International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Analysis of BT and SMS based Mobile Malware Propagation

Prof. R. S. Sonar
Associate Professor
Sinhgad College of Engineering,
Vadgaon. Pune, India.

Sonal Mohite
PG Scholar
Sinhgad College of Engineering,
Vadgaon. Pune, India.

ABSTRACT
In wireless eon mobile devices have turned out to be the integral part of all human communication. As a result, the computer malware is now drifting from computers to mobile phones. The purpose of this paper is to demonstrate the Bluetooth & SMS based mobile malware propagation, cloud based detection of both the malwares & at last, control the malware propagation. At first, mobile network is formed. It is also referred as geographical social network. It consists of mobile devices, cell towers & gateways for data transfer. Mobile malware propagates via two communication channels viz. Bluetooth/Wi-Fi, and SMS/MMS. BT based malware propagates in geometric proximity and thus has a short range spreading pattern. SMS based malware propagation has a long-range spreading pattern. SMS based malwares are dangerous when it comes to speed and scope of propagation. Signatures are used to detect the mobile malware. Signature matching is performed on externally implemented server which is a separately implemented module. This malware detection technique comes under cloud based mobile malware detection. When a message is sent from one device to another device, suspicious activity logs are sent to cloud server. When some predefined numbers of logs come from a specific device & signature matches, then that device is declared as malicious or attacker device. Malicious devices' details are sent back to mobile network in the form of patch. This patch prevents other devices from receiving the message sent by attacker.

Keywords
Bluetooth based malware, malware control, malware detection, mobile malware, malware propagation, SMS based malware.

1. INTRODUCTION
Few years back mobile phones were not as much used as computers. However the latest mobile devices are changing the whole scenario. Mobile devices are becoming the assisting computing devices with computers.

Latest mobile devices provide most of the functionalities of traditional computers.Moreover, various wireless communication functionalities such as GSM, UMTS, EDGE, and GPRS are also provided. Various networking functionalities such as Infrared, Bluetooth, Wireless LAN IEEE 802. have improved usability of smart phones. GPS is added advantage to communication & network functionalities. SMS, MMS, and calling are the basic facilities of mobile phones. All these basic and additional features have increased the danger of malware which was originally targeting computers only. The malware targeting mobile phones is popularly known as mobile malware. It has become very hazardous threat to mobile phones. According to recent Kaspersky researches it is stated as 'Serious business'. It is no longer fun and games. The damage made by mobile malwares is too severe to overlook, which includes stealing of one's private data from device, snooping of ongoing conversations, charging excess money by sending SMS to premium rate numbers, and sometimes even a location tracing of user. So, here comes the time to be exceptionally cautious about mobile malware &understanding various ways of mobile malware propagation, detect the mobile malware, and control its propagation. SMS & Bluetooth are the two major communication channels used by mobile malware for propagation mechanism. Cloud based detection is one of the efficient way to detect mobile malware. After a malware is detected, updated security patch is used to restrain the mobile malware propagation.

2. RELATED WORKS

Many researchers have implemented different mobile networks to study mobile malware propagation. Chao Gao and Jiming Liu (2013)[2], [3] have implemented a two layer generalized social network model which consists of two layers viz. Geographical layer and logical contact layer. BT based malware propagates in geographical layer whereas SMS based malware propagates in logical contact layer. They also demonstrate the effect of mobility & operational behavior of mobiles [4], [5], [6], [8], [9]. Shin-Ming Cheng et al. (2011)[1] have implemented the approach where malware propagation is studied on generalized social network model. It has two layers as personal social network & spatial social network. It shows the propagation of hybrid malware that can propagate by either end-to-end messaging service or by short-range wireless communication [6], [9]. Guanhua Yan and Stephan Eidenbenz (2009) [9] have specifically modeled propagation of Bluetooth worms. A comprehensive model showing propagation dynamics of Bluetooth worms is proposed. This model can also predict the spreading curves of Bluetooth worm. Due to discrete-event simulation the computational cost incurred is quite less.

