ISSN 2320 2610
Volume 3, No.4, July - August 2014
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://warse.org/pdfs/2014/ijmcis01342014.pdf

HYBRID MODEL FOR DETECTING VIRUSES IN MOBILE NETWORKS

M.Karpagavalli [1], K.Mythili[2]

[1]Research Scholar, Hindustan college of Arts and Science, India, mkarpagavalli09@gmail.com
[2]Associate Professor, Hindustan college of Arts and Science, India, mythiliarul@gmail.com

ABSTRACT

Malware is malicious software which disturbs the network computer operation, hacking the sensitive information and accesses the private systems. It is nothing but a program which is specifically designed to injure the computer it may be a virus or worm. So, in order to overcome this problem a two-layer network model is presented for simulating virus propagation through both Bluetooth and SMS. The two methods are analysed for controlling the mobile virus propagation. i.e., preimmunization and adaptive distribution methods drawing on the methodology of autonomy-oriented computing (AOC). But this method does not consider the hybrid viruses that disseminate via both BT and SMS channels. So, to increase the efficiency of restraining the propagation of mobile phone viruses, we introduce an innovative approach called a Hybrid virus detection model. The hybrid malware can be distributed by both end-to-end messaging services through personal social communications and short-range wireless communication services. In this method, a new differential equation-based method is proposed to examine the mixed behaviours of delocalized contagion and ripple based propagation for the hybrid malware in generalized social networks including of personal and spatial social relations. An experimental result shows that the proposed system is computationally effective to distinguish the hybrid malware.

Key Words: Mobile networks, mobile virus,

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 the organization 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 intellectual property of the company.

The damage of mobile viruses in the smart phones is 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, for describing BT-based and SMS based viruses a two-layer network model is used. In this model, the virus is propagates via Bluetooth and Short/Multimedia Message Services correspondingly. In this method, viruses are generated as a result of human behaviours, rather than contact probabilities in a harmonized model. There are two categories of human behaviour. The categories are operational behaviour and mobile behaviour. This method considers the impacts of the network structures in the virus dissemination. The objective of this work is to gain further insights into how human behaviours concern the dissemination dynamics of mobile viruses. But this method does not consider the hybrid viruses. So, in the proposed research an innovative technique is sued to effectually examine the speed and strictness for distribution the hybrid malware such as Commwarrior that targets multimedia messaging service (MMS) and BT.

This method can compute the injures which is caused by the hybrid viruses and the objective is to develop the detection and containment processes.

2. PREVIOUS RESEARCH

Jerry Cheng et.al [4] suggested presented a collaborative virus recognition and alert system which is named as Smart Siren for smart phones. Some of the smart phones are not provided with the anti-virus software and there are no advanced virus signatures. The main work is to stop the potential virus in the smart phones whereas reducing the number of smart phones affected by the virus. Every smart phone has a light-weight agent whereas a centralized proxy is utilized to sustain the virus detection and alert processes. The advantage of the proxy-based method is to diminish the processing complexity from the resource-constrained smart phones, and to shorten the association among the smart phones. Particularly, every smart phone agent tracks the activities of the communication in the device and the reports are given to the proxy in a periodic manner. The main feature of the smart siren is the protection of the user privacy. Most of the users are not prepared to disclose the activities on their phones to the proxy. This method considers the privacy concerns by using the anonymous and ticketed report submission scheme.

Fabrice Stevens et.al [5] suggested the threatening propagation vectors which facilitates the quick and extensive virus dissemination throughout a network of phones. According to the condition, one of the most important threats is propagation by MMS message attachments. This method focus on the mobile viruses propagating through MMS messages. The mobile phone security evaluates the influence preceding antivirus efforts against conventional computer viruses, but the usefulness of these measures must be computed in the context of the mobile phone network environment. The mobile phone is expected to follow an development comparable to that of computer viruses, only at an accelerated pace. The model of mobile phone virus propagation leverages associated work in computer virus modelling. Kephart and White introduced epidemiological models to the study of computer viruses. Some of the work utilizes the markov models for including the probability distributions of model behaviour. The same way of those models of email virus propagation include the user behaviour, this model of mobile phone viruses considers factors such as how speedily the mobile phone user reads a new MMS message and how expected a phone user is to open a dirtied attachment.

Zhichao Zhu et.al [6] suggested a new approach to include MMS worms within a restricted range at the earliest stage. In the cellular network, the mobiles are divides into multiple sections according to the social associations between the mobiles reclaimed from a real cellular network trace. The mobiles in the every section are intimately interacting with each other whereas mobiles across different sections are less associated. For the key nodes, the security patches are disseminated which separates the individual sections to block the worm propagation from one partition to other. Particularly, the contributions of this work are: The social association graph of the mobile devices is created by extracting their communication patterns according to the network trace. The social associations between the mobile phones are described by the graph which is typically demoralized by mobile worms for spreading. A new containment strategy is presented for the MMS worms by dividing the mobiles correctly according to the social association graph. There are two partitioning methods: balanced partitioning and clustered partitioning are suggested and their performance is computed.

