Why Mobile-to-Mobile Wireless Malware Won't Cause a Storm

Nathaniel Husted
Indiana University

Steven Myers
Indiana University

Abstract

The enhanced capabilities of smartphones are creating the opportunity for new forms of malware to spread directly between mobile devices over short-range radio. This has been observed already in Bluetooth radios, and WiFi capabilities of smartphones provide an opportune new spreading vector. The increasing complexity of phone operating systems coupled with disclosed vulnerabilities suggest it is simply a matter of time before WiFi based worms are possible. Works that have considered this problem for Bluetooth suggest outbreaks would result in epidemics [11,28,32]. We use traditional epidemiological modeling tools and high-fidelity realistic human mobility data to study the spreading speed of this emergent threat. As opposed to other works, we take in to account the effects of exposure times, wireless propagation radii, and limited population susceptibility. Importantly, we find that lowering the susceptibility of the population to infection gives significant herd immunity as with biological infections, *but unlike traditional Internet worms*, making such threats *unlikely* in the near to medium term. Specifically, with susceptibility rates below 10% the result is near total immunity of the population. We find exposure times, and wireless transmission radii have no significant effect on outbreaks.

1 Introduction

The popularity of smartphones has created new avenues for exploitation. As smartphones include advanced wireless capabilities such as Bluetooth, 802.11 access (WiFi), and even the ability to masquerade as access points (e.g., DroidX), they offer an open vector for the spread of mobile-to-mobile malware using its short-range radio, and eschewing the cellular 3G or 4G data network. Such malware is potentially concerning due to its ability to be spread off of major monitored network backbones, making detection and malware scrubbing impossible at the cellular carrier level. Three infamous examples of mobile-to-mobile malware include the Bluetooth Worms Mabir [4], Cabir [1], and Commwarrior [3]. These viruses used flaws in the phone's Bluetooth stack or basic social engineering to install themselves on discoverable bluetooth phones in the local vicinity. Numerous pieces of research have focused on studying Bluetooth viruses [10–12, 15, 18, 25, 28, 29, 33–35] as well as general articles on mobile malware [17]. With WiFi becoming a predominant feature on Smartphones, WiFi offers an emerging vector for moble-to-mobile malware.

The increasingly complex operating systems and applications that run on smartphones create yet other broad attack surfaces when compared to the traditional feature phones targeted by Mabir, Cabir, and Commwarrior. Modern smartphone operating systems have been found to have both minor [2, 9] and major [7] security flaws. The valuable data stored on such phones, and the transactions made with them, leads to a strong incentive to write malware to attack such phones.

WiFi offers a potentially superior mobile-to-mobile malware spread mechanism compared to Bluetooth: WiFi traffic is easily sniffable and forgeable; even when data packets are encrypted, management frames are unencrypted; and, there is no authentication performed on packets permitting spoofing (a predominant tactic in WEP cracking [31]). These all result in different techniques that can be used to attempt to inject traffic on to an unsuspecting device, leading to different avenues of attack. Finally, many phones always have WiFi on. Bluetooth not only must be on but must be in discoverable mode to be seen and exploited.

We provide preliminary results on our study of the dynamics of mobile-to-mobile, wireless, malware outbreak dynamics in metropolitan areas. Using a combination of realistic population data, simulated human mobility data, and epidemiological modeling, we propose a set of estimates predicting the speed at which the malware spreads. Our analysis is the first to comprehensively

study the spread of malware on a large urban scale, using fine grained realistic traces of human mobility. We are the first to consider the effects of varying levels of susceptibility of the population, something that we find is of the utmost importance to the spreading dynamics, and suggests that peer-to-peer spread is far less concerning than previously believed.

The remainder of this paper proceeds as follows: Sec. 2 discusses how WiFi based malware would spread and the feasibility of WiFi malware; Sec. 3 provides an overview of epidemiological models and a description of the model used in this paper; Sec. 4 discusses the methodology used in our simulations; Sec. 5 discusses the findings of our experiments; Sec. 6 discusses the differences between simulated and empirical data, and the need for simulated data; Sec. 7 discusses the defenses that will help stop WiFi based malware; Sec. 8 discusses related work; and, finally, Sec. 9 gives our final thoughts and plans for future work.

