International Journal of Future Generation Communication and Networking
Vol. 9, No. 9 (2016), pp. 35-46
http://dx.doi.org/10.14257/ijfgcn.2016.9.9.04

Bluetooth Worms Propagation in Smartphone Networks with Awareness

Yongwang Gong[1, *] and Haiyu He[2]

[1] *School of Information Engineering, Yancheng Institute of Technology, China*
[2] *Department of Information Technology, Dazhong News Group, China*
**gong_yw@126.com*

Abstract

In order to study impacts of awareness on the propagation of a Bluetooth worm in smartphone networks, a novel propagation model is proposed. In this model, the smartphone network is regarded as a two-layer network composed of a social network layer in which the awareness diffuses and a physical network layer in which the Bluetooth worm propagates. It is shown by theoretical analysis and simulations that: (1) awareness cannot change the propagation threshold, but can mitigate Bluetooth worm in terms of decreasing the propagation speed and the final infection size; (2) the structure of the social network layer has a profound impact on such mitigation effects. That is, for smaller effective infection rate σ, BA structure is always more effective than WS structure; while for larger σ, there exists a critical value of social reinforcement of awareness b_c, beyond which BA structure is more effective than WS structure, or else the reverse is true. In addition, the critical value b_c is larger with σ increasing.

Keywords: *Smartphone, Bluetooth worm, propagation model, Awareness*

1. Introduction

Smartphones, which constantly expands market share, along with the great improvement in functions, have become an integral of people everyday lives. According to the report of IDC (International Data Corporation) in 2014, smartphone shipments reached 1.3004 billion which grows 27.7% compared with that in 2013. Current smartphones provide not only the basic functions such as voice communication, SMS (short messaging service), and MMS (multimedia messaging service), but also Internet applications such as web surfing, online shopping, and email service. However, smartphones are also undergoing more and more attacks by virus/worms (e.g., Cabir and Zombie) and Trojans (e.g., Skulls and Mquito) [1-2]. For example, in 2010, more than 1 million smartphone phone users in China were infected by the Zombie worm [2].

The basic ways of virus/worms propagation are as follows [3]: (1) Through Bluetooth communication. Worms such as Cabir and ComWar can directly contaminate other reachable and vulnerable smartphones by Bluetooth connection. (2) By SMS and MMS. For example, ComWar also spreads by MMS, and Trojan such as FakeToken infects other smartphones by SMS. (3) By connection to Internet. For instance, smartphones often are infected with Trojan when connecting to Internet by using WIFI or 3G/4G technology. (4) Other infection ways such as files copy using USB interface.

Recently, smartphone worm behaviors have been studied in many literatures using complex network theory[4] and basing on classical epidemic models such as SIS (susceptible-infected- susceptible)[5] and SIR (susceptible-infected-recovered)[6] in order to understand the mechanism of worm propagation deeply and further propose the control strategies effectively. For example, Rhodes *et al* presented an opportunistic transmission model for Bluetooth worms in the smartphone network of mobile population [7]. Cheng *et*

ISSN: 2233-7857 IJFGCN

al studied propagation behaviors of the hybrid malware code that can infect other smartphones by means of both Bluetooth and MMS simultaneously [8]. Gao *et al* proposed a two-layer model to characterize the propagation of Bluetooth worm in the geographic network composed of cell towers and the propagation of SMS worm in the logical contact network composed of mobile phones [9]. Ramachandran *et al* formulated a comprehensive analytical model to explore dynamic behaviors of malwares propagation through Bluetooth, WLAN, MMS (or SMS) SMS, and downloads from the Internet [10].

However, in the previous studies, the anti-virus responses of smartphone users have not been considered. In reality, when a new worm occurs, awareness also diffuses among smartphone users, and those who receive the awareness often take some protective measures on their smartphones to reduce the risk of being infected. So, in the present paper, a novel model for describing worm propagation is proposed by incorporating awareness. In our model, the smartphone network is regarded as a two-layer network composed of a social network layer in which awareness diffuses and a physical network layer in which a Bluetooth worm propagates. The results show that awareness cannot change worm propagation threshold, but can decrease the worm propagation speed as well as the final infection size. It is also shown that the structure of social network layer has a profound impact on worm mitigation, and such impact is closely related to the social reinforcement of awareness and the effective infection rate.

