IISRC International Conference on Industrial Scientific Research Engineering
International Industrial Scientific Research Corporation
www.worldconferences.org

Enhanced Multivariate Correlation Analysis Model for Attack Detection System

SYED LARA[1], SK. NAZEER BASHA[2], P.BABU[3]
[1]PG Scholar, Dept of CSE, Quba College of Engineering and Technology, Nellore, AP, India.
[2]Assistant Professor, Dept of CSE, Quba College of Engineering and Technology, Nellore, AP, India.
[3]Associate Professor, Dept of CSE, Quba College of Engineering and Technology, Nellore, AP, India.

Abstract: As malware attacks become more frequently in mobile networks, deploying an efficient defense system to protect against infection and to help the infected nodes to recover is important to prevent serious spreading and outbreaks. The technical challenges are that mobile devices are heterogeneous in terms of operating systems, the malware infects the targeted system in any opportunistic fashion via local and global connectivity, while the to-be-deployed defense system on the other hand would be usually resource limited. In this paper, we investigate the problem of how to optimally distribute the content-based signatures of malware, which helps to detect the corresponding malware and disable further propagation, to minimize the number of infected nodes. We model the defense system with realistic assumptions addressing all the above challenges that have not been addressed in previous analytical work. Based on the framework of optimizing the system welfare utility, which is the weighted summation of individual utility depending on the final number of infected nodes through the signature allocation, we propose an encounter-based distributed algorithm based on Metropolis sampler. Through theoretical analysis and simulations with both synthetic and realistic mobility traces, we show that the distributed algorithm achieves the optimal solution, and performs efficiently in realistic environments.

Keywords: Key-Aggregate Cryptosystem (KAC), Transformation Key (TK), Random Oracles (RO).

I. INTRODUCTION

A. Motivations

The target landscape for malware attacks (i.e., viruses, spam bots, worms, and other malicious software) has moved considerably from the large-scale Internet to the growingly popular mobile networks, with a total count of more than 350 known mobile malware instances reported in early 2007. This is mainly because of two reasons. One is the emergence of powerful mobile devices, such as the iPhone, Android, and Blackberry devices, and increasingly diversified mobile applications, such as multimedia messaging service (MMS), mobile games, and peerto- peer file sharing. The other reason is the emergence of mobile Internet, which indirectly induces the malware? Malware residing in the wired Internet can now use mobile devices and networks to propagate. The potential effects of Malware propagation on mobile users and service providers would be very serious Understanding the behaviours and damages of mobile malware, and designing an efficient detection and defense system are necessary to prevent large-scale outbreaks and it should be an urgent and high-priority research agenda. Consider a mobile network where a portion of the nodes are infected by malware. Our research problem is to deploy an efficient defense system to help infected nodes to recover and prevent healthy nodes from further infection. Typically, we should disseminate the content-based signatures of known malware to as many nodes as possible. Consequently, distributing these signatures into the whole network while avoiding unnecessary redundancy is our optimization goal. However, to address the above problem in the realistic mobile environment is challenging for several reasons.

B. Problem Definition

Based on the malware spreading model, we first formulate the problem, and then give a greedy algorithm to achieve the optimal signature distribution. Based on the defined utility function, we use the sum of individual utilities with different weighting factors wk according to the final number of infected nodes as the system welfare. This is a standard and widely used definition. Consequently, we can specify the studied problem as the following optimization problem:

$$\begin{aligned} \text{maximize} \quad & \sum_{k\in\mathbb{K}} w_k F_k\left(\sum_{s\in\mathbb{S}} x_{s,k}\right) \\ \text{over} \quad & x_{s,k}\in\{0,1\}; \\ \text{subject to} \quad & \sum_{k\in\mathbb{K}} x_{s,k}\le A_s, \end{aligned} \tag{1}$$

Where x_s means helper s stores the signature of malware k; otherwise, x_s. W_k is the weighting factor, and F_k is the utility function for defending malware k. Related to wk, it is used

to weigh the system contributions of different malware defending effects under different fairness objectives. One special case is that all malware has the same defending contribution to the system. Then, the utility is obtained by setting the weighting factors wk with the same value. For example, by setting all wk ¼ 1, we have the system welfare utility of P k2IK FkP s2SS xs;kÞ. Usually, malware that destroys the system more seriously will be assigned with a relatively higher weighting factor. In the formulated problem, we note that the system utility is an increasing and concave function of uk, and the constraint is convex. Therefore, we can derive the optimal solution by gradient descent algorithm if xs;k is allowed to take real value. However, in the system, xs;k can either take 1 or 0. Therefore, we should design corresponding algorithms to solve this problem.