2 The Anatomy of Wireless Malware

There are multiple standards for wireless device-to-device communication, such as WiFi and Bluetooth. Bluetooth and WiFi malware are similar in that they both provide short-range, peer-to-peer (P2P) wireless communications. These differ from wireless communications with the cellular provider, as the channel is not managed by a large organization that might monitor or limit data in an effort to prevent the outbreak of malware on their network. However, malware would need to consider a number of different technical details when targeting transmission through one P2P technology versus the other. For example, Bluetooth malware must not only target a device with Bluetooth enabled, but the target must also be discoverable.[1] WiFi based malware may only require that WiFi be turned on, something that with todays usage patterns seems more likely.

2.1 Potential Methods of Spread

Mobile-to-mobile wireless malware needs to take advantage of mobile operating system vulnerabilities or mobile application vulnerabilities in order to spread. Bluetooth based malware has taken advantage of OBEX push vulnerabilities and human behavior in order to spread. The vulnerabilities that WiFi based malware could take advantage of include a vulnerability in the 802.11 networking stack or applications that frequently listen for incoming traffic (e.g. the i-Jetty web server for Android phones [13]). Of key importance is that for the wireless payload to spread, an infected phone must be in radio contact with the victim for a long-enough period of time to attack the victim's system, and upload the payload.

The start of a mobile-to-mobile infection requires a point of initial infection, which need not be over the P2P network. It might be transmitted through the use of social engineering to download malicious applications containing the malicious wireless P2P payload. Strategies for initial infection are well understood, and outside the scope of this paper.

Access points are not considered as a malware carrier in this paper. The current empirical datasets do not provide accurate positioning in three dimensions. Previous experiment have shown the contact between individuals and access points is negligible compared to phone-to-phone contact [16].

3 Epidemiological Models

Biological epidemiological models have been suggested as a way of modeling digital viral spreads since the first Internet worms [22]. Due to the scale-free nature of the Internet, essentially all computer viruses over traditional networks translated in to epidemics. Technically, this was due to the epidemiological constants being 0 (i.e, there was no herd resistance). However, with wireless P2P networks, the connectedness of the graph is greatly reduced, to models that are more like traditional biological models.

Compartmental models are the most frequently used forms of epidemiological models. In such models individuals in the population finds themselves in a given compartment at any given time. Compartments are labeled to represent the different states of illness and health individuals can be in. All compartmental epidemiological models, such as the SEIR (Susceptible-Exposed-Infected-Recovered) model we use in this paper, involve the use of two or more compartments. For most of these models, there are assumptions about homogenous mixing of individuals in the population that result in differential equations that are used to predict the relative susceptibility of populations to outbreaks of different pathogens. With no significant history of P2P worms, there is no data to validate these homogenous mixing assumptions, nor is it clear what effects attack times and transmission radii have on them, so the value of these differential equations for predicting P2P outbreaks is unclear. An overview of epidemiological models can be found in Piqueira et al. [24] and Serazzi et al. [26]. Pastor-Satorras and Vespignani also provide an analysis of epidemic spread in scale-free networks [23].

3.1 Overview of the SEIR Model

The Susceptible-Exposed-Infected-Recovered (SEIR) model is a well known compartmental model [26]. The model consists of four compartments representing i) a

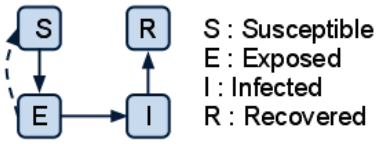

Figure 1: The movement between compartments is unidirectional except in the case of S to E.

susceptible population, ii) an exposed population, iii) an infected population, and iv) a recovered population. The susceptible population contains users who could potentially be infected by the worm. The exposed are those in the incubation period of the worm. In our case, the 'incubation' period is the time in which the worm is both attacking a victim and when its payload is being transferred between mobile devices. The infected are the individuals infected with the worm. The recovered are those who have recovered from the worm. In the model, recovered individuals can either be infected again (e.g. bacterial infections) or are now immune depending upon the disease under consideration. For worm modeling, we assume that the individuals become immune due to the installation of a patch.

4 Methodology

4.1 Agent Based SEIR Model

Our agent-based SEIR model depends upon a set of traces representative of human mobility. In principle, traces can be simulated or taken from empirical data sets. For our experiments we use simulated data whose generation is described in Sec. 4.4. We argue the difficulties of using empirical data in Sec. 6. All mobility traces and corresponding detections are done in three dimensions. Preliminary work showed that simulating a given population projected on to two dimensions created unrealistically high rates of close proximity between individuals [16].