It is noted that many epidemic models with awareness have been proposed [6, 11-13]. Different from these studies our work focuses on how the structure of underlying network structure of awareness diffusion influences the Bluetooth dynamics. At the same time, we consider three features of awareness (a kind of information) diffusion (i.e.., memory effects, social reinforcement, and non-redundancy of contacts [14]) when discussing how and to what to extent the awareness diffusion mitigates worm.

2. Network Model

In general, connectivity of smartphones forms a two-layer network [8, 15]. One layer, named is called social network layer, in which the nodes denote smartphone users and the edges represent the social contacts between friends (or coworkers) contact. The other layer is physical network layer characterizing the physical connections between the limited-distance smartphones by using Bluetooth or WIFI. Here we assume that one user only has one smartphone (see Figure1).

In the upper social network layer, the degree of each node is defined as the number of friends (or coworkers) of the node. So this kind of node degree is only related to the social relations of a node, not to its location. If we assume that the social relations of smartphone users are relatively fixed, the upper social network layer can be considered as a static network that each node degree does not change with time evolution.

In the lower physical network layer, the degree of each node represents the number of Bluetooth connections to other nodes (smartphones) within the communication range. This kind of degree is only related to a node location, not to the smartphone user's social contacts. So, the mobility of a smartphone user can change the corresponding node's degree. So the physical network layer corresponds to a dynamical network that its topology structure changes with time evolution. For example, the degree of node in the upper social network layer is 5, and instead 2 in the lower physical network layer.

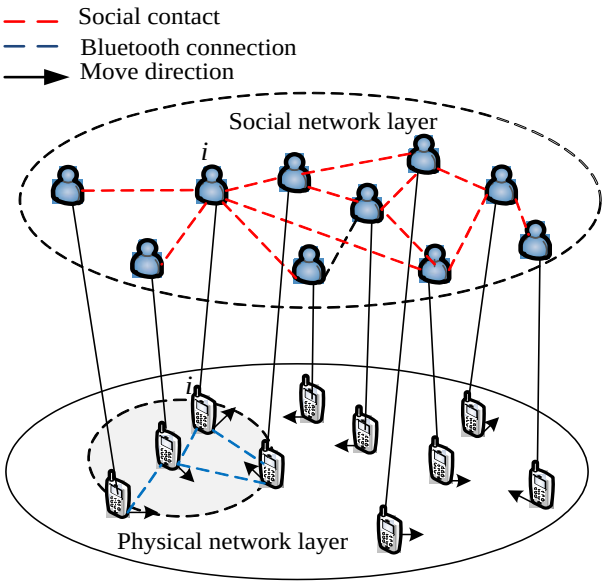

Figure 1. Sketch of a Two-layer Smartphone Network. The Upper Layer (Social Contact) Provides a Vector for Awareness Diffusion, and the Lower Layer (Physical Contact) Corresponds to the Network where the Bluetooth Worm Propagations

3. Propagation Model

3.1. Propagation process

Here assume that a two-layer smartphone network is composed of N nodes. The awareness information diffuses in the upper social network layer and the Bluetooth worm propagates in the lower physical network layer. The coupling dynamics process is as follows: (1) When smartphone i is infected with a Bluetooth worm, it infects the neighboring smartphone through Bluetooth connections in the physical network layer. (2) After a period of time，once the user of smartphone i finds the infection incident, he/she will send awareness information to his/her friends (i.e., neighboring nodes in the social network layer). At the same time, the worm is removed from and the system patches and anti-virus software are installed on smartphone i in case it will be infected again. (3) Smartphone users those who receive the awareness will take some protective measures on their smartphones to reduce the risk of being infected. Repeat steps (1)~(3) until the system evolution reaches the steady state.

3.2. Infection Rate

Here infection rate $q_{ij}(t)$ is defined as worm infection probability along the Bluetooth connection between susceptible smartphone i and infected smartphone j. Clearly, $q_{ij}(t)$ depends on not only the vulnerability of smartphone i but also the infectivity of worm from smartphone j. Similar to Ref. [12], it can be expressed as:

$$q_{ij}(t) = V_i(t)T_j(t),\ 0 < V_i(t) \le 1 \text{ and } 0 < T_j(t) \le 1 \quad (1)$$

where terms $V_i(t)$ and $T_j(t)$ represent the vulnerability of smartphone i and the infectivity from smartphone j at time t, respectively. In general, $T_j(t)$ is only related to the function of a worm rather than the infection source (e.g., smartphone j) and time t. Let $T_j(t)=\beta$, Equation (1) is rewritten as:

$$q_{ij}(t) = \beta V_i(t) \tag{2}$$

Let $V_i(t) = 1$ (maximal value of the vulnerability) correspond to the case of no awareness. In this case, $q_{ij}(t) = \beta V_i(t)$ can be simplified as $q_{ij}(t) = \beta$ which has been discussed in many literatures [7-10].

