International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 316– 318

Quantifying Response Mechanism Effectiveness of Hybrid Virus Propagation through BT and SMS Channel-A Review

Harsha P. Kubade[1]
[1]dept.Computer science and engineering
Agnihotri college of engineering Nagthana,wardha
Wardha, India
harshapkbd@gmail.com

Deepali M. Khatwar[2]
[2]dept.Computer science and engineering
Agnihotri college of engineering Nagthana,wardha
Wardha, India
Deepalikhatwar@gmail.com

***Abstract*—**With rapid development of mobile network, mobile phones are increasingly becoming the target of Malware. It is nothing but a program which is specifically designed to infect the mobile phone it may be a virus or worm or malware. The potential effects of malware propagation on user and mobile phone providers are severe, including identity and information theft, permanently disabling devices and excessive fees to user or loss of revenue for mobile phone providers.so in this paper designing a network topology for propagating hybrid virus through both Bluetooth and SMS channel and Quantify the response mechanism effectiveness of hybrid virus propagation and evaluate countermeasures for restraining hybrid virus propagation with optimizing result.

Keywords-*virus propagation, Bluetooth (BT) and SMS Channel, restraining virus propagation*

*****

I. INTRODUCTION

Many of the users use mobile phone including different application. Virus spread from computer network to mobile network. Mobile phone viruses is self-replicated and spread according to the network topology. In network topology there is two channel responsible for propagating a virus that is Bluetooth and SMS channel. A Bluetooth (BT) based virus is propagated through Bluetooth channel searching for another user mobile phone who's Bluetooth is on within the range of 10m to 30m distance to another user mobile phone. A SMS based virus is propagate through SMS channel by using address phone book of infected phones, or by randomly selecting contacts. Viruses which propagated through both Bluetooth and SMS channel known as Hybrid virus.

A. History of mobile phone virus

The history of mobile phone virus creation & first existence takes us back to June 2004. A group of professional virus writes known as 29A created the first virus for smart phones. This virus is called as 'Carbie'.[3] The Commwarrior virus arrived on the scene in January 2005 and is the first cell-phone virus to effectively spread through an entire company via Bluetooth .It replicates by way of both Bluetooth and MMS. Once you receive and install the virus, it immediately starts looking for other Bluetooth phones in the vicinity to infect. At the same time, the virus sends infected MMS messages to every phone number in your address list. Commwarrior is probably one of the more effective viruses to date because it uses two methods to replicate itself.[4]Mobile virus can cause the loss of important information stored in the mobile like Bank PIN, user logon credentials, infected files of user mobile phone address book and recent call history , can disable your basic mobile phone functions like prohibiting you to use Short Messaging Service, Camera, games etc., can make mobile completely disable , prevents from installing antiviral software, lock your memory card, Use up more phone battery than usual, disturb conversation by remote control, virus can jam wireless services by sending thousands of spam messages and reduce the quality of voice communication. In view of this situation, there is an urgent need for both users and service providers to further understand the propagation mechanisms of mobile viruses and to deploy efficient countermeasures.

In existing paper proposed a two-layer network model for characterizing BT-based and SMS-based viruses. A BT-based virus and SM-based virus which propagate through Bluetooth and Short/Multimedia Message Services, respectively. Viruses are triggered as a result of human behaviors, rather than contact probabilities in a homogeneous model [8]. Two types of human behavior, i.e., operational behavior and mobile behavior (mobility) are considered in our individual- based model. Different from existing work that focuses on the effects of network structures on virus propagation, also to gain further insights into how human behaviors affect the propagation dynamics of mobile viruses. The performance of a preimmunization strategy that draws on the methodology of autonomy-oriented computing (AOC) [8], [5], as reported in [6], in restraining mobile virus propagation.

In this paper designing the network for hybrid virus propagation through both Bluetooth and SMS/MMS. A hybrid virus (multipart or multiparty virus) is one that combines the characteristics of more than one. The Limitations of both Bluetooth and MMS viruses are overcome by Hybrid viruses that can simultaneously use both Bluetooth and MMS connections to spread. Quantify the response mechanism effectiveness of hybrid virus propagation and better immunization strategy on the SAOC (semi autonomy oriented computing) patch dissemination.

II. LITERATURE REVIEW

A Two-layer network model for characterizing BT-based and SMS-based viruses, which propagate through Bluetooth and Short/Multimedia Message Services, respectively, in order to address the above mentioned shortcomings. In our proposed model, viruses are triggered as a result of human behaviors, rather than contact probabilities in a homogeneous model [8]. Two types of human behavior, i.e., operational behavior and mobile behavior (mobility), are

considered in our individual- based model. Different from existing work that focuses on the effects of network structures on virus propagation; our work is aimed to gain further insight into how human behaviors affect the propagation dynamics of mobile viruses. The two strategies for restraining virus propagation in mobile networks, i.e., preimmunization and adaptive patch dissemination strategies drawing on the methodology of AOC.[1]

