Virus Propagation in Heterogeneous Bluetooth Networks with Human Behaviors

Jennifer T. Jackson and Sadie Creese, *Member*, *IEEE*

Abstract—The growth in the use of Smartphones and other mobile computing devices continues to grow rapidly. As mobile wireless communications become ubiquitous, the networks and systems that depend upon them will become more complex. In parallel with this, the spread of digital viruses and malicious content will be an ever increasing threat within this interconnected paradigm requiring counteracting mechanisms to continuously adapt. Current security solutions for mobile devices remain limited in their ability to protect particularly against zero-day attacks. Understanding the propagation characteristics of malware could provide a means to planning protection strategies, but modeling virus propagation behavior in mobile wireless and peer-to-peer communications devices is still immature. A compartmental-based virus propagation model has been developed for Bluetooth communication networks incorporating wireless technological traits and factors that are known to affect virus propagation including human behaviors, heterogeneous devices, and antivirus measures. The model is novel in the richness of its treatment of human factors alongside the technology factors that could impact spread. A simulation scenario, together with an analysis of the spreading dynamics has been conducted to determine how a Bluetooth virus might spread under different conditions. Although demonstrated through Bluetooth, the approach is applicable to malware propagation in general.

Index Terms—Human factors, invasive software (viruses, worms, trojan horses), pervasive computing, wireless

1 Introduction

Smartphones continue to be the mobile device of choice, with a recent Gartner report [1] estimating that the sale of smartphones is increasing by 74 percent year-on-year, with 107.7 million smartphones sold to end users worldwide during the second quarter of 2011. In spite of such rapid take up, the security solutions available for such platforms are limited and unlikely to offer any protection against previously unseen malware.

Smartphones are a major exploiter of Bluetooth technology allowing them to be easily connected in peer-to-peer networks allowing the exchange of files, messages, and other information. As the density of Bluetooth devices increase, so will the threat of the spread of digital viruses and malicious content via this medium. One well-known mobile virus is the Commwarrior [2], [3] launched in 2005 that propagates via both Bluetooth and Multimedia Messaging Service (MMS), and causes damage by resetting the infected device on the 14th day of any month. It is therefore important to understand how Bluetooth viruses propagate so that counteracting mechanisms can be put into place. Determining how quickly a Bluetooth virus might spread in a city such as London is one example which, if well understood, could lead to better preventative or more targeted treatment strategies for virus propagation in wireless environments.

Such mobile devices inherently have the tendency to move around with their user and therefore their use and movement patterns are dictated by human behaviors. This makes the methods used for modeling the spread of human viruses applicable to the spread of Bluetooth viruses. Inspired by such methods, we have developed a compartmental-based virus propagation model for predicting propagation characteristics of malware in peer-to-peer networks. We demonstrate the method through consideration of the Bluetooth protocol; however, the approach is applicable to malware propagation generally.

The remainder of this paper is organized as follows. Section 2 outlines Bluetooth, its vulnerabilities, and some virus propagation models. Section 3 details the developed model and how it incorporates technological traits, human behaviors, and heterogeneity. It also describes a simulation scenario and the general dynamics of the model. Results are given in Section 4, followed by a discussion and conclusion in Sections 5 and 6, respectively.

2 Bluetooth and Virus Spread

2.1 Vulnerabilities of Bluetooth

Bluetooth technology was originally intended to be a replacement for wired human interface devices such as computer keyboards, but is now also used for mobile devices. The operating range of Bluetooth depends on the device class. Class 1 radios have a range of 100 m, class 2 have a range of 10 m which is the most common for mobile devices, and class 3 radios have a range of 1 m [4].

Bluetooth viruses are spread as a result of user vulnerability as well as vulnerabilities of the Bluetooth technology. When a device has Bluetooth switched on, it can be in either invisible or discoverable mode. If the device is left in discoverable mode it can communicate with any

- *J.T. Jackson is with the Complexity Science Doctoral Training Centre, Department of Complexity Science, University of Warwick, Zeeman Building, Coventry CV4 8UW. E-mail: j.t.dudley@warwick.ac.uk.*
- *S. Creese is with the Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD. E-mail: sadie.creese@cs.ox.ac.uk.*

Manuscript received 31 Oct. 2011; revised 4 May 2012; accepted 23 July 2012; published online 13 Aug. 2012.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-2011-10-0246.
Digital Object Identifier no. 10.1109/TDSC.2012.72.

other device in range, leaving it open to the recipient of a virus. When a virus such as Cabir uses *proximity scanning* to search for devices in range, an invisible device has some short-term protection from an attack. *Brute force* proximity scanning however can find all hidden devices by guessing the unique identifier of each one. Many viruses continue to use social engineering techniques to lure people into opening attachments, clicking onto links or downloading files. Bluetooth allows peer-to-peer file sharing and synchronizing with another device such as between a smartphone and a laptop giving the opportunity for a virus to be propagated.

There are several versions of the Bluetooth standard in existence, each with their own vulnerabilities [5]. A larger threat than these vulnerabilities are programming flaws and incorrect implementation of Bluetooth protocols which can create exploits for a virus, leaving specific devices open to attack. Some mobile devices do not have the capability to be updated or users lack the necessary knowledge. As a result viruses can take advantage of known exploits. The BlueBag project, for example, used a covert Bluetooth attack device that demonstrated how such vulnerabilities and exploits could be targeted [6].

2.2 Learning from the Spread of Human Diseases

The mathematical study of the spread of human and animal diseases including viruses has been ongoing for over three centuries [7]. Because mobile Bluetooth devices have the tendency to move around with their user, the methods used for modeling the spread of human viruses are applicable to the spread of Bluetooth viruses. Compartmental-based modeling has been a traditional epidemiological technique for assessing the rate at which infectious diseases spread throughout the population. Within this technique, the population is divided up into compartments such as those who are *Susceptible* (S), those who are *Infectious* (I), and those who have *Recovered* (R). This *deterministic* technique is used for dealing with large populations [8]. Several variant versions have been used for modeling mobile viruses. The SI variant model has been used for modeling a mobile phone virus using two compartments [9]. The SEIS model includes an extra *Exposed* (E) compartment as there may be an incubation period before the virus attacks. This model was used for simulating virus propagation in peer-to-peer networks [10]. The SEIRD model was proposed to model virus propagation specifically via Bluetooth and MMS [3] to investigate the Commwarrior virus. The model includes an additional *Dormancy* (D) compartment to represent the condition when the virus drains the battery by sending out many MMS messages. *Stochastic* models are often used as a more realistic counter-part to deterministic models because they include an element of natural randomness. Ben-hua and Shao-hong [11], for example, use a stochastic SIS model for looking at how computer viruses spread on the internet. The *mobility patterns* of devices have also been investigated and considered to be an important factor for mobile devices [12]. Su and Chan [13] use *trace data* from smartphone activity to model how a worm might spread over Bluetooth. The advantage of this method is that temporal effects can be seen such as how the virus might spread at different times of the day. Wang et al. [14] use a combination of measured smartphone spatial data and the SI compartmental method. Wang predicted that once a mobile operating system's market share reaches a phase transition point, viruses will pose a serious threat.

3 Developed Bluetooth Virus Propagation Model

3.1 Model Requirements

Although the majority of the Bluetooth-based models discussed include some simple recovery measures, they tend not to include human behaviors, heterogeneity of the devices, and their users, or even different types of viruses. Su and Chan [13] have shown that temporal effects, such as users turning off their devices at night have an effect on the rate at which viruses spread. Other user-based factors affecting the vulnerability of the device such as leaving devices in discoverable mode are also important [15]. Gao and Liu [16] have recently considered human behaviors on Bluetooth and SMS virus propagation by analyzing the affect of simple mobility patterns based on the service area of cell towers, but do not include heterogeneity of devices or people, or different types of Bluetooth viruses.

The model developed here therefore uses a combination of the underlying link properties of Bluetooth and a novel compartmental model to allow human behaviors to be incorporated. The model accommodates heterogeneous devices, but also allows people to be separated into social classes with similar characteristics, such as school children or IT professionals. Bluetooth has a limited transmission range; viruses need a minimum amount of time to be transmitted; and people carry devices around at a particular velocity and density. These aspects are included as well as three types of Bluetooth virus spreading techniques. The following sections describe the model. Sections 3.2 to 3.4 model the link dynamics of Bluetooth, and derive an equation for the time-dependent infection rate of a Bluetooth network. Sections 3.5 to 3.8 describe the compartments of the model with different types of Bluetooth viruses, and how human behaviors and heterogeneity are included. Section 3.9 presents the dynamical system equations. A hypothetical scenario given in Sections 3.10 and 3.11 describes the model dynamics and stability.

3.2 Probability of Virus Transmission

In a network where Bluetooth devices move around with their user, the successfulness of a virus being transmitted across a single communication link is dependent upon the lifetime of the link and how much time is needed to transmit the virus. Fig. 1 shows the transmission radius R of node 1, and a second node moving inside node 1's transmission path from A to B.

