Journal of Information Security and Applications 37 (2017) 1–14

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Preventing malware pandemics in mobile devices by establishing response-time bounds

Stavros D. Nikolopoulos*, Iosif Polenakis

Department of Computer Science & Engineering, University of Ioannina, GR-45110 Ioannina, Greece

ARTICLE INFO

Article history:

Keywords:
Epidemics
Malicious software
Simulation

ABSTRACT

The spread of malicious software among computing devices nowadays poses a major threat to the systems' security. Since both the use of mobile devices and the growth of malware's propagation increase rapidly, we are interested in investigating how the time needed by a counter-measure (i.e., an antivirus or a cleaner) to detect and remove a malware from infected devices affects the malware's propagation. In this work, we study the effect of counter-measure's response-time on the propagation of a malicious software and propose a model for establishing reasonable response-time bounds for its activation in order to prevent pandemic. More precisely, given an initial infected population in a network of mobile devices and a specific city area (town's planning), our model establishes upper response-time bounds for a counter-measure which guarantee that, within a period of time, not all the susceptible devices in the city get infected and the infected ones get sanitized. To this end, we first propose a malware propagation model along with a device mobility model, and then we develop a simulator utilizing these models in order to study the spread of malware in such networks. Finally, we present experimental results for the pandemic prevention taken by our simulator for various response-time intervals and other factors that affect the spread deploying different epidemic models.

1. Introduction

A malicious software or *malware* may refer to any kind of software whose functionality causes harm to a user, computer, or network. The motivation of our research is triggered by the enormous grow and spread on the number of malicious software and, much more, on mobile devices. The structure of ad-hoc networks [1,9,14–16,30] as also the diversity of the nodes concerning so the protection software heterogeneity as the device capabilities [12,17,18,29] are motivating us to investigate the effect of counter-measure's (i.e., security software) response-time on the spread of malware and more precisely on pandemic avoidance. In other words, through this work we focus on investigating how the counter-measure's response time could be crucial on preventing a potential pandemic of a spreading malware, concerning the underlying epidemic model and other factors that affect the spread.

Epidemic Models. Epidemic models [2,7,13,19,20,23–25,27,28,31] can be applied to any network structures to describe the propagation of a disease [29] despite of its type (i.e., biological virus or computer virus) between a set of entities. The overall propagation can be described as a branching process, e.g., a tree that its root is the initial infected population and every level contains child nodes representing the population infected by the nodes of the previous level.

Epidemic models that describe the nodes - entities by a set of potential states or conditions they can go through the course of the epidemic, namely `Susceptible`, `Infected`, `Removed`, `Repaired`, `Immune` are called compartmental epidemic models. In the Susceptible state a node is potentially vulnerable to a disease, while when the node gets Infected (probably by its neighbors) then it goes to Infected state. On the other hand, depending on the modeled cases, if the disease is destructive for its host then after a period of time the Infected node goes to Removed state, while if a cure exist and is been applied to an Infected node then after a period of time (throughout this paper we shall call it sanitize-time) the node goes to Repaired state, where, depending again on the modeling demands, it can be either Immune or not. Next, we briefly present various epidemic models that can be deployed according to the needs of the simulated problem.

In our research field we utilize the SIRp epidemic model, where an Infected node can be Repaired in some fashion [11], as a node repair may provide immunization against the disease or not. Depending on the type of the modeled spread, two different types

* Corresponding author.
E-mail addresses: stavros@cs.uoi.gr (S.D. Nikolopoulos), ipolenak@cs.uoi.gr (I. Polenakis).

http://dx.doi.org/10.1016/j.jisa.2017.09.002
2214-2126/

of the SIR epidemic model are distinguished and described below, namely SIRpI and SIRpS epidemic models.

- **SIRpI**. The SIRpI model (the second 'I' stands for Immune) is applied as to describe the propagation of a disease where the applied repair immunizes/sanitizes [32] the Infected hosts [10,11,26].
- **SIRpS**. In SIRpS Epidemic Model, an Infected host may get Repaired and get Susceptible again as the repair process does not provide any immunization against the disease.

We selected the SIRpI and SIRpS epidemic models, as both meet the requirements to model the spread of proximity malware between mobile devices. SIRpI and SIRpS epidemic models can model the cases where the counter-measure (i.e., repair process) applied by the mobile devices is able to immunize them, or respectively, just remove the spreading malware, being still in Susceptible state.

Related Work. In [5], Chen and Ji focus on modeling the spread of topological malware (spreads based on topology information), as to understanding its potential damages, and developing countermeasures to protect the network infrastructure. Their model is motivated by probabilistic graphs, using a graphical representation to abstract the propagation of malwares that employ different scanning methods. Utilizing a spatial-temporal random process they describe the statistical dependence of malware propagation in arbitrary topologies. Finally, their results show that the independent model outperforms the previous models, whereas the Markov model achieves a greater accuracy in characterizing both transient and equilibrium behaviors of malware propagation.

