An Improved the Optimal Distributed Dummy Signature for Malicious Software in Mobile Network

Ashvini Bhatkal
Computer Engineering Department, Savitribai Phule Pune University,
Dhole Patil College of Engineering,
Wagholi, Pune

R.N. Phursule
Computer Engineering Department,
Savitribai Phule
Pune University
JSPM's Imperial College Engineering & Research,
Wagholi, Pune

ABSTRACT
Now a day the world is mobile and internet oriented, each and every person must have the both of things. While in using the mobile and internet we have to face many problems such as malware attacks in while in sending and receiving message. We consider a malware attack in sending an MMS and Bluetooth. We found many problems while sending message we used distributed algorithm and dummy signature to protect the message from malware [3].In mobile network malware attacks frequently occur while sending and receiving information [2]. Develop an efficient system to protect infection and infected nodes to recover and produce dummy signature to overcome of spreading and outbreaks of malware [1]. We found that the problem is how to optimally distribute content- based signature of malware, that help to detect malware and disable further propagation to minimize the no of infected nodes[4]. we can go through two different approaches 1. MMS 2. Bluetooth. In MMS a malware send a copy of itself to all devices whose numbers are found in address book of infected device. We use optimal distributed solution to efficiently avoid malware spreading and apply dummy signature to help infected nodes to recover [1].

Keywords
distributed algorithm, heterogeneous mobile networks, mobile malware, Security threat

1. INTRODUCTION
The mobile and Internet is most important now a days. All people in world having their own mobile and internet, while using the mobile and internet many security problems arise. Sending and receiving message from sender to receiver many warms, viruses attacked . following malware attacks like spam, worms, bots, virus and many malicious software. The rapidly growth of mobile network , more malware are produces. Many reasons of malware attack in mobile network such as " the powerful mobile devices like iphone , blackberry devices, android phones, and mobile applications rapidly increases like MMS , mobile games , file sharing", "the indirectly produces the malware" .Malware effect on mobile users and service providers are very dangerous and critical. Design the efficient and effective detection and defense system to reduce the malware attacks. following are the mobile malware 1. Bluetooth 2. MMS. The Bluetooth is an short range wireless media of proximity malware , it spread slowly because of limited range. Second is MMS , In MMS malware can send one copy of itself to all mobiles whose numbers are in address book of infected handset and that malware find out the address book and spread in network quickly , they have no any geographical limitations. We introduce an optimal distribution solution and dummy signature to avoid malware or repair the infected nodes. The mobile network have many nodes some of them are infected by malware we have to develop efficient defense system to recover the infected nodes and provide healthy nodes. The mobile devices have limited resources such as CPU , memory and battery. The storage capacity and CPU has been increases rapidly . the different systems are attacked by different malware , there is number of systems are present and malware also have different . while in designing and developing the system we have to consider the global and local connectivity.

We propose an optimal signature distribution for network contain heterogeneous devices as a node, distribute the signature and dummy signature to recover the infected nodes as a healthy node and send message.

2. OBJECTIVES OF THE RESEARCH
To craete the network and create the helper node.

To distribute Signature

To Apply dummy signature

Analysis malware and encounter

3. RELATED WORK
Optimal distributed signature have the problem with heterogeneity of mobile device and malware .The proposed system is used for MMS and Bluetooth. Distribute signature apply greedy algorithm for signature creation purpose and for creating dummy signature use MD5 and RSA algorithm .The proposed system find out the malware that is verify and validate the malware by applying dummy signature.

4. LITERATURE SURVEY
MHR Khouzani, S. Sarkar, Eitan Altman [1] has proposed the a framework for identifying intelligent defense strategies that can limit the damage by appropriately selecting network parameters. The propagation of malware in a battery-constrained mobile wireless network by an epidemic model in which the worm can dynamically control the rate at which it kills the infected node and also the transmission range and/or the media scanning rate. At each moment of time, the worm at each node faces the following trade-offs: (i) using larger transmission range and media scanning rate to accelerate its spread at the cost of exhausting the battery and thereby reducing the overall infection propagation rate in the long run or (ii) killing the node to inflict a large cost on the network, however at the expense of loosing the chance of infecting more susceptible nodes at later times. We mathematically formulate the decision problems and utilize Pontryagin

Maximum Principle from optimal control theory to quantify the damage that the malware can inflict on the network by deploying optimum decision rules. Next, we establish structural properties of the optimal strategy of the attacker over time. Specifically, we prove that it is optimal for the attacker to defer killing of the infective nodes in the propagation phase for a certain time and then start the slaughter with maximum effort. We also show that in the optimal attack policy, the battery resources are used according to a decreasing function of time, i.e., mostly during the initial phase of the outbreak.