Samar and Wicker [17] derive an equation for the link lifetime cumulative distribution F_{link}^{v1} of a particular node in a network moving with velocity $v1$, with a relative velocity between the two nodes of v. Assuming the time needed to transmit a virus is denoted by t_{virus}, then the probability of transmitting the virus is the probability that the link lasts for t_{virus} seconds or longer

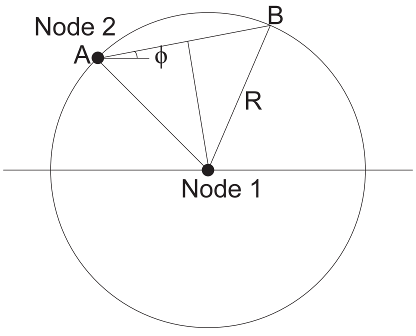

Fig. 1. Dynamics of node 2 moving within node 1's transmission path.

$$P_{t_{virus}} = 1 - F_{link}^{v1}(t_{virus}) \\ = \frac{1}{\pi(b-a)} \int_0^{\pi} \int_0^{\frac{2R}{t_{virus}}} v \sqrt{1 - \left(\frac{vt_{virus}}{2R}\right)^2} g(v,\phi,v1) dv d\phi, \quad (1)$$

where

$$g(v,\phi,v1) = \frac{u(h(v,\phi,v1)-a) - u(h(v,\phi,v1)-b)}{h(v,\phi,v1)}$$

$$h(v,\phi,v1) = \sqrt{v^2 + v1^2 + 2vv1cos\phi}.$$

The lower and upper velocity bounds are denoted by a and b, respectively, and $u(.)$ is the standard unit step function. The derivation of the probability distribution includes the following assumptions:

1. A node has a bidirectional communication link with any other node within a distance of R metres. The link breaks if the node moves to a distance greater than R.
2. A node in the network moves with a constant velocity which is uniformly distributed between a and b ms^{-1}.
3. The direction of a moving node is uniformly distributed between 0 and 2π radians.
4. A node's speed, its direction of motion, and its location are mutually independent.

Using assumption 2, the average node velocity can then be defined as

$$v_{average} = \frac{a+b}{2}. \quad (2)$$

The probability (1) cannot be solved analytically, but can be solved via numerical integration. Probability curves for a variety of average node velocities are given in Fig. 2. Su and Chan [13] undertook some practical measurements to determine how long it takes to send virus data across a Bluetooth link. It was found the time was in the order of 10 seconds, with the majority of this time used for establishing the communication channel rather than transferring the data. Therefore, from the probability graph given in Fig. 2, nodes traveling greater than 3 m/s have a very low probability of transmission for viruses that take 10 seconds to transfer their data.

3.3 Contact Rate

The rate at which a node comes into contact with other nodes is defined as the contact rate. The contact rate of a node infected with a virus will depend upon the number of new nodes within its transmission range in the time, t_{move}, it takes for the node to move one full distance from A to B as shown in Fig. 3 and the maximum possible rate of transmissions governed by t_{virus}.

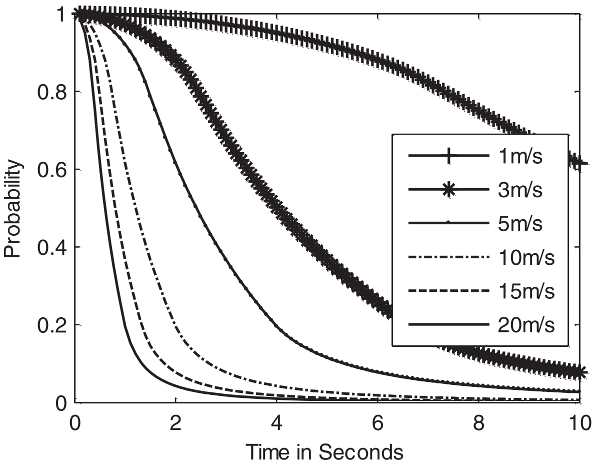

Fig. 2. Probability of virus transmission, with a transmission range R of 10 m for a variety of average node velocities.

The shaded region shows the area of transmission where new nodes are encountered. Due to symmetry, this region can be represented as a square with area $4R^2$. The rate of new nodes encountered is therefore defined as

$$nodes_{rate} = (density \times transmission\ area)/t_{move} \\ = \left(\rho \times 4R^2\right) \Big/ \frac{2R}{v_{average}}. \quad (3)$$

And the maximum rate of transmissions is defined as

$$trans_{rateMax} = \frac{1}{t_{virus}}. \quad (4)$$

Therefore, the contact rate is the minimum of the rate of new nodes in range and of the maximum possible rate of transmissions

$$Contact_{rate} = \min\{nodes_{rate}, trans_{rateMax}\}. \quad (5)$$

3.4 Infection Rate

The rate of infection caused by one infected node is the contact rate multiplied by the probability of transmission.

$$\beta_i = Contact_{rate} \times P_{t_{virus}}. \quad (6)$$

Fig. 4 shows how the infection rate β_i varies with density for several values of virus transmission times t_{virus}, with a

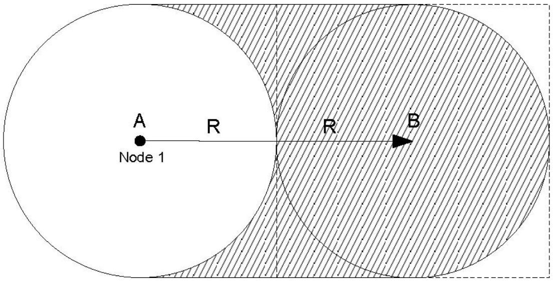

Fig. 3. Shows node 1 moving a full distance from A to B to a new area covered by its transmission range.

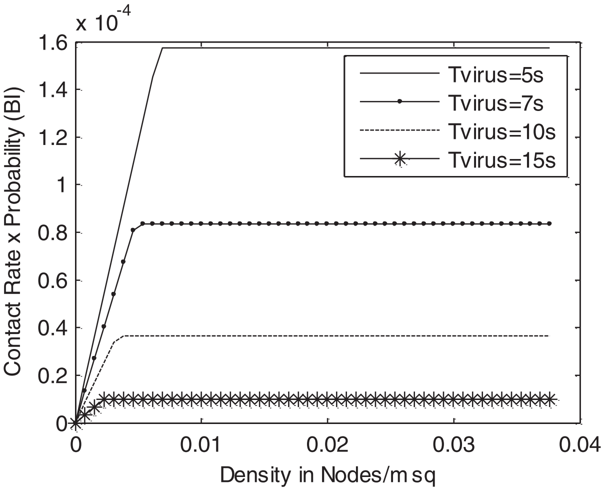

Fig. 4. Rate of infection from one infected node, with the average velocity fixed at $1.5\ \mathrm{ms}^{-1}$ for a variety of virus transmission times.

fixed average node velocity $v_{average}$ of $1.5\ \mathrm{ms}^{-1}$. The rate of infection increases as the density increases because there are more nodes coming into contact, until it reaches a plateau. This is where the rate is limited by the maximum transmission rate governed by t_{virus}.

Fig. 5 shows how the infection rate β_i varies with average node velocity $v_{average}$ for several values of the density ρ while the virus transmission time t_{virus} was fixed at 10 s. When the nodes are moving too fast, there is not sufficient time to propagate the virus and the infection rate is very low. As the node velocity is reduced, the rate of infection increases until it reaches a peak at the optimum velocity for the given virus transmission time. Reducing the velocity further then reduces the rate of infection as the nodes do not move around sufficiently fast enough to propagate the virus as quickly. For high density values, the peak is more prominent where the infection rate is very sensitive to the average node velocity. For low density values, the average node velocity has less of an impact on the infection rate.

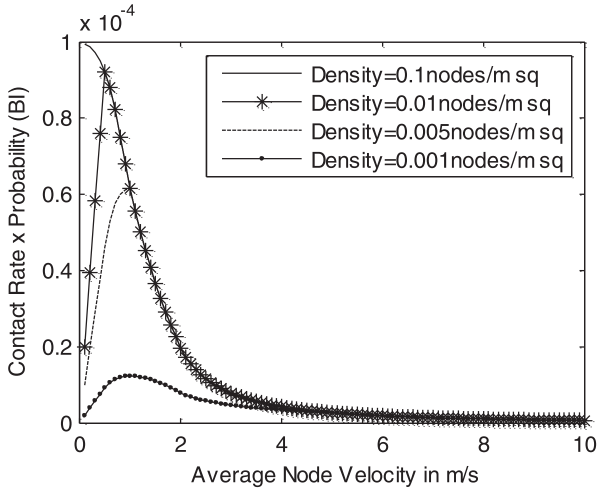

Fig. 5. Rate of infection from one infected node, with the virus transmission time fixed at 5 seconds for a variety of density values.

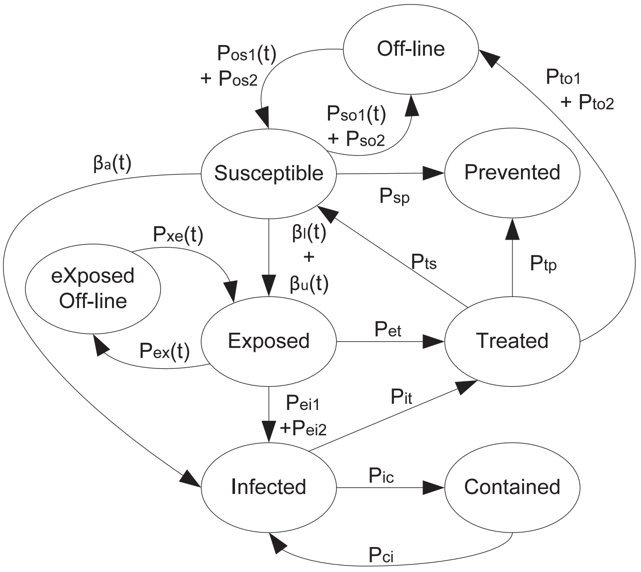

Fig. 6. SEPTICOX model showing the compartments and transitions.

The time-dependent infection rate $\beta(t)$ of the network is attributed to the proportion of the population who are already infected at a given time and is given by

$$\beta(t) = \beta i \times \left(\frac{I(t)}{N}\right), \tag{7}$$

where N is the total number of nodes in the network and $I(t)$ is the number of nodes infected at time t.