C. Objective of The Project

The main objective of this paper is Mobile malware that spreads in the mobile networks typically exploits both the MMS and opportunistic contacts to propagate from one device to another. In the network, there are different types of handsets and each malware only targets handsets with a specific OS. In the defense system, we use some special nodes named helper to distribute the signatures into the network. Generally speaking, the deployed helpers can be stationary base stations or access points. However, since mobile nodes are more efficient to disseminate content and information in the network we focus on the case of mobile helpers. Consequently, there is limitation in storage on each mobile device for deploying the defense system. Although currently most Smartphone's have gigabytes of storage, users usually will not allocate all of them for the usage of malware defense. Our goal is to minimize the malware infected nodes in the system by appropriately allocating the limited storage with the consideration of different types of malware. The ranking of form components is based on the captured user preference. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

D. Organization of Documentation

The rest of the document is organized as follows. The second chapter will gives a description on literature survey, i.e. what are the Existing methods are there that are helpful to us that are used in our thesis and also provides a brief survey on the Existing solutions. The third chapter will provides description on system Analysis. In fourth chapter we provide designing issues. In fifth chapter we will provide an implementation constraint of the previous work and present work. And the sixth chapter will describe the testing. And seventh chapter will provide conclusion of the proposed method, the scope for the future work and finally we provide references.

II. EXISTING SYSTEM

Mobile malware can propagate through two different dominant approaches. Via MMS, a malware may send a copy of itself to all devices whose numbers are found in the address book of the infected handset. This kind of malware propagates in the social graph formed by the address books, and can spread very quickly without geographical limitations. The other approach is to use the short-range wireless media such as Bluetooth to infect the devices in proximity as "proximity malware." Recent work of Wang et al. has investigated the proximity malware propagation features, and finds that it spreads slowly because of the human mobility, which offers ample opportunities to deploy the defense system. However, the approach for efficiently deploying such a system is still an ongoing research problem.

Disadvantages of Existing System:

- There is a problem for optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware.
- The existing system offers only protection against only one attack at a time.

III. PROPOSED SYSTEM

To Design a defense system for both MMS and proximity malware. Our research problem is to deploy an efficient defense system to help infected nodes to recover and prevent healthy nodes from further infection. We formulate the optimal signature distribution problem with the consideration of the heterogeneity of mobile devices and malware, and the limited resources of the defense system. Moreover, our formulated model is suitable for both the MMS and proximity malware propagation. We give a centralized greedy algorithm for the signature distribution problem. We prove that the proposed greedy algorithm obtains the optimal solution for the system, which provides the benchmark solution for our distributed algorithm design. We propose an encounter-based distributed algorithm to disseminate the malware signatures using Metropolis sampler. It only relies on local information and opportunistic contacts.

IV. CONTEXT DIAGRAM OF PROJECT

Mobile malware that spreads in the mobile networks typically exploits both the MMS and opportunistic contacts to propagate from one device to another. In the network, there are different types of handsets and each malware only targets handsets with a specific OS as shown in Fig.1. In the defense system, we use some special nodes named helper to distribute the signatures into the network. Generally

speaking, the deployed helpers can be stationary base stations or access points. However, since mobile nodes are more efficient to disseminate content and information in the network we focus on the case of mobile helpers. Consequently, there is limitation in storage on each mobile device for deploying the defense system. Although currently most Smartphone's have gigabytes of storage, users usually will not allocate all of them for the usage of malware defense. Our goal is to minimize the malware infected nodes in the system by appropriately allocating the limited storage with the consideration of different types of malware.

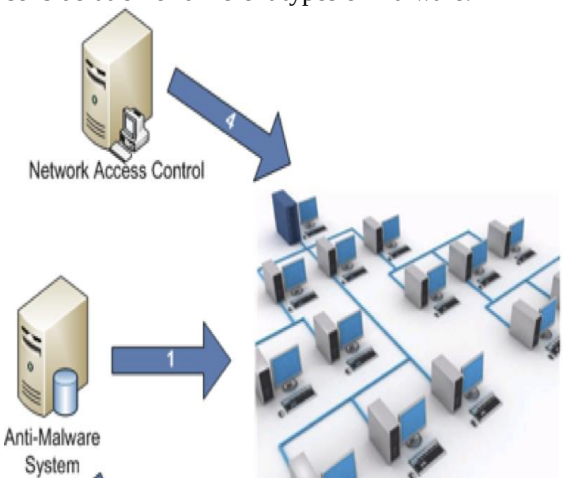

Fig.1. Context Diagram of malware network.

