Modeling Malware Propagation in Networks of Smart Cell Phones with Spatial Dynamics

Krishna Ramachandran and Biplab Sikdar
Department of ECSE, RPI, Troy NY 12180 USA

***Abstract*— Recent outbreaks of virus and worm attacks targeted at cell phones have have bought to the forefront the seriousness of the security threat to this increasingly popular means of communication. The ability of smart cell phones to communicate through both the Internet and the telecom networks along with the presence of a number of communication interfaces makes them vulnerable to attacks from a number of sources which can then propagate at extremely fast rates. In this paper we develop an analytic framework for modeling the dynamics of malware propagation in networks of smart phones that specifically accounts for the mobile nature of these devices. We also characterize the conditions under which the network may reach a malware free equilibrium and derive the necessary conditions for its global asymptotic stability. The model accounts for malware transfers through the Internet and peer to peer networks, through the telephone network and through Bluetooth and WLAN interfaces.**

I. Introduction

While malware such as worms and viruses have been prevalent in the Internet for more than a decade, such attacks have recently been reported in cell phones. Proof-of-concept worms for smart phones like `cabir` [2] as well as malicious code such as the `skulls` [4] and `mosquito` [3] trojans have recently been reported. As recently as August 2005, mobile phones at the world athletics championship held at Helsinki's Olympic stadium were compromised by a virus attack [12], as were the mobiles at a public concert in Germany [7]. With the growing popularity and prevalence of advanced cell phones with a myriad of communicational capabilities, such threats are extremely important and capable of causing extensive damage. Owing to their ability to inter-operate between the Internet and the cell phone or telephone network coupled with the improvements in their computational abilities, built in functionalities and mobility, malware propagation in these networks has the potential to spread extremely fast and compromise a large number of phones, in addition to crippling the telecom infrastructure.

The communication capabilities of the new generation of cell phones, as shown in Figure 1, can be broadly grouped into three categories **(1)** access to the telecom network through technologies like (GSM) and code division multiple access (CDMA) **(2)** access to the Internet which may occur either via accessing the telecom network or by using Bluetooth or wireless local area networking (WLAN) interfaces and **(3)** communication through other smart phones in its physical vicinity through Bluetooth interfaces etc. Consequently, the possible ways in which malware may spread in these devices are **(1)** malware downloads from the Internet and peer to peer networks (for example the `skulls` and `mosquito` trojans [3], [4]), **(2)** phone to phone spread which results when a compromised phone sends the malware to other phones either by random dialing or dialing the numbers in the address book (for example using mechanisms similar to the `timfonica` virus in Spain, 2000 and the `commwarrior` and `mabir` worms) and **(3)** phone to phone or computer to phone spread through Bluetooth or WLAN interface (for example the `cabir` worm [2]). Node mobility and the resulting variations in the number of other devices in the vicinity of a phone also affects the propagation of the malware, specially those that spread through the Bluetooth or WLAN interfaces.

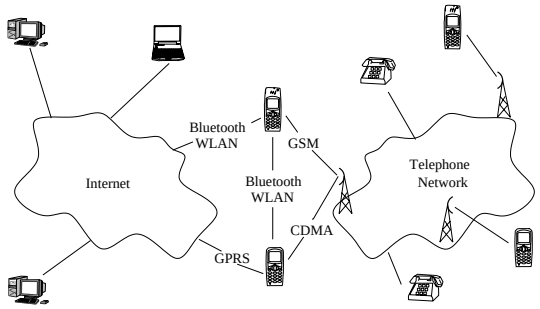


Fig. 1. Communication paradigms in smart cell phones.

There exists a slew of modeling work characterizing numerous aspects of worm spread, [9], [8], [10], [11] to name a few, but seldom has the setting been a wireless environment. Also, unlike our model, existing work only considers static nodes. We believe that new generation smart phones are largely vulnerable to, and can act as the catalysts for the spread of mobile viruses and thus are important from a practical perspective.