In following, we focus on the expression of $q_{ij}(t)$ in the case of considering awareness. To this end, two reasonable assumptions are proposed here. One is that awareness diffusion in social network layer can reduce the vulnerability of susceptible smartphones, and another is that awareness diffusion follows three rules [14]: (i) *Memory effects*: smartphone users can remember the total number of their having received awareness information contacts; (ii) *Social reinforcement:* the increasing of awareness information enhances the users' protective reaction; (iii) *Non-redundancy of contacts*: the infected smartphone users send the awareness information to their neighbors only once.

On the basis of above two assumptions, we define that $V_i(t) = e^{-b\varphi_i(t)}$ ($0 \le b \le 1$), where parameter b captures the social reinforcement effect and the memory effect is embodied by $\varphi_i(t)$ (i.e., the cumulative number of smartphone user i receiving awareness by the end of time t). Inserting the expression of $V_i(t)$ into Equation (2), we have

$$q_{ij}(t) = \beta e^{-b\varphi_i(t)} \tag{3}$$

Figure2 shows worm infection rate q as a function of φ for different b . It is easy to see that q gradually becomes smaller with the increasing of parameters φ and b .

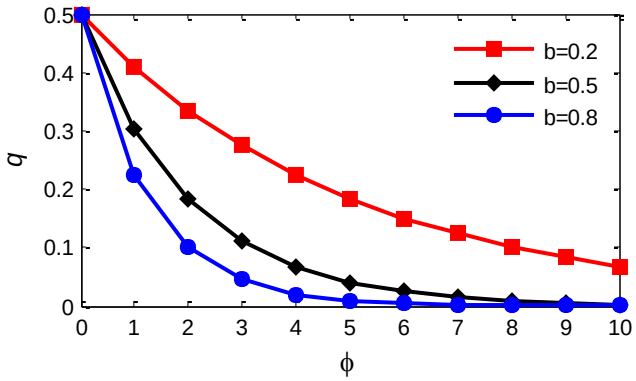

Figure 2. The Impact of Parameters b and ϕ on Worm Infection Rate q with $\beta = 0.5$

3.3. Mathematical Model and Analysis

The worm propagation model is formulated based on the classical epidemic model SIR. In this model, all smartphones are assumed to be one of three states in any time:

Susceptible (*S*): The susceptible smartphones are those who have not been infected by Bluetooth worms, but are vulnerable to Bluetooth worms and could be infected when contacting with an infected smartphone.

Infected (*I*): The infected smartphones are those who carry Bluetooth worms and can infect the susceptible smartphones.

Recovered (*R*): The recovered smartphones are those who used to be infected by Bluetooth worms, and now are clear of the Bluetooth worms and immune to the same type of worm by installing system patches and anti-virus software.

A Bluetooth worm propagates in lower physical network layer by wireless Bluetooth connection established between phones in limited distance. Mobility of phone users impacts connectivity of the physical network. Currently, there are three basic mobility patterns: Random Walk [16], Levy Flight [17], and Random Waypoint [18]. To make an easy for analysis and focus on the impact of awareness on worm propagation, we here consider the simplest mobility pattern of Random Walk described as follows: each phone user i is randomly located position coordinate (x_i, y_i) in a $L\times L$ plane with periodic boundary conditions. In each moving moment, phone user i randomly selects his/her speed and angle from system wide predefined ranges $[v_{min}, v_{max}]$ and $[-\pi, \pi]$ respectively, where v_{min} is the minimum speed and v_{max} is the maximum speed. The mathematical model of Random Walk can be described by:

$$\begin{cases} x_i(t+1) = x_i(t) + v_i \cos\varphi_i(t) \\ y_i(t+1) = y_i(t) + v_i \sin\varphi_i(t) \end{cases} \tag{4}$$

Where ($x_i(t)$, $y_i(t)$) and ($x_i(t+1)$, $y_i(t+1)$) are respectively position coordinates in time step t and time step t+1.

