RESEARCH ARTICLE   OPEN ACCESS

Hybrid Model for Detecting Malware in Mobile Networks with Heterogeneous Devices

G.Vamsi [1], A. Ravi [2], D. V. Subbaiah [3]

M.Tech [1], Assistant professor [2], Associate Professor [3]

Department of Computer Science and Engineering

H.O.D of computer science

Priyadarshini College of Engineering and Technology

Nellore

Andhra Pradesh - India

ABSTRACT

Malware attacks become more frequently in cellular networks (i e., viruses, worms, and also other malicious software). Spyware which disturbs your network computer function, hacking the hypersensitive information and accesses your private systems. It is only a program that's specifically designed to be able to injure the computer it can be a virus or perhaps worm. Mobile malware can propagate via two different dominating approaches those are usually MMS and Bluetooth. To avoid malware spreading and help the infected nodes to extract optimal signature dispersed method. But this kind of does not take into account the hybrid viruses which disseminate via both BT and MMS routes. So, to increase the efficiency of restraining your propagation of cell phone malwares, we introduce a new approach called any Hybrid virus detection model. The hybrid malware could be spread by both end to end messaging services via personal social devices and short-range Wi-Fi communication services. In this method, a new differential equation-based process is proposed to examine the mixed behaviors of delocalized contagion as well as ripple based propagation for the hybrid malware in generalized internet sites including of individual and spatial sociable relations. An experimental result signifies that the proposed technique is computationally effective to tell apart the hybrid malware.

Keywords:- Mobile malware, mobile networks, hybrid malware detection.

I. 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.

II. 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. [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.

III.   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.

IV.   HYBRID VIRUS DETECTION METHOD

In the proposed research, to increase theefficiency of the restraining the propagation ofhybrid viruses, an

innovative method is proposedwhich is called a Hybrid virus detection model. AHybrid malware can develop both messaging andshort-range wireless communication services tospread. It is essential to have a mathematical modelby analysing the mixed behaviours of long-rangeinfectivity pattern from dissemination throughmessaging service and ripple-based infectivitypattern from propagating through short-rangewireless communication.

In this work, a newanalytical model is proposed for examine the speedand harshness for dissemination the hybridmalware that targets MMS/SMS and BT in an efficientmanner. This analytical model based on thedifferential equations works more effectually and itact as a quick reference to collect estimatedknowledge of propagation speed and sternness ofhybrid malwares with a variety of settings ofcontagion rates and average node degrees incomprehensive social networks. Based on thesecurity assessment this method could adopt theresults to develop a detection and containment methods and processes so as to evade vitaloutbreak.

In this section, the measure of thepropagation of infections is considered within apopulation under risk. The communication betweena cooperated and a non-cooperated handset ispresented as a contact between a contaminatedindividual and a vulnerable one, in which avulnerable node attains infection and neverbecomes vulnerable again. This is because of theuser's lack of anxiety about the threat of malwaresand the inadequate capacity of current antiviralsoftware. The population in this model is nothingbut the total number of nodes$N$ in the networkwhich are assumed to be stationary and consistently distributed with node density ρ. Assume that theentire nodes are MMS and BT to assume that allnodes are MMS and BT facilitated to preserve theharmonized mixing property. Denote subpopulationfunction,$I(t)=I_{BT}(t)+I_{MMS}(t)$Represents the total number of cooperationHandsets at time t , in which $I_{BT}(T)$and$I_{MMS}(t)$are those that have been contaminated throughMMS and BT at time t, correspondingly. Similarly $S(t)$represents the set of vulnerable nodes at time t.Obviously, we have,$I(t) + S(t)= I_{BT}(t)+I_{MMS}(t)+ S(t)= N$, and$dI(t)/dt=dI_{BT}(t)/dt+dI_{MMS}(t)/dt$

Assume that only one handset is contaminated atthe starting stage that is, $I(0) = I_{MMS}(0) = 1$ and$I_{BT}(0) =0$. The rates of malware infection β_{BT} andβ_{MMS} correspondingly which denotes theprobabilistic rates at which an infective nodecommunicates with and compromises a vulnerable node through MMS and BT
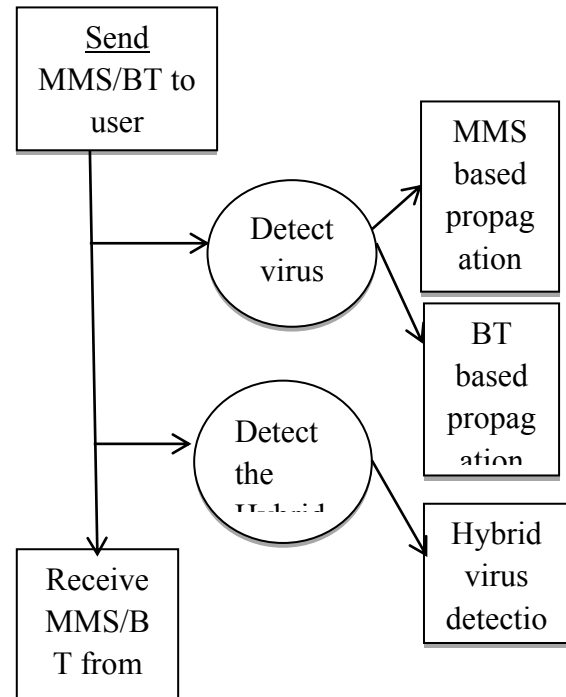

Figure1: Hybrid virus detection method

The average degrees of a node connecting through BT and MMS are denoted as η_{BT} andη_{MMS}.