3. METHODOLOGY

First of all, a mobile network is implemented which is further used to study propagation of mobile malware [2], [3], [7]. Mobile network is also known as generalized social network. It is formed from cell towers, gateways & mobile nodes. Tower acts as a head node for particular cluster & serves the mobile nodes working under it. Each tower has givena specific range value which determines the service area of specific tower. Gateways are used for the data transfer from one cluster to another cluster [7]. Mobile nodes are the mobile devices working under cell towers. These mobile nodes keep moving in the network. It has properties such as identification number, location data associated with it & buffer memory to store a data. SMS & Bluetooth based mobile malware propagation is shown on the network. Once the malware is propagated, next obvious step is to detect it. Signatures are used to detect the mobile malware. Signature matching is performed on externally implemented server which is separated from the mobile network. This malware detection technique comes under cloud based mobile malware detection where malware is detected on some external server & not on the mobile device itself. When a message is sent from one device to another device, suspicious activity logs are sent to this external server. When some predefined numbers of logs come from a specific device & signature matches, then that device is declared as malicious or attacker device. Malicious devices' details are sent back to mobile network in the form of patch. When such infected node tries to send data to any other nodes, the patch restrains other nodes from accepting the data. In this way the mobile malware propagation is controlled.

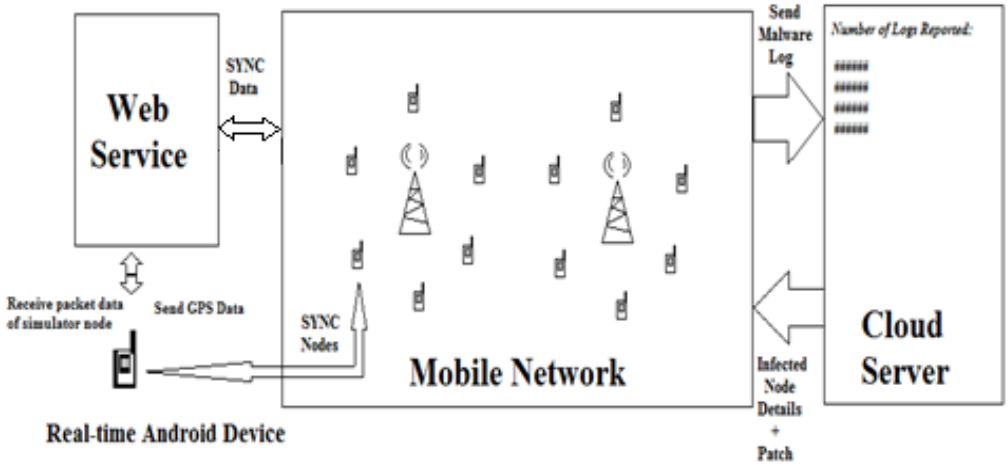

Figure 1. System Architecture

3.1 Mobile Malware Propagation Techniques

Based on communication media, mobile malware has 2 types: BT based malware & SMS based malware.

3.1.1 SMS based malware

SMS based mobile malware propagation does not have a geographical boundary restrictions. A SMS based malware can propagate from one device to other devices which are millions of kilometers farther. So this may create havoc. Operational behavior of users plays an important role in malware propagation. The pclick parameter associated with each device determines the message clicking probability of user. Low the message clicking probability, high the security awareness & less the infection of malware. The following algorithm is implemented to study SMS based mobile malware propagation [2], [3], [7], [8].

Algorithm 1: SMS based mobile malware propagation

I/P: G[N][N], T[Nt], P[Np]

O/P: SMSMCount[Step][K] stores the number of infected phones in the K'th time

// Phase I: Initializing the smart phones

1. **Propagation_SMS_InitPhone**( );

// Phase II: SMS-based virus propagation

2. **For** K=1 to *Runtime* // run 10 times
3. **While** (Step<Endsimul) // 500 steps
4. **For** I=1 to Np
5. **Check _Power_On**(Vi.On-Off);
6. **If** Vi.Ton>0 && Vi.On-Off==*true*
7. Probability← The message clicking probability based on Vi.Pclick
8. Send copies of virus to all users in its contact book;
9. SumI++; // Infected phones total
10. **EndIf**
11. **EndFor**
12. SMSMCount[Step][K]=SumI;
13. Step++;
14. **EndWhile**
15. **EndFor**

3.1.2 Bluetooth based malware

A BT-based malware is able to infect its geographical neighbors with same Operating System. When a phone is infected with Bluetooth based malware, it automatically turns on the Bluetooth service of itself. Then, the infected phone arbitrarily picks out a susceptible phone as its target. Susceptible phones are the mobile devices in the vicinity of infected mobile phone having its Bluetooth on. Now the infected phone sends out the mobile malware to such susceptible phones present in its Bluetooth range. The following algorithm is implemented to study Bluetooth based mobile malware propagation [2], [3], [7], [8].

