Survey on Modeling and Forbidding Cellular Virus Proliferation

Pavithra G N[1] Neelam Malyadri[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]HKBK college of Engineering, Bangalore

Abstract— Viruses and malwares can unfold from pc networks into mobile networks with the speedy increase of clever cell phone users. In a cellular community, viruses and malwares can reason privacy records leakage, extra charges etc.. Furthermore they are able to jam wireless servers by using sending lots of spam messages or tracking end user positions via GPS. Because of the capability damages of cellular viruses, it's miles essential for us to benefit a deep know-how of the propagation mechanisms of cell viruses. A two-layer network model has proposed for simulating virus propagation through both Bluetooth and SMS. Distinct from previous work, our work addresses the effects of human behaviors, i.e., operational behavior and cellular behavior, on virus proliferation. This simulation outcomes provide in addition insights into the determining elements of virus propagation in mobile networks. Moreover, we observe two techniques for forbidding cell virus propagation, i.e., preimmunization and adaptive dissemination strategies drawing at the technique of autonomy-orientated computing (AOC). The experimental outcomes display that our techniques can correctly guard massive-scale and/or rather dynamic cellular networks.

Key words: Autonomy-oriented computing, cellular networks, Preimmunization, Patch distribution

I. INTRODUCTION

According to many research it has been reported that mobile phones are getting damaged due to the viruses and also the malwares which are found in the smart phones. There are many examples where these viruses are affected these smart phones which caused a huge loss. One such example is"Zombie", where this virus damaged a million smart phones in china in the year 2010 where it created huge loss of $300,000 per day.

Nowadays smart phones has been increased world wide rapidly.These phones are used for various purpose such as performing several tasks in online i.e usage of mobile banking, browsing, sharing documents etc. Smart phones are also infected by sharing of documents using Bluetooth. Usage of smart phones in people daily life it has become an advantage to the malwares writers where these goal is to steal users private information. It has emerged as a huge threat for for users of smart phones where virus are reason for the jam in the wireless services, this is done by sending numerous of spam messages where to decrease the quality of the communication. A user sometimes encounters with many spam messages which this worm causes the quick exhaust in the phone battery and some of the virus may corrupt the hardware.

In this paper the survey on two layer network model is done. This model basically deals with depiction viruses which are based on Bluetooth and also SMS. This model is respectively on the human behavior instead of the probabilities of being in contact in the module which is homogeneous. Human behavior is categorized in to two different types such as operational behavior and the other is mobile behavior.

This work mainly deals with the behavior of human where it mainly concentrate on the propagation of viruses and detection and deletion of the malwares is done early before entering in to the smart phones which is basically on the AOC methodology.

There are different methods which have been proposed to control the propagation of mobile virus based on the technologies which is existed. Despite the fact that there is technology of anomaly detection. This technology works based on the system calls also API's can detect only the malware or viruses which has already been present i.e it has a limitation that it cannot detect the present day viruses. So, it is necessary for a user to update their detection technology databases or security providers. In order to calculate the notification to smart phones or patches to smart phones. It is unrealistic that the users security services to their smart phones for their limitations such as bandwidth and also time.

Strategies adopted to spread the notification such as one is based on phones which are connected in short range for communication and this is affected based on the pattern of human mobility. It is tough to obtain the signature files based on time manner. Some technologies which has been adapted to spread patches is difficult when it is for large scale and also network which is dynamic so, it is necessary for us to propose the strategies which are more efficient enough to spread patches to multiple smart phones.

II. LITERATURE SURVEY

According to survey there are many defense technologies for to restrain mobile viruses. There are many types of viruses which affect smart phone. In 2004 a group created virus which was self replicating but this did not affect phones but these days there are lot more different viruses existed.

Some viruses would cause a serious damage to the smart phones when compared to the viruses which are found in the internet. These viruses would contain some susceptible codes which would cause the damage to the smart phones which also cause economic loses.

There are various categories in viruses which affects the smart phones. These categories mainly depends on their targets i.e it might be on call center or cellular base station etc. the main 2 categories in mobile viruses which are based on Bluetooth and SMS.

Bluetooth based viruses are contact driven virus i.e locally contact driven which is harmfull for the phones which has local contact with the other phone with in its radio range, which is similar to the diseases which is spreaded based on contact for example H1N1.