In this paper, we present a comprehensive analytical model to explore the impact that the interplay between the communication capabilities and behavioral patterns such as node mobility and heterogenity in the locality of the smart cell phones has on the spread of malware in such networks. We then use the model to derive the necessary conditions for the existence of a malware free equilibrium and substantiate our claim with numerical results. A detailed explaination of the analytical procedure can be found in [13].

The rest of the paper is organized as follows: Section II further motivates the paper, Section III presents the analytical framework. We present numerical results and sensitivity analysis in Section IV and finally, Section V presents the concluding

remarks.

II. Motivation and Background

The first malicious code which specifically targeted mobile phones `cabir` appeared in June, 2004. Since then, numerous other forms of malware, with different degrees of sophistication, have continued to appear. Recent specimens of such malware exploit various capabilities, such as Bluetooth and MMS enhancements, associated with the cell phone in order to spread.

Most of the early malware for cell phones like `mosquito` and `skulls` were either trojans which infected a cell phone once they were downloaded from the Internet or like `cabir` and `lasco` which used Bluetooth to infect cell phones in its vicinity. Another example is the `commwarrior` worm which uses the infected host's multimedia messaging service (MMS) to spread itself to the phone numbers stored in the address book of the infected phone. Of greater cause of worry are the more recent specimen like `commwarrior` and `mabir` which use Bluetooth in addition to MMS for infecting other nodes. It is only a matter of time that more sophisticated malware appear which exploit all the communication capabilities of the host cell phone.

None of the existing forms of malware have been able to achieve epidemic proportions due to a number of factors. While some of the malware were proof of concept versions, others have slowed down due to errors (e.g. `comwarrior`) etc. However, as newer and more sophisticated malware appear, the threat they pose to users and service providers is becoming serious. For example, though the initial mode of attack employed by `cabir` was primarily through the Bluetooth interface thereby limiting the physical range within which it may infect others, subsequent and more advanced versions of the virus have since surfaced in 17 countries around the world. One only needs to note that while it took more than a decade for computer malware to evolve to their current state, it has taken less than two years for cell phone malware to achieve similar capabilities. At the extreme end, Warhol worms [6] for cell phones, which attack all possible systems in the shortest possible time, are now fast becoming a real possibility.

As the first step in developing effective defenses against these malware, this paper develops a model for their propagation under very general conditions. The model can then be used to gain insights into the most effective and efficient conditions for controlling the damage they may cause.

III. Modeling Framework

In this section we develop our model for the propagation of malware in smart phones. Due to space constraints, the mathematical derivations for the necessary conditions for the existence of a malware free equilibrium are not detailed here. The interested reader may refer [13] for a more complete version of this paper. We now provide an overview of the model and its assumptions.

A. Model Overview

This paper develops a modeling framework for the dynamics of malware propagation in smart cell phones. The model considers a network with a large number of smart cell phones. The phones are assumed to have the capability to communicate with other phones or computing using the telecom or cellular network as well as the Internet. The new generation of smart phones also have a number of communication devices including Bluetooth and infra red interfaces as well as Wifi or IEEE 802.11 based interfaces. Our model assumes that the phones are equipped with such devices. We also assume that the cell phone users are mobile and travel through a number of different regions, with varying degrees of node densities and connectivity.

Our model considers three different mechanisms through which malware may infect and propagate in cell phones. **First,** the malware may be inadvertently downloaded by a cell phone user from the Internet or another computer. Such malware often come in the form of trojans like `skulls` [4] and `mosquito` [3] that are downloaded and executed by unsuspecting users. **Second,** malware in infected phones may try to infect other phones which come in its vicinity by transferring its payload through the Bluetooth, infra red or WLAN interfaces. These methods are widely used by the malware specimen such as `cabir`, `lasco`, and `commwarrior`. **Third,** an infected phone may dial numbers stored in its address book or dial numbers randomly and transfer the malware code as a SMS or MMS message in an attempt to infect other phones. Note that both random and selective dialing have been used by existing specimens of malware such as `timfonica`, `commwarrior` and `mabir`. Our modeling framework facilitates the incorporation of all of the above three (or any subset thereof) spreading mechanisms and evaluate their individual as well as combined effect on the malware's dynamics.