3.5 Compartments of the Model

The SEPTICOX model as shown in Fig. 6 uses eight compartments: *Susceptible* (S), *Exposed* (E), *Prevented* (P), *Treated* (T), *Infected* (I), *Contained* (C), *Offline* (O), and *eXposed offline* (X). This model incorporates three types of virus spread: *automated* via Bluetooth, automated via Bluetooth with a *latency* period, and via Bluetooth requiring *user* interaction. The automated spread represents the case where devices that are switched on and in discoverable mode can automatically receive and forward a virus without user intervention. This is likely to happen while the user remains oblivious until the device begins to malfunction. The latency spread is similar to the previous case except that there is a delay before the virus acts so that the device becomes exposed to the virus before becoming infected. Fortunately, existing Bluetooth viruses that have been observed so far all require human intervention, but it is unclear how long this will last. User interaction spread occurs when the user is required to open a file or click onto a link before the virus becomes active. The Cabir worm [2] spreads in this way because it propagates automatically via Bluetooth but asks the user if they wish to launch the file. In this case, the device may become exposed to the virus but it is the action of the user that determines whether or not the device becomes infected. User spread may also happen via Bluetooth when exchanging files between friends, or from synchronizing the device to a laptop where various files including e-mail are exchanged.

Within the compartmental model devices that are *Offline* are not infected, and are either switched off or in invisible mode. While offline, they cannot be infected with a virus. While some users have their devices permanently switched on, a proportion of the population turn their devices on and off every day at a rate $P_{os1}(t)$ and $P_{so1}(t)$, respectively. Some people also inadvertently leave their device in discoverable mode and sometime later remember to switch them back to invisible mode at a rate P_{os2} and P_{so2}, respectively. Devices that are switched on and are operating in discoverable mode become *Susceptible* and may receive a virus. They may first become *Exposed* to the virus at a rate $\beta_l(t)$ or $\beta_u(t)$ or they may become immediately *Infected* at a rate $\beta_a(t)$ depending upon the type of Bluetooth virus being transmitted; *automated (a), latency (l), or user (u)* spread. A susceptible device may be prevented from being exposed or infected by installing a patch to remove the vulnerability at a rate P_{sp}. Once the device is exposed or infected with a virus, the virus may be removed via servicing, resetting the device or using antivirus treatment at a rate P_{et} or P_{it}. The device then becomes *Treated*. A patch can then be applied to remove the vulnerability so that the device does not become reinfected at a rate P_{tp}, or the user may decide to be more cautious and switch the device to invisible mode at a rate P_{to2}, or turn it off at a rate P_{to1}; otherwise, the device becomes susceptible again to the same virus at a rate P_{ts}. Once a device is infected, it may become switched off at a rate P_{ic} rendering the device *Contained*, but as soon as it is turned back on again at a rate P_{ci} it becomes infectious.

3.6 Incorporating Human Behaviors

Using trace data, Su and Chan [13] found that varying the initial time of the outbreak contributed to the rate at which devices became infected. It was found that Bluetooth worms were more likely to spread during the day than overnight. This could have been due to devices being switched off, or lack of movement overnight. The turning on and off of Bluetooth devices is therefore an important attribute of the SEPTICOX model. The time-dependent *"on"* $(P_{os1}(t), P_{xe}(t))$ and *"off"* $(P_{so1}(t), P_{ex}(t))$ switching rates are modeled as windowed normal distributions over a period of 24 hours with a mean μ corresponding to the time of day of the peak switching rate. The standard deviation σ is set to be one third of the time spread t_{spread} to achieve a normal curve that approaches zero at t_{spread} from the mean corresponding to the range over which the switching occurs. The windowed distribution is repeated every day and is given in (8), where t represents time of the day, and $\sigma = t_{spread}/3$.

$$f(t|\mu,\sigma) = \frac{1}{(\sigma)\sqrt{2\pi}} e^{\frac{-(t-\mu)^2}{2(\sigma)^2}}. \qquad (8)$$

Within the *user* spread model, it is necessary to understand human behaviors when it comes to clicking onto suspicious attachments, links, and files. There is very little data regarding human behaviors in this respect; however, an experiment was conducted by Stevens [18] in 2007 over a six month period using a Google advertisement word campaign. The word campaign was entitled "Is your PC virus-free? Get it infected here!" The Google word campaign was displayed 259,723 times and was clicked on 409 times. This gives a click probability of 0.0016. The link took the user to a fictitious website that could easily have contained a virus. Although the word campaign title clearly sounded suspicious, it did not stop some people from clicking onto it. The rate at which users might receive malware in the first place is a separate issue. For internet users, the 2008 Cisco Security Report [19] stated that in December 2008 people received an average of 100 spam e-mails per day and 0.35 percent of them had malicious content. This is equivalent to a rate of 4.05×10^{-6} malicious e-mails per second. In 2009, the global level of spam increased before dropping in 2010 with the current rate for mobile users likely to be less.

TABLE 1
Response Times Reported by AV-Test in 2008

Product	*Response times (hours)*
AVG	4-6
F-Secure 2009	0-2
Kaspersky	0-2
Microsoft	6-8
Norton 2009 (Symantec)	0-2
Sophos	2-4

There is very little published data regarding how and when users apply antivirus measures. If an antivirus tool is installed in a personal computer and automated updates are turned on, according to AV-Test as reported in September 2008 [20] a range of response times can be expected for a selection of products to a new virus as given in Table 1. These response times can be considered the *best case scenario* because in practice not everyone regularly uses antivirus tools or has automated updates turned on. For mobile phone viruses, the figures are likely to be worse as the tools and technology is less mature.

3.7 A Heterogeneous Population

Many viruses are targeted at specific vulnerabilities such as one associated with a particular version of Bluetooth [5], or vulnerabilities within an operating system, or even specific to a particular manufacturer due to the specific implementation. For example, the Cabir worm only affected smartphones running the Symbian operating system. Therefore, the diversity of the devices within the network will have an impact on virus propagation. According to Gartner Research [1], in quarter one of 2011, Android had 36 percent of the market share of worldwide smartphone sales by operating system, Symbian had 27.4 percent, and iOS had 16.8 percent, with various others making up the rest. Wang et al. [14] who modeled the spreading patterns of viruses using spatial data of phone locations looked at changes in the number of infected devices over time with different market share values. The results showed that the higher the market share, the faster the rate of infection.

Different groups of users may also behave differently, for example, the use of smartphones among a group of teenage friends will differ from their parents. The level of heterogeneity in the network will affect the spread of viruses. Heterogeneity has been included within the SEPTICOX model and is described in the next section.

3.8 Heterogeneous SEPTICOX

A method of adding heterogeneity to a compartmental model is by splitting the population up into classes [8]. This method was chosen because it allows devices or users displaying similar characteristics or behaviors to be grouped together, while still following the same underlying system dynamics. For the SEPTICOX model, this has been achieved by stacking up a number of the models shown in

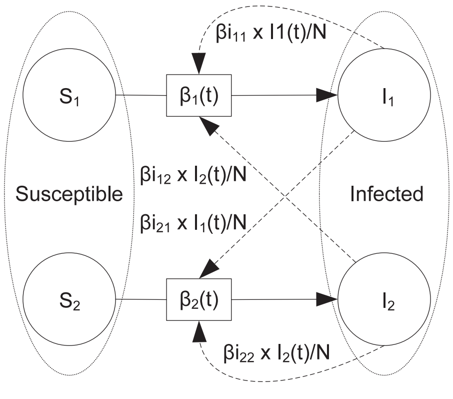

Fig. 7. Example of a compartmental model with two classes representing heterogeneity in the system.

Fig. 6 on top of each other, so that each compartment can be represented as a column vector comprising each class for that compartment.

The contact rate, and hence the individual infection rate βi, can then be represented as a matrix. This allows the contact rates *within* classes to be different, and also allows the contact rates *between* classes to be different. The advantage of this is that it represents a more realistic scenario. For example, if one class represented a group of children attending the same school with a smartphone, and another class represented their parents with a smartphone, then the contact rate between the children would be very different to the contact rate between parents of one child and the parents of another. Similarly, the contact rate between the children and the parents would be different again. In epidemiology, this is called the *Who Acquires Infection From Whom* (WAIFW) matrix. An example matrix is given below for a model comprising two classes with two compartments and is illustrated in Fig. 7 where only the *infected* nodes have an influence over the rate at which those *susceptible* become infected

$$\begin{bmatrix} \beta i_{11} & \beta i_{12} \\ \beta i_{21} & \beta i_{22} \end{bmatrix}, \tag{9}$$

where βi_{11} is the individual infection rate within class 1 and βi_{12} is the individual infection rate from classes 2 to 1. The time-dependent *infection* rate $\beta(t)$ for a particular class is now influenced by all the classes within the network and is summed to give an extended version of (7):

$$\beta_k(t) = \left\{ \sum_{j=1}^{n} \beta i_{kj} \frac{I_j(t)}{N} \right\}, \tag{10}$$

where k, j is the class number, n is the number of classes, $I_j(t)$ is the number infected in class j at time t, and N is the total number of devices in the network.

Within the model, the composition of the classes involves the selection of two independent parameters: device type and Bluetooth version. The choices within these parameters are given in Table 2. A choice for class 1 within the model, for example, could be *Smartphone X* using *Bluetooth V2*. These two parameters incorporate some heterogeneity and allow the simulation of targeted viruses to be either *device specific* or *version specific*.

TABLE 2
Choices within the Two Class Parameters

Device Type	***Bluetooth Version***
Smartphone X	V1 (encompassing1.0,1.0B,1.1,1.2)
Smartphone Y	V2 (encompassing 2.0,2.1)
Laptop A	V3 (encompassing 3.0)

The rate parameters within the model can be set for each class allowing different device characteristics and human behaviors to be modeled. For example, two classes may contain the same device type and Bluetooth version, but the behaviors of the users may be different; one class may consist of IT professionals that install patch updates every day, whereas another class may not install updates. The contact rates between such classes will be different to the contact rates within classes. These differences will influence the outcome of those infected.

The *automated* spread virus method can be modeled as shown in Fig. 7 where only the *infected* nodes have an influence over the rate at which those *susceptible* become infected. The *latency* spread virus includes an exposed compartment prior to infection. It is still the *infected* nodes that have an influence, but this time they affect the rate at which those *susceptible* become *exposed*, and (10) is still valid but becomes the time-dependent *exposure* rate.