To study the spreading patterns of mobile phone viruses. Observe the mobility of mobile phone users on account of a mobile phone virus outbreak to figure out the spreading patterns. Understand the different types of mobile phone viruses available which are potential threats to mobile phone users.[2]

The spreading of a potential Bluetooth and MMS virus are described in the Supporting Online Material (SOM). the spread of an MMS and Bluetooth infection starting from the same user, illustrating that Bluetooth and MMS viruses differ in their spatial spreading patterns as well: a Bluetooth virus follows a wave like pattern, infecting predominantly users in the vicinity of the virus's release point, while an MMS virus follows a more delocalized pattern, given that the users' address book often contains phone numbers of faraway individuals. To quantify the observed differences we measured the average distance between the cell phone tower where the first infected user is located and the location of towers servicing the newly infected users. While the most significant danger is posed by hybrid viruses that take advantage of both Bluetooth and MMS protocols, find that their spread is also limited by the phase transition: hybrid viruses. the understanding of the basic spreading patterns presented here could help estimate the realistic risks carried by mobile viruses and aid the development of proper measures to avoid the costly impact of future outbreaks.[3]

Design a system for AOC tackles a computing problem by defining and deploying a system of local autonomy-oriented entities. The entities spontaneously interact with their environments and operate based on their behavioral rules. They self-organize their structural relationships as well as behavioral dynamics, with respect to some specific forms of interactions and control settings. Such a capability is referred to, The goal of is to outline the key concepts in the design and development of an AOC system, and in addition, discuss the distinct roles and characteristics of self-organization in the performance of the AOC system.[5]

''equal graph partitioning (EGP)'' immunization strategy which we find to be significantly better than targeted methods, with 5% to 50% fewer immunization doses required (on the networks studied here).They used method is based on the heuristic optimal partitioning of graphs and is motivated. The main idea of the EGP is to fragment the network into many connected sub networks (clusters) of approximately *equal* size. This strategy leads to the need to immunize fewer nodes compared to the targeted strategies. This is since in targeted strategies a broad distribution of cluster sizes appears after fragmentation, including many very small clusters. Hence, one wastes many immunization doses to isolate these small clusters, which is unnecessary in the EGP method. Author confirm the improved efficiency of our approach on ER and SF networks, random regular graphs, and on several real networks.[7]

An efficient representation of malware behaviors based on a key observation that the logical ordering of an application's actions over time often reveals the malicious intent even when each action alone may appear harmless. Then, generate a database of malicious behavior signatures by studying more than 25 distinct families of mobile viruses and worms targeting the Symbian OS—the most widely-deployed handset OS—and their variants. Next, propose a two-stage mapping technique that constructs these signatures at run-time from the monitored system events and API calls in Symbian OS. Author discriminate the malicious behavior of malware from the normal behavior of applications by training a classifier based on Support Vector Machines (SVMs). And evaluation on both simulated and real-world malware samples indicates that behavioral detection can identify current mobile viruses and worms with more than 96% accuracy. Also find that the time and resource overheads of constructing the behavior signatures from low-level API calls are acceptably low for their deployment in mobile devices.[9]

III. PROPOSE METHODOLOGY

A. *System Architecture*

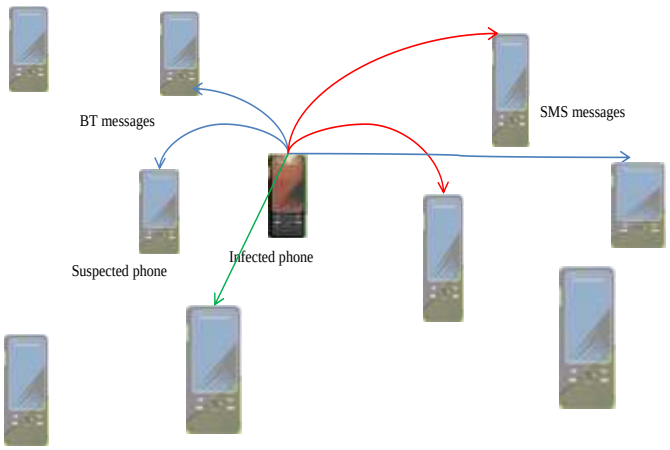

Figure.1 A Bluetooth virus can infect all phones found within Bluetooth range from the infected phone, its spread being determined by the owner's mobility patterns. An SMS/MMS virus can infect all susceptible phones whose number is found in the infected phone's phonebook, resulting in a long-range spreading pattern that is independent of the infected phone's physical location, Hybrid virus propagation through BT and SMS.