Let $S(t)$, $I(t)$ and $R(t)$ denote respectively the number of the susceptible, the infected, and the recovered phones at time step t with $S(t)+I(t)+R(t)=N$ being a constant. Based on Mean-Field approach and similar to Reference [17], the mathematical model of worm propagation is formulated:

$$\begin{cases} i(t+1) = i(t) + s(t)[1-(1-\beta e^{-b\varphi_i(t)} i(t))^{\alpha}] - \mu i(t) \\ r(t+1) = r(t) + \mu i(t) \\ s(t+1) = \rho - i(t+1) - r(t+1) \\ \varphi_i(t) = f(A) r(t) \end{cases} \tag{5}$$

where $s(t) = S(t)/L^2$, $i(t) = I(t)/L^2$ and $r(t) = R(t)/L^2$ are the density of the susceptible, the infected, and the recovered phones in plane $L\times L$. Exponent $\alpha = \pi r^2$ indicates the area covered by Bluetooth communication with r denoting the communication radius. The value of $\varphi_i(t)$ depends on the social network layer structure A and the infected density $r(t)$ in physical network layer. Near the critical point ($i(t) = 1$), we Taylor expand the first sub-equation in Equation (5) and ignore the high order terms to derive the following equation.

$$i(t+1) = i(t) + \beta\pi r^2 e^{-b\varphi_i(t)} s(t) i(t) - \mu i(t) \tag{6}$$

Inserting the fourth sub-equation in Equation (5) into Equation (6), we obtain

$$i(t+1) = i(t) + \lambda\pi r^2 e^{-bf(A)r(t)} s(t) i(t) - \mu i(t) \tag{7}$$

In fact, in the initial time step $t=0$, we have $s(0) \approx \rho = N/L^2$ and $r(0)=0$. If $i(1) > i(0)$, the Bluetooth worm will break out finally, or it will die out. Thus, we derive a critical propagation threshold:

$$\sigma_c = \frac{1}{\pi r^2 \rho} \tag{8}$$

where $\sigma = \beta/\mu$ is called effective infection rate [12,16].

It can be seen from Equation (8) that awareness diffusion cannot alert the propagation threshold.

4. Simulation Results

To validate the theoretical results obtained in Section 3, we have performed some Monte Carlo simulations on two-layer networks. Firstly, two two-layer networks are created with each network size $N = 1000$. The two networks have the same physical network layer that corresponds to a random dynamical network, and the distinct

social network layers with the same averaged degree of nodes (one is BA free-scale network and the other is WS small network).

For WS network, we set the reconnected probability $p = 0.2$ and the averaged degree $\langle k \rangle = 6$. The method of creating WS network can be found in Ref [19]. For BA network, we set $m_0 = m = 3$, where m_0 is the initial size of the network and m denotes the number of added edges in each step. Thus the final created BA network has the averaged degree $\langle k \rangle \approx 6$. The method of creating BA network can be found in Ref [20].

In our simulations, the communication radius of Bluetooth protocol $r = 1$, and the number of initial infected smartphones $I(0)$=10 if not otherwise specified. In the initial step, 1000 smartphones are random located in a $L \times L$ two-dimensional plane with periodic boundary conditions. In the following time steps, each smartphone i randomly moves with a velocity v_i drawn uniformly from $[v_{min}, v_{max}]$.

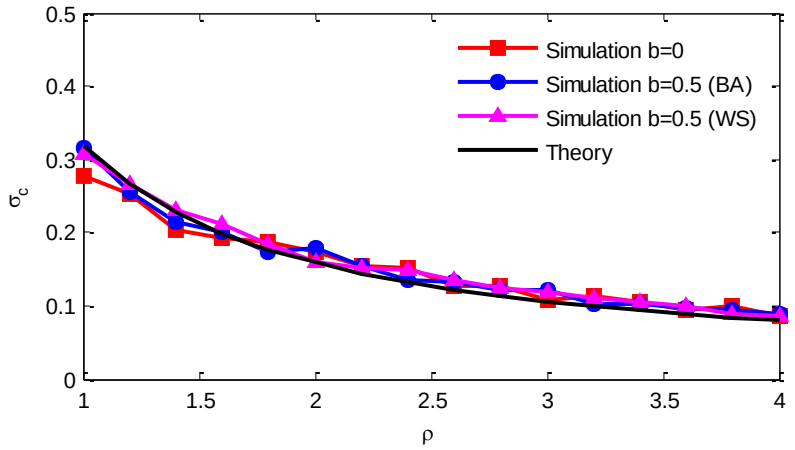

Figure 3. Theoretical Threshold Versus Simulated Thresholds ($\mu = 0.05$, v_{min}=0 and v_{min}=L)

Figure 3 compares the comparison of the propagation threshold obtained by MC simulations with that the numerical solution of Equation (8). To be clear, b=0 corresponds to the case of no awareness. From Figure 3, we can see that the simulated curves almost agree with the theoretical curve regardless of considering awareness ($b \neq 0$) or not (b=0) and the structure of social network layer is WS or BA. This validates the result that awareness cannot change the worm propagation threshold.