The model developed in this section is based on a compartmental epidemic model with four classes. At any given point in time, a cell phone is in one of the following four classes: susceptible, exposed, infected and recovered. Initially all phones belong to the susceptible phase and stay there until they come in contact with the malware. The exposed state corresponds to the latent period of an infection. In our case this corresponds to the case when a malware is sent to a phone which is currently turned off. The phones then stay in the infected state until they are either patched or quarantined upon which they move to the recovered state and stay there.

In our model, new phones may enter the network and some phones may leave the network. However, the birth and death rates are the same and the total population at any given instant is assumed to be a constant. This assumption is based on the fact that the time for a fast worm to spread can be considered to be quite small compared to the rate at which the cell phone population in a country or city changes. Also, we assume that the time taken to download the malware through any of the communication interfaces is quite small and may be

considered instantaneous. This assumption may be justified by noting the small size of most worms as well as the increasingly high data rates achieved by the new generation of smart phones.

We first present our model for capturing the effect of the physical movement of the phones through different environments and geographical locations in Section III-B. The model is then extended to account for the malware spread through the different communication paradigms in Section III-C.

B. Model for Spatial Dynamics

An inherent characteristic of cell phone usage is the associated mobility of the user. Over the course of a day, a user may move from a residential area to a workplace environment and pass through public places with reasonably high density of other cell phone users. In addition, users may occasionally pass through places like airports and other transportation hubs, stadiums etc. where it is quite likely that it may come in close proximity with infectious cell phones. To capture the impact of such heterogeneous environments, we classify each possible location that a cell phone may visit as one of $\mathcal{P}$ patches or regions [1]. Each patch is characterized by its own infection rate and visitation probabilities. Thus an airport and a small stadium, where an arbitrary cell phone may come across roughly the same number of other phones and may stay for roughly equal times are treated as belonging to the same patch. Similarly, two residential areas in opposite sides of a city or in two different cities may be classified into the same patch.

Classifying the locations that cell phone users may visit in terms of patches also aids in reducing the state space and the corresponding number of equations in the mathematical formulation. As opposed to having 4 equations to characterize *each* location that a cell phone may visit, classifying the locations into $\mathcal{P}$ patches reduces the *total* number of equations in our model to $4\mathcal{P}$. We denote the rate of travel from patch q to patch p by m_{pq}. The rate of change in the susceptible (S_p), exposed (E_p), infectious (I_p) and recovered (R_p) populations in patch p, $1 \leq p \leq \mathcal{P}$ due to *only* the movements between the patches is then given by

$$\frac{dS_p}{dt} = \sum_{q=1}^{\mathcal{P}} m_{pq} S_q - \sum_{q=1}^{\mathcal{P}} m_{qp} S_p \quad (1)$$

$$\frac{dE_p}{dt} = \sum_{q=1}^{\mathcal{P}} m_{pq} E_q - \sum_{q=1}^{\mathcal{P}} m_{qp} E_p \quad (2)$$

$$\frac{dI_p}{dt} = \sum_{q=1}^{\mathcal{P}} m_{pq} I_q - \sum_{q=1}^{\mathcal{P}} m_{qp} I_p \quad (3)$$

$$\frac{dR_p}{dt} = \sum_{q=1}^{\mathcal{P}} m_{pq} R_q - \sum_{q=1}^{\mathcal{P}} m_{qp} R_p \quad (4)$$

C. Incorporating Infection Mechanisms

We first consider the spread of the malware due to downloads from the Internet or a P2P network. Given that a cell phone is on and in patch p (which happens with probability p_{on}^p and is derived in Section (III-D)), we denote the probability that an arbitrary cell phone in patch p downloads the malware from the Internet or P2P network at time t by $\gamma_p(t)$. Also, $\gamma_p(t)$ is a decreasing function of time since users are less likely to download a malware with time because of factors like awareness and publicity etc.