Seongik Hong et.al [7] suggested a new mobility model which is called as Self similar Least-Action Walk (SLAW) model which generates the synthetic mobility traces. For developing SLAW, seriously rely on the GPS traces of human walks containing 226 daily traces gathered from 101 volunteers in five dissimilar outdoor sites. Specifically, the traces are used to share the general interests like students in the identical university campuses and tourists in a theme park. This method represents the intrinsic social circumstances among walkers patented as common meeting places and walk patterns therein. The power-law flights and fractal waypoints are modelled so that it express the regular and also impulsive trip patterns present in the daily mobility of humans. People naturally keep a routine of visiting the identical places every day like going to an office, but at the same time, make irregular trips. It is not the case where people would always arbitrarily decide places to visit and visit them in a arbitrary order. However, some work exists in expressing the regularity of daily trip patterns of humans; none of the existing work imitates realistic statistical patterns emerging in real human walk traces.

Alessandro Mei et.al [8] presented a effortless mobility model which is called (SWIM) which creates small worlds. This method is simple to develop and highly effectual in simulations. The nodes mobility pattern is based on the simple intuition on human mobility. This method is capable to raise social behaviour among nodes whereas consider to be the base of human mobility in real life. This model is validated by using the real traces and the allocation of inter-contact time, contact period and number of contact disseminations between nodes is compared.

Additionally, SWIM is used to predict the performance of forwarding protocols. The performance of the two forwarding protocols like epidemic forwarding and delegation forwarding are compared on the real traces and the synthetic traces generated with SWIM. The performance of the two protocols on the synthetic traces truthfully approximates their performance on real traces, following the assert that SWIM is an exceptional model for human mobility.

Gjergji Zyba et.al [9] considered the dynamics mobile virus which propagates by the propinquity contact and computes the potential defences against it. The dynamics of proximity dissemination intrinsically depend upon the mobility dynamics of a user population for a given geographic region. Unfortunately, for modelling the user mobility there is no ideal methodology. The traces of mobile user contacts reproduce concrete behaviour, but they are hard to simplify and only detain a subset of all connections because of a lack of geographic coverage. The analytic epidemiological models are proficient to calculate and high scalability. The Synthetic models are flexible and the necessary geographic coverage is provided but there is lack of full authenticity of user mobility traces. There are three methods for discovering and reducing proximity malware: local detection, in which devices distinguish when they become spoiled and immobilize further propagation; proximity signature allocation, in which devices generate content-based signatures of malware and distribute them through proximity communication as well; and broadcast signature dissemination, in which a centralized server combined explanation from individual devices, distinguishes propagating malware, and broadcasts signatures to mobile devices. These methods span the spectrum from the simple local detection to a globally synchronized defence. The malware propagation is restricted by the proximity signature dissemination to a fraction of the vulnerable population, and does so without relying upon provider network infrastructure.

Pan Hui et.al [10] presented an optimal signature allocation method by considering the following sensible modelling postulations, 1) the network includes heterogeneous devices as nodes, 2) dissimilar categories of malware can only contaminate the targeted systems, and 3) the storage resource of every device for the defence system is restricted. These postulations are typically not addressed in the analytical work. The contributions are summarized as follows: The optimal signature distribution problem is formulated with the heterogeneity of mobile devices and malware and the restricted resources of the defence system. The centralized greedy algorithm is used for the signature distribution problem. By using this method, the best solution is acquired for the system. An encounter-based distributed algorithm is suggested for distributing the malware signatures using Metropolis sampler.

Don Towsley et.al [11] suggested Email worm which is defined as a malicious code which disseminate through email by containing a copy of itself in the email attachment an email user will be contaminated if he or she opens the worm email attachment. If the attachment is opened by the user, the worm program will contaminate the user's computer and send to the entire email addresses which can be found in the user's computer. There are some of the email worms which attack the email user's vulnerabilities, and thus they can contaminate computers by basically being read by users.

Sajal K. Das et.al [12] consider the common scenario for the network-wide broadcasting of information and focussed on the understanding and modelling of their working process in terms of data propagation speed and reach ability. Particularly, a source node is compromised and it is being utilized along with the communication method of the broadcast protocol to cooperate the remaining nodes by disseminating a piece of malware over the network. Particularly, the contribution is a new framework which is based on the epidemic theory that serves as a general and flexible platform for detaining and distinguishing the spread of malware over dissimilar broadcast protocols, thus assisting a qualified investigation of their potential vulnerabilities. This epidemic model for the data propagation is created according to the local spatial interaction of the nodes in the neighbourhood. The spreading rate is derived for mapping the particular broadcast protocol to this model. Consequently, this rate is used in the epidemic model to examine the dynamics of the malware contamination spread over the particular protocol. Furthermore, the model also facilitates for the study of the impacts of concurrent recovery processes on the infectivity spread affected by the broadcast protocol.