Given a set of traces of individuals we choose, at random, a given fraction of the population to represent the susceptible population, and denote them by the compartment S. From this susceptible population, we choose, at random, a given fraction of the individuals to be those that are initially infected with the worm. These individuals are removed from S and placed in the compartment I. Next, time is simulated forward. We determine when infected agents are within wireless transmission range of susceptible agents. These individuals become members of the exposed, E, compartment so long as they are in transmission radius. If these individuals remain in the E compartment for a long enough period of time for the proposed attack and payload upload to be successful, then they become infected individuals and are moved to the I compartment. In principle, an infected individual may attempt to recover. If they recover from the infection, they are moved to the R compartment and are immune from future infection. In our models we do not present any recovery, as we are interested in short-term infectious spread, but the unsusceptible population is placed in the recovered compartment. The movement between compartments can be seen in Fig. 1.

4.2 Detecting Susceptible Wireless Users

We simulate the infection spread with wireless transmission radii of 15m, 30m, and 45m. These range from conservative to optimistic for 802.11g, but are conservative for 802.11n. In order to reduce computational effort, we use an inner and outer bounding cube around a spherical detection area to approximate transmission radii. Since the spherical transmission radius is an approximation, this seems a reasonable trade-off. In all data presented there was only minor differences between the results for the outer bounding cube, and the inner. For clarity in graphs, we present all of the results using the outer-bounding cube.

4.3 Metropolitan Topography and Population

For initial results, we wanted to generate mobility traces for high-density metropolitan areas. Intuitively these provide the best environments for wireless worms's propagations, due to population density. We chose a 3-by-3 block region in downtown Chicago: the area is bound on the north by W. Wacker Dr., the south by W. Washington St., the east by N. Clark St and the west by N. Franklin St, and is shown in Fig. 2. The simulator provides for three different classes of buildings with corresponding different behaviors of individuals within them: Offices (OF), Service (SR), and Residences (RE). We simulate a population of 9056 individuals. This population figure was gathered from the LandScan dataset [6].

4.4 Mobility Generation

To generate our mobility traces we use the UdelModels simulator [8]. The UdelModels simulator generates realistic human mobility for downtown metropolitan areas. The simulator bases its traces on research from the Bureau of Labor Statistics, Urban Planning Research, and worker meeting research. These simulated mobility traces are used for simulations of high-fidelity positioning for large urban populations.

The Bureau of Labor Statistics' 2003 American Time of Use study is used to determine realistic distributions

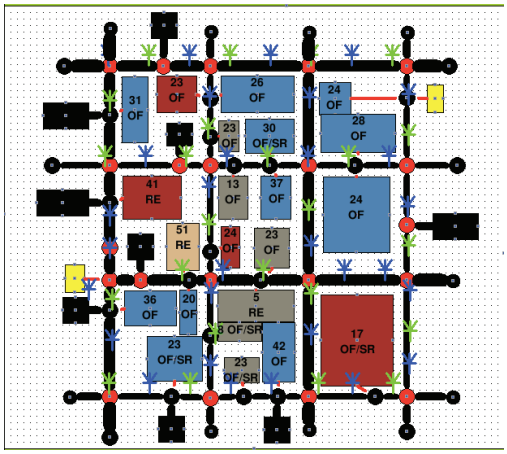

Figure 2: Metropolitan mobility maps include number of floors and building function (Courtesy of UDel Models MapBuilder Software [8])

for the time an individual arrives at work, the duration they're at work, when the individual takes a break from work, the number of activities they perform, and the duration of the activities. Urban planning research is used to determine the paths that individuals take between buildings and around the city. Worker meeting research is used to determine the mobility within buildings and between floors. The research determines where individuals have meetings, where the meetings are in relation to the individuals position in the building, and how long the meetings last. [19, 20]. The UDelModels simulator produces traces that statistically agree with the above data and models. While true experimental traces would be preferable, we discuss the high unlikelihood and difficulty of getting such traces in Sec. 6.

4.5 Homogeneity of the Population

A wireless worm would need to take advantage of a flaw in hardware or software in order to infect individuals, and only the population with said flaws would be susceptible. In this paper we model homogeneity through the use of a susceptibile percentage of the population. This allows us to easily abstract different forms of homogeneity (e.g., application, operating system family, hardware, and corresponding versions of each). Thus, if there is a $x\%$ susceptibility percentage, then $x\%$ of the devices in the area can be targeted by the malware and are considered homogenous for purposes of malware spread. The susceptible users are chosen uniformly at random from the overall population.

