Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.466 – 470

RESEARCH ARTICLE

DETECTING MALWARE BY SIGNATURE DISTRIBUTION ALGORITHM IN MANET WITH HETEROGENEOUS DEVICES

J.SOWMIYA

Computer Science & Engg, IFET College of Engineering, Villupuram, Tamilnadu

Dr. R.KALPANA

Professor, Computer Science & Engg, IFET College of Engineering, Villupuram, Tamilnadu

ABSTRACT: Malware are more frequently in mobile network, modeling an effective defence system in MANET to help the infected nodes to recover from the infection. MANET is a self-configuring, Infrastructure less network which connect the mobile nodes without wires. It has the access point with links between the nodes along the distribution system. In this work, the defence system is established to protect the mobile nodes form malware and stops the further propagation if it already exists. Furthermore, the problem of how to optimally distribute the content based signatures of malware is investigated, which help to detect the corresponding malware and disable further propagation, to minimize the number of infected nodes. By some theoretical analysis and simulations with both synthetic and realistic mobility traces, the distribution algorithm which achieved the optimal solution, and performs efficiently in MANET.

Key Terms- Signature, Dissemination, Proximity malware, Heterogeneous mobile devices.

I. INTRODUCTION

In the recent days, there is a drastic change in the growth of popular mobile networks[1]. Because of the transformation, It has made attractive to virus and worm writers in the existence of Mobile Ad-hoc Network(MANET). MANET is self-configuring, Infrastructureless networks which connect the mobile nodes without wires. Each device in this network is free to move independently in any direction, and will therefore changes its links to other devices frequently. Because the user keeps moving here and there. When the user is in mobile, the session may not hold good and the communication may get hand-off. In that situation, the MANET is come into the picture. MANET consists of a peer-to peer, self-forming, self-healing network in contrast to a mesh

network has a central controller which is used to determine, optimize and distribute the routing table. It typically communicates at radio frequencies of 30MHz-5GHz.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Shortly, It is the network connection that is build up for single session of communication between two entities. This network does not use a router or a wireless base station. For instance, when the user wants to transfer a file from mobile to other, they use Bluetooth or MMS. In this communication session, Bluetooth acts as an Ad-Hoc. The basic Characteristics of MANET is Energy-constrained operation in which the devices in the modern electronic world completely rely on batteries. The design of this network is to be optimized to conserve the energy consumed by the mobiles. In this model, it deals with the heterogeneous devices based on the operating system like iPhones, Android and Blackberry devices. So the Anti-Malware system should be supported for all types of operating system. The Malware is short form of malicious software which software used to disrupt the computer operation, gather sensitive information, or gaining access to private computer systems. Nowadays, this is major problem in the mobile network.

Primarily, Malware is an umbrella terms used to refer to a variety of forms of hostile or intrusive software including computer viruses, worms, Trojan horses, ransom ware, spyware, adware, scare ware and other malicious software programs. It can be in the form of executable code, scripts, active content and other software. To reduce the propagation of malware over network, this work is demonstrated. Consider a mobile Ad-Hoc network, where the particular portions of nodes are affected by malware. For this situation, the efficient defence system is needed to help the nodes for recovering and preventing the healthy nodes from further infection. By using the signatures which are the composition of private key and data to be transmitted of the user can avoid the redundancy in the network. This is major and optimization goal of this work. In this analysis, The introduction of distribution solution to avoid the propagation of malware efficiently.

II. RELATED WORKS

A number of studies have demonstrated the threat of malware propagation on mobile phones through Bluetooth. Su et al. gather Bluetooth scanner traces and use simulation to demonstrate that malware propagation via Bluetooth is viable, and explore its propagation dynamics [6].Here Defending against proximity malware is particularly challenging since it is difficult to piece together global dynamics from just pair-wise device interactions. Traditional network defenses depend upon observing aggregated network activity to detect correlated or anomalous behavior. Proximity contact, and was evaluated potential defenses against it. The dynamics of proximity propagation inherently depend upon the mobility dynamics of a user population in a given geographic region. Unfortunately, there is no ideal methodology for modeling user mobility. Traces of mobile user contacts reflect actual behavior, but they are difficult to generalize and only capture a subset of all contacts due to a lack of geographic coverage. Then It can be generally categorized into two main types. One class of works focuses on analyzing the proximity malware spreading. Yan et al. [22], [23] develop a simulation and analytic model for Bluetooth worms, and show that mobility has a significant impact on the propagation dynamics.

