Effective Response of BT and SMS Hybrid Virus Propagation and Prevention in MANET

Harsha Kubade, Deepali Khatwar, Dhananjay Sable

Abstract— **A rapidly increasing 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, disturbed voice communication, Denial-of-Service (DoS) attacks and excessive fees to user or loss of revenue for mobile phone providers.so it is important for us to gain a knowledge about virus, cause of virus propagation of virus and its prevention. In this paper we are quantifying response mechanism effectiveness of hybrid virus prevention and propagation through Bluetooth and SMS channel in terms of Increasing accuracy, throughput, packet delivery rate and reducing delay, traffic congestion in network.**

Index Terms— **virus propagation, Bluetooth (BT) and SMS Channel, restraining virus propagation**

I. Introduction

Traditional mobile phone devices had lesser threat for mobile phone viruses because they were designed not to share data, programs or information. It was almost impossible to intrude into another mobile phone. The advent of Smart phones in the market brought in new complications because it was built on a operating system and the information age we live in requires transfer of information from mobile phone in all forms like Bluetooth, Multimedia Messaging Service(MMS), Email, Wi-Fi. Smart phone available in market comes with higher computing power and uses extended memory storage cards. The virus can spread through even memory cards, or using any of the data transfer services mentioned. Thus, trends clearly show us that it opens up new horizons to malicious users and the potential threats are self evident.[1]The enhanced computational and communication capabilities of smartphones are beginning to attract viruses targeted at these increasingly sophisticated mobile phones .Attacks from mobile phone viruses can compromise personal information, delete data, drain the battery, and steal phone services by using expensive features. The impact of mobile phone viruses on phone service providers includes increased customer complaints concerning infected phones and extra network congestion due to the virus-related traffic. It is imperative that the mobile phone industry anticipate and act now against these looming threats to dependable and secure mobile phone services. Because mobile phones are communications devices with many connectivity options, there exist many possible infection vectors . Mobile phones can become infected by downloading infected files using the phone Internet browser, by transferring files between phones using the Bluetooth interface, by synchronizing with an infected computer, by accessing an infected physical memory card, or by opening infected files attached to multimedia messaging service (MMS) messages. MMS messages are similar to text messages between mobile phones, but MMS messages are capable of including attached files, much like email with attached files. The most threatening propagation vectors permit rapid and widespread virus penetration throughout a network of phones. Based on this criterion, one of the most significant threats is propagation by MMS message attachments . Another significant threat is virus propagation by the transfer of infected files between phones using the Bluetooth interface. [2]

Viruses that use SMS as a communication media can send copies of themselves to all phones that are recorded in victim’s address book. Virus can be spread by means of forwarding photos, videos, and short text messages, etc. For propagation, a long range spreading pattern is followed which is analogous to the spreading of computer viruses like worm propagation in e-mail networks[3].Viruses that use Bluetooth as a communication channel are local-contact driven viruses since they infect other phones within its short radio range. BT-based virus infects individuals that are homogeneous to sender, and each of them has an equal probability of contact with others[4]A Virus that propagate through BT channel and SMS channel known as hybrid virus because it uses both channel for propagation. Hybrid virus (sometimes called a *multi-part* or *multipartite* virus) is one that combines characteristics of more than one type.

II. LITERATURE REVIEW

In this paper, Author propose 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 this proposed model, viruses are triggered as a result of human behaviors, rather than contact probabilities in a homogeneous model. 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

***Manuscript received Jul, 2015**.*

Harsha Kubade, *Computer Science and Engineering, RTM NagpurUniversity, Wardha,India , 9561315152*

Deepali Khatwar*, Computer Science and Engineering, RTM Nagpur University, Wardha,India , 7387162308*

***Dhananjay Sable** ,Computer Science and Engineering, RTM Nagpur University, Wardha, India,*

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.[5]

Quick and efficient security patch dissemination strategy is necessary for the update of antivirus software so that it can detect mobile virus, especially the new virus under the wireless mobile network environment with limited bandwidth which is also large scale, decentralized, dynamically evolving, and of unknown network topology. In this paper, author proposed an efficient semi autonomy-oriented computing (SAOC) based patch dissemination strategy to restrain the mobile virus. In this strategy, some entities are deployed in a mobile network to search for mobile devices according to some specific rules and with the assistance of a center. Through experiments involving both real-world networks and dynamically evolving networks, we demonstrate that the proposed strategy can effectively send security patches to as many mobile devices as possible at a considerable speed and lower cost in the mobile network. It is a reasonable, effective, and secure method to reduce the damages mobile viruses may cause[6].