The *user* spread virus however is different from the other two, as it relies on the interaction of the user to spread the infection. For some classes, the devices may become exposed to the virus but never actually become infected. For example, a user opens a malicious attachment from an e-mail on the laptop but it does not become infected because the virus was not specific to the laptop. The user then synchronizes the laptop with the smartphone over Bluetooth downloading the attachment, and infecting the phone. In this model, both the *Infected* and the *Exposed* compartments have influencing effects on the spread of a virus. An example showing the dotted lines of influence is illustrated in Fig. 8 where class 1 is Laptop A, class 2 is Smartphone X, and the virus chosen is device specific to Smartphone X. Class 1 never becomes infected, but its exposure to the virus has some influence over the rate of exposure of class 2. Similarly, those infected within class 2 influence the exposure of class 1.

The time-dependent *exposure* rate $\beta(t)$ for a particular class is now influenced by all the classes within the *Infected*

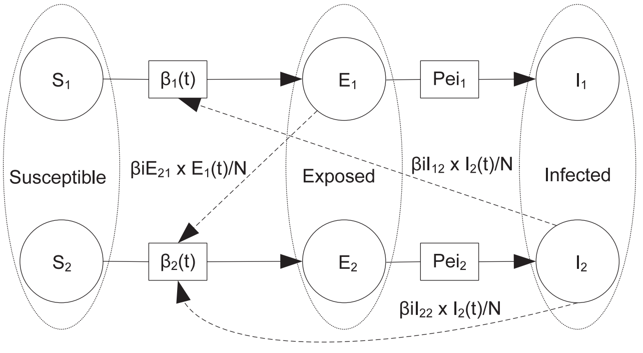

Fig. 8. User spread model with two heterogeneity classes.

and *Exposed* compartments and is summed to give an extended version of (10):

$$\beta_k(t) = \left\{ \sum_{j=1}^{n} \beta i_{I_{kj}} \frac{I_j(t)}{N} \right\}_I + \left\{ \sum_{j=1}^{n} \beta i_{E_{kj}} \frac{E_j(t)}{N} \right\}_E, \tag{11}$$

where k, j is the class number, n is the number of classes, N is the total number of devices in the network, $I_j(t)$ is the number infected, and $E_j(t)$ is the number exposed in class j at time t. Equation (11) can be generalized for all spread models where some of the values will be zero when the automated Bluetooth spread methods are chosen. The application of an Infected and an Exposed masking matrix is used to allow only the correct influences to be applied depending upon the classes chosen, the virus type, and the virus spread method.

3.9 Dynamical System Equations

The dynamical system equations for the model are

$$\begin{aligned}\frac{dS_k(t)}{dt} &= O_k(t)(P_{os1_k} + P_{os2_k}) + T_k(t)P_{ts_k} \\ &\quad - S_k(t)P_{sp_k} - S_k(t)\beta_{a_k}(t) \\ &\quad - S_k(t)(\beta_{u_k}(t) + \beta_{l_k}(t)) \\ &\quad - S_k(t)(P_{so1_k} + P_{so2_k}),\end{aligned} \tag{12}$$

$$\begin{aligned}\frac{dE_k(t)}{dt} &= S_k(t)(\beta_{u_k}(t) + \beta_{l_k}(t)) + X_k(t)P_{xe_k} \\ &\quad - E_k(t)P_{ex_k} - E_k(t)P_{et_k} \\ &\quad - E_k(t)(P_{ei1_k} + P_{ei2_k}),\end{aligned} \tag{13}$$

$$\frac{dP_k(t)}{dt} = S_k(t)P_{sp_k} + T_k(t)P_{tp_k}, \tag{14}$$

$$\begin{aligned}\frac{dT_k(t)}{dt} &= E_k(t)P_{et_k} + I_k(t)P_{it_k} - T_k(t)(P_{to1_k} + P_{to2_k}) \\ &\quad - T_k(t)P_{tp_k} - T_k(t)P_{ts_k},\end{aligned} \tag{15}$$

$$\begin{aligned}\frac{dI_k(t)}{dt} &= E_k(t)(P_{ei1_k} + P_{ei2_k}) + S_k(t)\beta_{a_k}(t) \\ &\quad + C_k(t)P_{ci_k} - I_k(t)P_{it_k} - I_k(t)P_{ic_k},\end{aligned} \tag{16}$$

$$\frac{dC_k(t)}{dt} = I_k(t)P_{ic_k} - C_k(t)P_{ci_k}, \tag{17}$$

$$\begin{aligned}\frac{dO_k(t)}{dt} &= T_k(t)(P_{to1_k} + P_{to2_k}) + S_k(t)(P_{so1_k} + P_{so2_k}) \\ &\quad - O_k(t)(P_{os1_k} + P_{os2_k}),\end{aligned} \tag{18}$$

$$\frac{dX_k(t)}{dt} = E_k(t)P_{ex_k} - X_k(t)P_{xe_k}, \tag{19}$$

where $\beta_{a_k}(t)$, $\beta_{l_k}(t)$, and $\beta_{u_k}(t)$ are the time-dependent infection rates of the automated, latency, and user spread, respectively. k is the class number.

3.10 Example Simulation Scenario: Around London with a Heterogeneous Population

A hypothetical scenario has been simulated with realistic parameters to show how two different types of Bluetooth virus might spread in a large city such as London over a period of days. The scenario uses three classes with market shares of 45, 34, and 21 percent, comparable to the market share values of the top three companies in quarter one of 2011. The range of a smartphone was assumed to be 10 m [4] and the virus transmission time was set to 10 s. A single smartphone was initially infected in both cases.

In a large city such as London, people work and live close to each other giving the opportunity to pass many Bluetooth devices. The 2010 national statistics report recorded the population of London in 2009 to be 7.75 million, of which 24 percent were under 20 years of age, with a density of 4,900 people per km^2 [21]. According to Ofcom, in 2011 27 percent of adults and 47 percent of teenagers in the United Kingdom owned a smartphone, with 81 percent of them leaving their phone switched on all of the time [22]. Using London's population figures, this equates to an average of 30 percent of the population owning a smartphone, or 2.3 million people, with a density of 0.001470 phones per m^2. According to Citroen, the average car speed around London is just 7 mph [23] ($3.1\ \text{ms}^{-1}$), close to twice the average walking speed of $1.5\ \text{ms}^{-1}$ [24], giving an average of the two speeds of $2.3\ \text{ms}^{-1}$ for the smartphones. The parameters used within this simulation are given in Table 3. Classes 1 and 3 users both have the same make of smartphone. Class 3 users like to keep up with the latest technology, installing new patches and antivirus tools and are cautious about clicking onto suspicious links.

Class 1 users however prefer to stick to the manufacturer's default; they do not want to be concerned with installing updates. If their phone stops working it may cause them to search for an antivirus treatment or just switch the device off in frustration. Class 1 users are also quite ready to click onto suspicious links out of curiosity. Class 2 users have similar behaviors to class 1 when it comes to suspicious links and updates, but they have a different make of phone, and 81 percent of them have their phones permanently in discoverable mode.

The first virus to be released is an automated Bluetooth virus targeted specifically at a Bluetooth V1 vulnerability, affecting all three classes. The second virus to be released is the user spread virus targeted specifically at the smartphone X, affecting classes 1 and 3. The results are shown graphically in Section 4.5.

3.11 Model Dynamics and Stability

The simulation scenario in Section 3.10 describes two single instances of what might happen given a fixed set of parameter values, but the general dynamics and long-term stability can be categorized into three possible outcomes for a single class model. For multiple classes, the combined network outcome is more complex. As given in Table 4, the *first outcome* for a single class model is governed only by the *basic reproduction number* (R_0) [25] which is an important quantity used in modelling disease epidemics in compartmental-based models. It is considered as a threshold parameter that determines whether the disease

TABLE 3
Parameter Values Used within the London Simulation

	Parameter	*Class1* *45%* *Smartphone X* *Bluetooth V1*	*Class2* *34%* *Smartphone Y* *Bluetooth V1*	*Class3* *21%* *Smartphone X* *Bluetooth V1*
1	No. nodes	1,046,250	790,500	488,250
2	Initial no. Off- line	50%	19%	50%
3	P_{os1} – turn on	Every morning	Every morning	Every morning
4	P_{os2} - sw itch to discoverable	1in1000 after 1 day	NA	1in1000 after 1 day
5	P_{so1} – turn off	50% Every evening	19% Every evening	50% Every evening
6	P_{so2} – sw itch to invisible	75% of those 1 in 1000 people after 3 days	75% of those 1 in 1000 people after 3 days	75% of those 1 in 1000 people after 3 days
7	P_{sp} – install patch	**No**	**No**	**After 5 days**
8	P_{xe} – turn on	Every morning	Every morning	Every morning
9	P_{ex} – turn off	50% every evening	19% every evening	50% every evening
10	P_{ei1} – user click onto a virus	**0.5 ×100 links × 0.35% after 1 day**	**0.5 ×100 links × 0.35% after 1 day**	**0.0016 ×100 links × 0.35% after 1 day**
11	P_{ei2} – latency time	NA	NA	NA
12	P_{et} – treatment	**After 5 days**	**After 5 days**	**After 3 days**
13	P_{it} – treatment	**After 3 days**	**After 3 days**	**After 2 hours**
14	P_{ic} - contained	50% after 3 hours	50% after 3 hours	50% after 3 hours
15	P_{ci} – turn on	1 day	1 day	1 day
16	P_{ts} – become susceptible	**After 12 hours**	**After 12 hours**	**25% after 12 hours**
17	P_{tp} – install patch	**No**	**No**	**50% after 12 hours**
18	P_{to1} – turn off	**No**	**No**	**10% after 12 hours**
19	P_{to2} – sw itch to invisible	**No**	**No**	**15% after 12 hours**