4.6 Malware Exposure Time

Different security flaws require differing amounts of time to exploit. Similarly, different payloads and transmission rates result in different payload transmission times. In our simulations we have chosen exposure times based on conservative transmission speeds and viruses sizes chosen by other researchers in prior work [12, 32, 33, 35]. These exposure times range from five seconds to two minutes.

4.7 Viral Infection Behavior: Serial vs. Parallel

Serial spreading allows a worm on an infected phone to only actively infect one other device at a time, whereas parallel spread allows multiple simultaneous infections. To simulate serial spreading for each infected agent (σ) let H_σ denote those susceptible individuals within the transmission sphere/cube at a given time. In the serial model, uniformly at random, one non-infected agent ($\gamma \in H_\sigma$) is chosen to be infected and placed in the exposed compartment E. If at any point during the exposure period γ leaves H_σ, then γ is returned to the susceptible compartment S, otherwise γ is infected and moved to the infected compartment I. The process is then repeated.

To simulate parallel spreading, each infected agent (σ) keeps a tally of how long *each* susceptible agent has been in (H_σ). All agents who remain continuously in H_σ for the exposure period are infected, and those that leave are reset back to susceptible.

Due to hardware specifications on wireless transmissions, serial spreading seems like the most likely behavior of a wireless P2P worm, but understanding parallel transmission can help us understand some worst-case behavior that may be possible in the near-future, say if many phones behave as access points (AP).

5 Results for Mobile Malware Outbreaks

We consider an initial experiment in which 1% of the population are chosen randomly in the population and infected. There is an unrealistically high 100% susceptibility rate to the worm. We fix an initially conservative broadcast radius of 15m. We run our simulation from 7am to 11am, starting at low-density period of the day when people commute to work, progressing towards the high-density lunch-hour. A four hour period was chosen due to the large computational and memory requirements of the simulation. Periods greater than four hours were not possible with the current computing systems available and computationally intractable. We choose these parameters, as we wish to see if the worm would spread

in the ideal condition of susceptibility, with conservative transmission estimates. We began with a short exposure time of 10 sec., and varied it longer to 120 sec. Figure 3 shows the results. Clearly, when there is a large susceptibility, the population is at risk over small periods of time (i.e., several hours). Exposure time has some effect on the speed of viral spread, but not the overall uptake of the worm. Similarly, we see that while parallel spread increases the speed of the spread somewhat, it has little effect on the overall uptake of the worm on even the fairly short time-scales of the several hours simulated. Given the simulation is over a four hour time frame, it has hard to imagine a scenario where the relatively small difference in viral spread times would have much effect.

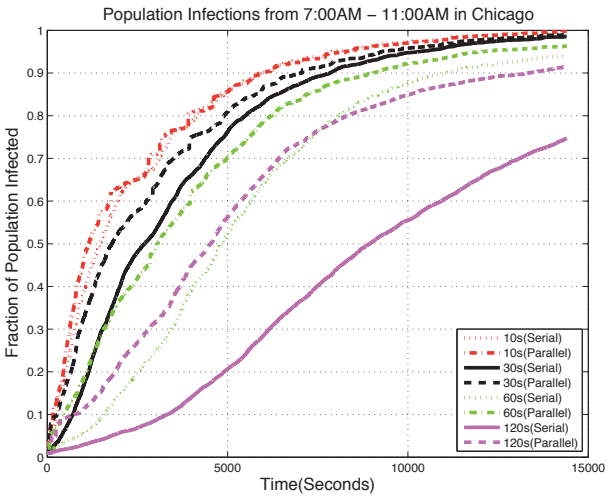

Figure 3: Effects of varying exposure time in Chicago at 7:00-11:00AM. 1% initial infection.

We performed an experiment similar to the one just described, but where we fixed the infection time at 30 seconds and varied the initially infected population from 1%-10% of the susceptible population. As would be expected given the previous results the infection rates quickly converge in a matter of three hours, making the initial infection rate fairly unimportant from a security perspective, given the small time frame. These results are not graphed due to space considerations.

An increase in wireless range will, logically, increase the speed in which mobile malware is able to spread from device to device, as it decreases the amount of time that no person is in range to infect. Further, as the range increases limitlessly, we get a fully connected graph which ensures epidemic spread. The results given in Fig. 4 validate this line of reasoning. In the experiment we fixed the initial infection percentage at 1% and the exposure time at 120s. We chose a long exposure time to better show the drastic effect an increase in wireless range has on the percentage of the population infected. We varied the wireless range from 15m, to 30m, to 45m.

