OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Malware Defense System within Mobile Networks

Sd. Lara[1], Sk. Nazeer Basha[2], B. Prathibha[3]

*(M. Tech, Department of Computer Science and Engineering, QUBA college of Engineering and Technology, Nellore, AP, India)

** (Assistant Professor, Department of Computer Science and Engineering, Nellore, AP, India)

*** (B. Tech, Department of Computer Science and Enigineerng, Atmakur Engineering college, Atmakur, Nellore, AP, India)

ABSTRACT: *The mobile web used for accessing the world wide web, i.e. the use of browser-based Internet services, from a handheld mobile device, such as a Smartphone or a feature phone, connected to a mobile network or other wireless network. Malware attacks can occur due to the mobile intent, Bluetooth devices and MMS (Multimedia Messaging Service). In this paper, we are going to present how the content based signature distributed among the mobile nodes which helps to detect and remove those malwares within the mobile devices. The system provides optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware.*

Keywords: *Malware, MMS, Bluetooth, Digital signature, Distribution.*

I. INTRODUCTION

Malwares attacks (I.e viruses, spam bots, worms, and other malicious software's) significantly large-scale internet to the increasing of popular mobile networks. This malwares can attack largely since of two reasons one is the appearance of powerful mobile devices, such as Iphones, android, and black berry devices, and more and more diversified mobile applications, such as multimedia messaging service (MMS), mobile games, and peer-to-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 effects of malware attacks on mobile users and service provided would be very serious. The Behaviors and damages of malwares on mobiles and should be understand and design an efficient detection and defenses system are necessary to prevent the large-scale of damages and this research is an urgent and high priority research agenda.

New mobile malware can spread through two different approaches. Via multimedia message services (MMS), a malware may attack to all systems whose numbers are found in the address book of the infected handset. This malware spreads very quickly without any limitations .In another way, by using short range wireless networks such as Bluetooth to infect the systems in proximity as "proximity malwares". In recent investigation the proximity malware propagation features were found.

To Design a defense system for both MMS and proximity malware. 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 propose an encounter-based distributed algorithm to disseminate the malware signatures using Metropolis sampler.

II. System Architecture

All the hosts are connected in network and this network contains network access control which acts as server. This network also contains Anti malware System which consists of malware signatures. All the host systems are connected through a centralized network. In this network systems consist of different Operating Systems. Malwares can move from one system to another system through Bluetooth and MMS.

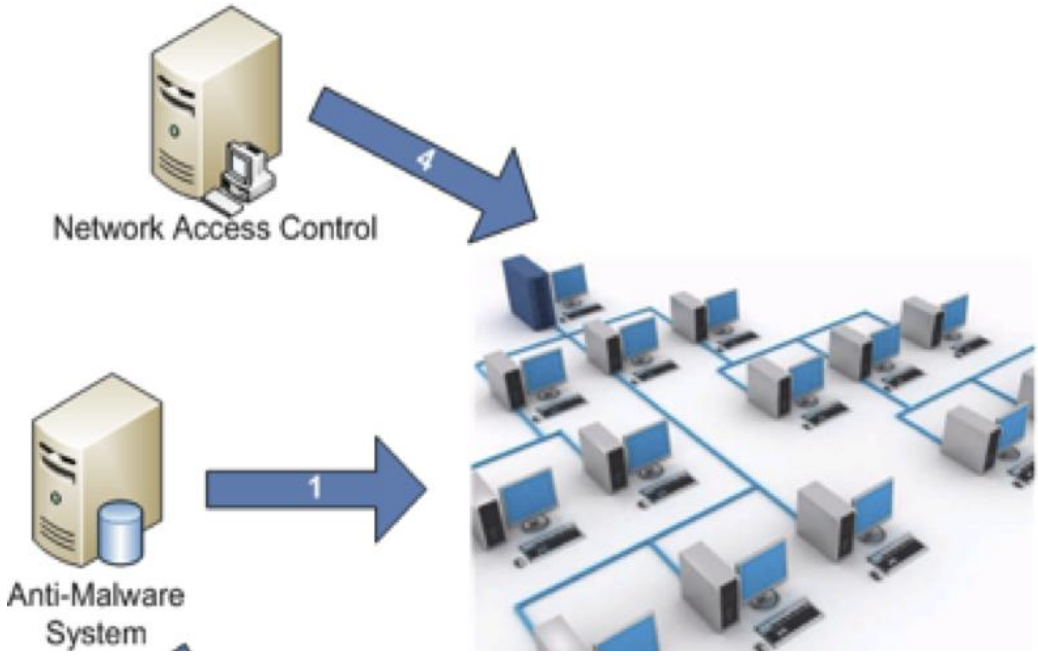

Fig.1.system architecture of hosts

Network Access Control acts as a server to the Host Network. It maintains the data of all the Hosts in the Network. It gives the accessing permissions to the system within the network and provides services to the systems. All the protocols and rules can be provided by access controller.