V.   RESULTS AND DISCUSSION

In this section numerous experiments are explained that are aimed to expose some keyfactors which impacts the virus propagation.Originally, the two phones are selected arbitrarilyfrom a network as the contaminated phones inorder to replicate a multiple-seed attack that isprobable to happen in the real world.
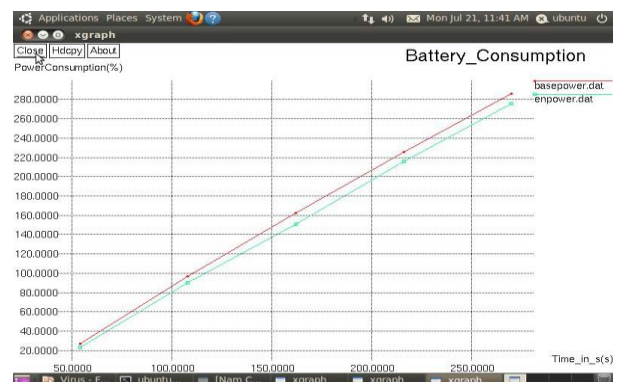
A. *Battery Consumption*

Figure 2: Shows Battery Consumption

Figure.2 shows that the batteryconsumption. In the existing system, for simulating viruspropagation through both MMS/SMSand Bluetooth is presented by a two layer model. Inthe proposed system, to increase the

effectivenessof inhibiting the propagation of mobile phone Viruses, a Hybrid virus detection model isproposed. When compared to the existing system,there is less battery consumption in the proposedsystem.
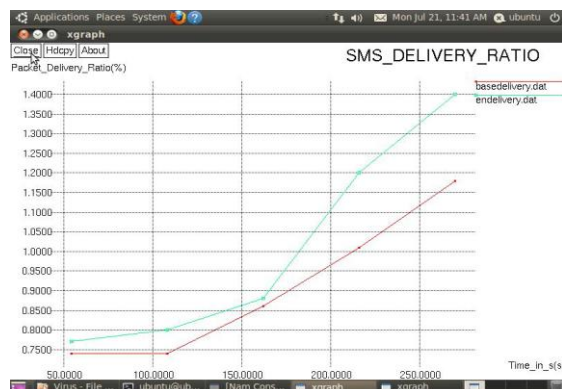
B. MMS delivery ratio

Figure 3: Shows MMS delivery ratio

Figure.3 shows that the MMS deliveryratio. In the existing system, for simulating virus propagation through bothBluetooth and MMS is presented by a two layer network. In the proposedsystem, to increase the effectiveness of inhibitingthe propagation of mobile phone viruses, a Hybridvirus detection model is proposed. When comparedto the existing system, there is high MMS deliveryratio in the proposed system.

C. Packet delivery ratio

Figure 4: Shows Packet delivery ratio

Figure.4 shows that the Packet deliveryratio. In the existing system, for simulating virus propagationthrough both Bluetooth and SMS/MMS is presented by a two layer network. In the proposedsystem, to increase the effectiveness of inhibitingthe propagation of mobile phone viruses, a Hybridvirus detection model is proposed. When comparedto the existing system, there is high packet deliveryratio in the proposed system.

VI. CONCLUSION

Mobile malware can multiply through two diverse dominant approaches people are MMS in addition to Bluetooth. To avoid malware spreading and also to help the infected nodes to recover optimal signature spread method. But this process does not consider the hybrid viruses that will disseminate via both equally BT and MMS channels. So, to raise the efficiency of restraining your propagation of mobile phone viruses, we introduce an innovative approach called some sort of Hybrid virus diagnosis model. The hybrid malware can be distributed by both end to separate messaging services by means of personal social devices and short-range cellular communication services.

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] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms," IEEE Trans. Mobile Computing, vol. 8, no. 3, p. 1071, 2008.

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

[6] C. Fleizach, M. Liljenstam, P. Johansson, G. Voelker, and A. Mehes, "Can You Infect Me Now? Malware Propagation in Mobile Phone Networks," Proc. ACM Workshop Recurring Malcode, pp. 61- 68, 2007.44, 2007.

[7] 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, 2009.

[8] A. Bose and K. Shin, "On Mobile Viruses Exploiting Messaging and Bluetooth Services," Proc. Securecomm and Workshops, pp. 1-10, 2006.NFOCOM, 2009.

[9] P. Wang, M. Gonzalez, C. Hidalgo, and A. Barabasi, "Understanding the Spreading Patterns of Mobile Phone Viruses," Science, vol. 324, no. 5930, pp. 1071-1076, 2009.

[10] D. Daley and J. Gani, Epidemic Modelling: An Introduction. Cambridge Univ, 2001.

[11] E. Altman, G. Neglia, F. De Pellegrini, and D. Miorandi, "Decentralized Stochastic Control of Delay Tolerant Networks," Proc. IEEE INFOCOM, 2009.

[12] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," Proc. IEEE INFOCOM, 2010.