ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Decentralized Malware protection System For Mobile Networks with Heterogeneous Devices

Sowmya.K
M.Tech Student,
Department of Computer Science and Engineering,
VEMU institute of Technology Pakala, Chittoor Dist
A.P, India.

B.Rama Ganesh
Associate Professor, Head of the Department
Department of Computer Science and Engineering,
VEMU institute of Technology Pakala, Chittoor Dist
A.P, India.

Abstract:

As malware attacks become more frequent in mobile networks, deploying an efficient defense system to protect against infection and to help the infected nodes to recover is important to contain serious spreading and outbreaks. The technical challenges are that mobile devices are heterogeneous in terms of operating systems, and the malware can infect 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 optimal distribution of content-based signatures of malware to minimize the number of infected nodes, which can help to detect the corresponding malware and to disable further propagation.

We model the defense system with realistic assumptions addressing all the above challenges, which have not been addressed in previous analytical work. Based on the proposed framework of optimizing the system welfare utility through the signature allocation, we provide an encounter-based distributed algorithm based on Metropolis sampler. Through extensive simulations with both synthetic and real mobility traces, we show that the distributed algorithm achieves the optimal solution, and performs efficiently in realistic environments.

Keywords:

Heterogeneous Devices, Malware Attacks, Mobile Networks, MD5.

I. INTRODUCTION:

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 growing popular mobile networks, with a total count of known mobile malware instances of more than 350 reported in early 2007. This is mainly because of two reasons. One is the emergence of powerful mobile devices, such as the iPhone, Blackberry, and Android devices, and increasingly diversified mobile applications, such as Multimedia Messaging Service (MMS), mobile games and peer-to-peer file sharing. The other reason is the introduction of mobile Internet, which indirectly induces the malware.

Malware which traditionally resides 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 can be very serious, including deterioration of mobile device performance, excessive charges to mobile users due to excessive mobile data usage, and large scale network breakdowns caused by malware outbreak related issues [3]. Designing an efficient detection and defense system are necessary to prevent such large-scale outbreaks [4][5]; and it should be an urgent and high priority research agenda.

2. EXISTING SYSTEM:

Currently, mobile malware can propagate by using two different dominant approaches. Via MMS, a malware can 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 phone address books, and can spread very quickly without geographical limitations. The other approach is to use short range wireless media such as Bluetooth to infect the devices in proximity as "proximity malware". Recent work of [1] has investigated the proximity malware propagation features, and finds that it spreads slowly because of the human mobility, which offers ample opportunities to deploy a defense system. However, the approach for efficiently deploying such system is still an ongoing research issue. In this paper, we are the first to address the challenge of designing a defense system for both MMS and proximity malware. We introduce an optimal distributed solution to efficiently contain 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 the infected nodes to recover and prevent the healthy nodes from further infection. Typically, we should disseminate the content-based signatures of known malware to as many nodes as possible. The signature is obtained by using algorithms such as an MD5 hash over the malware content, and they are used by the mobile devices to detect various patterns in the malware and then to disable further propagation. Therefore, distributing these signatures into the whole network while avoiding unnecessary redundancy is our optimization goal. However, to address the above problem in a realistic mobile environment is challenging for several reasons. First, typically we cannot rely on centralized algorithms to distribute the signatures since the service infrastructure may not be always available.

For example the existing centralized schemes such as social patching and broadcast signature dissemination have to rely on service provider networks and hence cannot be used without infrastructure support. Therefore, a sensible way for signature distribution is to use a distributed and cooperative way among users. Second, mobile devices in general have limited resources, i.e., CPU, storage, and battery power. Although their storage and CPU capacity have been increasing rapidly recently, it is still very resource-limited compared to desktops. Hence, in the to-be-deployed defense system, we should adequately consider the limitation of resources, especially the memory capacity to store the defense software and signatures.

In this aspect, existing distributed malware coping schemes, such as signature flooding , which may exhaust the system resources and induce overhead cost, and CPMC , which does not take into account the resource limitation at all, are not practical for mobile networks.

Finally, the mobile devices are heterogeneous in terms of operating systems (OS), and different malware target different systems. This heterogeneous feature as well as the propagation via both local and global connectivity should be taken into consideration in the design of the defense system for real use.