Anti-malware system defines digital signature .It distributes the digital signature to all the nodes in the network. Each and every malware should consist of unique digital signature .By using mapping techniques anti-malware system detects the malwares. After that malwares can be removed from the nodes.

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.

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. Second, mobile devices in general have limited resources, i.e., CPU, Storage, and battery power.

Although their storage and CPU capacity has been increasing rapidly, it is still very resource-limited compared with 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.

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

III. DATAFLOW WITHIN MOBILE NETWORKS

The mobile user has to register the mobile within the network with his own user name and password. After that the mobile user can login within the network by using his valid login id and password. If it is valid then he goes to memory booster otherwise it will display the login page.

Memory booster provides two services to users. One is running apps within the mobile; another one is killing running apps whenever it needs. After that it goes to check the battery information.

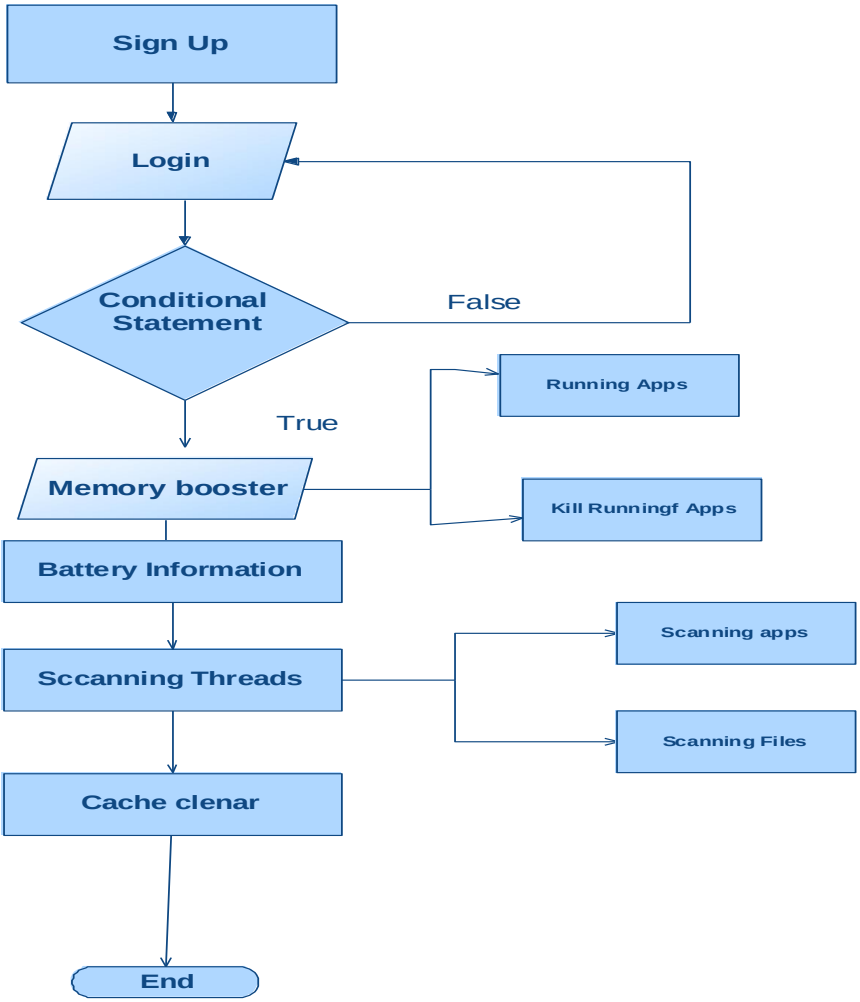

Fig.2. Data Flow Diagram

Battery information contains health, level, plugged, present, status, technology, temperature, voltage etc all the information was checked at the second stage that is battery information. Thus third stage was scanning threads.

Scanning threads identifies the junk files i.e, malware attacked files within the mobile nodes. In this stage malwares can be scanned and display the number of malware attacked files. Scanning threads will scans the apps and files. Then it goes to cache cleaner, in this section the malware attacked junk files are removed. Now the mobile nodes will free from malwares which are attacked through Bluetooth, and MMS based and mobile internet. Finally this application goes to logout.

All the above actions are performed in the data flow diagram are under the control of anti malware system.