Algorithm 2: BT based mobile malware propagation
I/P: G[N][N], P[Np], GridData
O/P: BTMCount[step][k] infected phone count in the k'th simulation
// Phase I: Initializing the state of cell towers and phones
1. **Propagation_BT_init**( );
// Phase II: BT-based malware propagation
2. **For** k=1 to Runtime // 10 run to obtain an average value
3. **While**(step<Endsimul) // 500 steps at each time, i.e.,Endsimul=500
4. **For** i=1 to Nt;
5. **If** Ti.ntp>0 && Ti.infectedBT phone!=0 **then**
6. vit=vit+**BT_SIR**(Ti); // SIR model in each cell tower
7. **EndIf**
8. **EndFor**
9. BTMCount[step][k]=vit;
10. **Human_Mobility**(step); // Simulating users' mobility
11. step++;
12. **EndWhile**
13. **EndFor**

3.2 Mobile Malware Detection

Mobile phones have limited computational capabilities & power. So it is not economical as well as feasible to run a full-fledged and well developed security mechanism on mobile phone itself. Cloud-based mobile malware detection is the best option for mobile phones in which security analysis & computations are moved to the remote server known as cloud [7]. Signature based mobile malware detection is implemented here. In this a client sends suspicious pattern through log to the cloud. This is known as signatures. When enough numbers of such logs are found in the cloud and if a signature is same in all the cases, the node is declared as malicious and further activity by that node is blocked.

3.3 Mobile Malware Control

Till now we have studied mobile malware propagation & detection. Along with detecting mobile malware, there is a need to control its propagation. Basically, there are two types of malware control strategies, viz. proactive & reactive control. Proactive control strategy is used before actual malware is detected. Whereas reactive malware strategy is implemented after certain malware is detected. We have used reactive control strategy here means when a malware is detected then the control strategy is implemented. So when any new malware is found, antivirus updates for that malware are implemented and forwarded to mobile network & from there to mobile phones. This process is known as patch dissemination [2], [3], [4], [5], [7].

4. IMPLEMENTATION

This system is implemented in total 4 modules. Mobile network & cloud server are the two basic modules. Mobile network consists of simulated cell towers, gateway nodes, & mobile devices. It is formed from the initial number of nodes count given by user [7]. Suppose a user says he wants to form a network of 100 nodes then a mobile network of 100 nodes consisting of cell towers, gateways, &mobile devices is formed. SMS & Bluetooth based mobile malware propagation is studied on this network. Figure 2 shows cell towers & gateways in Red & Yellow color nodes respectively. Mobile nodes are in various colors except Red & Yellow. Cloud server, the second module, detects mobile malware, sends updated security patched to mobile network & thus helps in control of mobile malware propagation. Both these modules are implemented in J2SE. RMI plays a major role in message passing between various objects.

The novelty of the system lies in third & fourth modules. Third module synchronizes a real-time Android device with one of the simulated random mobile nodes from mobile network. Fourth module is a web service that does the job of communication between simulated mobile node & real-time Android device. Synchronization is nothing but the activities happened on the simulator nodes are replicated on real-time Android device & vice versa. The activities consist of data packets received on simulated mobile node & location change of Real-time Android device. Third module is implemented as an App for Android device. The App accesses GPS co-ordinates of Android device so the location is synchronized. Fourth module is a web service implemented using J2EE, SOAP, HTML, and XML. SOAP is used for communication between Android device & web service. HTML & XML is also used for data transfer & data encoding respectively.