To explore worm behaviors with awareness above threshold ($\sigma > \sigma_c$), we further perform MC simulations with parameters $L = 50$, $\lambda = 0.5$, $\beta = 0.5$, $\mu = 0.01$, v_{min}=0 and v_{max}=50. In this case, we have σ=50 and $\sigma_c \approx 0.8$.

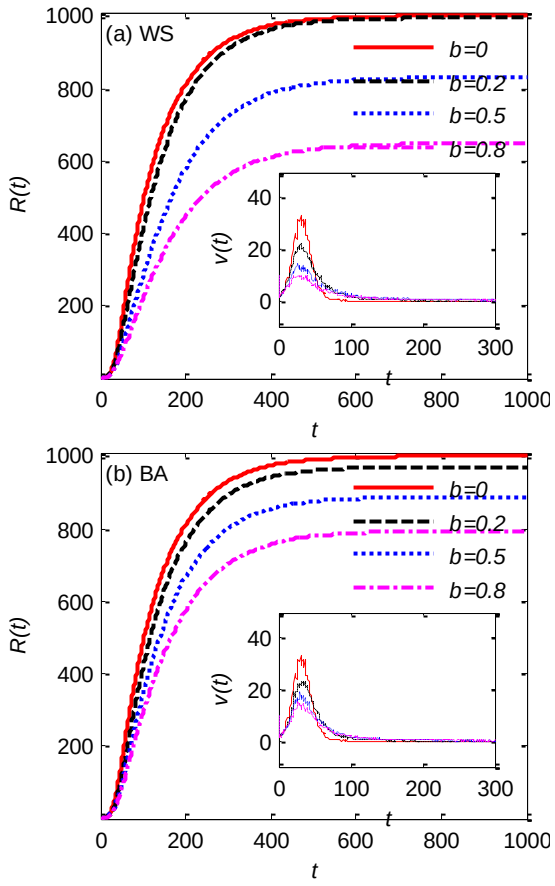

Figure 4. Time Evolution of $R(t)$ and $v(t)$

In Figure 4, we show that the time evaluation of the infection size $R(t)$ and the worm propagation speed $v(t)$ ($v(t)=I(t)+R(t)-(I(t-1)+R(t-1))$) for given different b ((a) awareness diffusion on WS network; (b) awareness diffusion on BA network).

The values of $R(t)$ and $v(t)$ in the case of considering awareness diffusion ($b \neq 0$) are always smaller than those in the case of no awareness ($b=0$) whether the social network layer is WS network (Figure 4 (a)) or BA network (Figure 4 (b)). This means that awareness diffusion can mitigate Bluetooth worm in terms of decreasing the propagation speed and infection size. It is also shown that the larger the social reinforcement b is, the better such worm mitigation effect is.

Moreover, we compare time evolution of $R(t)$ and $v(t)$ for b =0.2 and 0.5 when awareness diffuses respectively on BA network and WS network. Note that when b =0.2, values of $R(t)$ and $v(t)$ affected by BA network are lower than those affected by WS. So we can say awareness diffusing on BA network layer mitigates worm better than on WS network (see Figure 5 (a)). However, with the increasing of b (b =0.5), the reverse is true (see Figure 5 (b)). In other words, there exists a critical value of b leading to the emergence of phase transition on worm mitigation effect.