IV. IMPLEMENTATION

Algorithm: The Greedy Algorithm to Maximize the System Welfare

1: Set xs;k = 0, uk = 0, ΔFk = 0(k € IK,s€S);
2: Initialize set R={1; 2; . . .;K} and sum =0;
3: for Every malware k that k € R do
4: ΔFk <−wk(Fk(uk + 1) – Fk(uk));
5: end for
6: while sum ≤∑s€S As and R≠ do
7: Select i ¼=arg maxk{ΔFk|k € IK};
8: Select l = arg maxs{As -∑k€IR xs;k|xs;i ¼=0, s € S};
9: Set xl;i =1;
10: Update ui<− ui + 1, sum <−sum + 1;
11: Update ΔFi <−wi(Fi(ui + 1)- Fi(ui));
12: if ui ≥ S then

13: R−>R\{i};
14: end if
15: end while

The above greedy algorithm we identify the number of malwares and the types of malwares can be attacked to the mobile nodes. In this algorithm we check step by step total number of malwares attacked through bluetooth,MMs etc.

1: if xi;k ==xj;k for all k € IK then
2: End the process;
3: end if
4: if k: xi;k = 0 and xj;k = 1, which means there is at least one signature existing in node j, but does not exist in node i then
5: Set n ←n +1
6: Select a signature c from the buffer of user i uniform randomly such that xi;c = 1, and select a signature c0 from the buffer of user j uniform randomly such that xj;c0 = 1 and xi;c0 = 0;
7: Set the system temperature Tn = T0⁄Log(n_1);
8: Compute the acceptance probability _c0;c(Tn);
9: Draw a random number R uniform distributed in (0; 1];
10: if R < c0;c(Tn) then
11: User i selects signature of c0 and drops c with probability of 1/SK _c0;c(Tn);
12: end if
13: end if

In the above distributed algorithm the malwares which are identified the signatures was distributed. Here we check probability& temperature of a corresponding malware node by using this we can remove the malware.

TABLE 1
List of Commonly Used Variables Throughout the Paper

Variable	*Description*
N	Number of wireless nodes in the system
$\mathbb{K}$	Malware set, which includes K types
K	Number of the types of malware
v_k	Maximum number of nodes that malware k can infect
v_k^0	Number of infected nodes infected by malware k at the starting time
$x_{s,k}$	Indicator whether helper s has the signature to prevent malware k
A_s	Maximum number of signatures that can be stored at helper s
u_k	Number of helpers for malware k
h_k	Number of infected nodes by malware k in the system at time L
$\zeta_k(t)$	Number of infected nodes by malware k in the system at time t
λ_{k1}	Spreading rate of malware k
λ_{k2}	Recovering rate of malware k,
L	Final system time used to count the number of infected nodes in the network
$F_k(x)$	System utility function for defending malware k, introduced in Section III-A
w_k	System welfare factor to weight system contributions of defending malware k, introduced in Section III-C
T	Parameter in Gibbs ditribution named system temperature used in Algorithm 2 of Section IV

V. RESULT ANALYSIS

Here we have one mobile with our malware defense and removing software. After the installation it will appear on the screen. We can use this software with the authentication of server system. The mobile user has to register his details within server, after that he can get the username and system generated software.