The pattern which is followed by Bluetooth based virus is spatially localized spreading pattern. Epidemic modeling is used commonly to study such viruses where the assumption in this is that each of which consideres itself as homogeneous in the huge population of host's and where which has equal probability to contact with the other phones.

Wang et al worked on the Bluetooth based virus propagation model which is based on human mobility which was from data traces which are in real world and it was basically on extracting and then predicting .

Viruses which are based on SMS sends its copy by itself to all the phones which are there in the contact through which sending videos or images or messages etc. These pattern of spreading viruses is long range which is as similar as the viruses which are spreading through email.

As soon as a user receives the suspicious message the user would have options such as to open the message or to delete the message so user behavior would play very important role based on user operational behavior i.e whether the user opens or delete the suspicious message.

III. EXISTING DEFENSE STRATEGIES

There are many models to avoid the viruses which are based on SMS. There are two approaches to avoid these viruses which affect the phones. One is to improve the users awareness on security and I.e comparing on the risks which are caused by these viruses and the other approach is providing pop up messages which are warnings which the user installs new files or when user opens new files, but it does not considers the topology of network which is based on propagation of virus.

Zhu et al proposed a defense strategy which is based on selecting immunized phones and it is based on the clustered graph portioning and balanced graph partitioning.

Kim et al proposed a model where the detection is based on monitoring the lifetime of the battery from this it is find the threats of energy depletion

A. Disadvantages of existing system

The defense strategies which are used in the existing system would help to detect the malwares but it is difficult to detect and to avoid the new malwares and most of the time this fails to protect the phones from the various because these strategies or technologies which is used to detect the mobile viruses should be trained to detect the mobile viruses should be trained to detect behaviors whether it may be normal or abnormal i.e if a virus produces different patterns which are unknown to the existing model detection technology it is unable to detect such virus.

It is a challenge to detect such malwares which affects phone as it is difficult to send the patch messages to all the phones simultaneously due to constraints such as bandwidth. To avoid redundancy of communication some of the technologies user Bluetooth to send the patch messages to phones but this method fails to reach the users in the stipulated time.

Another approach which is used to send patches is by using central server, where the patches would be sent directly from central server to phones.

IV. PROPOSED SYSTEM

The following method which is used for stimulating viruses in mobile is network model which is two layered. This model basically has two layers where as shown in the figure1. The cell tower network which is geographically base is represented in the lower layer. In this layer the viruses which are based on Bluetooth is spreaded.

The upper layer network is logical based where the viruses propagation here is based on SMS which is constructed from address books which is saved in phone. Geographical network is represented in 2 dimensional grid where it is represented as G[N][N]. Here N is represented for size of grid and each lattice is considered as one service area.

The user may move from one lattice to another within the geographical network. The signals which are provided by towers. As the user moves the signals can be provided by same tower or other.

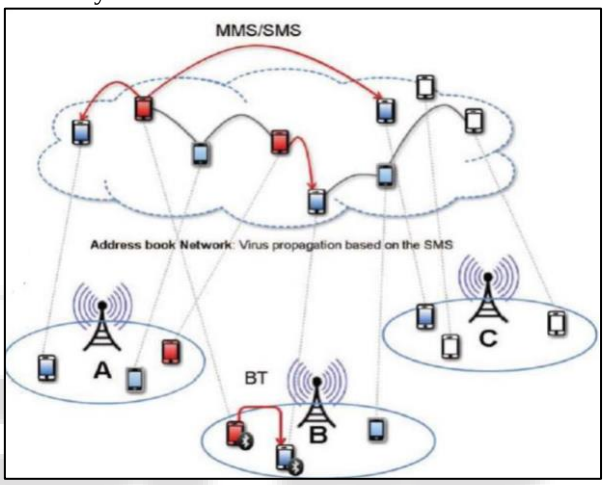

Fig. 1: Network model

A. Propagation based on SMS

The network is based on address books/contacts which are in the user smart phone. If the users phone is infected then the copies of there virus would be sent to the contact is the phone through SMS.

When the receiver gets these infected SMS the user would get 2 options one is to open and other is to delete. The probability of user opening such messages depends on the awareness regarding securing phone from viruses.If the phone is immunized then the virus cannot infect the phone though user opens the message

Steps

Propagation based on SMS

1) Step 1: if users phone is in power on state
2) Step 2: The status of the phone is dangerous and click the user to open or delete the message is random
3) Step 3: if user click to open the SMS then phone is infected
4) Step 4: If user click on delete the virus cannot infect the user phone

B. Proliferation based on Bluetooth

If a user phone is already infected from virus by a Bluetooth these phones automatically searches for other phones which

are within Bluetooth range then the replication of virus to the phones is done.