BT based Viruses
SMS based Virus
Hybrid Virus

1) *Hybrid Virus Module*

a) SMS Virus model: Each phone sub model is initialized and assigned a unique identification number, and each phone is given a contact list containing the identification numbers of some randomly selected phones. After the identification numbers have been assigned and the contact lists have been generated, the initialization sub model injects the initial virus infection into one randomly selected phone.

b) BT Virus Model: The initialization procedure for the Bluetooth virus model is similar. As with the MMS model, each phone sub model is initialized and assigned a unique identification number. In addition, each phone is randomly assigned to a location within a rectangular region called the

Bluetooth simulation arena. Since only phones in close geographic proximity can communicate via Bluetooth, the location of the phones in the arena determines which phones can and cannot communicate. After identification numbers and locations have been assigned, the initialization sub model injects the initial virus infection into one randomly selected phone.

2) Hybrid virus response effects module:

a) At the point of reception

Virus scan: SMS message passes through the SMS Gateway the SMS attachment for known virus signatures. Attachments identified as infected are prevented from reaching their intended recipients.

Virus detection algorithm: The virus detection algorithm approach is more universal and can detect previously unidentified viruses. The algorithm identifies infected MMS messages by looking for suspicious traits characteristic of a virus. When a virus is first detected, the virus detection algorithm in the MMS gateway analyzes the infected messages to determine the best way to recognize the presence of this virus in subsequent MMS messages.

Block sender option: The first Bluetooth response mechanism provides phone users with the option to manually block other phones from making repeated Bluetooth connection attempts.

Mobile Phone user Knowledge BT and SMS: Mobile phone user behavior on the basis of education of mobile phone.

b) At the point of infection

Immunization using software patches based on SAOC Strategy: Distributing patches on mobile network for immunization.

Mobile phone user Knowledge on file installation risk: Mobile phone user behavior on the basis of education of mobile phone

c) At the point of dissemination

Monitoring for anomalous behavior: When these measures exceed some specified threshold, then the phone is forced to rate-limit the number of outgoing Bluetooth connection attempts. This is intended to slow the spread of potential viruses but still allow communication to continue, albeit at a much slower rate, in case the phone has been falsely suspected of infection.

Blacklisting phones suspected of infection: The Bluetooth blacklisting response mechanism depends on phones to self-monitor their outgoing messages for suspicious behavior and, when appropriate, to self-impose a "blacklist" status that prevents further outgoing Bluetooth connection attempts. This self-monitoring is performed by anti-virus software installed on the phone.

B. Objectives of the proposed system

To propagate hybrid virus through both BT and SMS channel, understanding the patterns of mobile phone viruses at the point of reception, infection and dissemination to protect a mobile phone from virus and also to improve response effects of viruses with more accuracy and increase a time delay.

IV. CONCLUSION

In this paper it can effectively restrain the virus propagation. To increase the effectiveness of the reducing the propagation of mobile phone viruses by increasing time delay, work proposes a novel analytical model to efficiently analyze the accuracy for spreading the hybrid malware that targets multimedia messaging service(MMS)/(SMS) and BT.

V. FUTURE SCOPE

In next step, extend model to incorporate additional characteristics of human mobility and operations. In particular future computational model will consider the dynamic changes of users' behaviors in the course of mobile virus propagation.

VI. REFERENCES

[1] Chao Gao and Jiming Liu, Fellow, "Modeling and Restraining Mobile Virus Propagation" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 3, MARCH 2013.

[2] Sundararaman Natarajakumar, "Understanding the spreading patterns of mobile phone viruses" Hochschule Furtwangen University,2012

[3] Pu Wang ,Marta C. Gonzalez, Ronaldo Menezes, Albert-Laszlo Barabasi, "Understanding the Spread of Malicious Mobile-phone Programs and their Damage Potential"

[4] Athulya heera ben .k.raghu, "Cell phone virus and security", cochin university of science & technology, kochi,2008

[5] J. Liu, "Autonomy-Oriented Computing (AOC): The Nature and Implications of a Paradigm for Self-Organized Computing," Proc.Fourth Int'l Conf. Natural Computation (ICNC '08), pp. 3-11, 2008.

[6] C. Gao, J. Liu, and N. Zhong, "Network Immunization with Distributed Autonomy-Oriented Entities", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1222-1229, July 2011.

[7] D. Brockmann, L. Hufnagel, and T. Geisel, Nature, "The better immunization for patch dissemination," vol. 439, no. 7075, pp. 462-465, 2006.

[8] 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.

[9] A. Bose, X. Hu, K.G. Shin, and T. Park, "Behavioral Detection of Malware on Mobile Handsets," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 225-238, 2008.

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

[11] 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.

[12] C. Gao and J. Liu, "Modeling and Restraining Mobile Virus Propagation (Supplementary File)," IEEE Trans. Mobile Computing,2013.

[13] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling Time-Variant User Mobility in Wireless Mobile Networks," Proc.IEEE INFOCOM, pp. 758-766, 2007.

[14] C. Gao and J. Liu, "Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior," Proc. IEEE12th Int'l Symp. a World of Wireless, Mobile and Multimedia Networks
(WoWMoM '11), pp. 1-9, 2011.

[15] Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott,"Impact of Human Mobility on the Design of Opportunistic *Forwarding Algorithms," Proc. IEEE INFOCOM, pp. 606-620, 2006*..