ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices

Muli Venkata Devi
P.G. Scholar (M. Tech),
Department of CSE,
Srinivasa Institute of Technology & Sciences,
Ukkayapalli, Kadapa, Andhra Pradesh.

K.Rajasekhar Reddy
Assistant Professor,
Department of CSE,
Srinivasa Institute of Technology & Sciences,
Ukkayapalli, Kadapa, Andhra Pradesh.

Abstract:

In this project, we formulate an analytical model to characterize the spread of malware in mobile networks and to deploying an efficient defense system to protect and helps infected nodes. Using a compartmental model, we derive the system parameters or network conditions under which the mobile networks may reach a malware free equilibrium. Here we analyze in that mobile network how to distribute the signatures that is based on content. Which helps to detect the corresponding malware and disable further propagation used to minimize the infected nodes, here we propose the Encounter based distributed algorithm to achieve optimal solution. We show that the distributed algorithm achieves the optimal solution, and performs efficiently in realistic environments.

Index Terms:

Security threat, mobile malware, distributed algorithm, heterogeneous mobile networks.

1.INTRODUCTION :

In the mobile computing, mobile phone security is an important research topic. It is of particular concern as it associates to the security of personal information now accumulated on the Smart phone. Today most of the users and businesses utilize smart phones [1] [2] as communication tools but also as a means of planning and managing their work and private life. In the companies, these technologies are able to cause the profound modifications in theOrganization of the information systems and consequently they have become the source of new risks. Definitely, smart phones gather and accumulate a growing amount of responsive information to which access must be inhibited to defend the isolation of the user and the knowledgeableproperty of the company.

The damage of mobile viruses in the smartPhones are a significant issue. Among many possible damages, mobile viruses can cause private data leakage and perturb discussion by remote control. The mobile virus sends thousands of spam messages. Due to this it jams the wireless services and the quality of communication is decreased. So, that it is necessary for both users and service providers are learn about the dissemination methods of the mobile virus and create awareness among the users. To examine and predict the particular damages of the virus, some methods are used to investigate the dynamic process of virus propagation. The valid propagation methods can be utilized as test beds to: 1) compute the scale of a virus outbreak before it happens in reality and 2) compute new and/or enhanced countermeasures for limiting virus dissemination [3].

In the existing method, cell phone viruses may multiply as a result of two various dominant approaches. By means of MMS, any viruses may perhaps post any duplicate regarding by it to every one gadgets in whose volumes are simply in the target eBook on the infected handset. This sort of viruses propagates in the interpersonal chart made from the target books, and will distributed rapidly with no geographical limits. One other tactic is to use your short-range Wi-Fi mass media such as Wireless Bluetooth to help infect your gadgets with closeness seeing that “proximity viruses. ” we have been the first to handle your troubles regarding developing any protected system for equally MMS and Bluetooth. We all expose a great ideal distributed solution to efficiently avoid viruses spreading and also to support infected nodes to recuperate. However using this method won’t take into account the mix of both viruses. So, in the proposed research an innovative technique is used to effectually examine the speed and strictness for distribution the hybrid malware such as communication services that targets BT and multimedia messaging service (MMS). This method can compute the injures which is caused by the hybrid viruses and the objective is to develop the detection and containment processes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2. RELATED WORK:

With the growth of SMS/MMS, mobile games, mobile commerce, and mobile peer-to-peer file sharing, a numberof 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. [4], [5] 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. [6] evaluate the speed and severity of malware spreading by cell phone address books. Zhu et al. [7] 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 [8] consider the propagation of mobile worms and malwares 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. [9] model the mobility of mobile phone users by analysing a trace of6.2 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 bothProximity 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 [10] traditionally used in wired networks, has been extensively used in [9], 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 [11], which is widely used to model the epidemic forwarding in DTN [11]. 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.

3.HYBRID VIRUS DETECTION METHOD

innovative method is proposed which is called a Hybrid virus detection model. A Hybrid malware can develop both messaging and short-range wireless communication services to spread. It is essential to have a mathematical modelby analysing the mixed behaviours of long-range in fe ctivity pattern from dissemination through messaging service and ripple-based inf ectivity pattern from propagating through short-range wireless communication. In this work, a newanalytical model is proposed for examine the speedand harshness for dissemination the hybrid malware that targets MMS/SMS and BT in an efficient manner. This analytical model based on the differential equations works more effectually and itact as a quick reference to collect estimated knowledge of propagation speed and sternness ofhybrid malwares with a variety of settings of contagion rates and average node degrees incomprehensive social networks. Based on the security assessment this method could adopt the results to develop a detection and containment methods and processes so as to evade vital out break. In this section, the measure of thepropagation of infections is considered within a population under risk. The communication betweena cooperated and a non-cooperated handset is presented as a contact between a contaminated individual and a vulnerable one, in which a vulnerable node attains infection and never becomes vulnerable again.