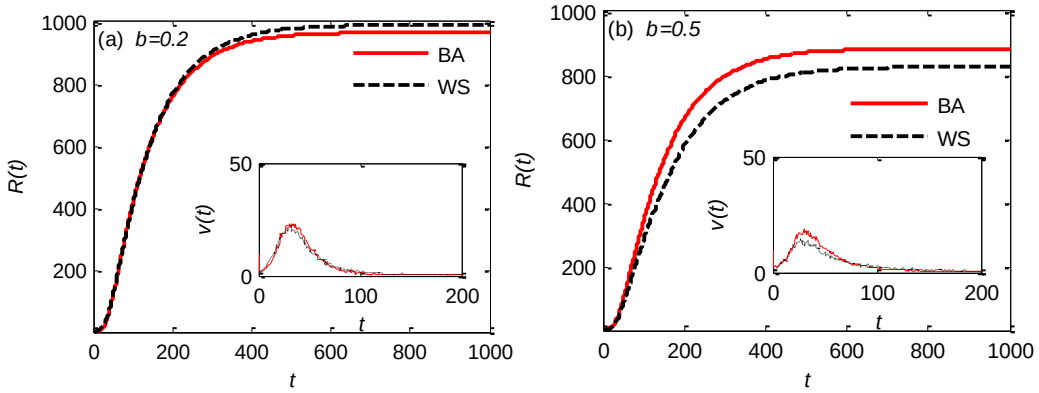

Figure 5. The Impact of Social Network Layer Structure on $R(t)$ and $v(t)$ (the Inset)

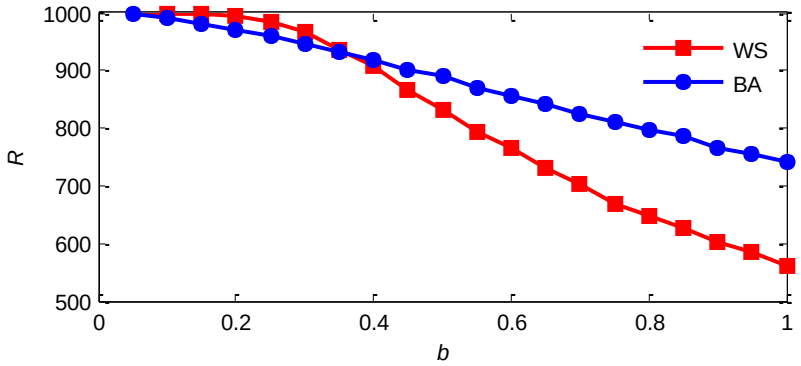

Figure 6. The Final Infection Size as a Function of the Social Reinforcement b

In order to derive the critical point, In Figure 6, we further report how the final infection size R changes with the social reinforcement b. Clearly, the infection curve affected by WS network drops slowly in the case of $b<0.3$, but drops fast (almost exponential speed) when $b>0.3$. By contrast, the infection curve affected by BA network always decline slowly (almost linear relationship). As a result, the two curves intersect at point $b\approx 0.35$ meaning the critical value of b is about 0.35. This indicates that worm mitigation effect relates to not only the social network structure but also the values of social reinforcement b.

Here we stress that the curves in Figure 6 are derived in the case σ=50. To further understand deeply the general result, more simulations are made in Figure 7 for more general values of $\sigma>\sigma_c$.