1) Dynamics of State Evolution- A susceptible node is a mobile wireless device which is not contaminated by the worm, but is prone to infection
2) Maximum Damage Attack- An attack can benefit over time from the infected hosts, by using the worms to (i) eavesdrop and analyze traffic that is generated or relayed by the infected hosts, or the traffic that traverses in the hosts' vicinity, and (ii) alter or destroy the traffic that is generated or relayed by the infected hosts. An attacker also benefits by inflicting a large death-toll by the end of the desired time window.

Zhichao Zhu , Guohong Cao, Sencun Zhu , Supranamaya Ranjan and Antonio Nucci [2] has proposed a social network based patching scheme for worm in cellular network. cellular networks may witness a similar evolution of worms as has been seen in the wired world. Further, mobile worms could impose unwarranted bandwidth charges to customers, deterioration in quality of service, and ultimately loss of revenue for service providers.The usual ways for mobile worms to propagate include Bluetooth interface and Multimedia Messaging Service (MMS) interface. One Bluetooth based mobile worm is Cabir , which can spread through Bluetooth connection to other Bluetooth-enabled devices it can find. As its name suggests, MMS messages are intended to contain media content such as photos, audios or videos, but they can also contain infected malicious codes. Due to characteristics of slow start and exponential propagation exhibited by mobile worms, it is challenging to detect a worm outbreak at the early stage while it is hard to mitigate it at a later stage. However, even if network operators are unable to detect a worm propagation during the earliest stage, they still have a window of opportunity to react before the worm spreads to a larger population. This is especially true in mobile worm in which user interactions are required to download and install the malicious files on mobile devices. Balanced Graph Partitioning- the significance level of each partition should be similar so that the worm damage to each partition can be balanced. As mentioned before, vertex weight and edge weight can be viewed as metrics for significance level. The vertex degree denotes how many victims an infected mobile is able to reach while the edge weight represents the probability that worms can propagate through this link successfully. Clustered Graph Partitioning- Balanced graph partitioning tries to maintain the significance level inach partition balanced, so that the damage to each partition is balanced and limited. However, it does not

give high priority to minimize the edge-cut, therefore does not guarantee that worms can always be successfully contained within individual partitions.

Gjergji Zyba, Geoffrey M. Voelker[3] has proposed defending mobile phones from proximity malware . we consider the dynamics of mobile phone malware that propagates by proximity contact, and we evaluate 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 . Unlike malware that propagates using the network, where the provider can employ centralized defenses, proximity malware can propagate in an entirely distributed fashion. In this paper we consider the dynamics of mobile phone malware that propagates by proximity contact, and we evaluate potential defenses against it. Defending against proximity malware is particularly challenging since it is difficult to piece together global dynamics from just pair-wise device interactions. Whereas traditional network defenses depend upon observing aggregated network activity to detect correlated or anomalous behavior, proximity malware detection must begin at the device. As a result, we explore three strategies for detecting and mitigating proximity malware that span the spectrum from simple local detection to a globally coordinated defense .

P. Wang, M. Gonzalez, C. Hidalgo, and A. Barabasi [4] has proposed understanding the spreading patterns of mobile phone viruses. The two common data transfer mediums Bluetooth & MMS is used to transmit the virus. The damage caused to one who owns the device will be the loss of vital information stored in the mobile. The virus transmits infected files to people in your address book and recent call history. Steal important information saved in the mobile like Bank PIN, user logon credentials. The virus can disable your basic mobile phone functions like prohibiting you to use Short Messaging Service, Camera, games etc. It can also make your mobile completely disable. It also prevents you from installing antiviral software, lock your memory card, Use up more phone battery than usual.