TABLE 4
Virus Outcomes under Different Conditions

	Short-term spread	*Long-term stability*	*Condition*
1	Dies aw ay	Dies aw ay	R0<1
2	Spreads	Dies aw ay	R0>1, Ptp>0 or Psp >0
3	Spreads	Persists	R0>1, Ptp=0 and Psp=0

dies away ($R_0 < 1$) or spreads ($R_0 > 1$) when one initial infective is introduced into the susceptible population. R_0 can be derived as a function of all the nonzero parameters in the model; however, it can also be observed through simulation as shown in Section 4.6. For the first outcome, when $R_0 < 1$, the Bluetooth virus will *die away*. For the remaining two outcomes when $R_0 > 1$, the Bluetooth virus will spread. The *second outcome* however is also governed by the *existence* of the *Prevented compartment* which occurs when the two patching parameters P_{tp} or P_{sp} are greater than zero. Because the SEPTICOX model has a constant population where nodes do not enter or leave the network, the Prevented compartment becomes an end state, where once entered the devices cannot leave. Under this condition, although the Bluetooth virus will *spread* in the network, it will eventually *die away* when all of the infected nodes have installed patches. The *third outcome* is additionally governed by the *removal* of the *Prevented compartment* which occurs when P_{tp} and P_{sp} are both zero. Under this condition, there is no longer an end state and the Bluetooth virus will *spread* before *persisting* in the network. This makes sense since simply removing a virus from a node via treatment will not prevent it from reoccurring and it is therefore important to remove vulnerabilities exploited by malware as a long term solution. These three outcomes are demonstrated in the results Section 4.6. The parameters used are those of class 3 users in the London simulation, with some parameters varied as stated in the results.

4 Results

For all results within Sections 4.1 to 4.4, the size of the population was fixed at 1,000 with a density of $0.000768\ \mathrm{nodes/m^2}$. The number initially infected was 1. In addition, for Sections 4.2 to 4.4, the average node velocity was fixed at $2.3\ \mathrm{ms^{-1}}$, the range was 10 m, and t_{virus} was 10 s.

4.1 Automated Bluetooth Spread in a Homogeneous Population

Within a homogeneous population, an *automated* Bluetooth virus replicates itself as fast as possible with nodes in range. Fig. 9 shows how fast this type of virus propagates when human behaviors are excluded, for a number of different virus transmission times. The average node velocity was $2.3\ \mathrm{ms^{-1}}$ and the transmission range was 10 m. For a transmission time of 10 s, the entire population of Bluetooth devices became infected within 1 hour giving an indication as to how quickly a virus like this could spread without any other human factors.

Fig. 10 shows how quickly the same population of devices within the network become infected for the three different Bluetooth transmission ranges of 1, 10, or 100 m, with t_{virus} fixed at 10 s. As expected, the range makes a big difference to how quickly the virus spreads. For a range of 1 m, the population takes 50 days to become infected, but less than 5 minutes for a 100 m range. To help reduce the spread of Bluetooth viruses, it is advisable that the transmission range

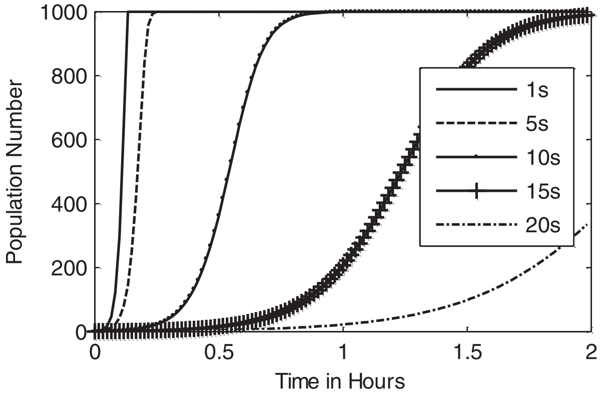

Fig. 9. Automated Bluetooth spread showing the effect of the virus transmission time on the number infected over time.

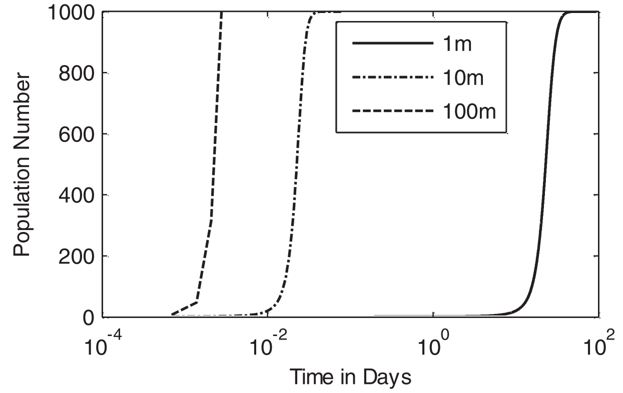

Fig. 10. Automated Bluetooth spread showing the effect of the node transmission range on the number infected over time.

is kept as small as possible without impinging on the task that it was designed to do.

Figs. 11 and 12 show how quickly the same population of devices within the network become infected for different average node velocity values while keeping the range and t_{virus} fixed at 10 m, and 10 s, respectively. For node velocities above $1\ \mathrm{ms}^{-1}$, the spread of the virus reduces as the velocity increases as there becomes less time available for the virus to be transmitted across the link, but for node velocities below $1\ \mathrm{ms}^{-1}$, when more time is available, the spread of the virus again reduces due to a combination of the low density and the lack of movement of the nodes. This effect does not happen for high density values where nodes are so close to each other that reducing the velocity below $1\ \mathrm{ms}^{-1}$ has little or no effect on the spread. This is in line with the graph shown in Fig. 5.

4.2 Automated Bluetooth Spread with a Latency Period in a Homogeneous Population

Fig. 13 shows how the spread of a Bluetooth virus in a homogeneous population is reduced by introducing a latency time into the model.

Some viruses such as the Commwarrior have a latency period before becoming destructive and infectious. For a latency time of 10 days, the rate of spread of the virus is much reduced as expected.

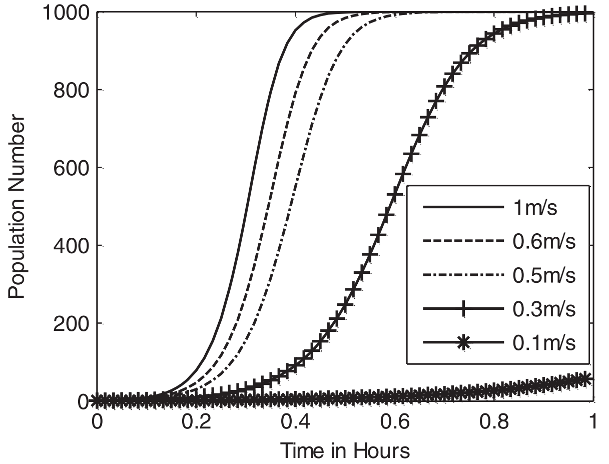

Fig. 12. Automated Bluetooth spread showing the effect of the average velocity below $1\ \mathrm{ms}^{-1}$ for a density of $0.000768\ \mathrm{nodes/m}^2$.

4.3 User Spread in a Homogeneous Population

If Bluetooth devices such as smartphones were to receive unwanted or malicious files and e-mail at the same rate as personal computer internet users receive spam e-mail of 100 per day (see Section 3.6), with a probability of opening a suspicious attachment of 0.0016, then the rate of virus spread for different percentages of files and e-mail containing a virus is shown in Fig. 14.

As shown in the graph, receiving malicious content of 0.35 percent takes approximately one year before 20 percent of homogeneous Bluetooth devices become infected. For a percentage of 5 percent, nearly 100 percent of the population become infected within the same time. This highlights that when users are involved in the spread of viruses the time scales can dramatically increase. There are many spam filters in wide spread use for internet users, but the filtering of mobile messages may also become important in the future to reduce the spread of viruses.

4.4 Incorporating Human Behaviors

The effects of human behaviors toward their Bluetooth devices such as turning them on and off contribute to how a virus might spread at various times throughout the day.

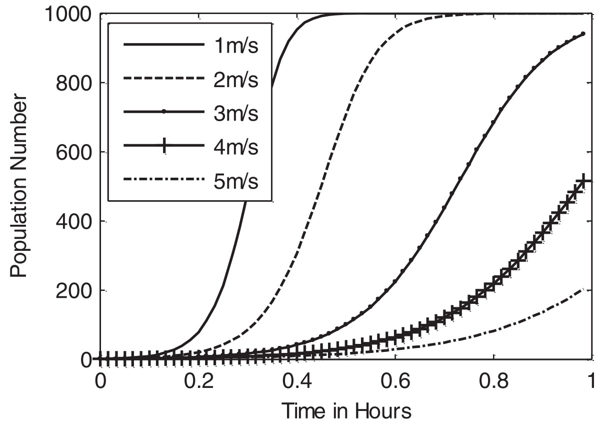

Fig. 11. Automated Bluetooth spread showing the effect of the average velocity above $1\ \mathrm{ms}^{-1}$ for a density of $0.000768\ \mathrm{nodes/m}^2$.

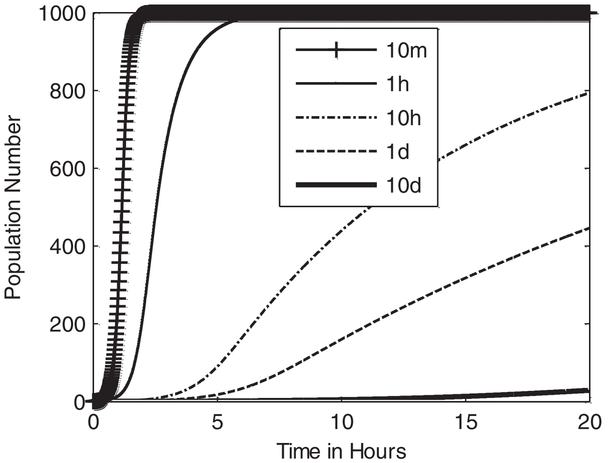

Fig. 13. A latency spread virus showing the effect in minutes (m), hours (h), and days (d) on the number infected over time.

