IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue I, December 2014
ISSN: 2394 - 6598

SECURE FOR HANDHELD DEVICES AGAINST MALICIOUS SOFTWARE IN MOBILE NETWORKS

Ms. K.Surya
Department Of CSE,
PG scholar, Kalasalingam Institute of Technology
Virudhunagar-626126.

Abstract

—As malware attacks become more frequently in mobile networks, deploying an efficient defense system to protect against infection and to help the infected nodes to recover is important to prevent serious spreading and outbreaks. The technical challenges are that mobile devices are heterogeneous in terms of operating systems, the malware infects the targeted system in any opportunistic fashion via local and global connectivity, while the to-be-deployed defense system on the other hand would be usually resource limited. In this paper, we investigate the problem of how to optimally distribute the content-based signatures of malware, which helps to detect the corresponding malware and disable further propagation, to minimize the number of infected nodes. We model the defense system with realistic assumptions addressing all the above challenges that have not been addressed in previous analytical work. Based on the framework of optimizing the system welfare utility, which is the weighted summation of individual utility depending on the final number of infected nodes through the signature allocation, we propose an encounter-based distributed algorithm based on Metropolis sampler. Through theoretical analysis and simulations with both synthetic and realistic mobility traces, we show that the distributed algorithm achieves the optimal solution, and performs efficiently in realistic environments.

1. Introduction

The target landscape for malware attacks (i.e., viruses, spam bots, worms, and other malicious software) has moved considerably from the large-scale Internet to the growingly popular mobile networks , with a total count of more than 350 known mobile malware instances reported in early 2007. This is mainly because of two reasons. One is the emergence of powerful mobile devices, such as the iPhone, Android, and Blackberry devices, and increasingly diversified mobile applications, such as multi-media messaging service (MMS), mobile games, and peer-to-peer file sharing. The other reason is the emergence of mobile Internet, which indirectly induces the malware. Malware residing in the wired Internet can now use mobile devices and networks to propagate. The potential effects of malware propagation onmobileusers and service providers would be very serious . Understanding the behaviors and damages of mobile malware, anddesigningefficientdetection and defense system are necessary to prevent large-scale outbreaks and it should be anurgent and high-priority research agenda.

Consider a mobile network where a portion of the nodes are infected by malware. Our research problem is to deploy an efficient defense system to help infected nodes to recover and prevent healthy nodes from further infection. Typically, we should disseminate the content-based signatures of known malware to as many nodes as possible .Consequently, distributing these signatures into the whole network while avoiding unnecessarsy redundancy is our optimization goal. However, to address the above problem in the realistic mobile environment is challenging for several reasons. First, typically we cannot rely on centra-lized algorithms to distribute the signatures because the service infrastructure is not always available. Therefore, a sensible way for signature distribution is to use a distributed and cooperative way among users.

Second,mobile devices in general have limited resources, i.e., CPU, storage, and battery power. Although their storage and CPU capacity has been increasing rapidly, it is still very resource-limited compared with desktops. Hence, in the to-be-connectivity should be taken into consideration in the design of defense system for

In this paper, we propose an optimal signature distribu-tion scheme by considering the following realistic modeling assumptions: 1) the network contains heterogeneous de-vices as nodes, 2) different types of malware can only infect the targeted systems, and 3) the storage resource of each device for the defense system is limited. These assumptions are usually not addressed in previous analytical works for simplicity reasons . Our contributions are summarized as follows:

.We formulate the optimal signature distribution problem with the consideration of the heterogeneity of mobile devices and malware, and the limited resources of the defense system. Moreover, our formulated model is suitable for both the MMS and proximity malware propagation.We give a centralized greedy algorithm for the signature distribution problem. We prove that the proposed greedy algorithm obtains the optimal solution for the system, which provides the bench-mark solution for our distributed algorithm design.

We propose an encounter-based distributed algo-rithm to disseminate the malware signatures using Metropolis sampler. It only relies on local information and opportunistic contacts. Through theoretical proof and extensive real and synthetic traces driven simulations, we show that our distributed algorithm approaches the optimal sys-tem performance.