In [3], Bose and Shin investigate the propagation of mobile worms and viruses that spread primarily via SMS/MMS messages and short-range radio interfaces such as Bluetooth. In that work, they study the propagation of a mobile virus similar to Commwarrior in a cellular network using data from a real-life SMS customer network, modeling each handheld device as an autonomous mobile agent capable of sending SMS messages to others (via an SMS center) and capable of discovering other Bluetooth equipped devices. Their results show that hybrid worms that use SMS/MMS and proximity scanning (via Bluetooth) can spread rapidly within a cellular network.

Fleizach et al. [8], evaluate the effects of malware propagating using communication services in mobile phone networks. Although self-propagating malware is well understood in the Internet, mobile phone networks have very different characteristics in terms of topologies, services, provisioning and capacity, devices, and communication patterns. To investigate malware in mobile phone networks, they developed an event-driver simulator that captures the characteristics and constraints of mobile phone networks, modeling realistic topologies and provisioned capacities of the network infrastructure, as well as the contact graphs determined by cell phone address books.

An interaction-based simulation framework to study the dynamics of worm propagation over wireless networks developed by Channakeshava et al. [4]. This framework is constructed by their proposed methods for generating synthetic wireless networks using activity-based models of urban population mobility. With this framework they study how Bluetooth worms spread over realistic wireless networks.

Recently, Liu et al. [17] investigate malware's spread taking into account the level of secure protection, in terms of users' security awareness. They develop a new compartmental model concerning heterogeneous immunization, partitioning the traditional Susceptible compartment into two sub-compartments, weakly-protected and strongly-protected (weakly-protected Susceptible computers have a higher rate of being Infected than strongly-protected Susceptible computers). The qualitative properties of their model are analyzed through Lyapunov method (taking quadratic functions of independent variables as the candidate Lyapunov functions), and a collection of effective measures for controlling malware spread is proposed, such as keeping as many systems strongly-protected as possible, through numerical simulations.

Latter, Liu et al. [18] investigate the spreading behavior of malware across mobile devices. Modeling mobile networks with complex networks (follow the power-law degree distribution) incorporating the model proposed in [17], and by using the mean-field theory, they propose a novel epidemic model for mobile malware propagation. They calculate the spreading threshold, and analyze the influences of different model parameters as well as the network topology on malware propagation. Through theoretical studies and numerical simulations they show that networks with higher heterogeneity conduce to the diffusion of malware, and complex networks with lower power-law exponents benefit malware spreading. Additionally, malware epidemics over complex networks are greatly different from the previously studied epidemics in fully-connected networks, and the epidemic threshold was found to be density dependent and for all densities considered significantly higher than the value predicted by the previous model.

In [12], Hosseini et al. propose a discrete-time SEIRS epidemic model, i.e., Susceptible - Exposed - Infected - Repaired - Susceptible, of malware propagation in scale-free networks (SFNs) considering software diversity. To prevent malware spreading, they use as a parameter the number of diverse software packages installed on nodes, which are calculated using a coloring algorithm. Investigating the existence of equilibria, they compute the basic reproductive ratio and the critical number of software packages for the proposed discrete-time SEIRS model under various conditions, analyzing moreover the local and global stability of the malware-free equilibrium of the model. Through a series of numerical simulations they show that defense mechanisms of software diversity and immunization have important roles in reducing malware's propagation, and that the proposed model is more effective than other existing epidemic models. Finally considering the immunization rate for the cases of uniform immunization and targeted immunization in the proposed epidemic model they show that the targeted immunization is more appropriate than random immunization for controlling malware spreading in SFNs.

Recently, Zema et al. investigate the case of defending against a spreading proximity malware in a network of wireless sensor (WSN) [33]. Using an autonomous flying robot they notify the spread of malicious software over the wireless sensors, by locate, track, access and cure the Infected ones. Additionally they propose a mathematical model to decide the optimal path that should be followed by the flying robot as to repair as quick as possible the Infected wireless sensors. The authors benchmark their proposed model by the results provided over extended simulations, where their model is compared against classic solutions in different network scenarios.

Our Contribution. In this paper we investigate the effect caused by the response-time of a counter-measure (i.e., an antivirus or a cleaner) on the spread dynamics [6] of a malware propagation to proximal mobile devices. We mainly aim to investigate how the response-time of a counter-measure affects malware's spread and thus to propose a model to establish an upper bound on counter-measure's response-time (i.e., a reasonable response-time interval) for pandemic avoidance. For this purpose, we first propose a *malware propagation model* along with a *device mobility model* and then we develop a simulator that we use to study the spread of malware in the network formed by the mobile devices while they are moving inside a city [22].

Road Map. The paper is organized as follows. In Section 2 we present a malware propagation model to simulate the spread of malware based on geological proximity and, then, a device mo-