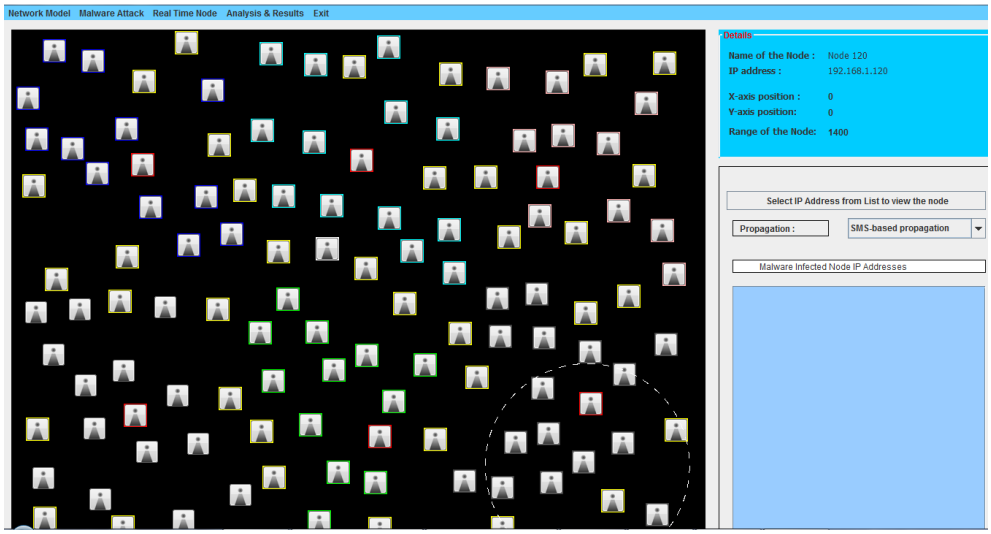

Figure 2. System Implementation

5. RESULT & DISCUSSION

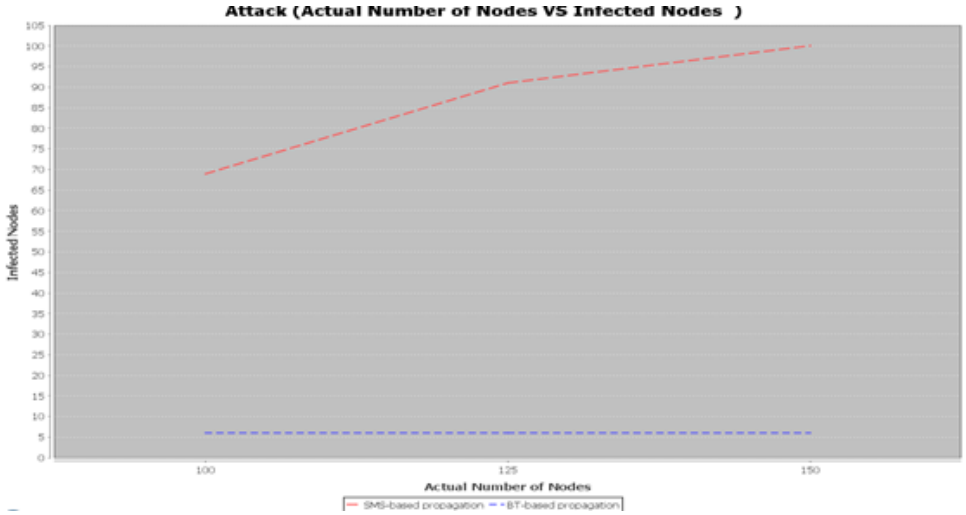

Figure 3. Actual Number of Nodes vs. Infected Nodes

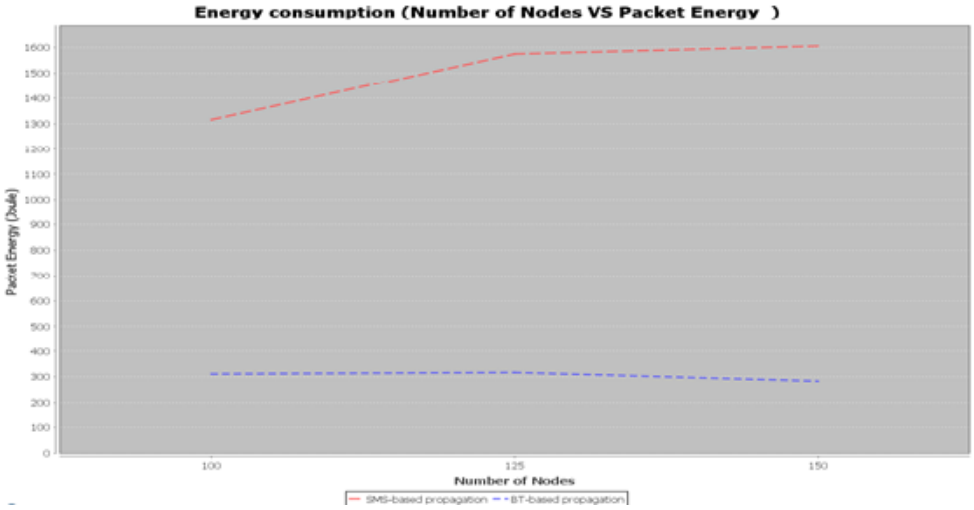

Figure 4. Number of Nodes vs. Packet Energy

From above graphs it is examined that SMS based mobile malware propagates in good speed. When number of nodes increases, SMS based mobile malware propagates in high speed. High the number of nodes, high is the malware count. On the other hand, with increase in number of nodes, Bluetooth based mobile malware don't change its behavior quite differently. Same number of malware count was found with slight increase in number of nodes.

When it comes to packet energy consumption, SMS based malware is again more dangerous than Bluetooth based malware. With increase in number of nodes, more energy is consumed by SMS based malware. Same is not the case with Bluetooth based malware. Almost same energy is consumed although there is a slight increase in number of nodes.

6. CONCLUSION

A generalized social network model is implemented which is used to study the propagation, detection and control of mobile malware. BT-based virus propagates such that it has localized propagation pattern. SMS-based virus propagates such that it has delocalized long-range infection pattern. Operational & mobility behavior of user play crucial role in Bluetooth based & SMS based virus propagation respectively. When it comes to propagation speed and severity, SMS-based viruses are more hazardous than BT-based viruses. After malware detection, the malicious device's details are sent back to mobile network in the form of patch. This patch prevents other devices from receiving the message sent by attacker. As mobile malware is going to create havoc in near future, so this is a right time to understand the

