile devices into a single state, which fails to accurately represent the intrinsic characteristics of mobile devices during virus propagation.

b) Lack of research on destructive viruses. Destructive viruses represent an extremely virulent class of malware that possesses both latent and burst states. The latent state focuses on infecting other nodes, while the burst state implements destruction. Such viruses can infect thousands of devices overnight, severely threatening network security [?, ?]. However, studies [?, ?, ?] typically do not differentiate between latent and burst states, often ignoring the latent phase entirely. They simplistically classify devices with latent infections as susceptible nodes and those with burst infections as infected nodes. Consequently, existing propagation models cannot reflect the propagation behavior of destructive viruses or reveal their intrinsic patterns.

To address these limitations, this paper employs propagation dynamics and complex network theory to propose a destructive virus propagation model for heterogeneous mobile networks, considering both the varying immunity levels of mobile devices and the latent/explosive nature of destructive viruses. We calculate the model' s equilibrium points and propagation threshold, prove local stability, conduct comparative simulation experiments on NW small-world and BA scale-free networks, and propose strategies for suppressing virus propagation in mobile networks.

---

1 Model Establishment

Destructive viruses exploit vulnerabilities in system or application software for propagation and destruction. Security software with virus scanning capabilities can protect mobile devices [?]. However, security software quality varies significantly, leading to substantial differences in protection levels and thus node immunity—that is, network node heterogeneity. Destructive virus infection comprises two phases: a latent period for infecting other nodes and a burst period

for implementing destruction [**?**].

Based on this analysis, we classify mobile network nodes into four states:

a) Old-system state (O): Nodes with low immunity, denoted as O nodes.
b) New-system state (N): Nodes with high immunity, denoted as N nodes.
c) Latent state (L): The pre-burst latent phase aimed at maximizing infection, denoted as L nodes.
d) Burst state (B): The destructive burst phase, denoted as B nodes.

Unlike traditional models, the ONLB model accounts for node heterogeneity by dividing susceptible nodes into new-system and old-system states to reflect immunity differences. It also considers both latent and burst states of destructive viruses.

The state transition diagram for the destructive virus model is shown in [Figure 1: see original paper]. Model assumptions are:

a) Old-system or latent node users may patch vulnerabilities or perform virus scans, causing each old-system or latent node to become a new-system node at constant probability α.

b) As system versions update and new vulnerabilities emerge, each new-system node becomes an old-system node at constant probability β if vulnerabilities remain unpatched.

c) Due to destructive virus intrusion, an old-system node becomes latent at constant probability γ_1 upon contact with a latent node.

d) A new-system node becomes latent at constant probability γ_2 upon contact with a latent node.

e) Due to the virus incubation period, each latent node transitions to burst state at constant probability σ.

f) As burst nodes exhibit obvious infection symptoms, users perform vulnerability patching and virus scanning, causing each burst node to become a new-system node at constant probability μ.

To incorporate node degree information in the complex network ONLB model, we jointly classify nodes by state and degree. Let $O_k(t)$, $N_k(t)$, $L_k(t)$, and $B_k(t)$ represent the proportions of degree-k old-system, new-system, latent, and burst nodes at time t, respectively. The differential dynamical system for the ONLB model is:

$$\begin{cases} \frac{dO_k(t)}{dt} = -\beta O_k(t) - \alpha O_k(t) + \gamma_1 \phi_k(t) O_k(t) + \mu L_k(t) \\ \frac{dN_k(t)}{dt} = \beta O_k(t) - \gamma_2 \phi_k(t) N_k(t) - \alpha N_k(t) + \mu B_k(t) \\ \frac{dL_k(t)}{dt} = \gamma_1 \phi_k(t) O_k(t) + \gamma_2 \phi_k(t) N_k(t) - \sigma L_k(t) \\ \frac{dB_k(t)}{dt} = \sigma L_k(t) - \mu B_k(t) \end{cases}$$

where $\phi_k(t)$ represents the conditional probability that a degree-k node connects to a degree-m node. In degree-uncorrelated networks, $\phi_k(t) = \sum_m p(m|k)L_m(t)$, with $p(m|k) = mp(m)/\langle k\rangle$ being the degree distribution function and $\langle k\rangle$ the average network degree. $\phi_k(t)$ denotes the total effective contact time of degree-k latent nodes per unit time, assuming equal contact duration per edge. Taking $\phi_k(t) = k\Theta(t)$ where $\Theta(t) = \sum_m mL_m(t)/\langle k\rangle$, the system becomes:

$$\begin{cases} \frac{dO_k(t)}{dt} = -\beta O_k(t) - \alpha O_k(t) + \gamma_1 k\Theta(t)O_k(t) + \mu L_k(t) \\ \frac{dN_k(t)}{dt} = \beta O_k(t) - \gamma_2 k\Theta(t)N_k(t) - \alpha N_k(t) + \mu B_k(t) \\ \frac{dL_k(t)}{dt} = \gamma_1 k\Theta(t)O_k(t) + \gamma_2 k\Theta(t)N_k(t) - \sigma L_k(t) \\ \frac{dB_k(t)}{dt} = \sigma L_k(t) - \mu B_k(t) \end{cases}$$

