Understanding the spread of malicious mobile-phone programs and their damage potential

Citation: Wang, Pu, Marta C. González, Ronaldo Menezes, and Albert-László Barabási. "Understanding the spread of malicious mobile-phone programs and their damage potential." International Journal of Information Security 12:5 (October 2013), pp. 383-392.

As Published: http://dx.doi.org/10.1007/s10207-013-0203-z

Publisher: Springer Berlin Heidelberg

Persistent URL: http://hdl.handle.net/1721.1/103101

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Noname manuscript No.
(will be inserted by the editor)

Understanding the Spread of Malicious Mobile-phone Programs and their Damage Potential

Pu Wang · Marta C. González · Ronaldo Menezes · Albert-László Barabási

Received: date / Accepted: date

Abstract The fast growing market for smart phones coupled with their almost constant on-line presence makes these devices the new targets of malicious code (virus) writers. To aggravate the issue, the security level of these devices is far below the state-of-the art of what is used in personal computers. It has been recently found that the *topological* spread of MMS (Multimedia Message Services) viruses is highly restricted by the underlying fragmentation of the call graph—the term *topological* here refers to the explicit use of the call graph topology to find vulnerable phones. In this paper, we study MMS viruses under another type of spreading behavior that locates vulnerable phones by generating a random list of numbers to be contacted: generally referred to as *scanning*. We find that hybrid MMS viruses including some level of scanning are more dangerous to the mobile community than their standard topological counterparts. Interestingly, this paper shows that the topological and scanning behaviors of MMS viruses can be more damaging in high and low market-share cases respectively. The results also show that given sufficient time, sophisticated viruses may infect a large fraction of susceptible phones without being detected. Fortunately, with the improvement of phone providers' monitoring ability and the timely installations of patches on infected phones, one can contain the spread of MMS viruses. Our findings lead to a better understanding on how one could prevent the spread of mobile-phone viruses even in light of new behaviors such as scanning.

Keywords Mobile-phone Viruses · Social Networks · Mobile Security

Pu Wang
School of Traffic and Transportation Engineering
Central South University, Changsha, P.R. China
E-mail: wangpu@csu.edu.cn

Marta González
Department of Civil and Environmental Engineering
Massachusetts Institute of Technology, Cambridge, USA
E-mail: martag@mit.edu

Ronaldo Menezes
BioComplex Laboratory
Department of Computer Sciences
Florida Institute of Technology, Melbourne, USA
E-mail: rmenezes@cs.fit.edu

Albert-László Barabási
Center for Complex Network Research
Department of Physics, Biology and Computer Science
Northeastern University, Boston, USA
E-mail: barabasi@neu.edu

1 Introduction

The history of technological viruses is intrinsically linked to the history of computational devices. Since the creation of the Internet, programmers began writing self-replicating executables with malicious purpose to: cause harm to computers, destroy information from computers, and profit from information stored in such devices. The infamous Creeper[1] is the first known instance of a computer virus. From there on, the field of computer security improved significantly but unfortunately so did the ability of programmers to write increasingly more sophisticated viruses. In recent years, mobile phones have become the new frontier for these self-replicating programs [16, 22, 14]. The availability of these mobile devices coupled with their constant on-line presence makes them an ideal breeding ground for technological viruses [16]. Mobile-phone viruses can steal user's private information [9, 14], drain handset's battery [14], track user's locations by GPS [26], to name but a few.

[1] http://en.wikipedia.org/wiki/Creeper_virus

They can infect a large number of mobile phones in stealth mode and later make these infected phones perform some simple malicious functions, such as sending short text messages to get the communication channels jammed [13].

Mobile-phone viruses are able to self-replicate and spread quickly. Similarly to their biological counterparts, they can spread based on physical proximity, when they use Bluetooth communication; and like PC viruses, they can spread by either targeting individuals in the address books of the infected phones (topological behavior), or by randomly selecting contacts/phone numbers to be contacted (scanning behavior) [21]. The pursuit to fully understand the spread dynamics of mobile-phone viruses and their damage potential starts with the introduction of spreading models; many have been proposed in the literature. Mickens and Nobel [18] proposed an epidemiological framework to model the topological properties of mobile networks. Su et al. [23] used trace-drive simulations to examine the propagation dynamics of Bluetooth worms; they found that Bluetooth worms can quickly infect a large population of susceptible devices. Yan et al. [27] used logistic equation to characterize the propagation dynamics of Bluetooth worms. Wang et al. [24] and Funk et al. [12] studied the important role of human mobility in the spread of Bluetooth viruses. Based on real mobile-phone data, Wang et al. [25] studied different spreading patterns of Bluetooth and MMS viruses; they predicted that once a mobile operating system's market share reaches a phase transition point, MMS viruses will become a serious threat to users.

Researchers also investigated the strategies to monitor or restrain the propagations of mobile-phone viruses. Cheng et al. [9] studied the approach to detect abnormal message sending behavior by collecting and sending communication data to remote servers. Bose et al. [2] proposed an approach to distinguish malicious behavior from normal operations through training a classifier based on support vector machines. Kim et al. [15] looked into a methodology to detect malware by monitoring battery-lifetime. Zhu et al. [28] studied counter-mechanisms to contain the propagation of a mobile worm at the earliest stage by patching an optimal set of selected phones. This counter-mechanism continually extracts a social relationship graph between mobile phones, which is representative of the most likely propagation path of a mobile worm. Gao et al. [13] studied a two-layer network for modeling virus propagation in mobile networks and designed a pre-immunization and adaptive patch dissemination strategy to restrain mobile virus propagation.

The spreading dynamics of mobile-phone viruses has been amply studied in recent years. However, previous works normally use a topological approach, ignoring the possibility that a virus can scan random phone numbers. Indeed, the mobile-phone world has already seen instances of scanning behavior such as the Timofonica virus[2] and more recently in a hybrid virus called Beselo[3]. At first glance, random scans seem to be a naive approach but what makes them dangerous is that a few successful scans may transfer the infection from one side of the network to another in a very short amount of time. Figure 1 depicts a scenario with topological and scanning behaviors in a mobile-phone network. Note that part of the network (depicted in light color) could never be reached without the scanning behavior. This simple example demonstrates the difference between topological viruses (which have to respect the existing connections between users) and scanning viruses (which are able to jump to anywhere in the network). We can observe that the topology formed by users having other users' numbers in their address books is not used for the scans (in dashed line). In this paper we study the effects of MMS viruses' topological behavior combined with a scanning behavior. We find that for high market-share mobile operating systems (hence forth called OS), viruses with topological behavior are more effective but for low market-share OS, the ones with some level of scanning behavior cause more harm.

