ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 6; Page No. 92-95

Systematic Approach for Modeling and Restraining Mobile Virus Propagation

Harshada S. Palve[1], Vrunda K. Bhusari[2]

[1]JSPM's Bhivarabai Sawant Institute of Technology and Research, Wagholi Pune 412 207, India

palve.harshada@gmail.com

[2]JSPM's Bhivarabai Sawant Institute of Technology and Research, Wagholi Pune 412 207, India

vrundabhusari82@gmail.com

ABSTRACT:
Rapid growth in computer networks and mobile networks causes the spread of viruses and malwares from one mobile network to another mobile network. This malware causes the damage in smart phones and many other issues like privacy data leakage, extra charges and. "Zombie" viruses attacked more than 1million cell phones and create huge loss .In some serious situations viruses can even jam wireless services by sending out thousands of spam messages. In this situation it is necessary for both users and service providers to understand the propagation mechanisms of mobile viruses. Here we use two-layer network model, for modeling virus propagation which characterizing Bluetooth based and SMS –based viruses. Two types of human behaviors are considered i.e. operational behavior and mobile behavior. By using this modeling two strategies are developed for restraining virus propagation i.e. preimmunization strategy and adaptive dissemination strategies. These strategies are drawing on the methodology of autonomy oriented computing (AOC).

Keywords: Autonomy oriented computing, dissemination, preimmunization

INTRODUCTION:

With increase in use of mobile devices many viruses can the spread in mobile network. Many applications are available on mobile such as messaging, video and Music sharing-commerce transactions, with this there is increase in risk and increase of malicious program [5].

Viruses are serious thread in mobile communication. These viruses cause many issues like privacy data leakage, extra charges and remote listening, unnecessary traffic.

Also this virus can damage the confidentiality, integrity of data in smart phone, sometimes jam wireless traffic by sending out thousands of spam messages. Some models already exist to predict dynamics of mobile virus propagation. However these models only consider limited aspects of human behaviors. Here two layer network model is used for modeling virus propagation.

Two types of viruses are considered:

A. Bluetooth based viruses (e.g. Cabir, Lasco)

B. SMS based viruses (e.g. Zombie)

Bluetooth virus send virus to another phone within a certain range and then replicate BT-based virus to that phone. Bluetooth virus follow wave like pattern. These viruses can infect all Bluetooth activated phones which are within its communication range means up to 10m to 30m it is like contact disease in human. Generally few days are required for Bluetooth viruses to infect all susceptible handsets, so lot of time is available to deploy antivirus program for BT-based viruses [2].

On other hand few minutes require for SMS virus to copy itself on new handsets. SMS-based virus follow more decolized pattern. When on mobile device is infected by SMS virus it send copy of virus to all mobile phones which are in address book of infected phone, means sends photos, videos, and short messages etc. the propagation of SMS -based virus is similar to spreading of computer virus, means overall SMS- based viruses are more dangerous than Bluetooth based viruses.

As shown in Fig.1 smart phones are communicate with short range wireless communication (SRWC) technology such as Wi-Fi or Bluetooth, building a spatial social network and causes the virus propagation through Bluetooth and SMS[1].

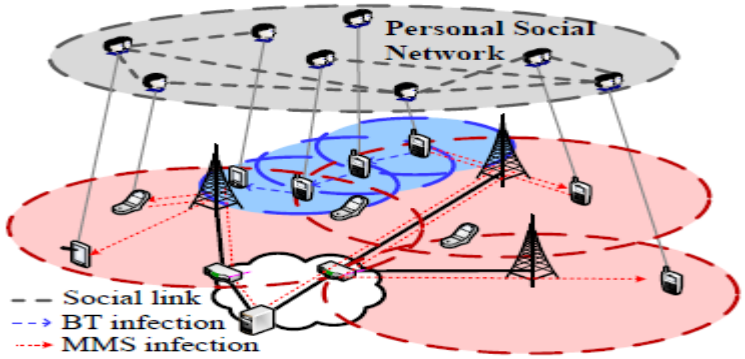

Figure 1: Hybrid malware propagation in generalized social network

1. Two layer Network model:

Here two layer network model used for modeling mobile virus propagation. And based on this modeling different strategies are further developed for restraining virus propagation. Much work is already done on this but in that work many aspects of human behavior are not consider. In this work two aspects of human behaviors are addressed i.e. operational behavior and mobile behavior. Operational behavior is primary factor contributing to SMS-based virus propagation while mobile behavior is primary factor in Bluetooth based virus propagation because Bluetooth viruses only infect the other mobile phones which are in certain communication range. In case of SMS -based viruses if user having enough knowledge regarding with virus propagation they will not open suspicious message.

Fig.2 gives the basic idea of two layer network model. We used ***two layers***:

- Lower layer represents a geographically base cell tower network
- Upper layer represents a logical network

Logical network is constructed from address books of phones.BT-based viruses are spread in lower layer of model while SMS-based viruses are spread in Upper layer of model following the social relationship among mobile users.

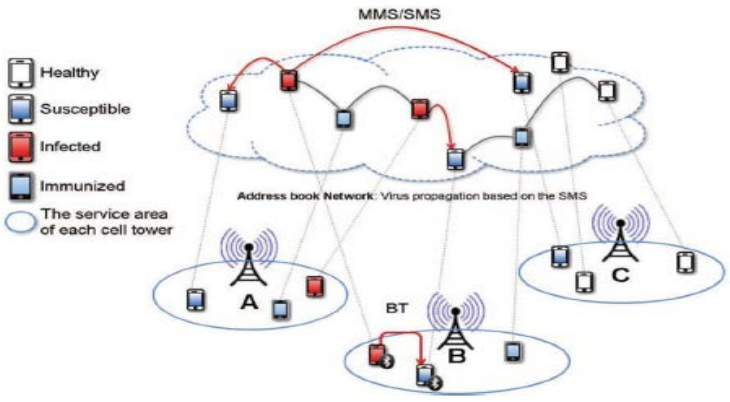

Figure 2: Two layer network model for modeling mobile virus propagation.