The global densities are $O(t) = \sum_m p(m)O_m(t)$, $N(t) = \sum_m p(m)N_m(t)$, $L(t) = \sum_m p(m)L_m(t)$, and $B(t) = \sum_m p(m)B_m(t)$, representing average proportions of old-system, new-system, latent, and burst nodes at time t.

Assuming a normalized system, the state distribution across different degrees satisfies:

$$O_k(t) + N_k(t) + L_k(t) + B_k(t) = 1$$

Thus, the initial condition for system (2) is:

$$O_k(0) = O_k^0 \geq 0, \quad N_k(0) = N_k^0 \geq 0, \quad L_k(0) = L_k^0 \geq 0, \quad B_k(0) = B_k^0 \geq 0$$

where O_k^0, N_k^0, L_k^0, and B_k^0 are the average initial proportions of degree-k old-system, new-system, latent, and burst nodes.

---

2 Model Analysis

This section presents theoretical analysis of the proposed model, including calculation of the propagation threshold [**?**], equilibrium points, and stability proof [**?**]. We first derive the propagation threshold from the existence condition of positive equilibrium.

Setting the right-hand side of system (2) to zero yields the equilibrium equations:

$$\begin{cases} -\beta O_k - \alpha O_k + \gamma_1 k\Theta O_k + \mu L_k = 0 \\ \beta O_k - \gamma_2 k\Theta N_k - \alpha N_k + \mu B_k = 0 \\ \gamma_1 k\Theta O_k + \gamma_2 k\Theta N_k - \sigma L_k = 0 \\ \sigma L_k - \mu B_k = 0 \\ O_k + N_k + L_k + B_k = 1 \end{cases}$$

From these equations and $L = \sum_m p(m)L_m$, we obtain:

$$L = \frac{\gamma_1 k\Theta O_k + \gamma_2 k\Theta N_k}{\sigma}$$

and

$$\Theta = \frac{\langle k\rangle(\gamma_1 O + \gamma_2 N)}{\sigma}\Theta$$

A positive solution exists. The necessary and sufficient condition for a unique positive solution is:

$$\left.\frac{dF(L)}{dL}\right|_{L=0} < 0, \quad F(0) > 0$$

where $F(L)$ is defined as:

$$F(L) = L - \frac{\langle k\rangle(\gamma_1 O + \gamma_2 N)}{\sigma}\Theta$$

This yields the propagation threshold:

$$R_0 = \frac{\langle k^2\rangle(\gamma_1\beta + \gamma_2\alpha)}{\langle k\rangle\sigma(\alpha+\beta)} < 1$$

Theorem 1: When $R_0 < 1$, the disease-free equilibrium $E_0 = \{0, 1, 0, 0\}$ of system (2) is locally asymptotically stable; when $R_0 > 1$, E_0 is unstable, and the virus persists.

Proof: From system (2), we derive the equivalent dynamics:

$$\frac{d\mathbf{x}}{dt} = J\mathbf{x}$$

where J is the Jacobian matrix:

$$J = \begin{pmatrix} -\beta-\alpha+\gamma_1 k\Theta & 0 & \mu & 0 \\ \beta & -\gamma_2 k\Theta-\alpha & 0 & \mu \\ \gamma_1 k\Theta & \gamma_2 k\Theta & -\sigma & 0 \\ 0 & 0 & \sigma & -\mu \end{pmatrix}$$

The eigenvalues are $\lambda_1 = -\beta-\alpha$, $\lambda_2 = -\mu$, and $\lambda_3 = -\sigma$. When $R_0 < 1$, all eigenvalues have negative real parts, proving local stability of the disease-free equilibrium. When $R_0 > 1$, positive real parts exist, indicating instability.

3 Simulation Analysis

Real mobile networks may exhibit both small-world and scale-free characteristics [**?**]. We generate two simulation networks to model destructive virus propagation in heterogeneous mobile networks: an NW small-world network and a BA scale-free network. Their topological parameters are listed in Table 1 , structures shown in [Figure 2: see original paper], and degree distributions in [Figure 3: see original paper].