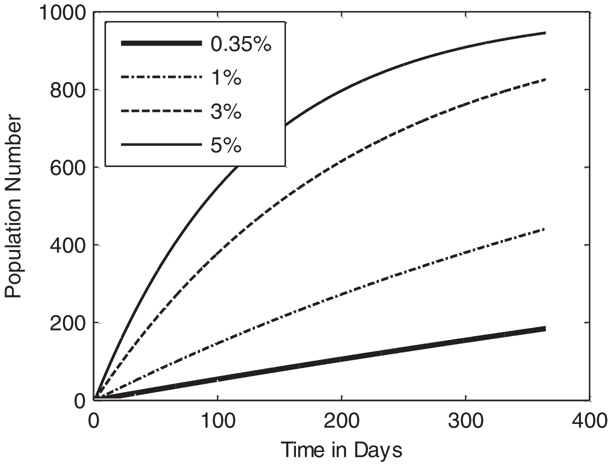

Fig. 14. User spread showing the effect of the percentage of malicious files and e-mail a mobile receives on the number infected.

Fig. 15 shows the effect of a virus being inserted into the network on day 2 of the simulation at different times of the day while modeling the behaviors of devices being turned on and off. For a switch on rate peaking at 9 am and a switch off rate peaking at 7 pm with a 3 hour spread (windowed Gaussian), the results are comparable to those found by Su and Chan [13] which used trace data of smartphone activity. They found that viruses released after 6 pm at night reached a lower plateau of infected devices by the end of the day. While the exact numbers are not identical due to the differences in the models and parameters, the underlying effect of this human behavior that has been included in this model is similar to that experienced in a real environment. Without any antivirus measures in place, the number of infected individuals increases the following day when more users turn their devices back on. Although not shown here, over several days all 1,000 devices eventually become infected.

Another human behavior included in the model is the use of antivirus measures. Fig. 16 shows the effect of users installing patches to remove vulnerabilities. Here, devices are switched on and off, and the virus is released at midnight on the first day. For the automated Bluetooth virus which can spread in a matter of hours, patching of vulnerabilities with typical times of one day has very little effect on the short term spread of the virus. For viruses that have latency periods, patching has more of an effect on reducing the spread.

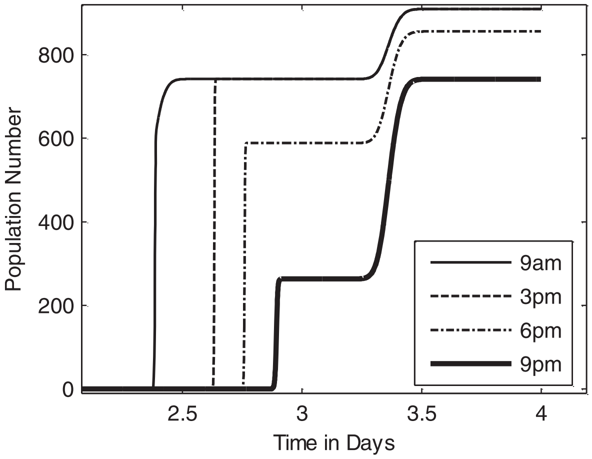

Fig. 15. Showing effect of virus start time on how the population become infected whilst users are switching on and off devices throughout the day.

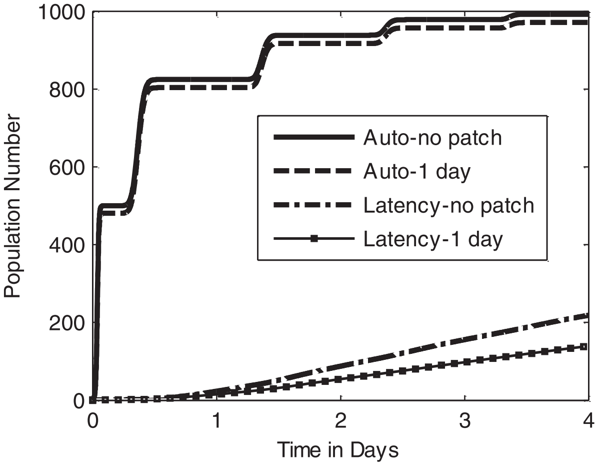

Fig. 16. Bluetooth virus spread showing the effect of patching vulnerabilities on the rate at which the population become infected.

Patching is not the only antivirus measure whose effect is incorporated into the SEPTICOX model. Fig. 17 shows how the addition of a number of other antivirus measures affects the spread of an automated virus. The graph shows that obtaining treatment for the virus after three days has some additional effect, but users simply switching off their devices as soon as they realize they have become infected has a large effect by containing its spread. With a best case scenario response time of two hours, the spread of the virus can be reduced further with the daily peak diminishing on successive days.

4.5 Example Simulation Scenario: Around London with a Heterogeneous Population

Using the parameters defined in Section 3.10, the first virus released in the London simulation was an *automated* Bluetooth virus targeted specifically at a Bluetooth V1 vulnerability, affecting all classes. Fig. 18 shows how the virus spread across the three classes of the heterogeneous population. Included in the graphs are the curves for each compartment showing user behavior and its impact on the

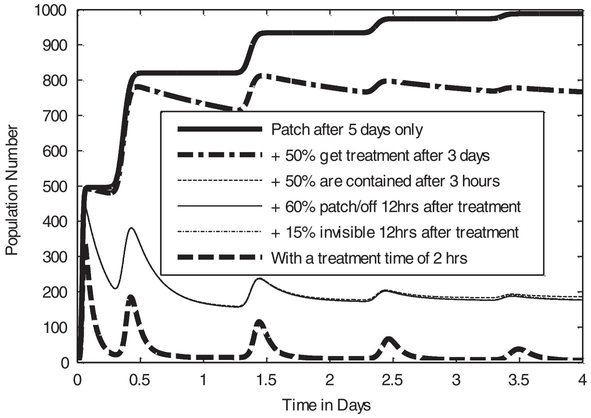

Fig. 17. Automated Bluetooth spread showing the cumulative effect of adding antivirus measures to the number infected over time.

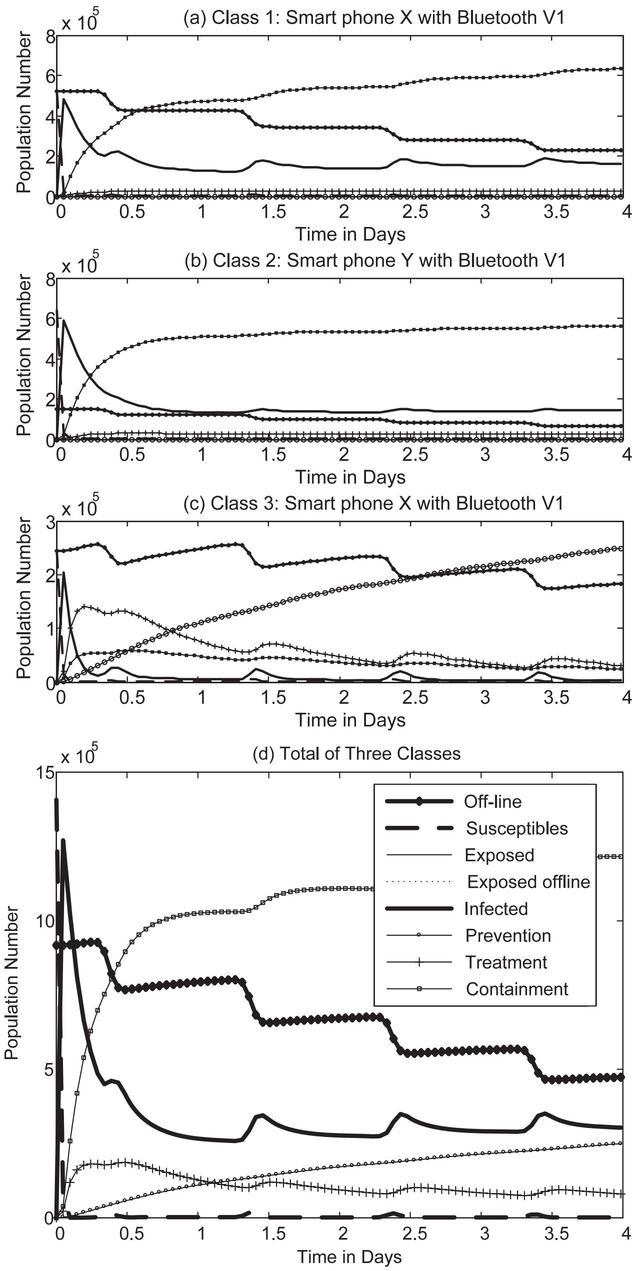

Fig. 18. London simulation showing the effect of an automated Bluetooth virus on a heterogeneous population of three classes.