3. VIRUS DETECTION MODEL

In the existing research, a two-layer network model is used for differentiating BT-based and SMS-based viruses, which proliferate via Bluetooth and Short/Multimedia Message Services, correspondingly. In this model, instead of using the contact probabilities in a homogeneous model, the viruses are triggered as a result of human behaviours. There are two categories of the human behaviour: One is operational behaviour and another one is mobile behaviour is considered in the individual- based model. The main objective of this work is to provide how the human behaviours concern the propagation dynamics of mobile viruses. This model considers the user behaviours in the mobile networks. According to this model, the performance of a preimmunization strategy is

investigated which draws the methodology of autonomy-oriented computing (AOC), as reported in preventing in the mobile virus propagation. The impact of the patch distribution delay is computed on the virus propagation and deploys the AOC-based preimmunization strategy into the network at dissimilar times. Additionally, an adaptive dissemination strategy is designed by extending local reactive behaviours of entities. The objectives of this work are as follows:

- By using the two-layer network propagation model, to uncover some key factors in deciding mobile virus dissemination
- The impacts of the operational patterns and mobility patterns are examined in the mobile virus dissemination
- The two methods are investigated for preventing virus dissemination in mobile networks. There are two methods such as preimmunization and adaptive patch distribution strategies drawing on the methodology of AOC

4. HYBRID VIRUS DETECTION METHOD

In the proposed research, to increase the efficiency of the restraining the propagation of hybrid viruses, an 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 model by analysing the mixed behaviours of long-range infectivity pattern from dissemination through messaging service and ripple-based infectivity pattern from propagating through short-range wireless communication. In this work, a new analytical model is proposed for examine the speed and harshness for dissemination the hybrid malware that targets SMS and BT in an efficient manner. This analytical model based on the differential equations works more effectually and it act as a quick reference to collect estimated knowledge of propagation speed and sternness of hybrid malwares with a variety of settings of contagion rates and average node degrees in comprehensive 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 outbreak.

In this section, the measure of the propagation of infections is considered within a population under risk. The communication between a 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 the user's lack of anxiety about the threat of malwares and the inadequate capacity of current antiviral software. The population in this model is nothing but the total number of nodes N in the network which are assumed to be stationary and consistently distributed with node density ρ. Assume that the entire nodes are SMS and BT to assume that all nodes are SMS and BT facilitated to preserve the harmonized mixing property. Denote subpopulation function,

$$I(t) = I_{BT}(t) + I_{SMS}(t)$$

Represents the total number of cooperation handsets at time t, in which $I_{BT}(t)$ and $I_{SMS}(t)$ are those that have been contaminated through BT and SMS at time t, correspondingly. Similarly $S(t)$ represents the set of vulnerable nodes at time t. Obviously, we have,

$$I(t) + S(t) = I_{BT}(t) + I_{SMS}(t) + S(t) = N,$$

and

$$\frac{dI(t)}{dt} = \frac{dI_{BT}(t)}{dt} + \frac{dI_{SMS}(t)}{dt}$$

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

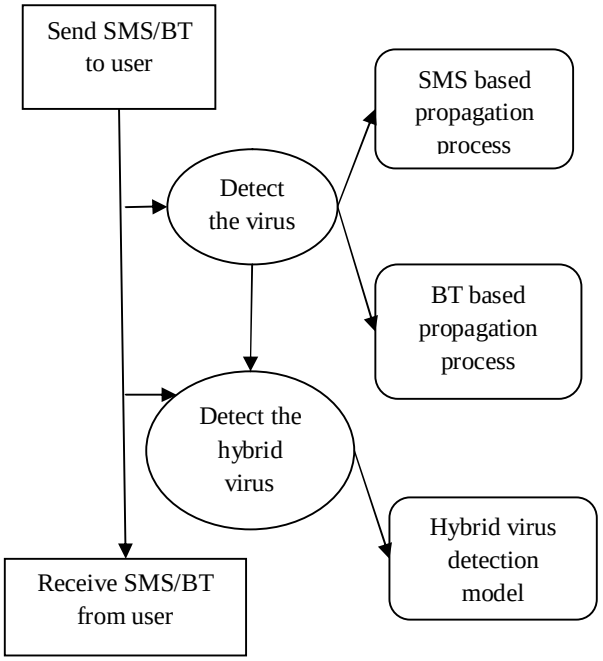

Figure 1 Shows Architecture Diagram

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

5. RESULTS AND DISCUSSION

In this section numerous experiments are explained that are aimed to expose some key factors which impacts the virus propagation. Originally, the two phones are selected arbitrarily from a network as the contaminated phones in order to replicate a multiple-seed attack that is probable to happen in the real world.