5. PROPOSED WORK

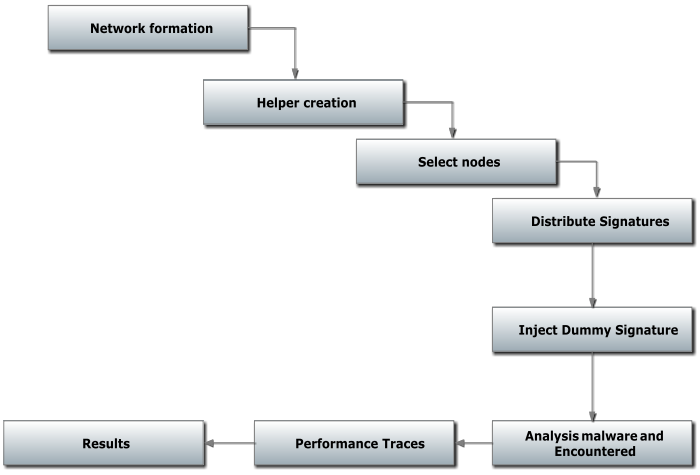

Fig 1. System Architecture

Fig 1. illustrate architecture of proposed system. The entire system is based upon comparative analysis between existing and proposed system. Create a mobile networks including a number of nodes. First defined number of nodes and also defined source node, destination node, intermediate nodes. The network contains heterogeneous devices as nodes. Mobile nodes are more efficient to disseminate content and information in the network. Helper nodes are referred to as

special nodes. This node is used to focusing the all nodes. Helper node is intermediate node for every nodes in the network. File can be transmit from source node to destination node through the help of helpers node. At the Same time special node of a helper node generate the signatures. This signatures are content-based signatures .This module is used to analyzing the malware nodes through passing the signatures. All intermediate nodes received a content based signatures. This signatures distributed for every intermediate node from source node to destination node with the help of the special node. The special node is the helper node. Apply greedy algorithm for generate the signature file and key file for the related content. Helper node distribute the signatures for every intermediate nodes based on the file contents key will be generated. And apply dummy signature for providing more security. We can used MD5 and RSA algorithm for dummy signature. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the surnames of Ron Rivest. MD5 Algorithm The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. Detect the malware with the help of a content based signatures. Exponential parameter obtained from the contact records between helpers and general nodes. Every intermediate node receive the signatures from helper node and which intermediate nodes receiving the signatures twice. Apply delay tolerant network technique to identify the malware nodes in the mobile networks. This time to detecting the malware spreading nodes and recovering the infected nodes. Simulate the malware spreading, and compare the simulation results of infected ratio with that obtained by the model. The number of infected nodes increases with the

growth of spreading rate can observe that the number of infected nodes decreases with the increase of recovering rate. For proximity malware propagation, we use both realistic mobility trace and synthetic trace for simulations. This modules determining the malware spreading time and malware recovering time will be calculated using the signatures receive traces.

6. MATHEMATICAL MODEL AND ALGORITHM

Input: Consider `n` number of user who are creator, reader and writer

C=ABE.Encrypt (MSG, χ)
Process: Sharing and accessing the data with secure manner.

Given plaintext are converted into ciphertext which is encrypted form of data
Output: privacy provided to data and securing the process
C=ABE.Encrypt (MSG, χ)
WHERE,
C=Cipher text,
ABE=Encryption
MSG=message (data)

X=access structure

Steps

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.

1) INPUT

- The input is a 64-bit data element, x

2) PROCESS

- Divide x into two 32-bit halves: xL, xR.
- Then, for i = 1 to 16:
  - xL = xL XOR Pi
  - xR = F(xL) XOR xR
  - Swap xL and xR
- After the sixteenth round, swap xL and xR again to undo the last swap.

3) OUTPUT

- Encryption uses a large number of sub keys. These keys must be pre computed before any data encryption or decryption.
- Ciphertext (C) is produced in result.