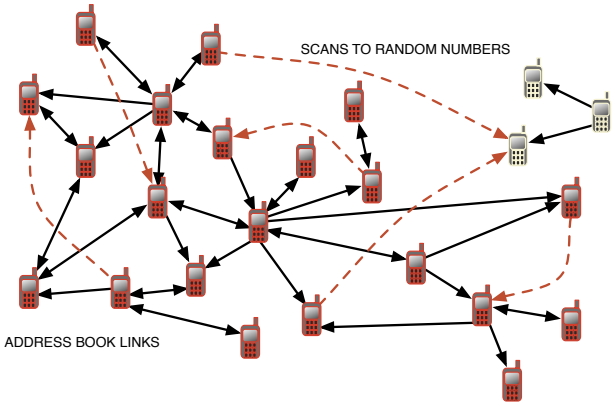

Fig. 1 Virus can contact phones based on the call graph (topological behavior) or generating numbers randomly (scanning behavior). The light-colored phones in this picture could never be reached using only topological behavior.

[2] http://www.kaspersky.com/about/news/virus/2000/TIMOFONICA_Virus_Questions_and_Answers

[3] http://www.f-secure.com/v-descs/worm_symbos_beselo.shtml

Unlike previous works, this paper investigates the interplay between spreading behaviors employed by MMS viruses and the ability that phone providers have to look for anomalies based on messaging volume as a function of time of the day and day of the week. MMS viruses can spread at different rates and this rate can be the difference between their success or failure. Hence we study the spread of viruses under different spreading rates. We find that the most dangerous MMS viruses may not have the fastest spreading rates.

Finally, we discuss two strategies that could be used to mitigate the spread of MMS viruses. First, with an improved monitoring ability on abnormal MMS volume, MMS viruses may be detected at an earlier stage of infection. Second, as expected, we find that the installation of patches on infected phones can help mitigate MMS viruses' potential damages—we discuss a few patching scenarios in this paper.

2 Dataset and Methodology

The dataset used in this paper was collected by a mobile-phone providers for billing and operational purposes during a 12-weeks period. The privacy of all callers is ensured through the use of a security key (hash code) for each user instead of users' real phone numbers.

2.1 Usage Pattern of MMS

We first analysed the use of MMS as form of communication. Figure 2 shows the result of such analysis for the MMS activity of approximately 6 million mobile-phone users over a period of 12 weeks with an average volume of 4.7 million messages per week. The figure shows a periodic usage of MMS peaking from Sunday to Tuesday. This analysis is important because this usage pattern is widely used by mobile-phone providers to protect their communication systems; abnormal usage can be stopped when one has a model of the normal cyclic usage pattern [9,7]. Moreover, in our simulations we assume that mobile-phone providers are able to use the global activity patterns to check for anomalies that may arise from big fluctuations in users' MMS activity. In the inset of Figure 2, we measured the maximum and average MMS volume in different two-hour periods of a week (Figure 2(a)). If the MMS volume generated by the spread of viruses is larger than the volume difference, ΔV, between the maximum and average MMS volume (depicted in the Figure 2(b)), phone providers are able to detect the viruses using simple anomaly detection approaches. In contrast, MMS viruses may spread without being detected if the MMS volume created by them is smaller than ΔV, because phone providers generally regard these slightly higher rates of messages as part of expected fluctuations in users' MMS usage [7].

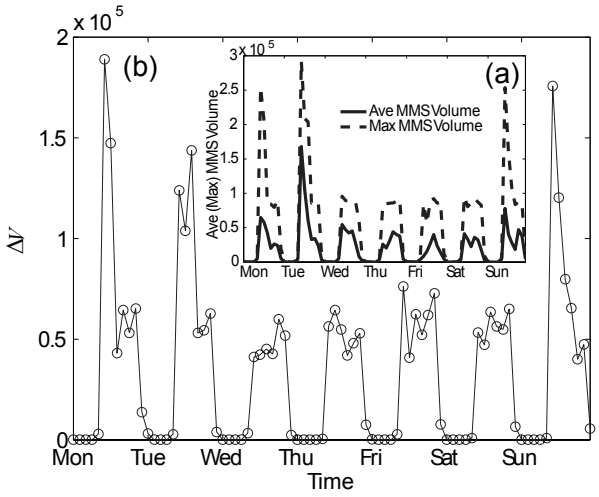

Fig. 2 (a) The maximum and average volume of MMS messages and (b) the threshold of MMS viruses being detected by phone providers.

2.2 SI and SIR Models

In this paper, we first use the SI model [1] to simulate the spread of MMS viruses. Under this model, mobile phones can be in only one of two possible states: susceptible (S) when they are vulnerable to infection, or infected (I) when they are transmitting the infection to other devices. Using the SI model, we study the initial spreading process in the absence of recovery or antiviral software. That is, we do not consider the possibility that the phones could recover from the infection; a reasonable assumption due to the limited capacity of some handsets for installing antiviral software [22,14,9], combined with the users' current lack of concern about the threat of mobile-phone viruses [22,14,9]. In Section 3.4 we also use the SIR model [1] to study the spread of MMS viruses under the scenario where patches can be installed on infected phones. In the SIR model, an infected mobile phone changes from infected state to recovered state (R) after the installation of patches.

In our simulations we assume that a virus does not need the user confirmation to be installed in the device, corresponding to the worst possible spreading scenario. Without confirmation, every phone that receives an infected MMS becomes infected.

In the SI model an infected mobile phone can infect a susceptible phone at a rate μ described by

$$S + I \xrightarrow{\mu} 2I. \quad (1)$$

In the SIR model an infected phone can recover at a rate γ by installing patches.

$$I \xrightarrow{\gamma} R. \quad (2)$$

2.3 Topological and Scanning Behaviors

Two spreading behaviors of MMS viruses are investigated in this paper: viruses behaving topologically send out malicious MMS to the phone numbers listed in its address book; viruses performing scanning send out malicious MMS to randomly generated phone numbers.