Figure 4 shows at 25% increase in the final infection rate when the wireless range is increased from 15m to 45m, but the trajectory suggests no effective difference in the longer term. The noticeable difference in spread between serial and parallel infections is also removed when the radius is increased, at least over the period of several hours. If immediate infection rates are of concern, then parallel infection has some benefit.

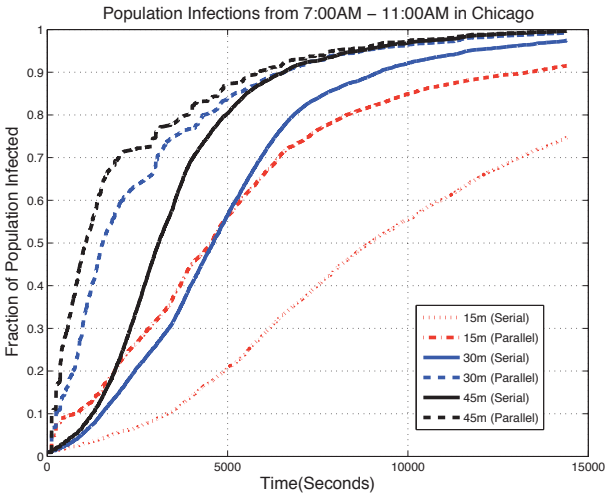

Figure 4: Effects of varying the size of the wireless broadcast radius in Chicago between 7:00-11:00AM. Initial infection of 1%.

Next, we considered the effects of lowering the overall population susceptibility on the spread of the worm. In Fig. 5 we show the worms progression with differing levels of population susceptibility. Of importance is that as the susceptibility of the population is lowered, there is a progressively large gap between the stable size of the infected population, and the susceptible population: we see the emergence of herd immunity. In particular, susceptibility below 10% results in a negligible infection rate.

Finally, we wanted to see if the ranges of 802.11n would negate the herd immunity generated by a population's low susceptibility. We performed another experiment with 25% of the population susceptible, but with variations on the wireless range. Results are given in Fig. 6, and it can be seen that even at low infection rates, wireless broadcast range has no mid- to long-term effects on the infected population size.

6 Simulated Vs. Empirical Mobility Data

Mobility data is available in both an empirical form and a simulated form. For our purposes the datasets *need* three properties: i) spatial fidelity, ii) temporal fidelity, and iii)

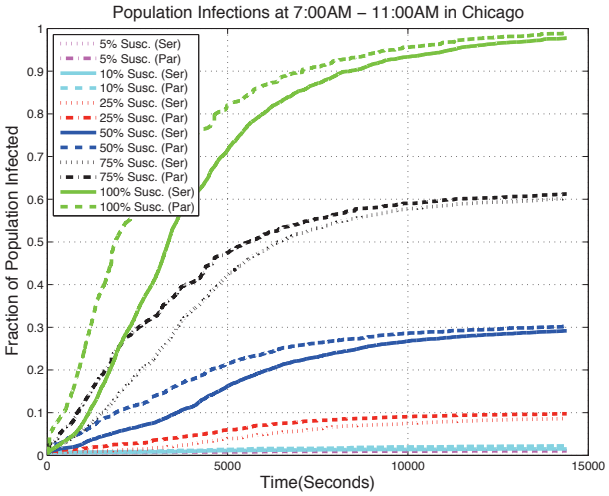

Figure 5: Effects of varying the size of the susceptible population in Chicago at 7:00-11:00AM. Initial infection of 30 devices.

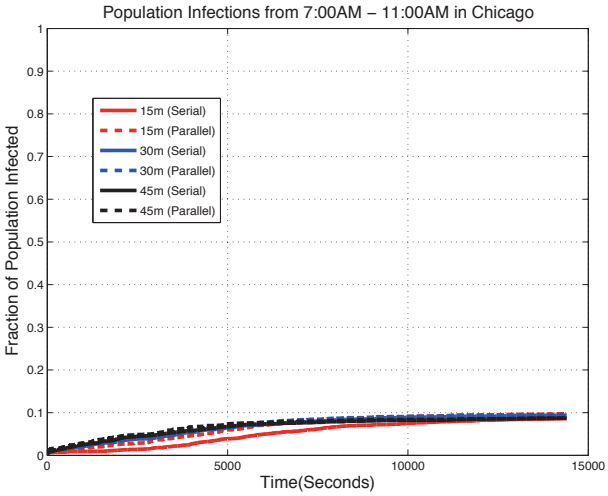

Figure 6: Effects of varying the wireless range in Chicago at 7:00-11:00AM with low susceptibility 25%. Initial infection of 30 devices.