4) Input: Number of nodes, digital signature

Output: Malicious Nodes

Process: Inject dummy signature to malware nodes

```
For(number of nodes){
If(digitalsignature)Mismatches(dum  my signature))
    {
        Message("Malware Nodes are found");
}
```

7. RESULTS OF PRACTICAL WORK

The work done results are as shown in figures given below. Figure 2 shows the output screen for nodes creation of the network

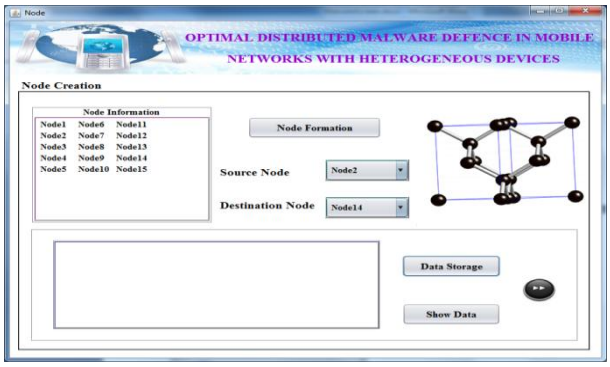

Figure 2 shows the selection of message type

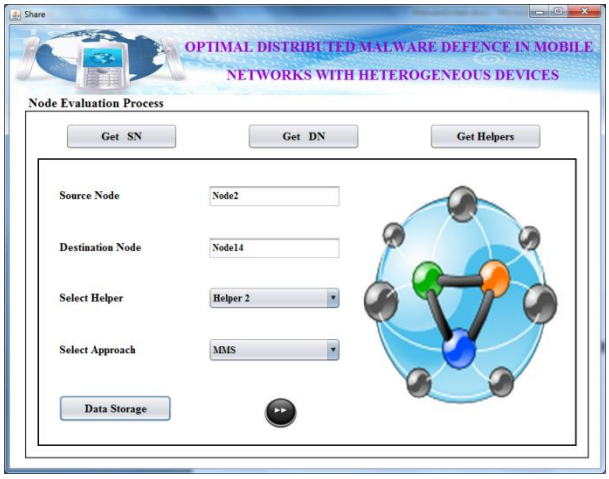

Figure 3. shows the creation of signature and send file

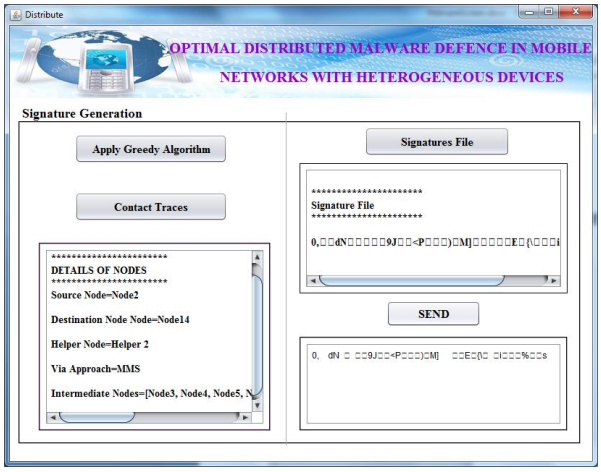

Figure 4. shows the creation of dummy signature

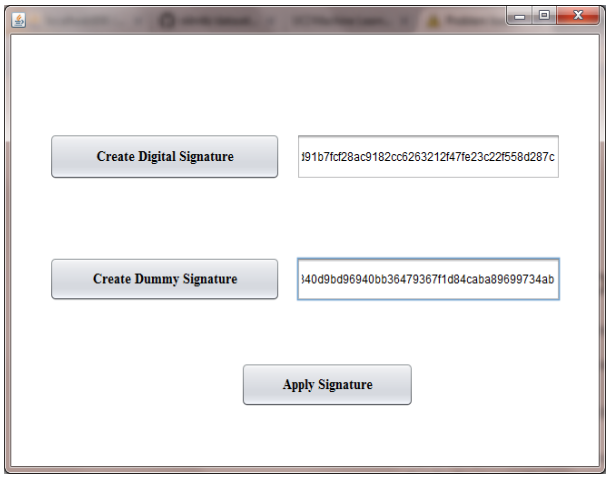

Figure 5. Performance Trace

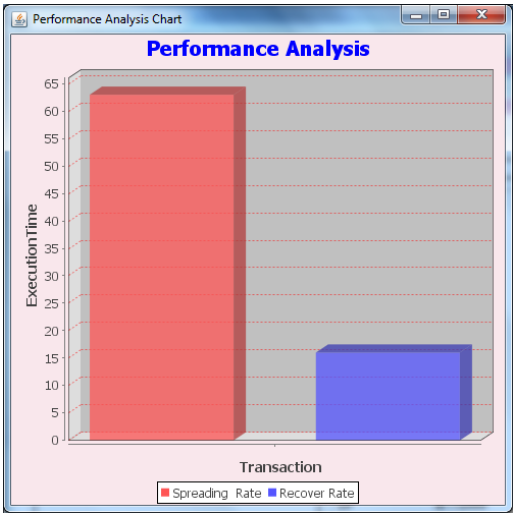

Figure 6. Performance Analysis

8. ACKNOWLEDGMENTS

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my work successfully. I express my gratitude towards project guide Prof. Rajesh Phursule and Head, Department of Computer Engineering, Dhole Patil College Of Engineering, Wagholi, Pune who guided work in scheduled time.

I would like to thanks our Principal Dr. S. B. Allampallewar, for allowing us to pursue my project in this institute.
I also thanks to ME Project Head,and our PG Coordinator for their guidance and for being a constant source of support.

9. CONCLUSIONS

The problems of optimal signature distribution of mobile network against the proximity and mms malware ,The distributed algorithm closely approaches to the optimal system performance of a centralized solutions. Some malicious nodes produces the dummy signature targeting no malware in network so use denial of service attack to the defense system. Considered the security and authentication mechanism considered, the OS targeting malware .Can efficiently deploy the defense system with cross-OS malware . The proposed system send the message without malware for that crate the network and creation of helper node , then set the destination and source node and helper node for sending purpose. Generate the signature and apply greedy algorithm and AES algorithm for distribute signature and dummy signature for avoid duplication of signature file . Select which file is to be send and apply signature and trace whether the malware is found or not. If malware found remove it and send message to destination without malware.

The proposed system is form the network first and create no of helper node , after that assign the helper id to the node for sending message. Evaluate the intermediate node that shows how many node are between source and destination.