Table 1 Relevant characteristic parameters of each network

Network Name	Node Count	Edge Count	Average Degree	Maximum Degree	Clustering Coefficient	Degree Correlation
NW Small-World	[value]	[value]	[value]	[value]	High	Positive (assortative)
BA Scale-Free	[value]	[value]	[value]	[value]	Low	Negative (disassortative)

The NW small-world network exhibits high clustering, follows a Poisson distribution, has positive degree correlation, and is assortative and homogeneous. The BA scale-free network follows a power-law distribution, has low clustering, negative degree correlation, and is disassortative and heterogeneous.

We conduct three experiments. **Experiment 1** examines temporal evolution of node densities to identify patterns. **Experiment 2** investigates how node immunity heterogeneity affects burst node dynamics. **Experiment 3** combines latent and burst states to study how destructive viruses impact nodes of different degrees. All experiments initialize with 2,490 old-system nodes, 2,490 new-system nodes, 10 latent nodes, and 10 burst nodes, with 2,000 iterations.

Experiment 1: Node Density Evolution

We examine density evolution of old-system, new-system, latent, and burst nodes. Model parameters are set to $\alpha = 0.1$, $\beta = 0.2$, $\gamma_1 = 0.5$, $\gamma_2 = 0.2$, $\mu = 0.8$, $\sigma = 0.5$.

[Figure 4: see original paper] shows that after initial transients, all node densities stabilize. Old-system node density rises rapidly to a peak before declining to steady state. New-system node density drops quickly initially then gradually stabilizes. Latent and burst node densities increase slowly to steady state. Despite equal initial quantities, the stable state contains more old-system nodes, fewer latent nodes, minimal new-system nodes, and very few burst nodes.

Both networks show similar patterns but with key differences. In the NW network, old-system node density $O(t)$ declines slowly after peaking, stabilizing

around iterations 60-70. In the BA network, $O(t)$ drops rapidly then stabilizes by iterations 10-20. Latent and burst nodes stabilize around iterations 40-50 in the NW network but by iterations 5-10 in the BA network. The BA network (non-homogeneous) reaches steady state faster than the NW network (homogeneous), indicating faster propagation in non-homogeneous networks.

Comparing steady-state values, the NW network has more old-system nodes and fewer latent nodes, while the BA network has more latent nodes and fewer old-system nodes. This suggests that although the NW network contains more low-immunity devices, it harbors fewer latent viruses, whereas the BA network —with fewer low-immunity devices—contains more latent viruses.

Experiment 2: Impact of Node Immunity Heterogeneity

Parameters α and β relate to security updates and affect node immunity. We study their impact on burst nodes B. Model parameters: $\gamma_1 = 0.5$, $\gamma_2 = 0.2$, $\mu = 0.8$, $\sigma = 0.5$.

[Figure 5: see original paper] and [Figure 6: see original paper] show final burst node density versus α for different β values. In the NW network, burst nodes can be eliminated entirely, but in the BA network, burst nodes persist for all α and β values. This stems from the small-world network' s epidemic threshold property versus the scale-free network' s lack of such a threshold due to its power-law degree distribution. Thus, in BA networks, no anti-virus measures can completely eradicate the virus.

Further analysis reveals that for fixed β, burst node density decreases as α increases in both networks, showing that timely updates and patching significantly suppress burst viruses. For fixed α, in the NW network, burst density starts low and rises slowly with β, stabilizing when β reaches 0.6-0.7. In the BA network, burst density starts higher, rises faster with β, and stabilizes by $\beta = 0.3 - 0.4$. This indicates that in NW networks, β strongly affects burst nodes—neglecting updates increases infection risk. In BA networks, burst density varies significantly with β only when β is small; for large β, changes are minimal. This suggests that while infrequent updates in BA networks initially increase burst viruses, prolonged neglect yields little further change.

Experiment 3: Impact on Nodes of Different Degrees

Destructive viruses have latent and burst states that infect and damage nodes differently. We study the average time distribution of infection and damage across node degrees. Parameters match Experiment 1.

[Figure 7: see original paper] shows that average infection time increases with node degree in both networks, indicating higher-degree nodes are more likely to be infected. This suggests that connecting to numerous applications increases infection risk, and closing unnecessary background apps can effectively prevent infection.