population density. Empirical forms of data such as the MIT Reality Mining data set [14] and smaller sets on the CRAWDAD data repository [5] all lack at least one of the three properties. Wang et al. [32] used a cellular phone company's data-set which had high density and temporal fidelity, but only positional information to the nearest cell tower. Thus there are no known empirical data-sets we could use for our study. In contrast, simulated data can either be created via abstract mathematical models (e.g., brownian motion, levy flights, and random waypoints), or it can be created using stochastic processes based on observed and measured data similar to methodologies used by UdelModels [8, 19, 20]. The simulated processes allow us to satisfy our three properties, but we argue processes that are based on or made to agree with measured data are more likely to be representative of the real movements. Fig. 7 provides a comparison between a walk generated by UDelModels and a walk generated by brownian motion; it is clear that UDelModels provides a more realistic walk.

7 Defending Against WiFi Malware

We've shown that susceptibility rates below 10% result in negligible infections. Therefore, given the current distribution of major smartphone OSes, the likelihood of flaws, etc... it seems unlikely that there is the possibility of major transmission from peer-to-peer malware in large metropolitan centers. We note that our analysis does not simulate large gatherings of people in close confinement, such as sporting events in colosseums, social gatherings, etc; therefore, in these occasions more transmission may be possible, and in fact there is precedent for such with bluetooth viruses [17]. However, in such events we can remind users to keep their radios off or remind them to only use WiFi when it is necessary. An alternate possibility is to simply have a phone shut off its wireless radio if not in active use in locations where it finds large numbers of other phones.

As previously mentioned, unlike traditional Internet worms where anti-virus software and up-to-date patches provide security only to those who install them, in the case of mobile-to-mobile wireless worms we see that lowering the susceptibility of the population has a significant effect of the population at risk, and grants herd immunity. Therefore, patching and anti-virus software will be a more formidable defense in this arena. The protection against mobile malware gained from heterogeneity can be viewed as a property stemming from two different "levels" of the smartphone device. One level being protection gained from heterogeneity at a software level. The other being protection gained from heterogeneity at the hardware level. One can argue that malware affecting one version of Android (e.g. 2.2) would not affect

(a) Udel (b) Random

Figure 7: A visualization of the distinction between a sample UDEL Walk and brownian motion. Both represent approximately 1000 steps.

another version of Android (e.g. 2.1). If malware can only affect one version at a time, platforms which tend to have many different versions of the operating system in circulation would have greater protection against malware outbreaks. The diversity of operating system versions would be an example of software heterogeneity. One could also argue that the malware depends upon the underlying hardware of the device (e.g. if the malware attacked vulnerabilities in a WiFi driver). If the malware is device specific, then platforms with many different hardware platforms (e.g. Android and Windows Mobile) would be protected by hardware heterogeneity.

Further, the ability of different vendors to kill applications on phones (e.g., iPhone and Android) would be effective even if not all instances of the application are killed. This might allow for an opt-in, where people could choose to allow applications to be killed, while others would continue with the application. A rapid revocation of known malicious software from application markets also limits the initial infection vector of mobile malware. A rapid revocation policy is most needed for open application markets such as Google's. Alternately, cellular carriers could push patches to populations who are willing to receive them, and still grant some herd immunity.

8 Related Work

Much works has been done on the epidemic modeling of computer viruses, with a focus on successful internet worms (e.g., [21, 27, 36]). The first work looking at mobile-to-mobile viruses focused on Bluetooth based malware. Wang et al. [32] discuss Bluetooth worms spreading at a metropolitan scale but do not have high fidelity movement data. Specifically, their dataset is limited to the range of a cellular tower which has a much larger range then a bluetooth device: populations are placed uniformly at random within a cell-towers broadcast region. Channakeshava et al. [12] also provided an analysis of bluetooth worms propagating at a metropolitan scale but did not discuss propagation occurring during pedestrian movement. Yan et al. created an analytical bluetooth worm model and compared it to the same model implemented in the NS-2 network simulator and found their analytical model matched the simulated results to a close degree [33, 34]. Yan et al. also study the spread of a bluetooth virus using their epidemiological model under the conditions of different simplified mobility models. The authors tested the random waypoint, random walk, random direction, and random landmark mobility models and found that the mobility model significantly effects results [35].