In the topological approach, we approximate a user's address book with the list of numbers the user communicated with during the 12 weeks of observation. As shown in Figure 3, the size of user's address book N follows a power-law distribution defined as $P(N) = N^{-\lambda}$ with an exponent $\lambda = 4.5$. The measured average address book size $\langle N \rangle$ is 9.17 (Figure 3).

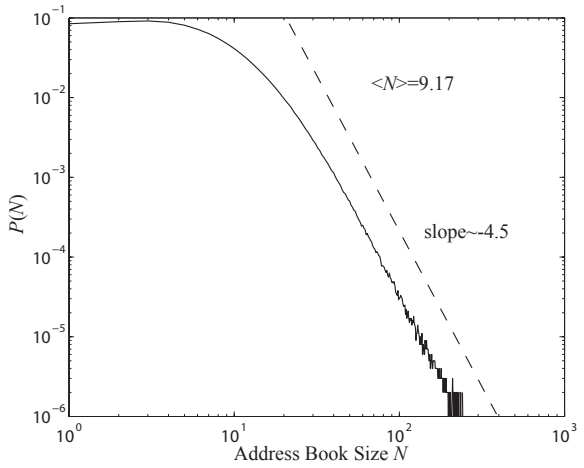

Fig. 3 The distribution of user's address book size $P(N)$ follows a power-law for a wide range of N.

To understand the spreading dynamics, we assign an initial virus to a randomly chosen handset, which in turn will send infected MMSs to its identified contacts. The MMS service is not instantaneous, there is time delay on receiving a MMS. In our simulation we choose 2 minutes as the time required for a MMS virus to be received by another handset and to install itself [3]. The simulation time step is also chosen as 2 minutes.

In the scanning behavior, we need to estimate the effective scanning probability p. This is necessary because one can expect that a large number of scans will reach mobile numbers that are not active (ineffective scan). To get an educated estimate of this probability, we divided 6 million (an approximation of the mobile-phone user base) by 100 million (the total phone numbers that 8 digits can generate), obtaining an effective scanning probability $p = 0.06$.

To quantify the topological/scanning behavioral level in the spread of MMS viruses, we define the random attack probability, ρ, that a virus will attack a random phone number rather than a number listed in the address book. The value of ρ varies from zero to one, showing viruses' different attack strategies: from completely topological to completely scan based. Lastly, we define the maximum attack number s for each infected handset, viruses generally limit and control the number of times they attack to prevent them from being detected due to abnormal MMS volume caused by the attacks.

2.4 The Naive and Temporal Spread Models

In this paper, we study two spreading models: naive and temporal. The difference between them is on their ability to utilize temporal patterns of MMS volume to prevent being detected. Given the information about MMS volume during a day, the temporal spread model enable us to understand viruses that try to avoid detection by phone providers. The model can simulate the interplay between MMS viruses' spreading strategies and phone providers' ability to monitor global MMS volume. On the other hand, the naive model is studied to understand the worst-case scenario of a viral outbreak, ignoring MMS temporal usage patterns and possible monitoring by phone providers. We use OS market share values of $m = 0.30$ and $m = 0.03$ to study the viral spread in different types of call graphs [19,7,17, 20]. When the market share $m = 0.3$ there is a giant component in the call graph and in the small $m = 0.03$ case no giant component exists and the call graph is fragmented into small isolated clusters. In the following sections, we describe that topological and scanning behavior are more effective in high market-share OS and low market-share OS respectively.

3 Experimental Results

3.1 The Effect of Scanning

To understand the effect of the scanning behavior of mobile virus, we first use an illustrative example based

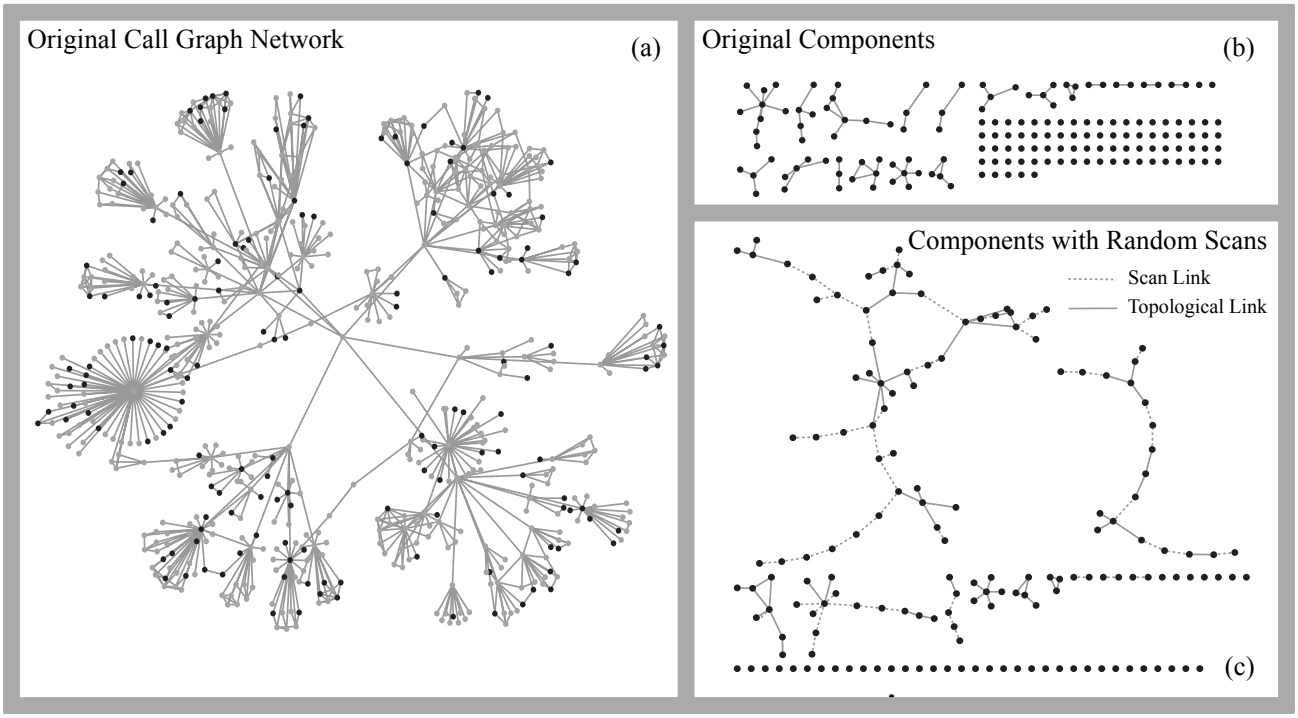

Fig. 4 Illustrative example of the effect of scanning behavior in mobile viruses (this picture is presented to exemplify the effect of scans and does not depict the real data used in the simulations).