Now, only the susceptible cell phone population may inadvertently download the malware from the Internet and the number of such downloads per second is proportional to the susceptible population in the patch. Also, since the downloads are completed in a very small amount of time, the susceptible cell phones move directly to the infected phase. The rate of change in the populations of the four classes due to downloads from the Internet is then: $\frac{dS_p}{dt} = -\frac{dI_p}{dt} = -p_{on}^p \gamma_p(t) S_p$, $\frac{dE_p}{dt} = \frac{dR_p}{dt} = 0$. Now consider the spread of the malware through Bluetooth or WLAN interfaces when susceptible phones come in the physical vicinity of infected phones. The rate of spread through these interfaces depends on the type of patch as well as the number of susceptible and infectious cells phones in a patch. We denote by β_p the rate at which a cell phone in patch p tries to infect other phones through the Bluetooth and WLAN interfaces. Again, since only phones currently turned on may be infected with this mechanism and the malware transfer between two devices is considered instantaneous, the susceptible population directly moves to the infectious state. The contributions to the rate of change of populations of the four classes in this case are given by: $\frac{dS_p}{dt} = -\frac{dI_p}{dt} = -p_{on}^p \beta_p S_p \frac{I_p}{N_p}$, $\frac{dE_p}{dt} = \frac{dR_p}{dt} = 0$.

Finally, we consider the case where the malware may spread when a compromised phone randomly or selectively dials other numbers and transfers the malware through MMS or SMS. The dialed number may be in any of the $\mathcal{P}$ patches and thus a phone in one patch may infect a phone in another patch. The rate of such infections is proportional to the strength of the infectious population in the patch and given by I_p/N_p for patch p. We denote the rate at which a compromised phone tries to dial other numbers by α. Also, some of the randomly dialed or out-dated numbers in the address book numbers may be non-existent and thus all infection attempts will not be successful. We denote by ρ the probability that a dialed number is non-existent. Finally, some of the dialed cell phones may be switched off and in these cases, we assume that the malware gets queued up in the base station and is delivered once the phone is switched on. For this spreading mechanism, we thus have: $\frac{dS_p}{dt} = -\frac{dE_p}{dt} = -\sum_{i=1}^{\mathcal{P}} \alpha(1-\rho) S_p \frac{I_i}{N_i}$, $\frac{dI_p}{dt} = \frac{dR_p}{dt} = 0$. Note that in the equations above, all phones infected through random or selected dialing pass through the exposed state, even though the phones that are turned on get infected immediately. This does not result in any inaccuracies because in Section III-D, we evaluate and incorporate the estimated time that a phone spends in the exposed state in patch p, $1/\epsilon_p$, based on whether it was turned on or not when it was infected.

D. Combined Model

We now combine the various contributions along with the arrival and departures of cell phones to complete the model. First, we note that while new phones may join only in the susceptible phase, cell phone uses may decide to quit the

network permanently while they are in any of the four states. With the average phone lifetime in patch p denoted by $1/d_p$, the rate of population change due to the joining on new phones and departure of old ones is $-d_pE_p$, $-d_pI_p$ and $-d_pR_p$ for the exposed, infected and recovered classes and $d_pN_p - d_pS_p$ for the susceptible state. Note that the birth term of d_pN_p is devised to keep the total cell phone population constant.