Carettoni et al. [11] perform a more empirical study of bluetooth malware propagation. They created a "BlueBag" device that can be used to both scan and simulate infection of nearby bluetooth devices. They collected data on the number of susceptible devices at high-transit locations in Milan. Finally, they provide a small scale simulation of a bluetooth infection using a simulated trace methodology similar to our, but on the scale of an individual shopping mall. Importantly, they do not consider susceptibility levels in the population other than 100%, nor do they consider the effects of alternate wireless ranges, exposure times, etc... Tang et al. [30] use three empirical datasets from the low population data sets available in the CRAWDAD project [5] to model the spread of malware using mathematical models of temporal graphs. Su et al. [28] also perform data collection as a foundation for building an epidemiological model. The authors also look at spreading dynamics, e.g. they answer the question on whether or not infections can spread to devices moving in opposite directions. They provide a simulation with 10,000 devices but their model does not take into account physical proximity and geographical distribution.

9 Conclusions & Future Work

In this paper we used realistic, simulated, mobility data and agent-based epidemiological modeling to analyze the potential spread of mobile-to-mobile malware in a dense Metropolitan environment. We show in this preliminary work that a mobile-malware outbreak is not likely a threat in the short or medium term, due to the limited ability of malware to spread when susceptibility is below 10% of the population, a likely scenario given the distributions of phones and software in todays smartphone market. We also show that a planned changes in wireless transmission radius do not have a significant effect on viral spread. We similarly show that parallel spread does not greatly effect the threat of worms. For future work, we will consider mobile malware spread under a number of different assumptions including topography and susceptibility. While mobile-to-mobile malware will most likely appear within the next few years, it will not be as devastating as a number of bluetooth epidemiology papers state it will be. In fact, with given hetrogeneity, the use of patches and anti-virus software, there should be heavy mitigation of the threat of mobile-to-mobile malware; with the possible exceptions of large gatherings of people in close proximity. In the future we plan to work on combining the traditional analytical form of epidemiology modeling with the insights provided by an agent-based mobility approach, with the goal of providing analytic micro-models that can take in to account geographical, social and population features of a given area along with spread properties of a given worm, without the need for computationally expensive modeling.

References

[1] Bluetooth-Worm:SymbOS/Cabir. http://www.f-secure.com/v-descs/cabir.shtml.

[2] The Verizon Wireless HTC Eris 'SilentCallBug. http://slashdot.org/story/10/07/11/1714240/The-Verizon-Wireless-HTC-Eris-Silent-Call-Bug.

[3] Worm:SymbOS/Commwarrior. http://www.f-secure.com/v-descs/commwarrior.shtml.

[4] Worm:SymbOS/Mabir.A. http://www.f-secure.com/v-descs/mabir.shtml.

[5] CRAWDAD: A Community Resource for Archiving Wireless Data At Dartmouth. http://crawdad.cs.dartmouth.edu/ (July 2010).

[6] LandScan. http://www.ornl.gov/sci/landscan/ (July 2010).

[7] The Web-Based iOS Jailbreak Tool - How Does It Work? http://www.pcworld.com/article/202367/the_webbased_ios_jailbreak_tool_how_does_it_work.html (2010).

[8] UDel Models. http://www.udelmodels.eecis.udel.edu/ (July 2010).

[9] ADHIKARI, R. Apple Blames Bar Bug for iPhone Reception Woes. http://www.macnewsworld.com/rsstory/70347.html (July 2010).

[10] BOSE, A. *Propagation, Detection and Containment of Mobile Malware*. PhD thesis, The University of Michigan, 2008.

[11] CARETTONI, L., MERLONI, C., AND ZANERO, S. Studying bluetooth malware propagation: The bluebag project. *IEEE Security and Privacy 5*, 2 (2007), 17–25.

[12] CHANNAKESHAVA, K., CHAFEKAR, D., BISSET, K., KUMAR, V., AND MARATHE, M. EpiNet: a simulation framework to study the spread of malware in wireless networks. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques* (2009), ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 1–10.

[13] DAVIES, C. i-Jetty turns Android cellphone into mobile webserver. *phonemag* (Mar. 2008).