on a small neighborhood of the call graph (approx. 600 nodes and 1,000 links). The graph was generated by starting from a randomly chosen phone and including all mobile-phone contacts up distance 4 from the initial one. The nodes in Figure 4 are represented using two colors that correspond to the two kinds of OSs used in the simulation, with market shares 0.25 (25%) represented by dark nodes and 0.75 (75%) in lighter color. Because a virus can only infect the OS it was designed for, the largest components $[11, 6, 10, 4, 8, 5]$ formed by the same color connected nodes represent the maximum number of handsets that a virus can infect. Without random scans, the dark nodes are fragmented into small islands and the largest cluster size represents only 6% of the total number of dark nodes (see Figure 4(b)). To simulate the continuous attacks of scanning behavior, we randomly add 800 links between the nodes in this local network. The dashed lines shown in Figure 4(c) represent links generated from scanning behavior—they connect the originally disconnected small clusters. One can see that the structure of the call graph changes significantly, the largest component (35% of the total number of dark nodes) is about 6 times bigger than its counterpart without random links. In this illustrative example, we densely add random links to make the effect of scanning more prominent. In what follows, we show that the addition of scanning also makes the virus more dangerous under realistic conditions.

3.2 Naive Viral Spread (Worst-Case Scenario)

In the naive viral spread model, where we disregard the possibility of monitoring of abnormal MMS activity, a phone handset sends out viral MMS messages every 2 minutes from the time it gets infected. This approach can be easily detected by phone users or phone providers. However, this model is interesting as a study of the worst-case of a virus spread, given that it helps us understand how OS market share, maximum attack number, and attacking strategy influence the spreading dynamics of MMS viruses.

After looking at the worst case, we move to a study on how the OS market share m influences the spread of MMS viruses. The solid and dashed lines in Figure 5 represent the average (solid line), maximum (dashed line) and minimum (dashed line) infection fraction (I/N) respectively. Different symbols correspond to different maximum-attack numbers s. The average (I/N) is obtained from 10 simulations where the virus starts at a randomly chosen mobile-phone user. For a small OS market share $m = 0.03$, independently of what attack

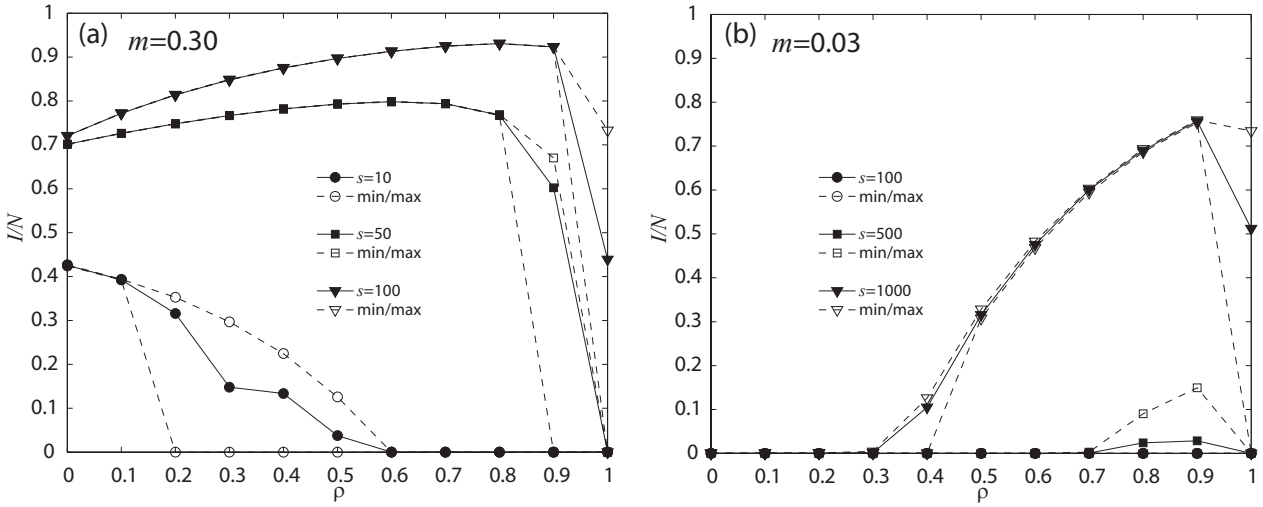

Fig. 5 Spread behavior using the naive viral spread model.

strategies (ρ value) that the viruses utilize, they cannot spread if the maximum attack number (s) is small (Figure 5(b)). In contrast, for a large OS market share $m = 0.30$, a MMS virus can infect a large fraction of susceptible handsets even when the maximum-attack number (s) is as small as 10, showing that large market-share OS handsets are much more vulnerable (Figure 5(a)). These results strengthen the results in Wang et al. [25], revealing again the crucial role of market share in the spread of mobile-phone viruses. We also explore the effect of maximum-attack number (s) in the spread of MMS viruses. As shown in Figure 5, the increase of s makes MMS viruses reach more susceptible handsets. This shows that the maximum-attack number (s) also plays a key role in the spreading process.