The average time spent by an arbitrary cell phone in the exposed phase in patch p is denoted by $1/\epsilon_p$. With $1/\lambda_{on}^p$ and $1/\lambda_{off}^p$ denoting the average on and off times of a cell phone in patch p, we have: $p_{on}^p = \frac{\lambda_{off}^p}{\lambda_{on}^p+\lambda_{off}^p}$ and $p_{off}^p = 1 - p_{on}^p$. The expected duration of the exposed state in patch p, $1/\epsilon_p = E[\text{latent period}|\text{on}]p_{on}^p + E[\text{latent period}|\text{off}]p_{off}^p$, is then given by $\frac{1}{\epsilon_p} = \frac{\lambda_{on}^p}{\lambda_{off}^p(\lambda_{on}^p+\lambda_{off}^p)}$. Exposed cell phones in patch p leave the exposed state at a rate of ϵ_pE_p and thus enter the infected state at the same rate. Finally, with $1/\delta_p$ denoting the average time spent by a cell phone in patch p in the infected state, infected phones leave the infected state at a rate of δ_pI_p and enter the recovered phase at the same rate.

Combining the models of the previous two subsections with the contributions to the population change rates described above, we obtain the following equations which complete our model for malware propagation in cell phones:

$$\begin{aligned}
\frac{dS_p}{dt} &= d_p(N_p - S_p) - p_{on}^p\gamma_p(t)S_p - p_{on}^p\beta_pS_p\frac{I_p}{N_p} \\
&\quad - \sum_{i=1}^{\mathcal{P}}\alpha(1-\rho)S_p\frac{I_i}{N_i} + \sum_{q=1}^{\mathcal{P}}m_{pq}S_q - \sum_{q=1}^{\mathcal{P}}m_{qp}S_p \qquad (5)\\
\frac{dE_p}{dt} &= \sum_{i=1}^{\mathcal{P}}\alpha(1-\rho)S_p\frac{I_i}{N_i} - (d_p+\epsilon_p)E_p + \sum_{q=1}^{\mathcal{P}}m_{pq}E_q \\
&\quad - \sum_{q=1}^{\mathcal{P}}m_{qp}E_p \qquad (6)\\
\frac{dI_p}{dt} &= p_{on}^p\gamma_p(t)S_p + p_{on}^p\beta_pS_p\frac{I_p}{N_p} - (d_p+\delta_p)I_p \\
&\quad + \epsilon_pE_p + \sum_{q=1}^{\mathcal{P}}m_{pq}I_q - \sum_{q=1}^{\mathcal{P}}m_{qp}I_p \qquad (7)\\
\frac{dR_p}{dt} &= \delta_pI_p - d_pR_p + \sum_{q=1}^{\mathcal{P}}m_{pq}R_q - \sum_{q=1}^{\mathcal{P}}m_{qp}R_p \qquad (8)
\end{aligned}$$

where we have $N_p = S_p + E_p + I_p + R_p$, $\sum_{p=1}^{\mathcal{P}} N_p = C$, $N_p > 0$ and $S_p, E_p, I_p, R_p \geq 0$ at $t = 0$.

E. Discussion of Assumptions

We now discuss the implications of some of the assumptions made in this paper and the justifications behind these assumptions. First implicit assumption in our analysis is that that of homogeneous mixing of cell phones inside a patch. Locations are classified into patches based on factors like the expect time a phone spends in the location, the density of phones etc. Since only locations with similar characteristics are grouped together, the behavior of phones in any of these locations will be similar. Also, if the requirement of uniform node density is used in demarcating the patches, the homogeneous mixing assumption is justified. Note that node density can be assumed to be uniform in places like stadiums, residential areas, office spaces etc.

In real life cell phones use a number of different operating systems and have hardware manufactured by different vendors. Consequently, not all phones are vulnerable to a given malware. Our model can be easily extended to this case by considering the cell phone population C to correspond to the population of the vulnerable cell phones. Also, the infection rates β_p through the Bluetooth, WLAN and infrared interfaces and the probability $(1-\rho)$ that an infection attempt through SMS or MMS messaging is successful need to be scaled by the fraction of vulnerable cell phones in the entire cell phone population.