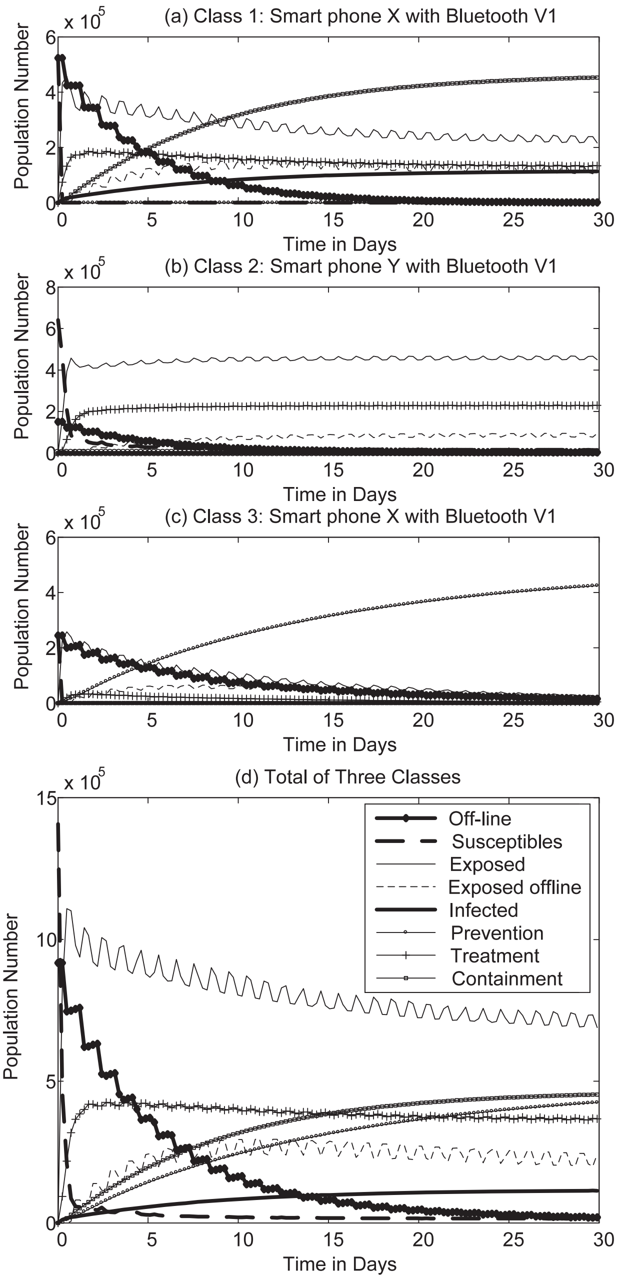

Fig. 19. London simulation showing the effect of a user virus on a heterogeneous population of three classes.

spread. As expected, all three classes were affected by the virus. Within each class, an initial peak of infection occurs before the actions of users begin to take effect. Subsequent peaks of infection are caused by users turning their phones on and off and switching them between modes of discovery. Despite only 34 percent of the population belonging to class 2, they still have the highest initial outbreak of the virus owing to the fact that 81 percent of users had their phone permanently switched on and in discoverable mode, as per Ofcom's 2011 report [22]. This highlights the growing danger of our current trend toward the "always on" society and its affect on the spread of viruses. This is a change in behavior from a few years ago where more devices would be switched off, especially at night. As Su and Chan [13] highlighted, and shown here, the short-term spread of a virus can be reduced by phones being in invisible mode or switched off when not in use. Although classes 1 and 3 users turn their phones on and off at the same rate, the security consciousness of class 3 has reduced the number of infected individuals further through their installation of patches and turning devices off. This action has an effect on the long-term spread of the virus by causing it to die away. Graph (d) in Fig. 18 shows the resulting virus spread over the whole network.

The second virus released was the *user* virus targeted at the smartphone X, affecting classes 1 and 3 users. Fig. 19 shows how the virus spread across the three classes of the population. This virus requires human input, reducing the rate of spread compared to the first example. Because of the action taken by class 3 users to prevent and treat viruses, the preventative measures stopped the spread of the virus within this class. The class 3 graph shows the

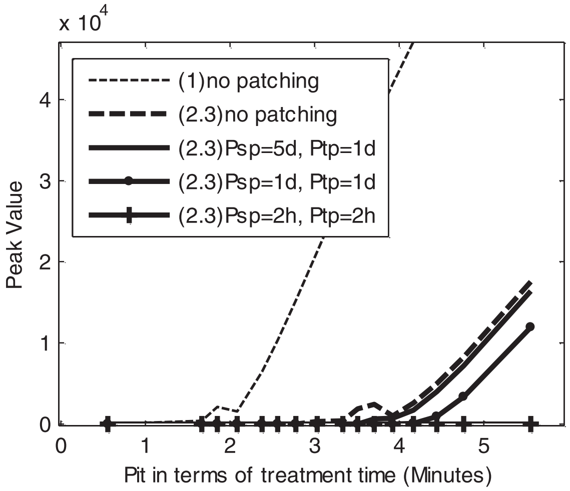

Fig. 20. Single class example for the automated virus showing the short-term outcomes of dying away or spreading.

number of devices within the *Prevented* compartment increasing accordingly. This highlights how important human behaviors are on how a virus spreads. Simply ensuring software and antivirus tools are patched and updated can reduce the spread across the network. Within class 1, however, the virus did spread and remained in the network after 30 days. Due to the frustration of the inoperable phones, some were turned off providing some level of containment, which can be seen by the *Contained* compartment increasing. As expected, class 2 users were not affected by the virus.

4.6 Model Dynamics and Stability

The three possible spreading outcomes of the Bluetooth virus can be shown for a *single class* via simulation by looking at the short-term peak of the spread and the long-term limit value while varying some of the parameters. The parameters used are based upon those of *class 3 users* in the London simulation scenario when the prevented compartment exists, and when it is removed. To illustrate how human behaviors can affect the *short-term outcome* of a Bluetooth virus between *immediately dying away or spreading* (peak rises above initial infection of one device), the peak of the spread has been measured as the treatment time parameter (P_{it}) is varied until a threshold can be seen where $R_0 < 1$ changes to $R_0 > 1$. Figs. 20 and 21 show how the peak of the spread varies for the automated and the user virus, respectively. The dashed curves show how the peak of the spread varies when there is no patching for both node velocities of 1 and $2.3\ \mathrm{ms}^{-1}$. The remaining curves show the spread when patching is applied. In the *automated* case, the treatment time needed to stop the spread is in the order of minutes, even when patching is carried out daily. As indicated by the lower most curve, all users would need to install a patch within 2 hours and treat those initially infected within minutes to stop the spread. This is why the automated virus spread, rather than dying away among class 3 users in the London simulation. In the *user* case, the treatment time needed to stop the spread is in the order of days. As shown by the lower most curve, when susceptible patching of five days and infected patching of 1 day is carried out as per the London simulation the virus dies away. The point at which the virus dies away illustrates how the parameters can change the state of R_0 giving rise to the *first outcome* in Table 4.

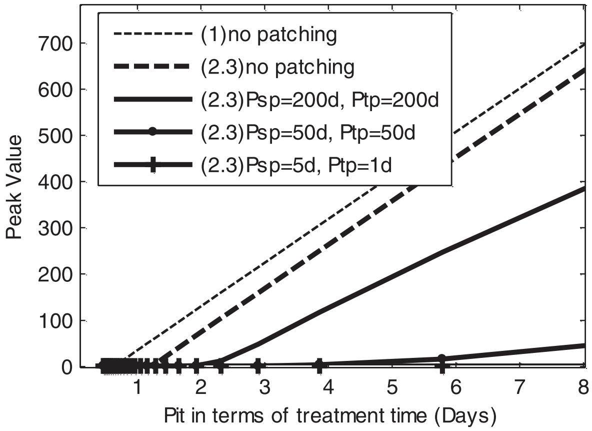

Fig. 21. Single class example for the user virus showing the short-term outcomes of dying away or spreading.

To illustrate how human behaviors can affect the *long-term outcome* of a Bluetooth virus between *dying away* and *persisting*, the limit value of the spread has been measured as P_{it} is again varied. For the SEPTICOX model, in the limit when persistence of the virus is present in the network, repetitive peaks of infection occur due to the nature of devices being turned on and off. The curves in Figs. 22 and 23 show how the maxima of the limit value varies for the automated and user virus, respectively. In both cases, when patching is applied, the limit value is always zero because the long-term stability of the virus always dies away, regardless of whether it initially spreads, and demonstrates the *second outcome* as given in Table 4. This outcome happened in the London simulation for class 3 users where the *automated* Bluetooth virus spread, and then died away. When no patching is applied, Figs. 22 and 23 show that once the threshold treatment time is reached, the virus persists in the network after its initial peak. Finally, this demonstrates the *third outcome* as given in Table 4. In the London

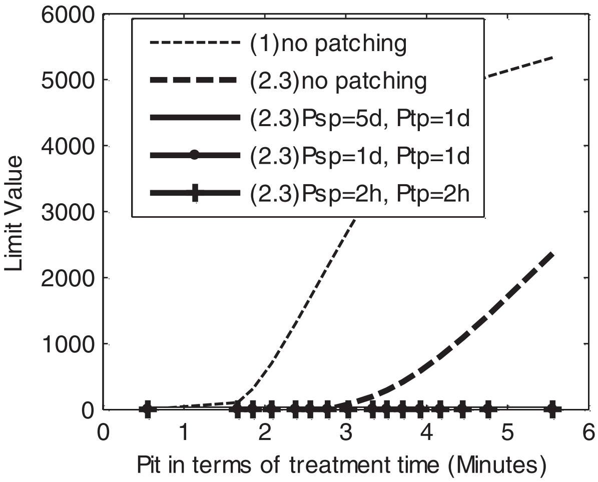

Fig. 22. Single class example for the automated virus showing the long-term outcomes of dying away or persisting.

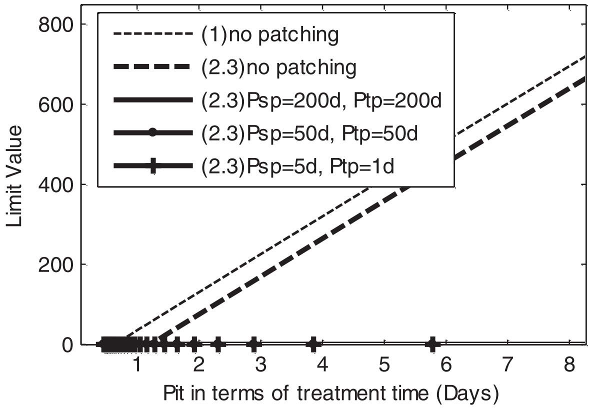

Fig. 23. Single class example for the user virus showing the long-term outcomes of dying away or persisting.

simulation, classes 1 and 2 users did not patch which resulted in the third outcome, except for the user spread virus within class 2 because they were immune.