In this paper an attempt has been made to compare the performance of three prominent on demand reactive routing protocols for MANETs:- Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) protocols and Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) . DSR and AODV are reactive gateway discovery algorithms where a mobile device of MANET connects by gateway only when it is needed. AOMDV was designed primarily for highly dynamic ad hoc networks where link failures and route breaks occur frequently. It maintains routes for destinations in active communication and uses sequence numbers to determine the freshness of routing information to prevent routing loops. It is a timer-based protocol and provides a way for mobile nodes to respond to link breaks and topology changes. The performance differentials are analyzed using varying simulation time. These simulations are carried out using the ns-2 network simulator. The results presented in this work illustrate the importance in carefully evaluating and implementing routing protocols in an ad hoc environment[7].

In this paper present a new way to assess and restrain virus propagation by proposing the concepts of two-layer network model for simulating virus propagation through both Bluetooth and SMS. An efficient autonomy-oriented computing (AOC) based patch dissemination strategy to restrain the mobile virus. In this strategy, some entities are deployed in a mobile network to search for mobile devices according to some specific rules and with the assistance of a center. Mobile networks, formed by the connection of mobile devices following some relationships among mobile users, provide good platforms for mobile virus spread. Quick and efficient security patch dissemination strategy is necessary for the update of antivirus software so that it can detect mobile virus, especially the new virus under the wireless mobile network environment with limited bandwidth which is also large scale, decentralized, dynamically evolving, and of unknown network topology. Simulation results provide further insights into the determining factors of virus propagation in mobile networks[8].

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, we 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[9].

III. PROPOSED METHODOLOGY

A. *SMS Virus Process*

If a phone is infected with SMS based virus, the virus regularly sends its copies to other phones whose contact number is found on the address book of the infected phone. After receiving such distrustful message from others, user may open or delete it as per his alertness. If user opens the message, he is infected. But, if a phone is immunized with antivirus, it will not send out viruses even if user opens an infected message. Therefore, the security awareness of mobile users plays a key role in SMS-based virus propagation. Same process is applicable for MMS-based virus propagation whereas MMS carries sophisticated payload than that of SMS. It can carry videos, audios in addition to the simple text & picture payload of SMS.

B. *BT Virus Process*

Unlike SMS based viruses, if a phone is infected by a BT-based virus, it spontaneously & atomically searches another phone through available Bluetooth services. Within a range of sender mobile device, a BT-based virus is replicated. For that reason, users' mobility patterns and contact frequency among mobile phones play crucial roles in BT-based virus propagation. Same process is followed for Wi-Fi where Wi-Fi is able to carry high payload in large range than that of BT.

C. *SAOC Patch Dissemination Strategy*

The advantages of SAOC-based strategy could be described as follows: (1)it sends security patches to as many phones as possible at a considerable speed and lower cost in the mobile network with limited bandwidth which is also large scale, decentralized, dynamically evolving, and of unknown network topology; (2) it can control the number of patches disseminated at each time step and make adjustment according to the network conditions. Thus the network congestion can be avoided; (3) the selected phones which receive the patches are always the most important ones of the phones found by the entities at each time step for the virus propagation, and thus the virus propagation can be effectively restrained;(4) each phone receives the patch only once, which is beneficial to avoiding the network congestion and the waste of network resource. The SAOC-based patch dissemination strategy is a reasonable, effective, and secure method to send security patches in mobile networks and reduce the damages mobile viruses cause.[6]

IV. SIMULATION RESULTS

A. Simulation Tool Setup

Channel type	Wireless Channel
MAC type	Mac/802_11
Number of mobile nodes	30
Define Routing protocol	AOMDV
Simulation area	300x300