Battery Consumption

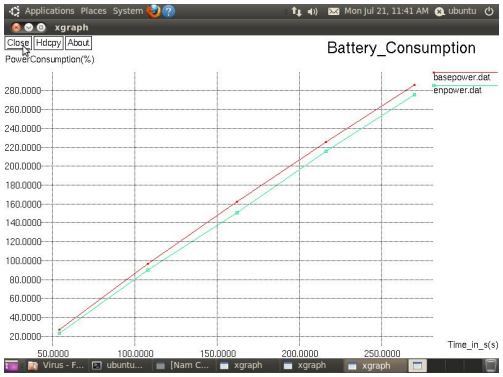

Figure 2 Shows Battery Consumption

Figure.2 shows that the battery consumption. In the existing system, a two-layer network model is presented for simulating virus propagation through both Bluetooth and SMS. In the proposed system, to increase the effectiveness of inhibiting the propagation of mobile phone viruses, a Hybrid virus detection model is proposed. When compared to the existing system, there is less battery consumption in the proposed system.

SMS delivery ratio

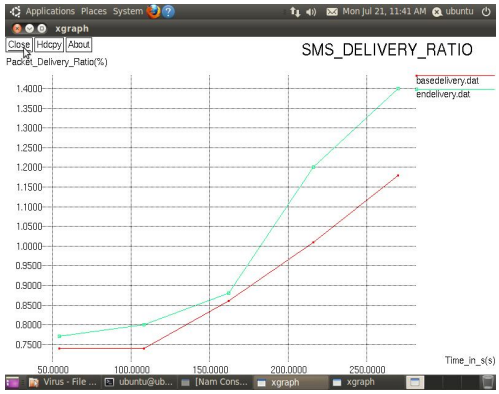

Figure 3 Shows SMS delivery ratio

Figure.3 shows that the SMS delivery ratio. In the existing system, a two-layer network model is presented for simulating virus propagation through both Bluetooth and SMS. In the proposed system, to increase the effectiveness of inhibiting the propagation of mobile phone viruses, a Hybrid virus detection model is proposed. When compared to the existing system, there is high SMS delivery ratio in the proposed system.

Packet delivery ratio

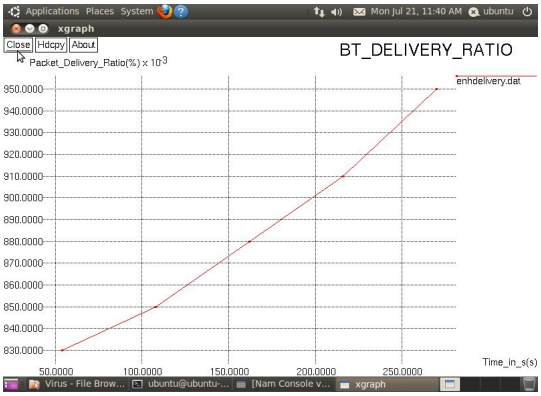

Figure 4 Shows Packet delivery ratio

Figure.4 shows that the Packet delivery ratio. In the existing system, a two-layer network model is presented for simulating virus propagation through both Bluetooth and SMS. In the proposed system, to increase the effectiveness of inhibiting the propagation of mobile phone viruses, a Hybrid virus detection model is proposed. When compared to the existing system, there is high packet delivery ratio in the proposed system.

6. CONCLUSION

A two-layer network model is used for replicating and analysing the propagation dynamics of SMS-based and BT-based viruses to alleviate the viruses and malwares in the mobile networks. This model characterizes two categories of the human behaviours: such as operational behaviour and mobile behaviour for examining and uncovering the propagation mechanisms of mobile viruses. But this work does not consider the hybrid viruses which propagate through both BT and SMS channels. So, the Hybrid virus detection model is proposed to increase the efficiency of the inhibiting the propagation of mobile phone viruses. This method is based on the differential equations works more resourcefully and could act as a speedy reference to collect estimated knowledge of propagation speed and sternness of hybrid malwares with a variety of settings of contagion rates and average node degrees in generalized social networks. For future work, a new method is

proposed for detecting the virus and deleting the virus file.

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, "Quantifying the 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 Model to 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.

[10] Yong Li, Pan Hui, Depeng Jin," An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices," proceedings in IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks

[11] C.C. Zou, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105- 118, Apr.-June 2007.

[12] P. De, Y. Liu, and S.K. Das, "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 8, no. 3, pp. 413-425, Mar. 2009.