A. Modules

- Malware signature finder and Spreading Module
- Problem Formulation And Centralized Algorithm
- The Metropolis Sampler.
- Performance Evaluation.

Malware signature finder and Spreading Model: In this module, malware signature will be analyzed and distributed over connected node. We 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. In the defense system, we assume that there are S helpers, denoted by set SS, storing the signatures to help other nodes with detecting the malware.

Problem Formulation and Centralized Algorithm: Based on the malware spreading model, we first formulate the problem, and then give a greedy algorithm to achieve the optimal signature distribution. Now, we validate the proposed malware spreading model expressed, which is based on the epidemic model for malware spreading and the fluid model in DTN. Since our model characterizes the fraction of the malware infected nodes, we simulate the malware spreading, and compare the simulation results of infected ratio with that obtained by the model. As we have claimed that this model characterizes the MMS and proximity malware spreading, we validate the malware spreading in both the proximity and MMS scenarios.

The Metropolis Sampler: In this module we develop the distributed algorithm for the signature distribution problem. The designed algorithm is based on a simulated annealing technique called Metropolis sampler. In the following sections, we first describe the basic notions and the framework of Metropolis sampler, then design the distributed algorithm based on simulated annealing with the Metropolis sampler, and finally prove that the proposed algorithm converges to the optimal performance.

Performance Evaluation: We present numerical results with the goal of demonstrating that our greedy algorithm for the signature distribution, denoted OPT, achieves the optimal solution and yields significant enhancement on the system welfare compared with prior heuristic algorithms. Related to the heuristic algorithms, we consider 1) Important First (IF), which uses as many helpers as possible to store the signature of the most popular malware, 2) Uniform Random (UR), where each helper randomly selects the target signatures to store, and 3) Proportional Allocation (PA), which is a heuristic policy that assigns signatures with the uniform distribution proportional to the market sharing and the weights of different malware.

V. IMPLEMENTATION AND RESULTS

Recent work has investigated the proximity malware propagation features, and finds that it spreads slowly because of the human mobility, which offers ample opportunities to deploy the defense system. However, the approach for efficiently deploying such a system is still an ongoing research problem. In this paper, we are the first to address the challenges of designing a defense system for both MMS and proximity malware. We introduce an optimal distributed solution to efficiently avoid malware spreading and to help infected nodes to recover. Consider a mobile network where a portion of the nodes are infected by malware. Our research problem is to deploy an efficient defense system to help infected nodes to recover and prevent healthy nodes from further infection. Typically, we should disseminate the content-based signatures of known malware to as many nodes as possible as shown in Figs. 2 to 5. Consequently, distributing these signatures into the whole network while avoiding unnecessary redundancy is our optimization goal. However, to address the above problem in the realistic mobile environment is challenging for several reasons. First, typically we cannot rely on centralized algorithms to distribute the signatures because the service infrastructure is not always available. Therefore, a sensible way for signature distribution is to use a distributed and cooperative way among users. we propose an optimal signature distribution scheme by considering the following realistic modeling assumptions:

- The network contains heterogeneous devices as nodes,
- Different types of malware can only infect the targeted systems, and
- The storage resource of each device for the defense system is limited. These assumptions are usually not

addressed in previous analytical works for simplicity reasons.

Fig.2.Malware Defence.

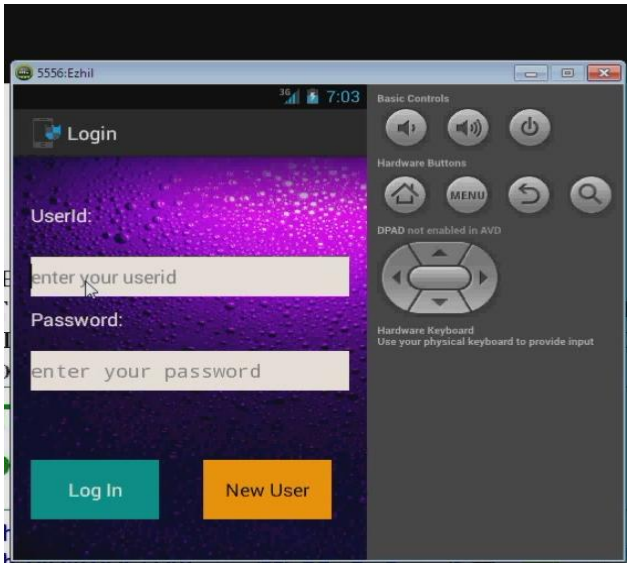

Fig.3. Login page.