The rest of the paper is organized as follows: We describe the system model in Section 2, and then formulate algorithm in Section 3. In Section 4, we design a distributed algorithm to approach the optimal solution. In Section 5, we introduce the experimental environment for performance evaluation and provide extensive simulation results. Finally, we present the related work in Section 6 and conclude the paper in Section 7.

2. SYSTEM DESCRIPTION

In this section, we first give an overview description of signature distribution in the defense system, and then present the ordinary differential equation (ODE) model for the studied system.

2.1 System Overview

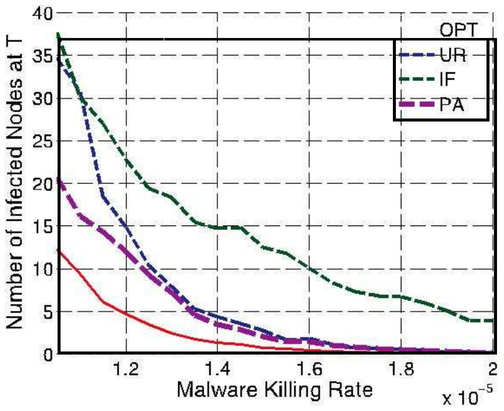
Mobile malware that spreads in the mobile networks typically exploits both the MMS and opportunisticcontacts to propagate from one device to another. In the network, there are different deployed defense system, we should adequately consider the limitation of resources, especially the memory capacity to store the defense software and signatures. Finally, the mobile devices are heterogeneous in terms of operating systems (OS), and different malware targets different systems. These heterogeneous features as well as the propagation via both local and global types of handsets and each malware only targets handsets with a specific OS. In the defense system, we use some special nodes named helper to distribute the signatures into the network. Generally speaking, the deployed helpers can be stationary base stations or access points. However, since mobile nodes are more efficient to disseminate content and information in the network [9], we focus on the case of mobile helpers. Consequently, there is limitation in storage on each mobile device for deploying the defense system. Although currently most smartphones have gigabytes of storage, users usually will not allocate all of them for the usage of malware defense. Our goal is to minimize the malware infected nodes in the system by appropriately allocating the limited storage with the consideration of different types of malware.

3.The Greedy Algorithm

Now, we give a greedy algorithm described in Algorithm 1 for the formulated problem. The obtained result by Algorithm 1 is the optimal solution, which is proved by Theorem 1. The algorithm repeatedly chooses signatures to store in the helpers: in each step, it tries to select one signature that brings the maximum system utility for a helper that still has enough storage. Therefore, our algorithm is likely to allocate more helpers to store the signatures of malware whose corresponding malware-defending utilities are larger than others, which is achieved by using the heterogeneous features in terms of devices and malware.

In this section, we present numerical results with the goal of demonstrating that our greedy algorithm for the signature distribution, denoted OPT, achieves the optimal solution and yields significant enhancement on the system welfare compared with prior heuristic algorithms. Related to the heuristic algorithms, we consider 1) Important First (IF), which uses as many helpers as possible to store the signature of the most popular malware, 2) Uniform Random (UR), where each helper randomly selects the target signatures to store, and 3) Proportional Allocation (PA), which is a heuristic policy that assigns signatures with the uniform distribution proportional to the market sharing and the weights of different malware. To simulate a more realistic scenario, we model the malware in the system according to the market share of different handset OS of 2009. In the simulation, we change the malware killing rate and spreading rate, and consider a system with nodes that can be infected by five different types of malware, which are RIM targeted malware 36 percent; Android targeted 28 percent; iPhone 21 percent; Windows Mobile 10 percent, and others 5 percent. We set N ¼ 500 and have 100 helpers with uniform random storage size from one to five signatures to deploy in the antimalware software. In the experimental setup, the number of initial infected nodes is set to be 10 percent of all nodes. Related to the utility function and weighting factors, we set G$_k$ð_$_k$^{L}Þ ¼ __$_k$^{L}, L ¼ 2 _ 10^4 s and w ¼ ½1=2; 1=4; 1=8; 1=16; 1=16& to