Intuitively, one can see the different characteristics of topological and scanning behaviors. Topological attacks always reach active phone numbers but they are sometimes trapped in isolated clusters of the underlying fragmented call graph. In contrast, scanning has a much lower probability to reach active phone numbers, but just a few of them can link the isolated clusters together. As depicted in Figure 5(a), for an OS with high market share, when the maximum-attack number (s) is small, MMS viruses with more topological attacks can infect more phones. This is because given the small maximum-attack number, scanning has a limited ability to reach active phone numbers. For a large maximum attack number ($s = 50$), MMS viruses with a random attack probability $\rho \approx 0.6$ can potentially cause the most damage. This situation occurs because with a large s, topological attacks can be ineffective by reaching already infected phone numbers. In Figure 5(b) we find that MMS viruses with a big random attack probability ρ can infect more susceptible handsets in an OS with a low market share $m = 0.03$. This can be explained by the scanning viruses' ability to connect isolated clusters. However, pure scanning may result in the failure of spread due to its low probability to reach active phone numbers.

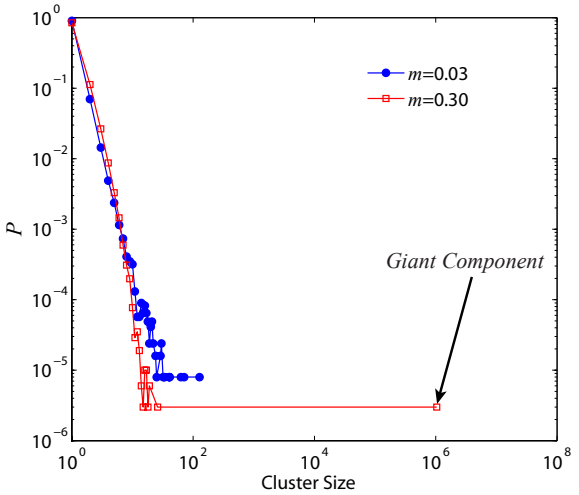

Fig. 6 The distribution of cluster sizes in the call graph.

According to Figure 5, under specific conditions of OS market share and maximum-attack number, the combination of topological and scanning behaviors in mobile virus can cause the most damage. Generally, we notice that MMS viruses with a high scanning rate are

more dangerous for an OS with low market share, while MMS viruses with a low scanning rate are more dangerous for an OS with high market share. These findings can be addressed by the topological properties of the underlying call graph. As depicted in Figure 6, given that there is already a giant component in the call graph formed by the handsets using a high market share OS, attacks virus with scanning behavior are not able to help significantly increase the size of the giant component. Furthermore, when the maximum-attack number (s) is limited (small), scanning will create too many ineffective attacks that make the virus fail to spread. For an OS with low market share ($m = 0.03$) no giant component exists in the call graph (Figure 6), making the effect of scanning in connecting isolated communities more prominent. Thus, we find that MMS viruses with high scanning rate are more effective for an OS with low market share. The different spreading pattens of MMS viruses in OSs with high and low market shares can be explained by the different structural properties of the call graphs formed in the two situations. Interestingly, in next section we also find similar results in the temporal volume-based spread model.

In this section, our simulations provided an indication of the values for market share as well as maximum-attack number in which the mobile-phone base becomes susceptible to global epidemics. Unfortunately, this is not the entire story as viruses are being written to be more stealth to detection. In the next section we delve into a spread mode that attempts to be stealth by using the patterns in MMS volume on different times of the day and different days of the week.

3.3 Temporal Volume-based Viral Spread (Stealth Mode)

Given that the pattern of people sending MMS can be analysed and predicted, a MMS virus may utilize latent periods of usage to avoid detection by the phone providers. One of the common ways virus can do the above is by using an approach based on the time of the day and day of the week, as well as limiting the virus' attack frequency. Therefore estimating the real danger posed by these kinds of viruses becomes an important problem. In the model proposed here, MMS viruses spread solely during the daytime according to the temporal MMS volume pattern—during the day the volume of messages make detection of virus harder. We calculate the probability of the infected phone sending out a viral message each 2 minutes [3]. For example:

1. If 2% of the weekly MMS volume is generated between 6pm and 8pm on Tuesday and each infected phone sends out one viral MMS per day on average ($T = 1$ day), an infected handset would send out 7 viral MMSs per week. Thus the infected handset has a probability of $7 \times 0.02 = 0.14$ to send out a viral MMS between 6pm and 8pm on Tuesday.
2. Between 6pm and 8pm (2 hours) there are sixty two-minutes time steps, thus we get that the infected handset has a probability of $0.14/60 = 0.0023$ to send out a viral MMS in each two-minutes during 6pm and 8pm on Tuesday.

In the temporal, volume-based spread model, we set $s = 100$ and $s = 1000$ for the high market share case and low market share case respectively, because these values have been shown to be the most dangerous in the study of worst case scenario. In Figure 7, we predict the amount of spreading (I/N) for MMS viruses using different average attack periods T. The different symbols in Figure 7 show the results under different values of T. Figure 7(a)-(d) corresponds to four scenarios respectively: (a) high market share $m = 0.30$, low scanning rate $\rho = 0.2$. (b) high market share $m = 0.30$, high scanning rate $\rho = 0.8$. (c) low market share $m = 0.03$, low scanning rate $\rho = 0.2$ (d) low market share $m = 0.03$, high scanning rate $\rho = 0.8$. The pictures show, the ratio of infected handsets (I/N) decreases with the attack frequency, revealing that the average attack period T controls the speed of a MMS virus' spread.

An important question we would like to answer is whether MMS viruses could infect a large population of susceptible handsets without being detected by the phone provider. We can see in Figure 7, the smaller the average attack period T, the faster the virus spreads but that would make it very easily detectable. The dashed lines with different colors mark the time when MMS viruses utilizing different attacking frequencies are detected by the phone provider via an abnormal MMS volume check. At the time of being detected, the overall volume of the viral MMS exceeds the threshold volume ΔV (Figure 2). For example, if a MMS virus infects the handsets with an OS market share $m = 0.30$ and uses a scanning rate $\rho = 0.2$, a maximum attack number $s = 100$ and an average attack period $T = 12$ hours, it can infect 15% of the overall susceptible handsets (approx. 0.27 million handsets) in 37 days without being detected (circles in Figure 7(a)).