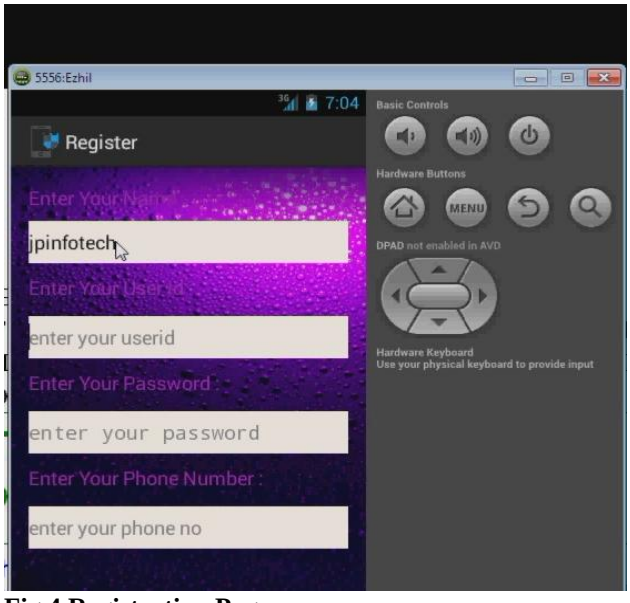

Fig.4.Registration Page.

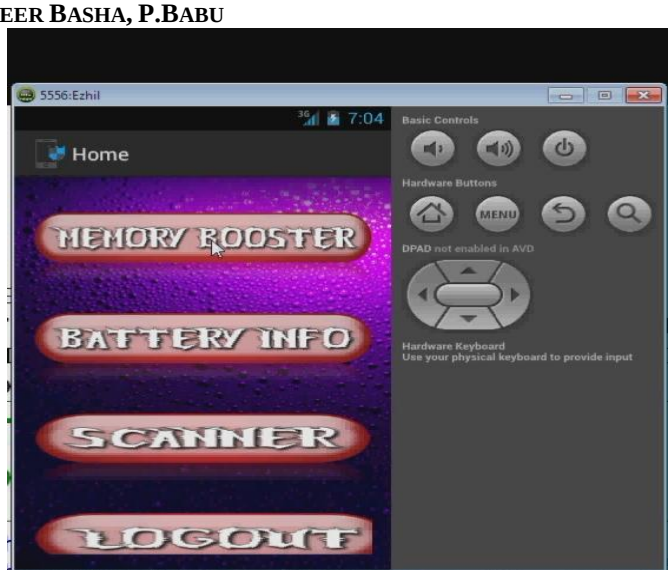

Fig.5. Home page.

VI. CONCLUSION

In this paper, we investigate the problem of optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware. We introduce a distributed algorithm that closely approaches the optimal system performance of a centralized solution. Through both theoretical analysis and simulations, we demonstrate the efficiency of our defense scheme in reducing the amount of infected nodes in the system. At the same time, a number of open questions remain unanswered. For example, the malicious nodes may inject some dummy signatures targeting no malware into the network and induce denial-of-service attacks to the defense 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.

VII. REFERENCES

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

[2] M. Hypponen, "Mobile Malwar," Proc. 16th USENIX Security Symp., 2007.

[3] G. Lawton, "On the Trail of the Conficker Worm," Computer, vol. 42, no. 6, pp. 19-22, June 2009.

[4] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," Proc. IEEE INFOCOM, 2010.

[5] 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.

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

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

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

[9] M. Grossglauser and D. Tse, "Mobility Increases The Capacity of Ad-Hoc Wireless Networks," Proc. IEEE INFOCOM, pp. 1360- 1369, 2001.

[10] R. May and A. Lloyd, "Infection Dynamics on Scale-Free Networks," Physical Rev. E, vol. 64, no. 6, p. 066112, 2001.

[11] E. Altman, G. Neglia, F. De Pellegrini, and D. Miorandi, "Decentralized Stochastic Control of Delay Tolerant Networks," Proc. IEEE INFOCOM, 2009.

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

[13] Shanghai Jiao Tong Univ., Traffic Information Grid Team, Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab. sjtu.edu.cn/, 2013.

[14] A. Kera¨nen, J. Ott, and T. Ka¨rkka¨inen, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques, pp. 1-10, 2009.

[15] J. Kumpula, J. Onnela, J. Sarama¨ki, K. Kaski, and J. Kerte´sz, "Emergence of Communities in Weighted Networks," Physical Rev. Letters, vol. 99, no. 22, p. 228701, 2007.