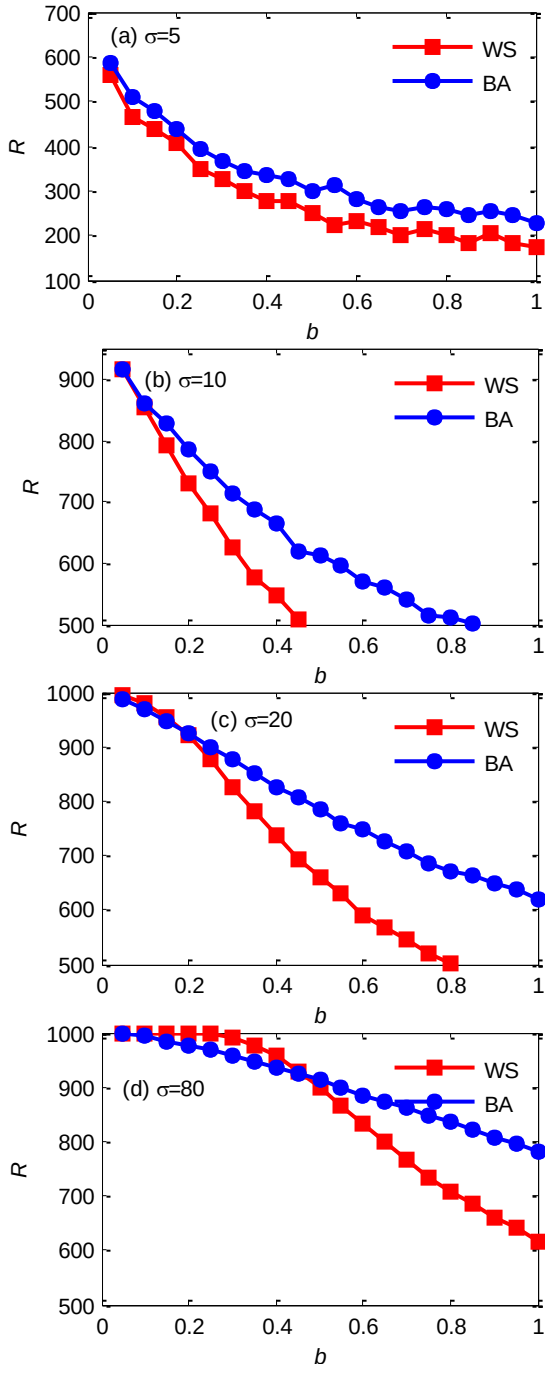

Figure 7. Final Infection Size as a Function of the Social Reinforcement b for different β

As Figure7 shows, for the smaller σ (e.g., σ=5 in Figure 7(a)), BA structure always has better mitigation effect than WS structure no matter b being any value. However, with the increasing of σ value, there exists a critical value b_c, below which BA structure is more effective, and above which the WS structure is more effective (see Figure 7 (b)-Figure 7 (d)). Moreover, the larger σ value is, the larger b_c value is. Therefore, when evaluating how the topological structure of the underlying social network layer of awareness diffusing influences the mitigation effect, the factors of both social reinforcement b and effective infection rate σ must be considered.

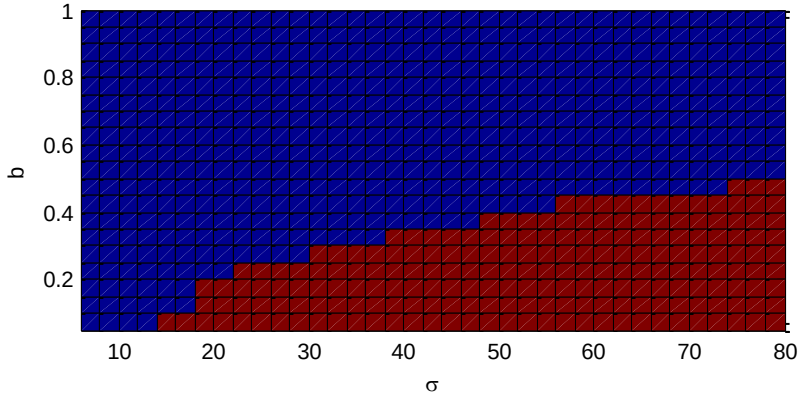

Figure 8. Comparison of Worm Mitigation Effect between WS Structure and BA Structure

To derive a general result of b_c, we introduce quantity ΔR as follows:

$$\Delta R = \frac{R_{\mathrm{WS}} - R_{\mathrm{BA}}}{R_{\mathrm{BA}}} = \frac{R_{\mathrm{WS}}}{R_{\mathrm{BA}}} - 1 \tag{9}$$

Where R_{WS} and R_{BA} are respectively the final infection size impacted by WS network and that by BA network. So, $\Delta R > 0$ means that BA network has the better worm mitigation effect than WS network. Otherwise (i.e., $\Delta R < 0$), the opposition is true. In Figure8, we report ΔR as a function of b and σ where the blue color denotes $\Delta R < 0$ and red color denotes $\Delta R < 0$. We also can draw the same conclusions as that from Figure7.

5. Conclusion

In this paper, we have proposed a novel propagation model to character the coupled dynamical process of Bluetooth worm and awareness on a two-layer smartphone network. One layer is the social network layer in which awareness diffuses and the other is the physical network layer in which the Bluetooth worm propagates. We have shown that awareness diffusion cannot change the propagation threshold, but can mitigate its propagation in terms of decreasing propagation speed and the final infection size. More important, we also have fond that the social network layer structure in which awareness diffuses has a great impact on worm mitigation: (a) BA structure is always more effective on worm mitigation than the WS structure for smaller effective infection rate; (b) there exists a critical value of the social reinforcement for larger effective infection rate, beyond which BA structure is more effective than WS structure, or else the reverse is true; (c) the critical value gradually becomes larger with the transmission rate increasing.