The other class focuses on the malware spreading by SMS/MMS. Initial work has explored defending mobile devices against malware propagating using the provider network. Bose and Shin propose a proactive approach to identify vulnerable devices, and to rate-limit and quarantine SMS communication [12]. To prevent the malware spreading by MMS/ SMS, Zhu et al. [5] propose a counter-mechanism to stop the propagation of a mobile worm by patching an optimal set of selected phones by extracting a social relationship graph between mobile phones via an analysis of the network traffic and contact books. This approach only targets the MMS spreading malware and has to be centrally implemented and deployed in the service provider's network. To defend mobile networks from proximity malware by Bluetooth, Zyba et al. [6] explore three strategies, including local detection, proximity

signature dissemination, and broadcast signature dissemination. For detecting and mitigating proximity malware, Li et al. [7] propose a community-based proximity malware coping scheme by utilizing the social community structure reflecting a stable and controllable granularity of security.

The former one has the limitations that signature flooding costs too much and the local view of each node constrains the global optimal solution. But Proximity malware propagation fundamentally depends upon user mobility dynamics. Previous approaches to represent mobility have used scanner traces, synthetic random walk models, and analytic techniques. It drawn upon all three approaches to inform this study. But, the primary goal is to understand the effectiveness of defenses, not to develop new mobility and modeling techniques.

First, this scheme targets both the MMS and proximity malware at the same time, and considers the problem of signature distribution. Second, all these works assume that malware and devices are homogeneous, But it take the heterogeneity of devices into account in deploying the system and consider the system resource limitations. Third, The proposed algorithm is distributed, and approaches to the optimal system solution.

III. DETECTION OF MALWARE IN MANET

In this work, the malware can be propagated by two methods, one is MMS another one is Bluetooth. Through MMS, the malware can replicate the copy of itself and sent to the contacts which are available in the address book. By Bluetooth, it uses the short-range wireless media to infect the devices in proximity as "proximity malware. From the related work there are two major problems. First, it cannot rely on any centralized algorithms to disseminate the signature to the nodes. Second, the storage of mobile devices are limited, i.e., CPU, storage, and battery power. Eventhough the CPU-resource is increased drastically, it is still resource limited when compared to the desktops. Hence, the to-be-deployed defence system is having the limited resources on CPU memory to store the defence software. Finally the mobile devices which are using is considered to be Heterogeneous devices in terms of Operating system.

There are two major algorithms to distribute the signatures to the nodes.

- It formulates the optimal signature distribution problem in the heterogeneity of mobile devices. Moreover it is suitable for both MMS and Bluetooth for malware propagation.
- It gives the centralized greedy algorithm for signature distribution. And it proves that gives the optimal solution.
- It proposes the Encounter-Based distribution algorithm to disseminate the signature using the metropolis sampler. It relies on the local opportunistic contacts.

Consider, a system of N heterogeneous wireless nodes belonging to K types (e.g., type of OS), which can be infected by K types of malware, denoted by set IK. Then, S be the helpers nodes to store the signatures. let As denote the maximum number of signatures that can be stored at helper s, and uk denote the number of helpers for malware k and v0k denote the number of infected nodes at the starting time. It first consider the number of nodes affected by malware in time t is represented.