[14] EAGLE, N., AND PENTLAND, A. S. CRAWDAD data set mit/reality (v. 2005-07-01). Downloaded from http://crawdad.cs.dartmouth.edu/mit/reality, July 2005.

[15] FOUQUET, M., AFSHAR, E., AND CARLE, G. The Threat of Mobile Worms. In *THIRD ERCIM WORKSHOP ON EMOBILITY*, p. 89.

[16] HUSTED, N., AND MYERS, S. Mobile location tracking in metro areas: malnets and others. In *Proceedings of the 17th ACM conference on Computer and communications security* (2010), ACM, pp. 85–96.

[17] HYPPONEN, M. Malware goes mobile. *Scientific American 295*, 5 (2006), 70–77.

[18] JUNHUA, C., SHENGJUN, W., AND WU, P. General worm propagation model for wireless ad hoc networks.

[19] KIM, J. Realistic mobility modeling and simulation for mobile wireless network in urban environments.

[20] KIM, J., SRIDHARA, V., AND BOHACEK, S. Realistic mobility simulation of urban mesh networks. *Ad Hoc Networks 7*, 2 (2009), 411–430.

[21] MOORE, D., PAXSON, V., SAVAGE, S., SHANNON, C., STANIFORD, S., AND WEAVER, N. Inside the slammer worm. *Security & Privacy, IEEE 1*, 4 (2003), 33–39.

[22] MURRAY, W. The application of epidemiology to computer viruses. *Computers & Security 7*, 2 (1988), 139–145.

[23] PASTOR-SATORRAS, R., AND VESPIGNANI, A. Epidemic spreading in scale-free networks. *Physical review letters 86*, 14 (2001), 3200–3203.

[24] PIQUEIRA, J., DE VASCONCELOS, A., GABRIEL, C., AND ARAUJO, V. Dynamic models for computer viruses. *Computers & Security 27*, 7-8 (2008), 355–359.

[25] SARAT, S., AND TERZIS, A. On using mobility to propagate malware. In *Proceedings of the 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Network (WiOpt)* (2007), Citeseer.

[26] SERAZZI, G., AND ZANERO, S. Computer virus propagation models. *Performance Tools and Applications to Networked Systems* (2004), 26–50.

[27] STANIFORD, S., PAXSON, V., AND WEAVER, N. How to own the internet in your spare time. *Proc. 11th Security Symp. (SEC 02)* (2002).

[28] SU, J., CHAN, K., MIKLAS, A., PO, K., AKHAVAN, A., SAROIU, S., DE LARA, E., AND GOEL, A. A preliminary investigation of worm infections in a bluetooth environment. In *Proceedings of the 4th ACM workshop on Recurring malcode* (2006), ACM, p. 16.

[29] SUN, B., YAN, G., AND XIAO, Y. Worm Propagation Dynamics in Wireless Sensor Networks. *Communications* (2008), 19–23.

[30] TANG, J., MASCOLO, C., MUSOLESI, M., AND LATORA, V. Exploiting Temporal Complex Network Metrics in Mobile Malware Containment. *Sat 9*, 10–11.

[31] TRAPANI, G. How to Crack a Wi-Fi Network's WEP Password with BackTrack. http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack (Oct. 2010).

[32] WANG, P., GONZALEZ, M., HIDALGO, C., AND BARABASI, A. Understanding the spreading patterns of mobile phone viruses. *Science 324*, 5930 (2009), 1071.

[33] YAN, G., AND EIDENBENZ, S. Bluetooth worms: Models, dynamics, and defense implications.

[34] YAN, G., AND EIDENBENZ, S. Modeling Propagation Dynamics of Bluetooth Worms (Extended Version). *IEEE transactions on mobile computing* (2008), 353–368.

[35] YAN, G., FLORES, H. D., CUELLAR, L., HENGARTNER, N., EIDENBENZ, S., AND VU, V. Bluetooth worm propagation: mobility pattern matters! In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security* (New York, NY, USA, 2007), ACM, pp. 32–44.

[36] ZOU, C., GONG, W., AND TOWSLEY, D. Code red worm propagation modeling and analysis. In *Proceedings of the 9th ACM conference on Computer and communications security* (2002), ACM, pp. 138–147.

Notes

[1] Brute force scanning of Bluetooth ID's is possible but is not feasible given realistic time constraints of device interactions. Similarly, Bluetooth hardware that scans all channels is not found in traditional phones.