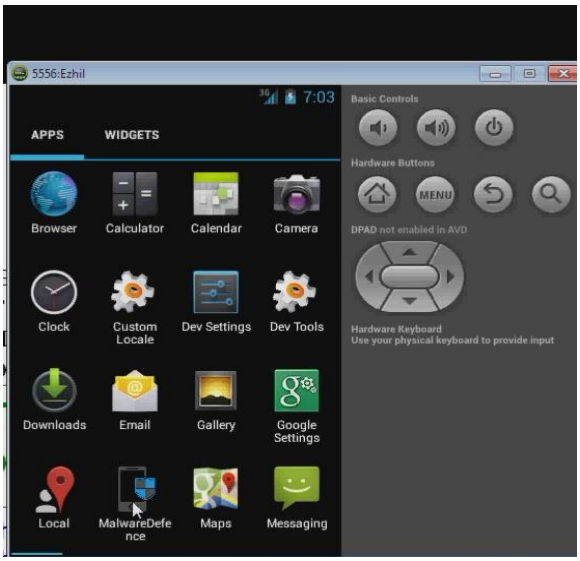

Fig.3.Screen shot 1

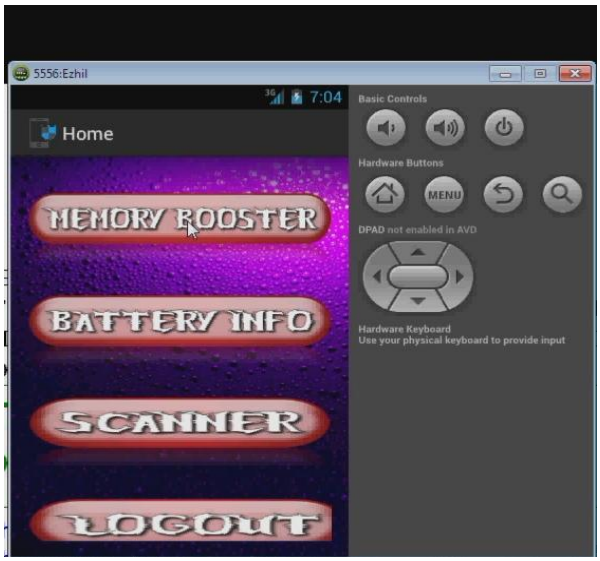

Fig.4. Screen shot2

Sreen shot 1 consist of of the software shortcut , after the completion of login process user get the screen like screen shot 2. It consist of Memory Booster,Battery Info,Scanner and logout. All those modules are present at the home page of the system. By using those four modules we can detect and remove the malwares which present at our system. The malware signature will send to the each and evry system which present at the network.

Fig.5.Screen shot 4

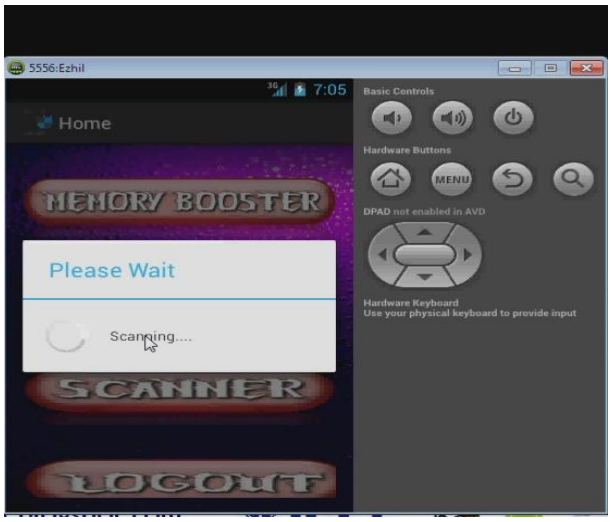

Fig.6.Screen shot 5

Screen shot 4 consist of information about the battery left within the mobile device and screen shot 5 consist of scanner which scans the malwares through the digital signature. It takes some time to find out malwares and gives the details about the malwares which present at the screen shot 6. The user can remove the malwares by selecting remove all button which is present at screen shot 7. Finally we can defend our mobile with the malware attacks which are raised at the networking.

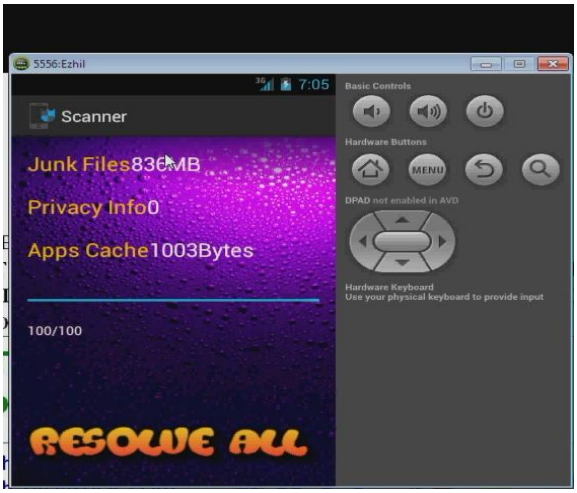

Fig.7.Screen shot 6

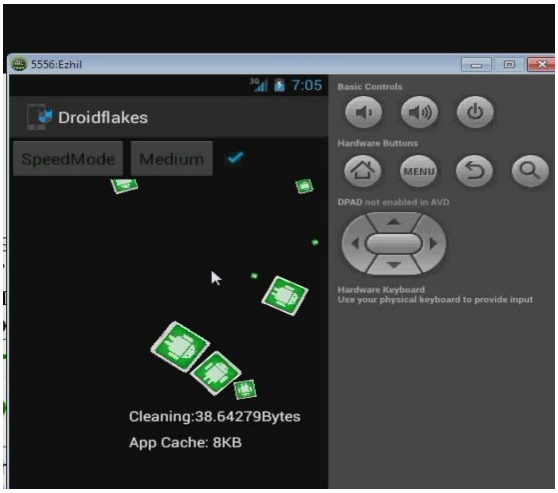

Fig.8.Screen shot 7

REFFERENCES

[1]. Yong Li, Pan hul, depeng jin, Lisu and Lieguang Zeng, "optimal distributed malware defense in mobile networks with heterogeneous devices", IEEE transactions on mobile computing, VOL.13, NO.2, February 2014.

[2]. 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.

[3]. M. Hypponen, "Mobile Malwar," Proc. 16th USENIX SecuritySymp., 2007.

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

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