The simulation results are shown in Fig. 2. Fig. 2a shows the number of infected nodes according to the malware recovering rates caused by the signature distribution in the centralized greedy algorithm. We can observe that the number of infected nodes decreases with the increase of recovering rate. Among different algorithms, IF provides the worst performance. Compared with other heuristic algorithms, our OPT algorithm reduces the number of infected nodes by 355.6, 127.3, and 56 percent over the FI, UR, and PA on average, respectively. Fig. 2b shows the number of infected nodes according to the malware spreading rates. Different from Fig. 2a, the number of infected nodes increases with the growth of spreading rate. From these results, we can observe that PA obtains relatively better performance than FI and UR, which are expected underperform. However, this well-organized heuristic policy still performs about 34 percent worse than



(a)

Fig 1.Performance of different algorithms for the malware defense system with (a) variable malware recovering rate; and (b) variable malware spreading rate.

4.Distributed Algorithm

In this section, we carry out simulations to evaluate the distributed algorithm by addressing the following goals: 1) demonstrating the distributed algorithm converges to the optimal system performance in different environment settings and large scale networks, 2) demonstrating our scheme of deploying the defense system achieves good performance of preventing the malware propagation under the real-world mobility traces. To achieve these two points, we cover a broad set of parameters as follows: 1) extensive mobility models of both real and synthetic traces, in which real traces include both human and taxi mobility traces, while synthetic traces include the Small World In Motion (SWIM) and Self-similar Least Action Walk (SLAW) models, where the number of system nodes can be changed in the simulation, 2) small and large system scale with respect to the number of nodes and kinds of malware, and 3) various compared schemes including our centralized optimal greedy algorithm, UR and IF. According to the malware propagation, we use the opportunistic contacts between nodes to spread the proximity malware, while using the phone books generated by the social model introduced in Section 3.2 to spread the malware via MMS. More specifically, the infected nodes will transmit the malware to the nodes in its phone book one by one, and the time interval and malware transmission and receiving time are set as exponential distribution. But if they encounter other nodes in proximity, these nodes will be infected immediately. In the simulation of the distributed algorithm, instead of simply assuming each node has the exact global knowledge, we run the proposed EWMA method to estimate the global information of the number of nodes and system states in the network. That is to say, the global information is also obtained by the distributed approach in the simulation, which sets up an objective environment to evaluate our proposed distributed algorithm.

5.Related work

With the growth of SMS/MMS, mobile games, mobile commerce, and mobile peer-to-peer file sharing, a number of studies have demonstrated the threat of malware propagation on mobile phones. They can be generally categorized into two main types. One class of works focuses on analyzing the proximity malware spreading. Yan et al.develop a simulation and analytic model for Bluetooth worms, and show that mobility has a significant impact on the propagation dynamics. The other class focuses on the malware spreading by SMS/MMS. Fleizach et al.evaluate the speed and severity of malware spreading by cell phone address books. Zhu et al.]studied the characteristics of slow start and exponential propagation exhibited by MMS malware. Besides, a small amount of works also look at both MMS and proximity malware. For example, Bose and Shin [25] investigate the propagation of mobile worms and viruses using data from a real-life SMS customer network, and they reveal that hybrid worms using both MMS and proximity scanning can spread rapidly within cellular networks. Wang et al.model the mobility of mobile phone users by analyzing a trace of 6.2 million mobile subscribers from a service provider. They study the fundamental spreading patterns that characterize a mobile virus outbreak and find that the greatest danger is posed by hybrid viruses that take advantage of both proximity and MMS. Obtaining the insights of these two works, our model considers both the MMS and proximity propagation in our defense system design.

For performance evaluation and modeling of mobile malware spreading, the epidemic model, based on the classical Kermack-Mckendrick model

traditionally used in wired networks, has been extensively used in , and so on. Actually, the system performance of the epidemic model can be approximated by the Ordinary Differential Equations with a well-known technique called fluid model , which is widely used to model the epidemic forwarding in DTN . In the fluid model, the solution of the ODE converges in probability to the system's sample paths. These works show that when the number of nodes in a network is large, the deterministic epidemic models can successfully represent the dynamics of malware spreading, which is demonstrated by simulations and matching with actual data. We use an ODE model to analyze and design the signature distribution problem in the malware defense system. Therefore, our model in this work is reasonable.