In Figure 8, we show the ratios of infected handsets when the virus is detected for different average attack period T. We find that under phone provider's monitoring (using the value ΔV), the spread of MMS viruses is well constrained independently of what attacking strategies that MMS viruses use. Interestingly, the spreading patterns show different characteristics for high market share case and low market share case. Sim-

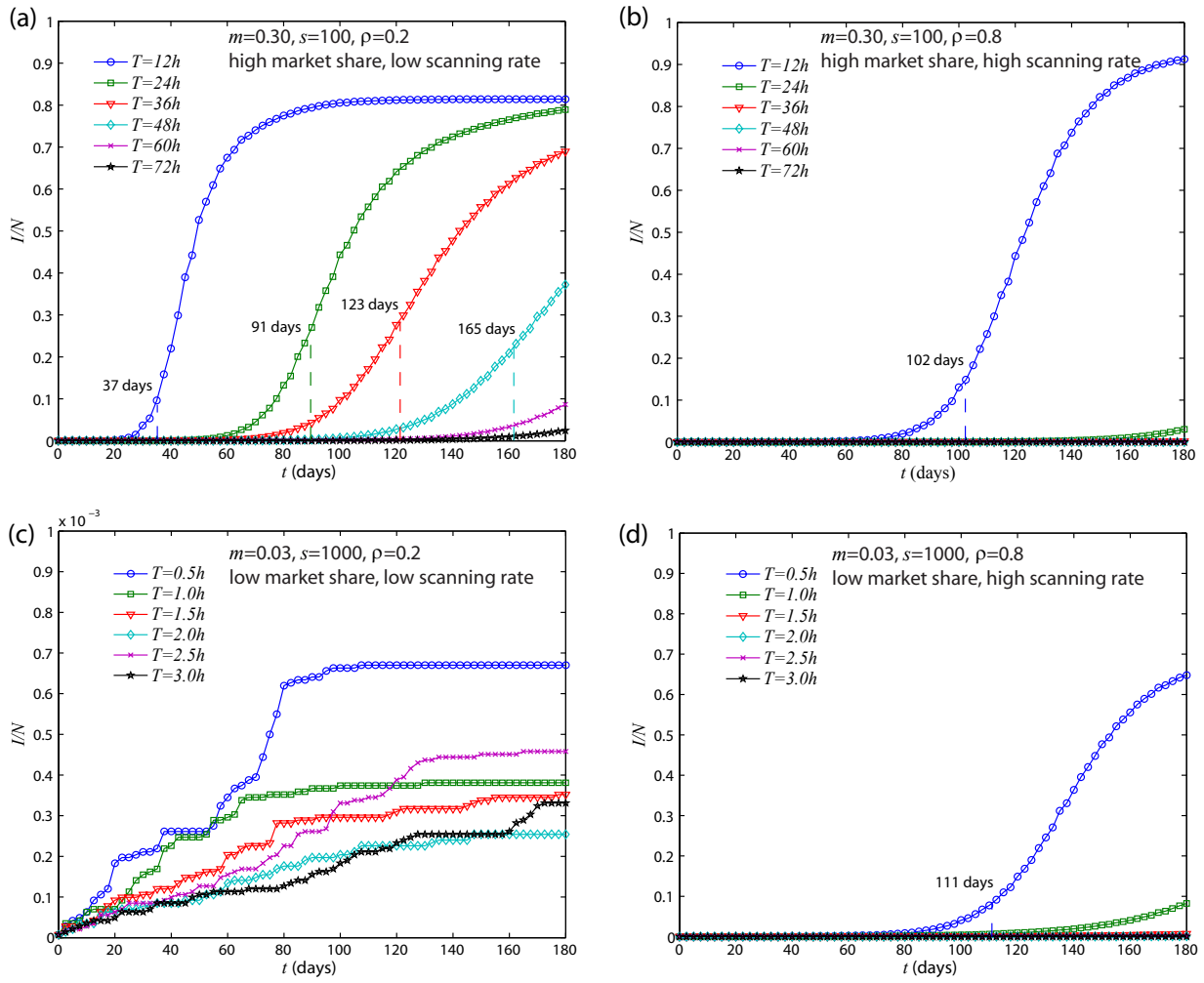

Fig. 7 The spreading behavior of MMS viruses under the monitoring of phone providers. The dashed line corresponds to the time that a MMS virus is detected.

ilar to what we found in the naive model, a virus with low scanning rate ρ is more dangerous for a high market share OS, a virus with high scanning rate ρ is more dangerous for a low market share OS (see the circles and squares in Figure 8). This result can also be explained by the properties of the underlying call graphs.

3.4 Containing the Spread of MMS Viruses

Without having phone providers monitoring the system, a MMS virus can potentially infect a large fraction of susceptible handsets in just a few hours [25]. However, in our simulation MMS viruses can at most infect 0.55 million handsets without being detected by the phone provider in 123 days (the red dashed line in Figure 7(a)). The long latent period offers ample time for identifying the virus earlier by other approaches and deploying antiviral software and patches. This finding reminds us of an important countermeasure to protect the communication system: improve our monitoring ability to detect the virus. We perform the experiments on condition of $m = 0.30$ and $\rho = 0.2$, which corresponds to the experiments performed in Figure 7(a). This scenario is selected because it is the most dangerous case we find in the temporal volume-based model. We study the ratios of infected handsets (I/N) under new detecting thresholds $0.75\Delta V$, $0.5\Delta V$ and $0.25\Delta V$. Figure 9 quantitatively shows that if phone providers successfully decrease the detecting threshold ΔV, the viral spread can be better restrained. However, one has to be careful with decreasing this threshold because it may lead to false positives. One should allow for some