IV. SYSTEM ARCHITECTURE

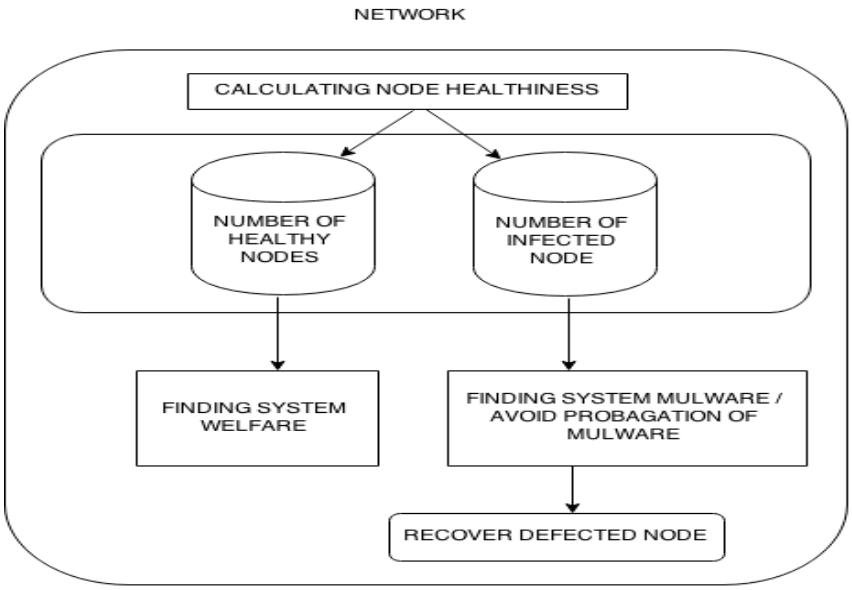

Fig. System Architecture

In this architecture, it describes about the complete process of the malware detection. then in this detection, it consists of two nodes like healthy node and infected node. Based on the system welfare, the infected node is found then it will be recovers the infected node from further propagation. Hence, the malware can be reduced its penetration in the mobile network.

V. CONCLUSION

In this system, it investigates the problem of signature distribution to protect the mobile network from the malware propagation of both the attacks. It closely approaches the optimal solution by using the centralized algorithm. Through both theoretical analysis and simulations, It demonstrates the efficiency of the defense scheme in reducing the amount of infected nodes in the system. Therefore, security and authentication mechanisms should be considered. From the aspect of malware, since some sophisticated malware that can bypass the signature detection would emerge with the development of the defense system, new defense mechanisms will be required.

REFERENCES

[1] P. Wang, M. Gonzalez, C. Hidalgo, and A. Barabasi, "Under- standing the Spreading Patterns of Mobile Phone Viruses," Science, vol. 324, no. 5930, pp. 1071-1076, 2009.

[2] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A Social Network Based Patching Scheme for Worm Containment in Cellular Networks," Proc. IEEE INFOCOM, 2009.

[3] G. Zyba, G. Voelker, M. Liljenstam, A. Me´hes, and P. Johansson, "Defending Mobile Phones from Proximity Malware," Proc. IEEE INFOCOM, 2009.

[4] F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, 2009.

[5] P. Bre´maud, Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues. Springer Verlag, 1999.

[6] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble Rap: Social-Based Forwarding in Delay Tolerant Networks," Proc. ACM MobiHoc, 2008.

[7] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms," IEEE Trans. Mobile Computing, vol. 8, no. 3, p. 1071, 2008.

[8] G. Yan, H. Flores, L. Cuellar, N. Hengartner, S. Eidenbenz, and V. Vu, "Bluetooth Worm Propagation: Mobility Pattern Matters!" Proc. ACM Symp. Information, Computer and Comm. Security, pp. 32- 44, 2007.

[9] C. Fleizach, M. Liljenstam, P. Johansson, G. Voelker, and A. Mehes, "Can You Infect Me Now? Malware Propagation in Mobile Phone Networks," Proc. ACM Workshop Recurring Malcode, pp. 61- 68, 2007.

[10] A. Bose and K. Shin, "On Mobile Viruses Exploiting Messaging and Bluetooth Services," Proc. Securecomm and Workshops, pp. 1- 10, 2006.

[11] D. Daley and J. Gani, Epidemic Modelling: An Introduction. Cam- bridge Univ, 2001.

[12] E. Altman, A.P. Azad, and F. De Pellegrini, "Optimal Activation and Transmission Control in Delay Tolerant Networks," Proc. IEEE INFOCOM, 2010.

[13] M. Khouzani, S. Sarkar, and E. Altman, "Dispatch then Stop: Optimal Dissemination of Security Patches in Mobile Wireless Networks," Proc. IEEE 49th Conf. Decision and Control (CDC), pp. 2354-2359, 2010.

[14] Kalpana,R. and Rengarajan, N. "Mobile Anonymous Trust Based Routing Using Ant Colony Optimization", American Journal of Applied Sciences. ISSN:1546-9239, Vol. 9 No. 8, pp. 1283-1289, 2012.