Comparing networks, in the NW network, infection time increases with degree up to the maximum degree. In the BA network, infection time increases with degree up to 50, then stabilizes at a maximum value. Thus, NW networks show larger variation across degrees, while BA networks show minimal variation for high-degree nodes (>50). The maximum average infection time in the NW network is less than the minimum in the BA network, indicating that BA network nodes suffer more severe infection and damage. This reflects the BA network' s connectivity, where propagation speed and infection time increase with node degree.

Prevention Strategies: Based on these results, we propose: (1) Regularly update system and security software to enhance immunity; (2) Perform timely virus scans and vulnerability patching; (3) Close unused background applications to reduce infection time.

---

4 Conclusion

This paper proposes a destructive virus propagation model for heterogeneous mobile networks. Considering node heterogeneity, we divide uninfected nodes into new-system and old-system states. Accounting for destructive virus latency and explosiveness, we partition infected nodes into latent and burst states. Theoretical analysis shows the model has a locally asymptotically stable disease-free equilibrium whose stability depends on the propagation threshold. Simulations on NW and BA networks demonstrate different propagation speeds: the NW network can eliminate viruses (consistent with theoretical analysis), while the BA network cannot. System updates, virus scanning, and application management effectively suppress propagation. Future work will focus on modeling destructive virus propagation in dynamic networks.

References

[1] Wang Chunxin, Li Xi, Yu Ran, et al. Research on security technology of power mobile intelligent terminal [J]. Information Network Security, 2014(4): 70-77.

[2] Fan Hong, Du Dahai, Wang Guan. Research on key technologies of mobile internet security assessment [J]. ZTE Communications Technology, 2015(3): 38-40.

[3] Lin Xin. Research on sandbox-based android malware detection technology [J]. Electronic Design Engineering, 2016, 24(12): 48-50.

[4] Liu Caixia, Ji Xinsheng, Wu Jiangxing. A mobile communication user data mimetic defense mechanism based on MSISDN virtualization [J]. Journal of Computer Science, 2018, 41(2): 275-287.

[5] Zhang Zizhen, Wang Yougang. Bifurcation analysis for an SEIRS-V model with delays on the transmission of worms in a wireless sensor network [J]. Mathematical Problems in Engineering, 2017, 2017: article ID 9898726.

[6] Xiao Xi, Fu Peng, Dou Changsheng, et al. Design and analysis of SEIQR worm propagation model in mobile Internet [J]. Communications in Nonlinear Science and Numerical Simulation, 2017, 43(2): 341-350.

[7] Nallusamy T, Ravi T. Node energy based virus propagation model for Bluetooth [J]. Journal of Engineering and Applied Sciences, 2018, 13(2): [pages].

[8] Lu Yanling. Research on the transmission of complex network viruses based on human behavior [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2015.

[9] Zhai Lidong, Guo Wei, Jia Zhaopeng, et al. Worm propagation model for heterogeneous network [C]//Proc of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Washington DC: IEEE Computer Society, 2012: 151-154.

[10] Guo Wei, Zhai Lidong, Ren Yunlong, et al. Intelligent heterogeneous network worms propagation modeling and analysis [C]//Computer Science and Its Applications. Dordrecht: Springer, 2012: 515-524.

[11] Huang Fang, Liu Yuanjun, Chen Bo, et al. A virus propagation model for heterogeneous bluetooth networks containing human behavior [J]. Computer Applied Research, 2014, 31(7): 2144-2147.

[12] Li Yong, Hui Pan, Jin Depeng, et al. Optimal distributed malware defense in mobile networks with heterogeneous devices [J]. IEEE Trans on Mobile Computing, 2014, 13(2): 377-391.

[13] Yang Luxing, DRAIEF M, Yang Xiaofan. The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model [J]. Physica A: Statistical Mechanics & Its Applications, 2016, 450: 403-415.

[14] Tian Chang, Zheng Shaoren. Research on computer virus computing model [J]. Journal of Computer Science, 2001, 24(2): 158-163.

[15] Yang Luxing, Yang Xiaofan, Zhu Qingyi, et al. A computer virus model with graded cure rates [J]. Nonlinear Analysis: Real World Applications, 2013, 14(1): 414-422.

[16] Wang Yuchen. Principle of system vulnerability and common attacking methods [J]. Computer Engineering and Application, 2001, 37(3): 62-64.

[17] Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks [J]. Physical Review Letters, 2001, 86(14): 3200-3203.

[18] Liu Junli, Zhang Tailei. Epidemic spreading of an SEIRS model in scale-free networks [J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(8): 3375-3384.

[19] Du Haifeng, Li Shuzhuo, Marcus W F, et al. Research on community structure of small world network and scale-free network [J]. Journal of Physics, 2007, 56(12): 6886-6893.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.