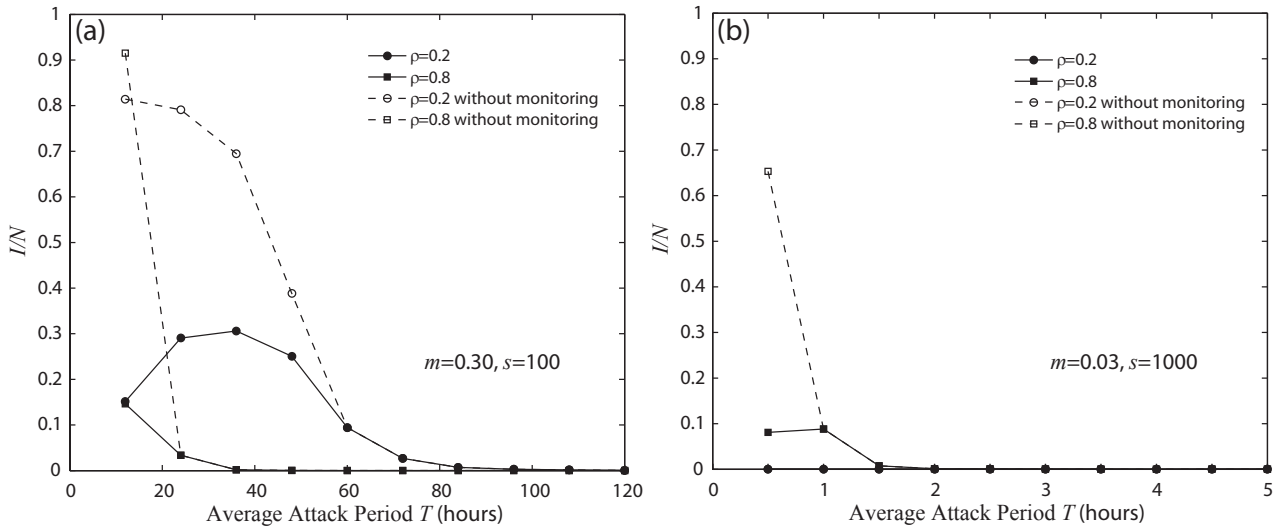

Fig. 8 The ratio of infected handsets I/N when the virus is detected in the four scenarios described in Figure 7. The dashed lines correspond to the ratio of infected handsets I/N without monitoring.

flexibility in the ΔV so that users can change their pattern of MMS usage.

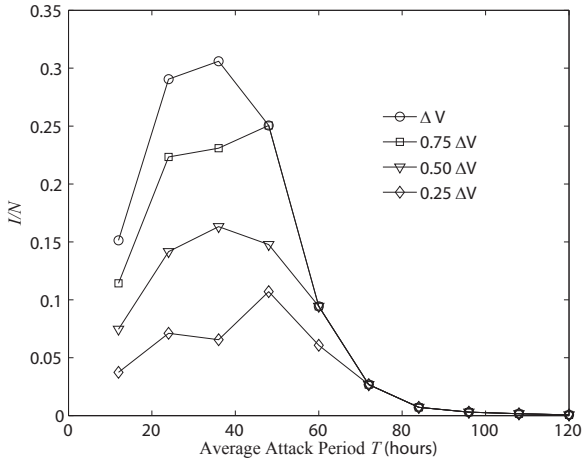

Fig. 9 The ratio of infected handsets I/N when the virus is detected in the scenario described in Figure 7(a) with improved monitoring ability of phone providers.

We next study the effect of patches installations in mitigating the damages. Again we perform the experiments on scenario with $m = 0.30$ and $\rho = 0.2$. In this simulation, an infected handset changes to removed state (R) by installing a patch after a certain time period from 1 week to 4 weeks (Figure 10 and Figure 11). We find that installing patches can mitigate the damages caused by the virus. The faster the infected phones receive the patches, the better the virus is restrained. Hence the installation patches on infected phones in time is also a good way to restrain the spread of MMS viruses. This installation is time sensitive and should be done at the earlier stages of the outbreak whenever possible.

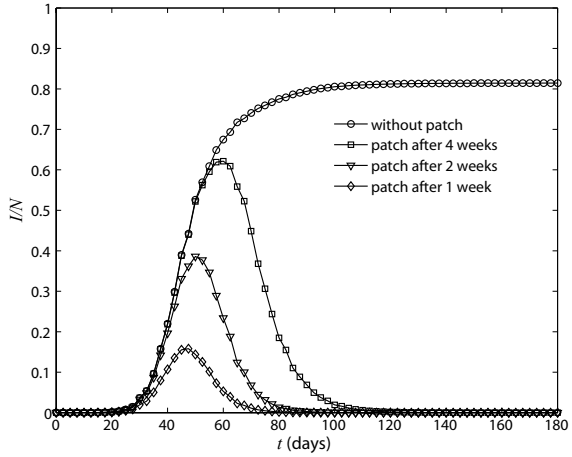

Fig. 10 The spreading behavior of MMS viruses with patches installed on infected handsets after a certain period.

4 Discussion and Conclusion

We demonstrated that the addition of random scans to the behavior of mobile viruses can increase the possibil-

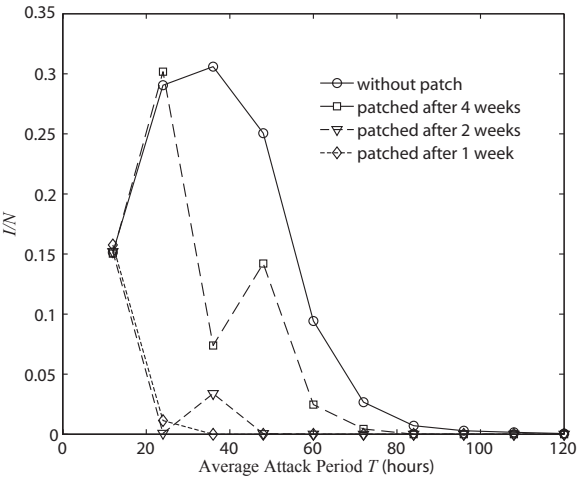

Fig. 11 The ratio of infected handsets I/N when the virus is detected in the scenario described in Figure 7(a) with patches installed on infected phones after a certain period.

ity of an epidemic outbreak in mobile phones. Interestingly, we discovered that the topological and scanning behaviors of MMS viruses cause more damage in high and low market-share OS respectively. We investigated the interplay between attack strategies of MMS viruses and abnormal MMS volume monitoring by phone providers. We found that given enough time, sophisticated viruses can infect a large fraction of susceptible phones without being detected by phone providers. Fortunately, independent of the attack strategy used, the epidemics would still be limited by the market share of handsets and providers' monitoring ability. When phone providers improve their monitoring ability and install necessary patches on infected phones quickly, MMS viruses can be better restrained. We believe our findings could provide mobile-phone providers with a guide to put in place proper countermeasures to avoid the costly impact of major outbreaks. Added to a good understanding of the network formed from connections between users, smart anomaly detection schemes may be able to prevent mobile phones to become the next platform for virus writers hence avoiding the situation typical in computer systems where virus writers seem to be winning the battle.