The present finding points out the importance of considering awareness on modeling correctly Bluetooth worms' propagation in smartphone networks. Note that our results, exception to the propagation threshold, are mainly obtained using Monte-Carlo simulations due to complexity of theoretical analysis. So how to derive more theoretical results is our future work.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61374180, 61373136), Science and Technology Support Program of Jiangsu Province in China (Grant No. BE201467)

References

[1] S. Coursen, "The future of mobile malware, Network Security", vol. 8, **(2007)**, pp. 7-11.
[2] S. Peng, S. Yu and A. Yang, "Smartphone Malware and Its Propagation Modeling: A Survey", IEEE Communications Surveys & Tutorials, vol. 16, no. 2, **(2014)**, pp. 925-941.
[3] H. N. Nguyen, Y. Ohara and Y. Shinoda, "A stochastic framework to depict viral propagation in wireless heterogeneous networks", IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum, **(2010)**.
[4] S. N. Dorogovtsev, "Lectures on Complex Networks", Oxford University Press, New York, **(2010)**.
[5] H. W. Hethcote, "The mathematics of infectious diseases", SIAM review, vol. 42, no. 4, **(2000)**, pp. 599-653.
[6] Y. W. Gong, Y. R. Song and G. P. Jiang, "Epidemic spreading in scale-free networks including the effect of individual's vigilance", Chinese Physics B, vol. 21, no. 1, **(2012)**.
[7] C. J. Rhodes and M. Nekovee, "The opportunistic transmission of wireless worms between mobile devices", Physica A, vol. 387, no. 27, **(2008)**, pp. 6837-6844.
[8] S. M. Cheng, W. C. Ao, P. Y. Chen and K. C. Chen, "On modeling malware propagation in generalized social networks", IEEE Communications Letters, vol. 15, no. 1, (2011), pp. 25-27.
[9] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation", IEEE Transaction on Mobile Computing, vol. 12, no. 3, **(2013)**, pp. 529-541.
[10] K. Ramachandran and B. Sikdar, "Modeling malware propagation in networks of smart cell phones with spatial dynamics", INFOCOM 2007 26th IEEE International Conference on Computer Communications, **(2007)**.
[11] S. Funk, E. Gilad, C. Watkins and V. A. Jansen, "The spread of awareness and its impact on epidemic outbreaks", Proceedings of the National Academy of Sciences, vol. 106, no. 16, **(2009)**, pp. 6872-6877.
[12] Q. Wu, X. Fu, M. Small and X. J. Xu, "The impact of awareness on epidemic spreading in networks", Chaos, vol. 22, no. 1, **(2012)**.
[13] Y. L. Lu, G. P. Jiang and Y. R. Song, "Epidemic spreading on a scale-free network with awareness", Chinese Physics B, vol. 21, no. 10, **(2012)**.
[14] L. Lü, D. B. Chen and T. Zhou, "The small world yields the most effective information spreading", New Journal of Physics, vol. 13, no. 12, **(2011)**.
[15] X. Wei, N. C. Valler, M. Faloutsos, I. Neamtiu, B. A. Prakash and C. Faloutsos, "Smartphone viruses propagation on heterogeneous composite networks", Proceedings of the 2013 IEEE 2nd International Network Science Workshop, **(2013).**
[16] A. Buscarino, L. Fortuna, M. Frasca and V. Latora, "Disease spreading in populations of moving agents", Europhysics Letters, vol. 82, no. 3, **(2008)**.
[17] I. Rhee, M. Shin, S. Hong, K. Lee, S. J. Kim and S. Chong, "On the levy-walk nature of human mobility", IEEE/ACM Transactions on Networking, vol. 19, no. 3, **(2011)**, pp. 630-643.
[18] N. C. Valler, B. A. Prakash, H. Tong, M. Faloutsos and C. Faloutsos, "Epidemic spread in mobile ad hoc networks: Determining the tipping point", NETWORKING 2011, **(2011)**, pp. 266-280.
[19] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks", Nature, vol. 393, no. 6684, **(1998)**, pp. 440-442.
[20] A. L. Barabási and R. Albert, "Emergence of scaling in random networks, Science, vol. 286, no. 5439 **(1999)**, pp. 509-512.

Authors

Yangwang Gong, He received M.S. degree in computer science from Information Engineering University, Zhengzhou, China, in 2005, and the Ph.D. degree from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2014. He is currently an associate professor of Yancheng Institute of Technology, Yanchen, China. His main research interests are information security, and complex network theory.

Haiyu He, He received M.S. degree in computer science from Information Engineering University, Zhengzhou, China, in 2005. He is currently an engineer of Dazhong News Group, Jinan, China. His main research interests are information security, and computer networks.