C. Strategies against mobile viruses

Viruses based on Bluetooth can be avoided by switching off the user Bluetooth service. Viruses which are infects through SMS are considered as most dangerous when compared to Bluetooth so to restrain from this virus we describe 2 methods.

D. Prior minimizing strategy

The common method which is adopted to avoid propagation of viruses is minimizing the network by immunizing some set of nodes in prior based on some defined rules.

These nodes which are immunized are selected to protect from viruses. One of the strategy is to divide a mobile network and these divided network is called clusters. The main disadvantage of this strategy is that it is very difficult to deal with the network which is large- scale or with decentralized network or with dynamic network.

E. Patch Distribution Strategy

In this strategy the immunization of phones is based on AOC . in this method it would select phones where the capability of transmission is larger for patching. Security patches are different for different companies. Patches are sent to the phones.

Due to constraints such as bandwidth the notification of security cannot be sent simultaneously to all the users therefore adaptive documentation strategy is used to send the notification of security.

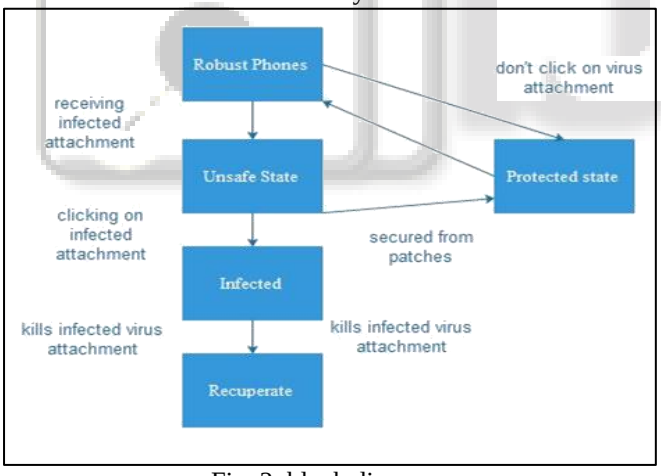

Fig. 2: block diagram

If a phone is not infected then it is robust phone and if it all it receives the virus attached file then it would be in unsafe state. As when the user receiver this infected attachment if a user opens the message then the phone gets infected and if the strategies used to kill viruses then the phone is received from prior security strategy then it would be in protected state.

V. CONCLUSION

In this paper, survey regarding is on strategies which are used to restrain the virus propagation through mobile is done which is propagated through Bluetooth and SMS. The strategies such as prior immunization and path message are illustrated to avoid the phones which are getting infected.

Future work will be on to deal with the survey on the viruses which are hybrid which are transmitted through Bluetooth and also SMS.

REFERENCES

[1] P. Wang, M.C Gonzalez etal "understanding the spreading patterns of mobile phone viruses,"science,vol 324,2009
[2] B.Lin, M.-H. Shih etal "security Aspects of Mobile Phone Virus/; A critical Survey," Industrial Management and data System, 2008
[3] S. Cheng, W.C. Ao, P.Chenand K. Chen, "On Modeling Malware Propagation in Generalized Social Networks," IEEE Comm.Letters, 2011
[4] Z. Zhu, G. Cao, S. Zhu etal, "A Social Network Based Patching Scheme for Worm Containment in Cellular Networks," Proc. IEEE INFOCOM, 2009
[5] A. Mei and J. Stefa,"SWIM: A Simple Model to Generate Small Mobile Worlds," Proc IEEE INFOCOM, 2009
[6] C.Song,P.Wang etal " Modeling the Scaling Properties of Human Mobility," Nature Physics,2010
[7] A. Gao, J.Liu, "Network Immunization and Virus Propagation in Email Networks : Experimental Evaluation and Analysids," Knowledge and Information Systems, 2011
[8] Chao Gao and Jiming Liu, Fellow," Modelling and Restraining Mobile virus Propagation", IEEE 2013
[9] S. Bansal, J. Read etal , " The Dynamic Nature of Copntact Networks in Infectious Disease Epidemilogy," j. Biological Dynamics. 2010
[10] P. Holme, B.J kim," Attack Vulnerability of Complex Networks." Physical Rev 2002