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.

3. PROPOSED SYSTEM:

In this paper, we propose an optimal signature distribution scheme by considering the following realistic modeling assumptions, 1) the network contains heterogeneous devices as nodes, 2) different types of malware can only infect the targeted systems, and 3) the storage resource of each device for the defense system is limited. These assumptions are usually not addressed in previous analytical work for simplicity reasons. Our contributions are summarized as follows:

» 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.
» We give a centralized greedy algorithm for the signature distribution problem. We prove that the proposed greedy algorithm can obtain 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 . Through extensive real and synthetic-trace driven simulations, we show that our distributed algorithm approaches the optimal system performance.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

ADVANTAGES OF PROPOSED SYSTEM:

» The system provides optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware.
» The proposed system offers protection against both MMS based attack and Bluetooth based attack at the same time.

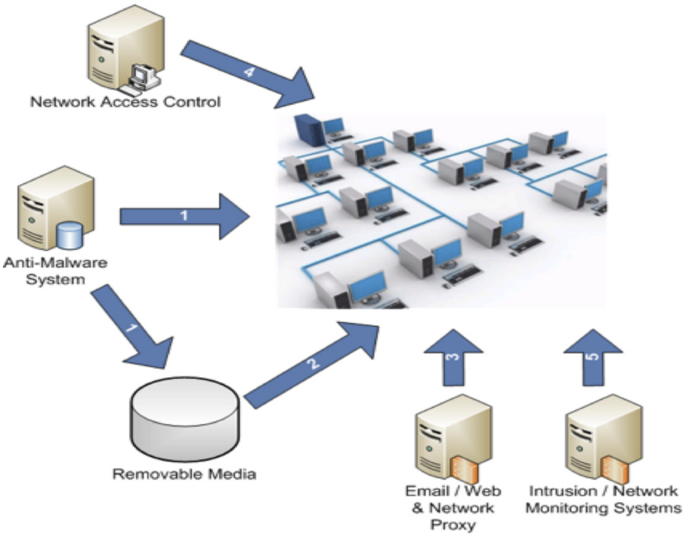

Network Access Control
Anti-Malware System
Removable Media
Email / Web & Network Proxy
Intrusion / Network Monitoring Systems
1
1
2
3
4
5

Fig.1: Proposed System Model

4. IMPLEMENTATION:

The framework of our proposed system has the accompanying modules alongside the following prerequisites.

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

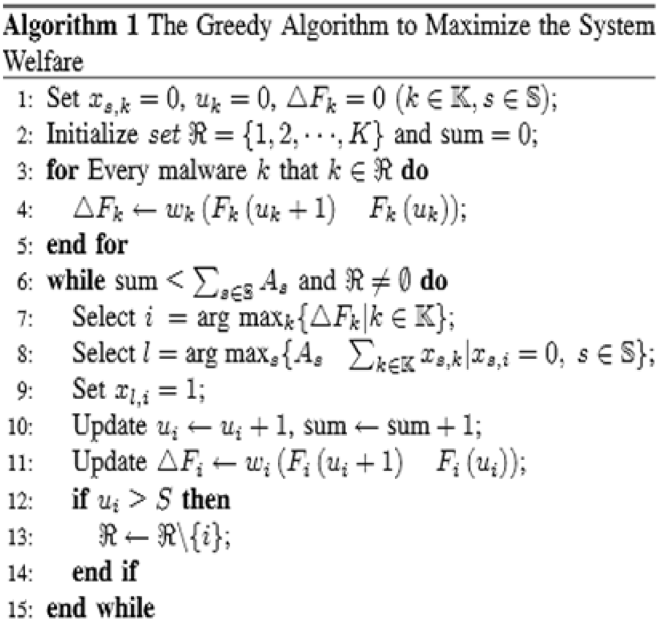
Malware signature finder and Spreading Model:

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:

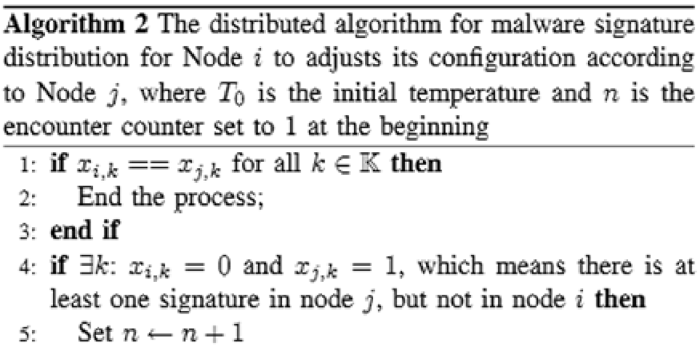
Based on the malware spreading model, we first formulate the problem, and then give a greedy algorithm to achieve the optimal signature distribution. Now, we validate the proposed malware spreading model expressed, which is based on the epidemic model for malware spreading and the fluid model in DTN. 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.

Algorithms Used are:



Algorithm 1 The Greedy Algorithm to Maximize the System Welfare

```
Set $x_{s,k} = 0$, $u_k = 0$, $\triangle F_k = 0$ $(k \in \mathbb{K}, s \in \mathbb{S})$;
Initialize set $\Re = \{1, 2, \cdots, K\}$ and sum $= 0$;
for Every malware $k$ that $k \in \Re$ do
    $\triangle F_k \leftarrow w_k (F_k (u_k + 1) \quad F_k (u_k))$;
end for
while sum $< \sum_{s \in \mathbb{S}} A_s$ and $\Re \neq \emptyset$ do
    Select $i = \arg\max_k \{\triangle F_k | k \in \mathbb{K}\}$;
    Select $l = \arg\max_s \{A_s \quad \sum_{k \in \mathbb{K}} x_{s,k} | x_{s,i} = 0, \ s \in \mathbb{S}\}$;
    Set $x_{l,i} = 1$;
    Update $u_i \leftarrow u_i + 1$, sum $\leftarrow$ sum $+ 1$;
    Update $\triangle F_i \leftarrow w_i (F_i (u_i + 1) \quad F_i (u_i))$;
    if $u_i > S$ then
        $\Re \leftarrow \Re \backslash \{i\}$;
    end if
end while
```



Algorithm 2 The distributed algorithm for malware signature distribution for Node i to adjusts its configuration according to Node j, where T_0 is the initial temperature and n is the encounter counter set to 1 at the beginning

```
if $x_{i,k} == x_{j,k}$ for all $k \in \mathbb{K}$ then
    End the process;
end if
if $\exists k$: $x_{i,k} = 0$ and $x_{j,k} = 1$, which means there is at
least one signature in node $j$, but not in node $i$ then
    Set $n \leftarrow n + 1$
    Select a signature $c$ from the buffer of user $i$ uniform randomly such that $x_{i,c} = 1$, and select a signature $c'$ from the buffer of user $j$ uniform randomly such that $x_{j,c'} = 1$ and $x_{i,c'} = 0$;
    Set the system temperature $T_n = \frac{T_0}{\log(n \; 1)}$
    Compute the acceptance probability $\alpha_{c',c}(T_n)$.
    Draw a random number $R$ uniform distributed in $(0, 1]$;
    if $R < \alpha_{c',c}(T_n)$ then
        User $i$ select signature of $c'$ and drop $c$ with probability of $\frac{1}{SK}\alpha_{c',c}(T_n)$
    end if
end if
```

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.

5. 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. At the same time, our work considers the case of OStargeting malware. Although most of the current existing malware is OS targeted, cross-OS malware will emerge and propagate in the near future.

How to efficiently deploy the defense system with the consideration of cross-OS malware is another important problem. We are continuing to cover these topics in the future work.

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.

ABOUT AUTHORS:

Sowmya.K is currently pursuing his master’s degree from Vemu Institute Of Technology, Pakala, Chittoor Dist, A.P, JNTUA in the department of Computer Science. His current interests include Computer Networks and Data Mining.

Mr. B. Rama Ganesh is currently working as Associate professor, HOD, Dept of CSE in Vemu institute of technology Pakala, Chittoor Dist, A.P, JNTUA. He received M.Tech degree from St. Mary’s college of Engineering; Hyderabad in 2009.He is currently doing his PhD work at Rayalaseema University, kurnool on subjects. His current interests include Computer Networks, Microprocessors and Computer architecture Multimedia Technology.