5 Discussion and Future Work

Infection curves presented in Sections 4.1 and 4.2 suggest that a Bluetooth virus without human involvement requires propagation times only in the order of minutes to spread to the entire population. The situation is made worse for Bluetooth devices that have large transmission ranges. Fortunately, the existing Bluetooth viruses that have been observed so far all require human intervention, which slows down their propagation. The internet-based Slammer worm however is an example of how quickly a virus without human intervention can actually spread. In January 2003, it spread so quickly in a matter of minutes that human response was ineffective [26]. In comparison, the London automated Bluetooth virus spread so fast that the short-term human reaction time was also ineffective. To reduce or eliminate, the spread would require treatment times in the order of minutes and regular patching in the order of hours. The spread in class 1 was not as bad as it could have been due to phones being switched off or in nondiscoverable mode indicating that preventative measures rather than reactive measures are more effective for fast spreading viruses. Even for class 3 users where some patching was applied, it was more effective at removing the virus from the network over longer time scales. Once Bluetooth viruses can spread automatically, the result could be similar to the slammer worm, especially now most smartphones are permanently switched on. On a longer time scale, user behaviors had a greater impact on the spread of user or latency-based viruses. In the London simulation, class 3 users were good at installing updates, using antivirus tools, and not clicking onto suspicious links. Their actions, combined with the slower infection rate caused the virus to die away.

A defence mechanism against the spread of a virus is heterogeneity including different hardware and operating systems as this reduces the number of devices vulnerable to the same exploit. This has been observed from the London simulation where different smartphones and Bluetooth versions affect the spread of the virus. The density of the devices also has an impact on virus spread. When the density is low, and the average velocity of the nodes is low the speed of the spread is slow. As the density increases so too will the spread even if the devices are relatively stationary, because under this condition the devices are close enough to each other to spread the virus quickly. Areas involving crowds of people with a high density of devices may be the place of the future for propagating viruses or committing other cyber crimes.

The SEPTICOX model currently does not include spatial topology or human mobility models and is a limiting factor for accurately analyzing the spread of a virus across different areas of a city, for example. However the density in places such as train stations can be assumed to be uniform over a short period of time and therefore the results are expected to be more accurate under these conditions. If the density of the different areas of a city were known then the model could be partitioned into classes of areas as well as devices and users. Each class within the model is homogeneous with similar characteristics and behavior, but in reality no two people behave the same and so there are some limitations regarding the natural randomness of human behavior. This could be improved by adding stochasticity to the model. Propagation modeling of this type could be used to understand the likely impact of attacks targeted around specific geographical locations and events. The analysis should elucidate possible outcomes for populations of users, and give guidance on the utility of response strategies which could include targeted quarantine or patching. Future work would also include a full derivation of the reproduction number and an analysis of the dynamics for multiple classes. Finally, the model could extend beyond Bluetooth to include other transmission media allowing the analysis to be applied to polymorphic malware.

6 Conclusion

The developed SEPTICOX model uses eight compartments: Susceptible (S), Exposed (E), Prevented (P), Treated (T), Infected (I), Contained (C), Offline (O), and eXposed offline (X). This model incorporates the underlying link properties of Bluetooth, three types of virus spread, heterogeneity, and human behaviors such as general patterns of turning on and off devices and the use of antivirus measures. For a homogeneous model, the short-term spread and the long-term stability has been analyzed leading to three possible outcomes: 1) the virus dies away, 2) the virus spreads and then dies away, 3) the virus spreads and then persists in the network. The first outcome is governed by the infection rate and a critical range of human parameter values that prevents the virus from spreading. The remaining outcomes are additionally governed by the existence or removal of the Prevented compartment controlled by two patching parameters. The spread of viruses is also affected by the heterogeneity of the devices and their users which is incorporated by splitting the population into classes so that the interaction within classes can be different to that between classes. A simulation scenario using realistic parameters to determine how a Bluetooth virus might spread in a large city such as London has been analyzed. It has been shown that without human intervention a Bluetooth virus could spread in a matter of minutes. A defence mechanism against the spread of such a virus is heterogeneity combined with a critical range of human behaviors. These human behaviors can affect both the short-term spread, and the long-term stability of different types of Bluetooth viruses.

REFERENCES

[1] "Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent," www.gartner.com, 2012.

[2] "Mobile Malware Evolution: An Overview, Part 1,"Kaspersky, http://www.viruslist.com/en/analysis?pubid=200119916#fams, 2012.

[3] W. Xia, Z. Li, Z. Chen, and Z. Yuan, "Dynamic Epidemic Model of Smart Phone Virus Propagated through Bluetooth and MMS," *Proc. IET Conf. Wireless, Mobile and Sensor Networks,* pp. 948-953, 2007.

[4] "Bluetooth Special Interest Group," http://www.bluetooth.com, 2012.

[5] K. Scarfone and J. Padgette, *Guide to Bluetooth Security,* Nat'l Inst. of Standards and Technology, 2008.

[6] L. Carettoni, C. Merloni, and S. Zanero, "Studying Bluetooth Malware Propagation: The BlueBag Project," *IEEE Security and Privacy,* vol. 5, no. 2, pp. 17-25, Mar. 2007.

[7] D.J. Daley and J. Gani, *Epidemic Modelling: An Introduction.* Cambridge Univ. Press, 1999.

[8] M.G. Roberts and J.A.P. Heesterbeek, "Mathematical Models in Epidemiology," *Mathematical Models,* EOLSS, 2003.

[9] H. Zheng, D. Li, and Z. Gao, "An Epidemic Model of Mobile Phone Virus," *Proc. Symp. Pervasive Computing and Applications,* pp. 1-5, 2006.

[10] R.W. Thommes and M.J. Coates, "Modeling Virus Propagation in Peer-to-Peer Networks," *Proc. Conf. Information, Comm. and Signal Processing,* 2005.

[11] G. Ben-hua and C. Shao-hong, "The SIS-BD Model of Computer Virus Spreading on Internet," *Proc. Conf. Wireless Comm., Networking and Mobile Computing,* pp. 2200-2203, 2007.

[12] G. Yan, L. Cuellar, S. Eidenbenz, H.D. Flores, N. Hengartner, and V. Vu, "Bluetooth Worm Propagation: Mobility Pattern Matters!" *Proc. ACM Symp. Information, Computer and Comm. Security,* pp. 32-44, 2007.

[13] J. Su and K.K.W. Chan, "A Preliminary Investigation of Worm Infections in a Bluetooth Environment," *Proc. ACM Workshop Recurring Malcode (WORM),* 2006.

[14] P. Wang, M.C. Gonzalez, C.A. Hidalgo, and A.-L. Barabasi, "Understanding the Spreading Patterns of Mobile Phone Viruses," *Science,* vol. 324, no. 22, pp. 1071-1076, May 2009.

[15] A. Bose and K.G. Shin, "On Mobile Viruses Exploiting Messaging and Bluetooth Services," *Proc. Conf. Securecomm and Workshops,* pp. 1-10, 2006.

[16] C. Gao and J. Liu, "Modeling and Restraining Mobile Virus Propagation," *IEEE Trans. Mobile Computing,* Early access article, no. 99, 2012.

[17] P. Samar and S.B. Wicker, "On the Behavior of Communication Links of a Node in a Multi-Hop Mobile Environment," *Proc. ACM Symp. Mobile Ad Hoc Networking and Computing,* 2004.

[18] D. Stevens, "Is Your PC Virus-Free? Get It Infected Here!" http://blog.didierstevens.com/2007/05/07/is-your-pc-virus-free-get-it-infected-here/, 2012.

[19] *Ann. Security Report,* Cisco, 2008.

[20] "AV-Test Release Latest Results,"Virus Bull., http://www.virusbtn.com/news/2008/09_02, 2012.

[21] J. Hollis, *Focus on London 2010: Population and Migration,* O.f.N. Statistics, 2010.

[22] "A Nation Addicted to Smartphones," http://media.ofcom.org.uk/2011/08/04/a-nation-addicted-to-smartphones/, 2012.

[23] *Average Speed of a Car in London is Just 7mph, Says Citroen,* http://www.bikeforall.net/news.php?articleshow=229, 2006.

[24] "Orders of Magnitude (Speed)," http://en.wikipedia.org/wiki/Orders_of_magnitude_(speed), 2012.

[25] J.M. Heffernan, R.J. Smith, and L.M. Wahl, "Perspectives on the Basic Reproductive Ratio," *J. Royal Soc. Interface,* vol. 2, no. 4, pp. 281-293, Sept. 2005.

[26] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," *IEEE Security & Privacy,* vol. 1, no. 4, pp. 33-39, July/Aug. 2003.

Jennifer T. Jackson received the MEng degree in electrical and electronic engineering from Loughborough University, and the MSc degree in complexity science from the University of Warwick where she is currently working toward the PhD degree in same subject. From 1999 to 2000, she worked for the Ministry of Defence. From 2000 to 2004, she worked as a research engineer at QinetiQ specializing in the application of field-programmable gate arrays. From 2004 to 2008, she worked as a project manager at QinetiQ. She is a chartered engineer and a member of the IET.

Sadie Creese received the BSc (Hons) degree in mathematics and philosophy from the University of North London and the MSc degree in computation and the DPhil degree in computer science from the University of Oxford. She is professor of cybersecurity at the University of Oxford, Department of Computer Science. She has authored numerous papers on cyber security. Her research interests include human factors, risk perception, data privacy and dynamic consent models, usability of security technology, risk management, threat and vulnerability modelling, situational awareness and information provenance, security architectures and network defence, bioinspired security, spontaneous security protocols, and visual analytics. She is a member of the IEEE and the IEEE Computer Society.