In proposed system enter the source node , destination node , helper node and select approach that is which type of data we have to send select it. Which file you have to send select that file and display the file content . In proposed system apply greedy algorithm for signature generation and create signature file and send the signature.

In proposed system the dummy signature for more security and reliability purpose . In dummy signature the MD5 and

RSA algorithm is used . In malware detection and encounter firstly , detect the malware if found or not ,if found then encounter and send data to the destination . In proposed system malware encounter nodes also display, which node contain malware that display into the list so it is easy to remove malware from that particular malware.

In proposed system trace the performance on the basis of showing all the information like sender node , destination node , helper node , intermediate node, which approach you used for sending the file, malware attacked node.

The proposed system is compare with existing system in terms of dummy signature for providing more security and reliability for sending message. Existing system only verifies that malware in present , proposed system is verified and validate that malware and send data to the destination. Our 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 , we take the heterogeneity of devices into account in deploying the system and consider the system resource limitations. 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 OS-targeting 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.

10. REFERENCES

[1] "Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices"

[2] Yong Li, Member, IEEE, Pan Hui , Member, IEEE, Depeng Jin, Member, IEEE, Li Su, and Lieguang Zeng, Member, IEEE

[3] 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.

[4] M. Hypponen, "Mobile Malware," Proc. 16th USENIX Security Symp. , 2007.

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

[6] M. Khouzani , S . Sarkar , and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," Proc. IEEE INFOCOM, 2010. 390 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2, FEBRUARY 2014

[7] 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.

[8] G. Zyba , G. Voelker, M. Liljenstam, A. Mahesh, and P. Johansson, "Defending Mobile Phones from Proximity Malware," Proc. IEEEINFOCOM, 2009

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

[10] P. Bremaud, Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues. Springer Verlag, 1999.

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