A. Geographic network structure:

Cell towers provide the wireless signal, mobile phones are connected each other using In two layer network model cell towers geographical network is presented using 2D grid. Based on mobile behavior of users their cell phones are travelled in geographical network, by moving one lattice to another lattice. In 2D grid location of cell tower is presented using co-ordinate p(x,y).

B. Logical network structure:

From address book of mobile phones logical relationship network is emerged out .In this network node represents the mobile phones while edges represent the

communication link between them. Logical relationship network follows
power–low distribution in terms of node degrees.

2. Different strategies for restraining mobile virus propagation:

Many strategies are developed for restraining mobile viruses' propagation. Some strategies send patches or security notification through Bluetooth by selecting some "important phones"; but this type of strategy cannot applied in real word because of highly dynamic topology of network. In this study from the observation of two layer network model, some strategies are developed which are used for restraining mobile virus propagation. This strategies drawing on methodology of Autonomy oriented computing (AOC).

These 2 strategies are:

A. Preimmunization Strategy

B. Adaptive dissemination Strategy

A. Preimmunization Strategy: - For preventing virus propagation immunization techniques are used means some nodes are immunized to preventing them by infection. Internet is complex network for such network immunization strategies are means for preventing viruses to be propagated.

Many immunization strategies were already developed but they can only applied to centralized and stable network, means it is difficult to apply them at decentralized network. Autonomy oriented computing(AOC) is best solution to this problem[3],[4].It is decentralized and scalable immunization strategy based on self-organized computing approach which vaccinate highly connected important node thus cutting epidemic path. Self-organization is core of AOC. There are two main types of AOC immunization strategy.

- Acquaintance immunization
- D-steps immunization

Advantages:

1. It is useful in highly decentralized and robust network.

2. Select group of phones which are important and having highest degree of transmissions capabilities in mobile network for protection.

Limitations:

1. Structure of Network is ignored.
2. D-step immunization is too costly.
3. The node with highest second degree is ignored

B. Adaptive dissemination strategy: - This strategy distributes security notification to as many phones are possible with low communication redundancy. Initially few dissemination entities are deployed into mobile network. Entity with security patches first routed to highly connected phones and then to another phones. Diagram 3 shows how state transition of phones takes place in SMS - based viruses.

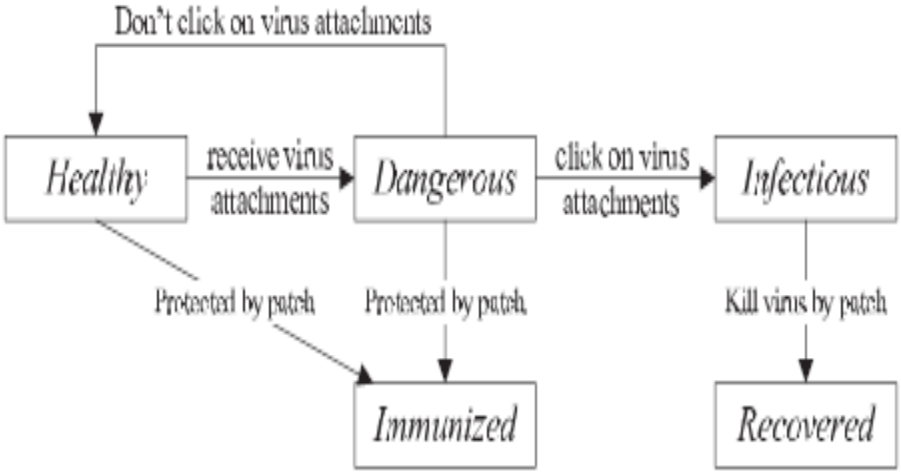

Figure 3: State transition in smart phones

a. State of phone is changed to *Healthy ->Dangerous when* it receives the virus embedded attachment.

b. There are two operational behaviors after receiving an infected message: If user opens infected message then phone state changed to *Dangerous ->Infectious*; or not open it, *Dangerous -> Healthy.*

c. If phone is already infected and security patches is received to phone, it will recover from infected state, *Infectious -> Recovered*.

Behavior of entities in this strategy as follows [4]

Rational Move - If dissemination entity present in highest degree phone, it will move to non-resided highest degree phone.

Random jump - In order to avoid to stuck in local optima entity moves along the edges.

Wait - If any required phone is not available then entity will stay at current position.

Advantages:

1. Lower communication cost to cover all network.
2. No matter how network structure is this strategy effectively protect mobile network from potential damage.

Limitations:

Flooding technology used for network search which causes overloaded traffic in network.

4. CONCLUSION:

In this paper we have presented two layers Network model for modeling virus propagation of BT-based virus and SMS-based virus, here two types of Human behavior are consider i.e. operational behavior and mobile behavior. Based on two layer network model we have developed two strategies named AOC based preimmunization strategy and AOC based Adaptive dissemination strategy for restraining mobile virus propagation.

5. REFERENCES:

1. 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.
2. P. Wang, M.C. Gonzalez, C.A. Hidalgo, and A.-L. Barabasi, "Understanding the Spreading Patterns of Mobile Phone Viruses," Science, vol. 324, no. 5930, pp. 1071-1076, 2009.
3. 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.
4. 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.
5. F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, pp. 2811-2819, 2010.