Acknowledgements We thank G. Xiao and C. Song for discussions and comments on the manuscript. This work was supported by National Natural Science Foundation of China (No. 51208520), the James S. McDonnell Foundation 21^{st} Century Initiative in Studying Complex Systems, the National Science Foundation within the DDDAS (CNS-0540348), ITR (DMR-0426737) and IIS-0513650 programs. P. Wang acknowledges support from Shenghua Scholar Program of Central South University.

References

1. Andersen, R., May, R.: Infectious Diseases of Humans: Dynamics and Control. Oxford Science Publications (1992)
2. Bose, A., Hu, X., Shin, K., Park, T.: Behavioral detection of malware on mobile handsets. In: Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys08), pp. 225–238. New York (2008)
3. Bose, A., Shin, K.: On mobile viruses exploiting messaging and bluetooth services. In: Securecomm and Workshops, pp. 1–10. Baltimore (2006)
4. Bunde, A., Havlin, S. (eds.): Percolation and Disordered Systems: Theory and Applications, vol. 266. Physica A (1999)
5. Caldarelli, G.: Scale-Free Networks: Complex Webs in Nature and Technology. Oxford University Press (2007)
6. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J.: Network robustness and fragility: Percolation on random graphs. Phys. Rev. Lett. **85**(25), 5468–5471 (2000)
7. Candia, J., González, M.C., Wang, P., Schoenharl, T., Madey, G., Barabási, A.L.: Uncovering individual and collective human dynamics from mobile phone records. Journelof Physics A: Mathematical and Theoretical **41**, 224,015 (2008)
8. Chen, Y., Paul, G., Cohen, R., Havlin, S., Borgatti, S.P., Liljeros, F., Stanley, H.E.: Percolation theory applied to measures of fragmentation in social networks. Phys. Rev. E **75**(4), 046,107 (2007)
9. Cheng, J., Wong, S.H., Yang, H., Lu, S.: Smartsiren: Virus setection and alert for smartphones. In: Proceedings of the 5th international conference on Mobile systems, applications and services, pp. 258–271. ACM, New York, NY, USA (2007)
10. Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. Phys. Rev. Lett. **85**(21), 4626–4628 (2000)
11. Dorogovtsev, S.N., Mendes, J.F.F., Samukhin, A.N.: Giant strongly connected component of directed networks. Phys. Rev. E **64**, 025,101 (2001)
12. Funk, S., Salathe, M., Jansen, V.: modelling the influence of human behaviour on the spread of infectious diseases: A review. Journal of the Royal Society Interface **7**, 1247–1256 (2010)
13. Gao, C., Liu, J., Zhong, N.: Network immunization and virus propogation in emial networks: Experimental evaluation and analysis. Knowledge and Information System **27**(2), 253–279 (2011)
14. Hypponen, M.: Malware goes mobile. Scientific American pp. 70–77 (2006)
15. Kim, H., Smith, J., Shin, K.G.: Detecting energy-greedy anomalies and mobile malware variants. In: Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys08), pp. 239–252. New York (2008)
16. Kleinberg, J.: The wireless epidemic. Nature **449**, 287–288 (2007)
17. Lambiotte, R., Blondel, V.D., de Kerchove, C., Huens, E., Prieur, C., Smoreda, Z., Dooren, P.V.: Geographical dispersal of mobile communication networks. Physica A: Statistical Mechanics and its Applications **387**(21), 5317–5325 (2008)
18. Mickens, J., Nobel, B.: Modeling epidemic spreading in mobile enviroment. In: Proc. ACM Workshop Wireless Security, pp. 77–86. New York (2005)

19. Onnela, J.P., Saramaki, J., Hyvonen, J., Szabo, G., Lazer, D., Kaski, K., Kertesz, J., Barabási, A.L.: Structure and tie strengths in mobile communication networks. Proceedings of the National Academy of Sciences **104**(18), 7332–7336 (2005)
20. Palla, G., Barabási, A.L., Vicsek, T.: Quantifying social group evolution. Nature **446**, 664–667 (2007)
21. Schechter, S., Jung, J., Berger, A.: Fast detection of scanning worm infections. In: E. Jonsson, A. Valdes, M. Almgren (eds.) Recent Advances in Intrusion Detection, *Lecture Notes in Computer Science*, vol. 3224, pp. 59–81. Springer Berlin Heidelberg (2004)
22. Shevchenko, A.: An overview of mobile device security. http://www.viruslist.com/ (2005)
23. Su, J., Chan, K.W., Miklas, A., Po, K., Akhavan, A., Saroiu, S., de Lara, E., Goel, A.: A preliminary investigation of worm infections in a bluetooth enviroment. In: Proc. 5th ACM Workshop Rapid Malcode (WORM), pp. 9–16. New York (2006)
24. Wang, P., González, M.C.: Understanding spatial connectivity of individuals with non uniform population density. Philosophical Transactions of the Royal Society A **367**, 3321–3329 (2009)
25. Wang, P., González, M.C., Hidalgo, C.A., Barabási, A.L.: Understanding the spreading patterns of mobile phone viruses. Science **324**, 1071–1076 (2009)
26. Xie, L., Zhang, X., Chaugule, A., Jaeger, T., Zhu, S.: Designing system-level defenses against cellphone malware. In: Proceedings of the 28th IEEE International Symposium on Reliable Distributed Systems (SRD09), pp. 89–90. SRD09, New York (2009)
27. Yan, G., Flores, H., Cuellar, L., Hengatner, N., Eidenbenz, S., Vu, V.: Bluetooth worm propagation: Mobility pattern matters. In: Proc. 2nd ACM Symposium on Information, Computer and Communication Security, pp. 32–44. New York (2007)
28. Zhu, Z., Cao, G., Zhu, S., Ranjan, S., Nucci, A.: A social network based patching scheme for worm containment in cellular networks. In: Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM09), pp. 1476–1484. Rio de Janeiro, Brazil (2009)