spreading patterns & severity of mobile malware. This paper concludes that the attention is needed over mobile malware propagation especially SMS based mobile malware & preventive measures to control the malware propagation.

REFERENCES

[1] Cheng, S., Ao, W. C., Chen, P., Chen, K., 2011. *On Modeling Malware Propagation in Generalized Social Network,* IEEE Comm. Letters, Vol. 15, No. 1, pp. 25-27.

[2] Gao, C., and Liu, J., 2013. *Modeling and Restraining Mobile Virus Propagation,* IEEE transactions on mobile computing, Vol. 12, No. 3, pp. 529-541.

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

[4] Gao, C., Liu, J., and Zhong, N., 2011. *Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis,* Knowledge and Information Systems, Vol. 27, No. 2, pp. 253-279.

[5] Gao, C., Liu, J., and Zhong, N., 2011. *Network Immunization with Distributed Autonomy-Oriented Entities,* IEEE Trans. Parallel and Distributed Systems, Vol. 22, No. 7, pp. 1222-1229.

[6] Meng, X., Zerfos, P., Samanta, V., Wong, S.H., and Lu, S., 2007. *Analysis of the Reliability of a Nationwide Short Message Service*, Proc. IEEE INFOCOM, pp. 1811-1819.

[7] Mohite, S., and Sonar, R.S., 2014. *Proliferation, Detection, and Suppression of Mobile Malware,* Cyber Times International Journal of Technology and Management, ISSN: 2278-7518, Vol. 7, Issue 1, pp. 129-134.

[8] Wang, P., Gonzalez, M.C., Hidalgo, C.A., and Barabasi, A.L., 2009. *Understanding the Spreading Patterns of Mobile Phone Viruses*, Science, Vol. 324, No. 5930, pp. 1071-1076.

[9] Yan, G., and Eidenbenz, S., 2009. *Modeling Propagation Dynamics of Bluetooth Worms (extended version),* IEEE transactions on Mobile Computing, Vol. 8, No. 3, pp. 353-368.

This paper may be cited as:

Sonar, R. S. and Sonal, M., 2014. Analysis of BT and SMS based Mobile Malware Propagation. *International Journal of Computer Science and Business Informatics, Vol. 14, No. 2, pp. 16-24.*