Recently, some malware coping schemes have been proposed to defend mobile devices against malware propagation. To prevent the malware spreading by MMS/ SMS, Zhu et al. [5] propose a counter-mechanism to stop the propagation of a mobile worm by patching an optimal set of selected phones by extracting a social relationship graph between mobile phones via an analysis of the network traffic and contact books. This approach only targets the MMS spreading malware and has to be centrally imple-mented and deployed in the service provider's network. To defend mobile networks from proximity malware by Bluetooth, Zyba et al. [6] explore three strategies, including local detection, proximity signature dissemination, and broadcast signature dissemination. For detecting and mitigating proximity malware, Li et al. propose a community-based proximity malware coping scheme by utilizing the social community structure reflecting a stable and controllable granularity of security

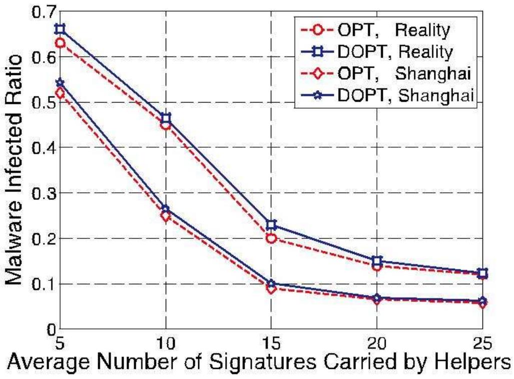


Fig.2 System performance of malware infected ratio with Reality human mobility trace and Shanghai vehicle trace when changing the number of signatures carried by the helpers.

. These two works both target the proximity malware. The former one has the limitations that signature flooding costs too much and the local view of each node constrains the global optimal solution. Although the aftermath scheme integrates short-term coping components to deal with individual malware and long-term evaluation components to offer vulnerability evaluation toward individual nodes, the social community information still need to be obtained in a centralized way. Khouzani et al. investigate the optimal dissemination of security patches in mobile wireless network to counter the proximity malware threat by contact. It uses the SIR model to formulate the tradeoffs between the security risks and resource consumption as optimal control problems under the assumptions of homogeneous network setting. There are significant differences between these works and ourwork.

First, our scheme targets both the MMS and proximity malware at the same time, and considers the problem of signature distribution. Second, all these works assume that malware and devices are homogeneous, we take the heterogeneity of devices into account in deploying the system and consider the system resource limitations. Third, our proposed algorithm is distributed, and ap-proaches to the optimal system solution.

CONCLUSIONS

In this paper, we investigate the problem of optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware. We introduce a distributed algorithm that closely approaches the optimal system performance of a centralized solution. Through both theoretical analysis and simulations, we demonstrate the efficiency of our defense scheme in reducing the amount of infected nodes in the system.

At the same time, a number of open questions remain unanswered. For example, the malicious nodes may inject some dummy signatures targeting no malware into the network and induce denial-of-service attacks to the defense system. Therefore, security and authentication mechanisms should be considered. From the aspect of malware, since some sophisticated malware that can bypass the signature detection would emerge with the development of the defense system, new defense mechanisms will be required. At the same time, our work considers the case of OS-targeting malware. Although most of the current existing malware is OS targeted, cross-OS malware will emerge and propagate in the near future. How to efficiently deploy the defense system with the consideration of cross-OS malware is another important problem. We are continuing to cover these topics in the future work.

References

1 P. Wang, M. Gonzalez, C. Hidalgo, and A. Barabasi, “Under-standing the Spreading Patterns of Mobile Phone Viruses,”Science,vol. 324, no. 5930, pp. 1071-1076.

2 M. Hypponen, “Mobile Malwar,”Proc. 16th USENIX SecuritySymp.

3 G. Lawton, “On the Trail of the ConfickerWorm ,” Computer, vol. 42, no. 6, pp. 19-22.

4 Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, “A Social Network Based Patching Scheme for Worm Containment in Cellular Networks,”Proc. IEEE INFOCOM