This is because of theuser's lack of anxiety about the threat of malwares and the inadequate capacity of current antiviralsoftware. The population in this model is nothingbut the total number of nodesN in the networkwhich are assumed to be stationary and consistently distributed with node density . Assume that the entire nodes are MMS and BT to assume that allnodes are MMS and BT facilitated to preserve the harmonized mixing property. Denote subpopulation function,I(t)=IBT(t)+IMMS(t)Represents the total number of cooperationHandsets at time t , in which IBT(T)and IMMS(t)are those that have been contaminated through MMS and BT at time t, correspondingly. Similarly S(t)represents the set of vulnerable nodes at time t.Obviously, we have,I(t) + S(t)= IBT(t)+IMMS(t)+ S(t)= N, anddI(t)/dt=dIBT(t)/dt+dIMMS(t)/dt Assume that only one handset is contaminated atthe starting stage that is, I(0) = IMMS(0) = 1 andIBT(0) =0. The rates of malware infection βBT andβMMS correspondingly which denotes theprobabilistic rates at which an infective node communicates with and compromises a vulnerable node through MMS and BT,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

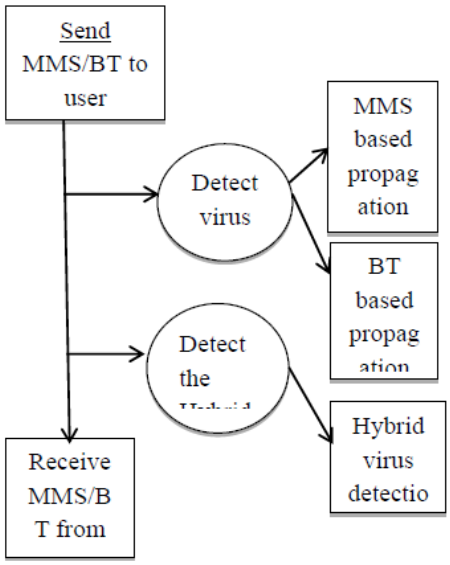

Figure1: Hybrid virus detection method

4. VIRUS DETECTION MODEL:

In the existing method, mobile malware can pass on through two different dominant approaches. Through MMS, a malware may possibly send a backup of itself to everyone devices whose numbers are only in the address book from the infected handset. These kinds of malware propagate inside social graph formed by the address books, which enable it to spread very quickly without geographical limits. Anothermethod is to use the short-range wireless media for example Bluetooth to infect the devices within proximity as "proximity malware". We are the first to address the challenges regarding designing a support system for equally MMS and proximity malware. We introduce a great optimal distributed strategy to efficiently avoid malware spreading in order to help infected nodes to recuperate. Consider a mobile network in which a portion of the nodes are infected by malware. Our research problem is always to deploy a useful defence system to help you infected nodes to recuperate and prevent wholesome nodes from additional infection. Typically, we have to disseminate the content-based signatures regarding known malware to as many nodes as achievable. Consequently, distributing these signatures into your whole network while avoiding unnecessary redundancy is our optimization purpose. However, to address the aforementioned problem in the realistic mobile atmosphere is challenging for a number of reasons.

First, typically we cannot rely on centralized algorithms in order to distribute the signatures because the service infrastructure is just not always available. The mobile units are heterogeneous in terms of operating systems (OS), and different malware targets different systems. These heterogeneous features in addition to the propagation via equally local and worldwide connectivity should be evaluated in the design of immune system for real make use of. We propose a great optimal signature submission scheme by taking into consideration the following realistic modelling assumptions: 1) the multilevel contains heterogeneous units as nodes, 2) different types of malware can merely infect the precise systems, and 3) the storage resource of device for the immune system is limited. These assumptions tend to be not addressed within previous analytical performs for simplicity reasons [12]. Our contributions are summarized the following:

• We formulate the suitable signature distribution problem with all the consideration of the heterogeneity of mobile phones and malware, and the limited resources from the defences system. In addition, our formulated model would work for both the MMS and proximity malware propagation.

• We offer a centralized greedy algorithm with the signature distribution dilemma. We prove which the proposed greedy algorithm obtains the suitable solution for the system, which provides the benchmark solution for the distributed algorithm pattern.

• We propose great encounter-based distributed criteria to disseminate the malware signatures applying Metropolis sampler. It only relies upon local information and also opportunistic contacts.Through theoretical proof and extensive real and synthetic traces driven simulations, we show that our distributed algorithm approaches the optimal system performance.