Table.1 Network Scenario

B. Simulation Result

In this fig3shows that red color graph due to the virus attack in manet data sending speed get decreases and delay is increases but green graph indicates after removing virus attack from manet data sending speed get increases and delay is decreases. In this fig4 shows that red color graph due to the virus attack in manet data sending speed get decreases delay is increases energy decreases but green graph indicates after removing virus attack from manet energy increases. In this fig5shows that red color graph due to the virus attack in Manet less amount of data transfer from one node to another node in specific amount of time but green graph indicates after removing virus attack from Manet more amount of data transfer from one node to another n ode in specific amount of time. In fig6 shows that red color graph due to the virus attack in manet data sending speed get decreases and delay is increases that's why jitter is increases but green graph indicates after removing virus attack from manet data sending speed get increases, delay is decreases and jitter is decreases. In fig7 shows that red color graph due to the virus attack in manet data sending speed get decreases packet delivery rate decreases but green graph indicates after removing virus attack from manet packet delivery rate increases.

V. CONCLUSION AND FUTURE WORK

In this project effectively restrain the virus propagation. The optimized result after removing the mobile phone viruses propagation by decreasing 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.Quantifying response of hybrid virus propagation in mobile network through SMS and BT channel in terms of Increasing accuracy, throughput, packet delivery rate and reducing delay, jitter, traffic congestion in network.

In future work, extend model to incorporate 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. Some assumptions about human mobility and operational patterns in this paper have been based on some empirical studies and statistical data.

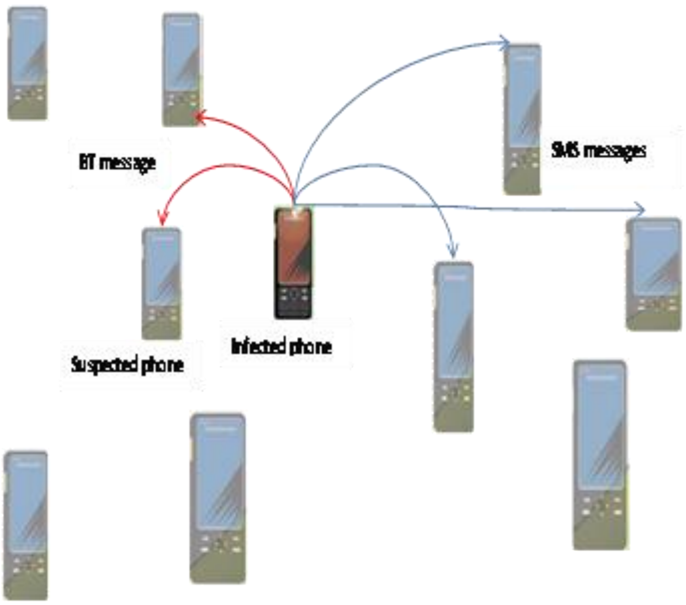

Fig.1 Virus propagation through BT and SMS Channel

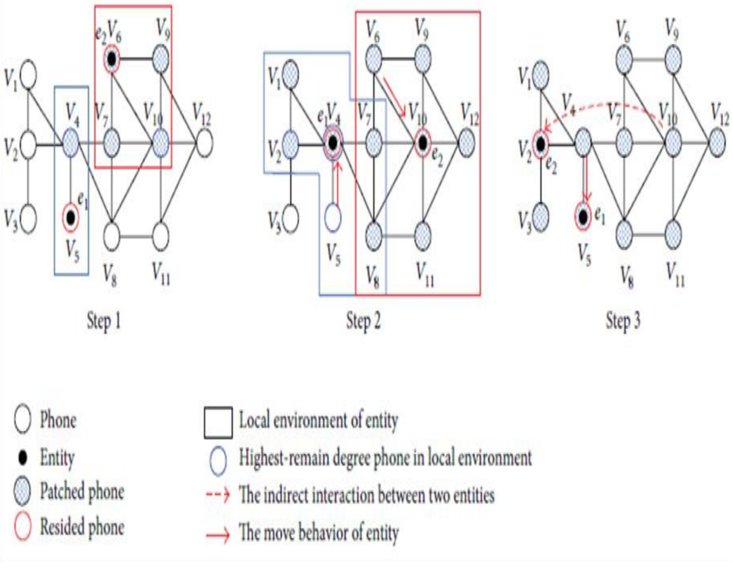

Fig2 An Example of SAOC Patch Dissemination Strategy.