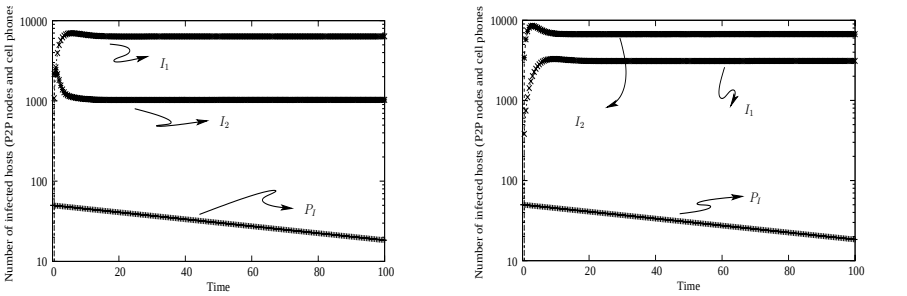
The assumption of instantaneous download of the malware is justified when one considers the high data transfer rates achieved by the new generation of cell phones and the small size of typical malware. Also, the fact that the duration of a typical malware infestation is quite small compared to the rate of change in the cell phone population in a country or city justifies the assumption of constant cell phone population.

IV. Numerical Results

In this section we evaluate the model presented in the previous two sections in order to explore the impact of various parameters on the dynamics of malware propagation. To easily isolate the effects of various parameters, we consider a simple scenario where the mobility of the cell phones is limited to two patches.

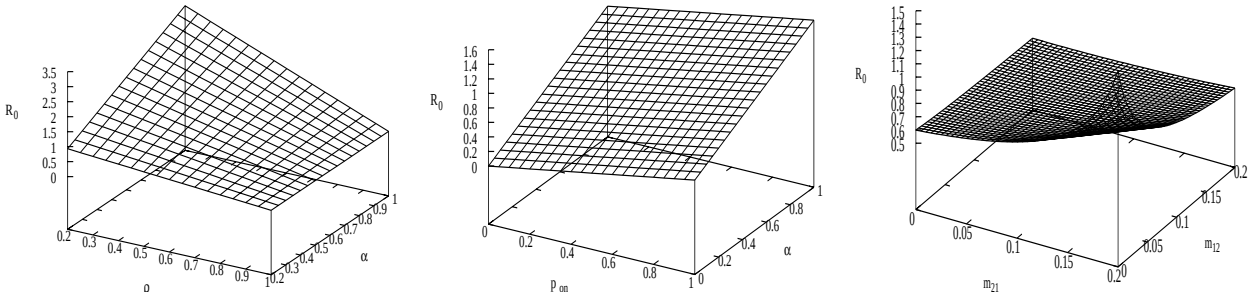
Figures 2(a) and 2(b) show the number of infected hosts in the two patches as a function of time for two different cases. In Figure 2(a) we have a case where the basic reproduction number, $\mathcal{R}_0 < 1$, and thus the system reaches a virus free equilibrium while in Fig. 2(b), $\mathcal{R}_0 > 1$ and thus the malware achieves an endemic state in the network.

In both the figures, the impact on node mobility on malware spread can be infered from the rate at which it spreads in the two patches. The greater mobility of patch 2 nodes ($m_{12} = 0.1$ and $m_{21} = 1$) results in the malware spreading more rapidly in the first patch due to the high influx of external infected phones and low departure rate of native infected phones. The parameter values used in the results presented so far, enumerated in [13], reflect only one instance of the possible system settings. We now explore the dynamics of malware propagation in the network as the values of various parameters are varied. In Fig. 3 we show the impact of the various parameters on the basic reproduction number, $\mathcal{R}_0$. We observe that α is more dominant as compared to p_{on} and ρ in terms of its effects on $\mathcal{R}_0$. This is evident from Figures 3(a) and 3(b), where the graph shows a faster increase in $\mathcal{R}_0$ for high α values even when the other corresponding parameter is numerically insignificant. This is intuitive too since a higher dialing rate increases the likelihood of contacting a susceptible cell phone. We also note from Fig. 3(c) that for our 2 patch wireless model parameters, the rate of travel from patch 1 to