5. DISTRIBUTRED LGORITHM.

Algorithm 1. The distributed algorithm of malware signature distribution for Node i to adjust its configuration when encountering Node j, where T0 is the initial temperature and n is the encounter counter that are set to be 1 at the beginning
1: if xi;k ¼¼ xj;k for all k 2 IK then
2: End the process;
3: end if

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4: if 9k: xi;k ¼ 0 and xj;k ¼ 1, which means there is at least one signature existing in node j, but does not exist in
node i then
5: Set n n þ 1
6: Select a signature c from the buffer of user i uniform randomly such that xi;c ¼ 1, and select a signature c0 from the buffer of user j uniform randomly such thanxj;c0 ¼ 1 and xi;c0 ¼ 0;
7: Set the system temperature Tn ¼ T0 logðn_1Þ ;
8: Compute the acceptance probability _c0;cðTnÞ;
9: Draw a random number R uniform distribute in ð0; 1_;
10: if R < _c0;cðTnÞ then
11: User i selects signature of c0 and drops c wit probability of 1
SK _c0;cðTnÞ;
12: end if
13: end if

In the distributed system, each node, says i, maintains values of local uk, where k 2 IK and xi;k ¼ 1, and updates through the exponential smoothing when two nodes meetm ith each other by exchanging local information throughthe contact. For example, when nodes i encounters node j and their local states are ui k and uj k for signature k. For all signatures that both nodes i and j carry, node i updates as ui k _ þ ð1 _ _Þui k, and for all other signatures uik ð1 _ _Þui k, where _ is the exponential decay rates.

This mechanism is used widely, and its efficiency is verified by recent works of.It has been demonstrated in [16] that EWMA converges as long as the nodemobility, and the convergence speed is exponential [19]. We note that the convergence speed of Algorithm 2 is geometric that will be introduced in the next section, which is much slower than the system state coverages.

This ensures each node can obtain a relatively accurate system state to perform the distributed algorithm. At the same time, we will demonstrate the effectiveness of EWMA and the distributed algorithm by simulation..

6. RESULTS:

Figure 2.

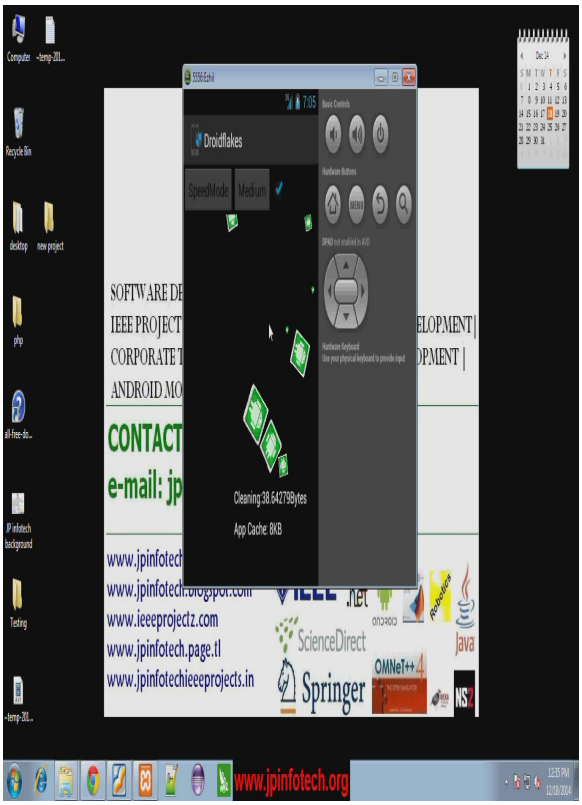

Figure 3.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

7. CONCLUSION:

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 mal ware 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 OStargeting malware. Although most of the current existing malware is OS targeted, cross-OS malware will emerge an propagate in the near future. How to efficiently deploy th 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] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, "Security Aspects of Mobile Phone Virus: A Critical Survey," Industrial Management and Data System, vol. 108, no. 4, pp. 478-494, 2008.

[2] H. Kim, J. Smith, and K.G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 08), pp. 239- 252, 2008.

[3] S. Cheng, W.C. Ao, P. Chen, and K. Chen, "On Modeling Malware Propagation in Generalized Social Networks," IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.

[4] Jerry Cheng, Starsky H.Y. Wong, Hao Yang, and Songwu Lu," SmartSiren: Virus Detection and Alert for Smartphones," Proceedings of the 5th international conference on Mobile systems, applications and services, pp. 258-271,2007.

[5] E.V. Ruitenbeek and F. Stevens, "Quantifyingthe Effectiveness of Mobile Phone Virus Response Mechanisms," Proc. 37th Ann. IEEE/ IFIP Int'l Conf. Dependable Systems and Networks (DSN '07), pp. 790- 800, 2007.

[6] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A SocialNetwork Based Patching Scheme for Worm Containment in Cellular Networks," Proc. IEEE INFOCOM, pp. 1476-1484, 2009.

[7] K. Lee, S. Hong, S.J. Kim, I. Rhee, and S. Chong, "SLAW: A Mobility Model for Human Walks," Proc. IEEE INFOCOM, pp. 855-863, 2009.

[8] A. Mei and J. Stefa, "SWIM: A Simple Modelto Generate Small Mobile Worlds," Proc. IEEE INFOCOM, pp. 2106-2113, 2010.

[9] G. Zyba, G.M. Voelker, M. Liljenstam, A. Mehes, and P. Johansson, "Defending Mobile Phones from Proximity Malware," Proc. IEEE INFOCOM, pp. 1503-1511, 2009.