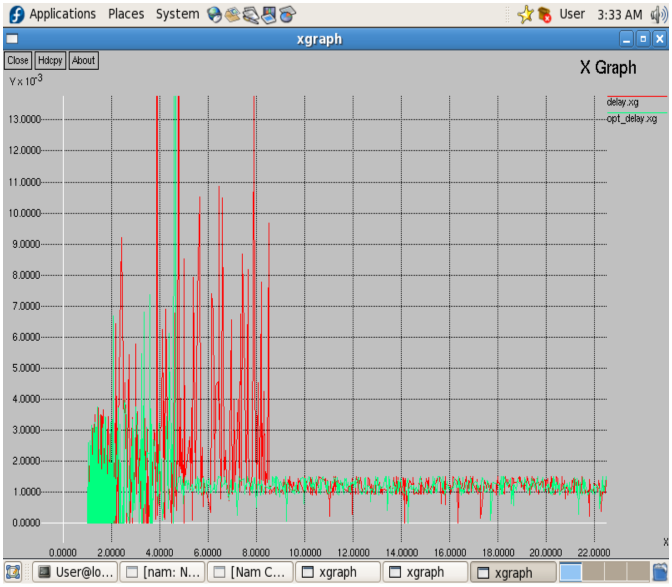

Fig.3 Snapshot of optimized delay graph

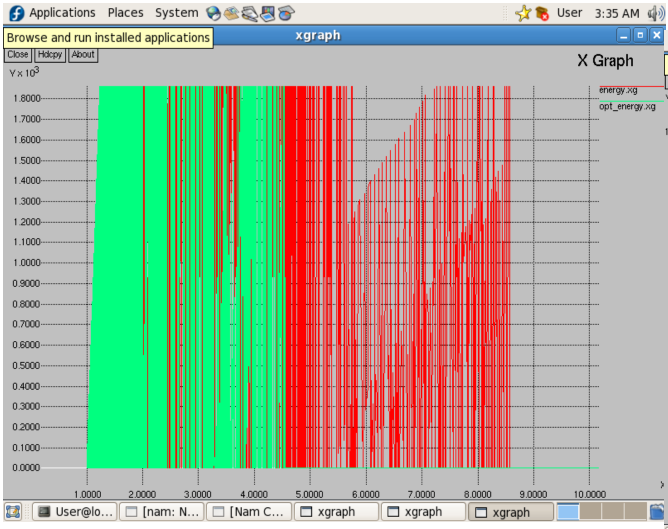

Fig.4snapshot of optimized energy graph

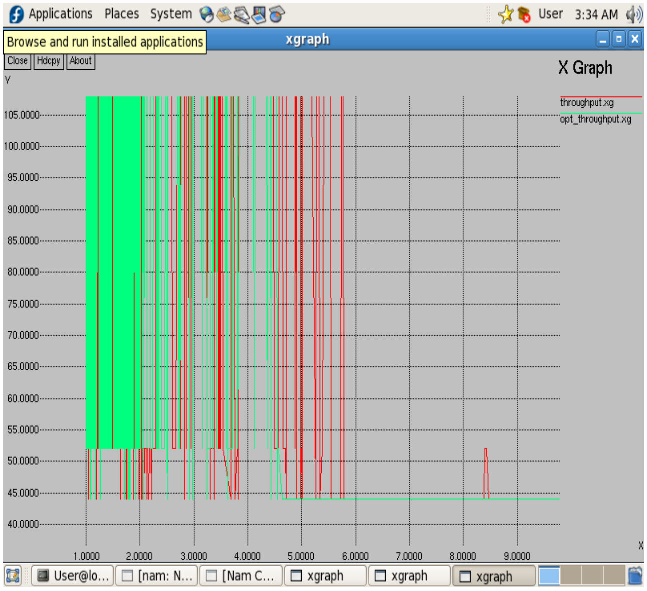

Fig.5Snapshot of optimized throughput

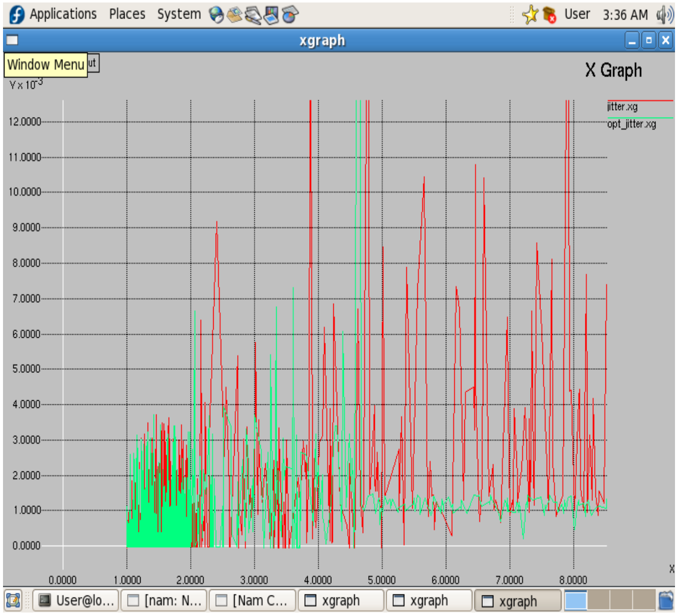

Fig.6 Snapshot of optimized Jitter

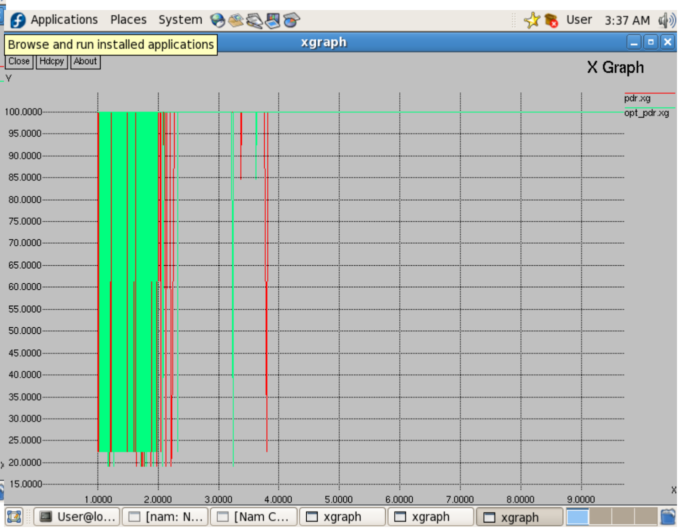

Fig.7Snapshot of Optimized PDR

REFERENCES

[1] "Understanding the spreading patterns of mobile phone viruses" by PuWang, Marta C. González1, César A. Hidalgo&Albert-LászlóBarabási.ses"HochschuleFurtwangen University,2012.

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

[3] C. Gao, j. Liu, and N. Zhong, "Network immunization and virus propagation in Email networks: experimental evaluation and analysis," Knowledge and information systems, vol. 27, no. 2, pp. 253-279, 2011.6

[4] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of Bluetooth worms (extended version)," IEEE transactions on Mobile Computing, Vol. 8, No. 3, pp. 353-368, March 2009.7

[5] "Modeling and Restraining Mobile Virus Propagation" by Chao Gao and Jiming Liu, Fellow, IEEE

[6] "An Efficient Patch Dissemination Strategy for Mobile Networks" by Dawei Zhao, HaipengPeng, Lixiang Li, Yixian Yang, and Shudong Li

[7] "Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs" by Manveen Singh Chadha, RambirJoon, Sandeep

[8] "Modeling and Automatic Detection 0f Virus in Mobile Environment" by Lakshmi.D, Thamizharasi.H, Prakash.R, Divyalakshmi.

[9] SundararamanNatarajakumar, "Understanding the spreading patterns of mobile phone virus.

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

Harsha Kubade , Computer Science & Engineering,Agnihotri College of Engineering Nagthana,Wardha,RTM,Nagpur University.
Deepali Khatwar Computer Science & Engineering,Agnihotri College of Engineering Nagthana,Wardha,RTM,Nagpur University.
Dhananjay Sable Computer Science & Engineering,Agnihotri College of Engineering Nagthana,Wardha,RTM,Nagpur University.