(a) $m_{12} = 0.1$, $m_{21} = 1$ (b)$m_{12} = 0$, $m_{21} = 0$ and $\gamma_1 = 0.05$, $\gamma_2 = 0.5$

Fig. 2. Malware distribution in P2P and wireless networks



(a) $R_0 = f(\alpha, \rho)$ (b) $R_0 = f(\alpha, p_{on})$ (c) $R_0 = f(m_{12}, m_{21})$

Fig. 3. Impact of various parameters on R_0

patch 2, m_{21}, has a bigger impact as compared to the rate of travel from patch 2 to patch 1, m_{12}. This is because in the parameters chosen here, the rate of infections from Bluetooth or WLAN interfaces is smaller in patch 1 than in patch 2 ($\beta_1 < \beta_2$).

V. Conclusion

In the current work, we motivated the need to understand the dynamics of malware spread, especially in the context of interacting heterogeneous environments such as wired and wireless networks. Analysis for the impact of various spreading mechanisms such as downloads from the Internet or P2P networks, transfers through Bluetooth, WLAN and infra red interfaces and through MMS or SMS messages on the dynamics of malware propagation in networks of smart cell phones was presented and conditions for a malware free wireless network state were derived. Further, conditions for the global asymptotic stability of the malware free equilibrium of the network was derived.

References

[1] L. Sattenspiel and K. Dietz, "A structured epidemic model incorporating geographic mobility among regions," *Mathematical Biosciences*, pp. 71-91, vol. 128, 1995.

[2] Kaspersky Labs, "Viruses move to mobile phones," 2004. `http://www.kaspersky.com/news?id=149499226`

[3] CNET News, "Mosquito software bites smart phones," `http://news.com.com/Mosquito+software+bites+smart+phones/2100-1039_3-5308164.html?tag=nl`, August 2004.

[4] CNET news, "Skulls program kills cell phone apps," `http://news.com.com/Skulls+program+kills+cell+phone+apps/2100-7349_3-5460194.html?tag=nl`, November 2004.

[5] "Malware evolution," `http://www.viruslist.com/en/analysis?pubid=162454316`.

[6] S. Staniford, V. Paxson and N. Weaver, "How to own the Internet in your spare time," *Proceedings of USENIX Security Symposium*, 2002.

[7] "Mobiles get anti-virus protection," `http://news.bbc.co.uk/2/hi/technology/4207476.stm`.

[8] Z. Chen, L. Gao and K. Kwait, "Modeling the Spread of Active Worms," *Proceedings of IEEE INFOCOM*, April 2003.

[9] M. Garetto, W. Gong and D. Towsley, "Modeling Malware Spreading Dynamics," *Proceedings of IEEE INFOCOM*, April 2003.

[10] B. Stephenson and B. Sikdar, "A Quasi-species Approach for Modeling the Dynamics of Polymorphic Worms," *Proceedings of IEEE INFOCOM*, Barcelona, Spain, April 2006.

[11] C. C. Zou, W. Gong and D. Towsley, "Worm Propagation and Analysis under Dynamic Quanrantine Defense," *Proceedings of the ACM workshop on Rapid Malcode*, 2003

[12] COMPUTERWORLD, "Mobile phone virus infects Helsinki championships," `http://www.computerworld.com/securitytopics/security/virus/story/0,10801,103835,00.html`, August 2005.

[13] K. Ramachandran and B. Sikdar, "Modeling Malware Propagation in Networks of Smart Cell Phones with Spatial Dynamics," *Technical Report*, 2006.