RESEARCH ARTICLE OPEN ACCESS

A Study on Behavioural Malware Detection by Using Delay Tolerant Networks

K.Ravikumar [1], V. Vinothkumar[2]

[1](Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu),Thanjavur)

[2] (Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur.)

----------**********----------

Abstract:

The delay-tolerant-network (DTN) model is becoming a via communication alternative to the traditional infrastructural model for modern mobile consumer electronics equipped with short-range communication technologies such as Bluetooth, NFC, and Wi-Fi Direct. Proximity malware is a class of malware that exploits the opportunistic contacts and distributed nature of DTNs for propagation. Behavioral characterization of malware is an effective alternative to pattern attaching in detecting malware, especially when dealing with polymorphic or obfuscated malware. In this paper, we first propose a general behavioral characterization of proximity malware which based on Naive Bayesian model. We identify two unique challenges for extending Bayesian malware detection to DTNs and propose a simple yet effective method, look-ahead, to address the challenges. Furthermore, we propose two extensions to look-ahead, dogmatic filtering and adaptive look-ahead, to address the challenge of "malicious nodes sharing false evidence". Real mobile network traces are used to verify the effectiveness of the proposed methods.

Keywords **— DTN,WiFi.**

----------**********----------

I. INTRODUCTION

A delay-tolerant network is a network designed to operate effectively over extreme distances such as those encountered in space communications or on an interplanetary scale. In such an environment, long latency -- sometimes measured in hours or days -- is inevitable.

The popularity of mobile consumer electronics, like laptop computers, PDAs, and more recently and prominently, smart phones, revives the delay-tolerant-network (DTN) model as an alternative to the traditional infrastructure model.

The widespread adoption of these devices, coupled with strong economic incentives, induces a class of malware that specifically targets DTNs. We call this class of malware proximity malware. Proximity malware based on the DTN model brings unique security challenges that are not present in the infrastructure model. In the infrastructure model, the cellular carrier centrally monitors networks for abnormalities moreover the resource scarcity of individual nodes limits the rate of malware propagation.

A prerequisite to defending against proximity malware is to detect it. In this paper, we consider a general behavioural characterization of proximity malware. Behavioural characterization, in terms of system call and program flow, has been previously proposed as an effective alternative to pattern matching for malware detection. In our model, malware-infected nodes behaviours are observed by others during their multiple opportunistic encounters: Individual observations may be imperfect, but abnormal behaviours of infected nodes are identifiable in the long-run.

1.1.OBJECTIVE

Network is the combination of Nodes. Each node will communicate with its neighbors and share their data. If a node is affected by a malware it's necessary to clear it else its neighbors will communicate with it and they also affected by

malware. Hence detection of malware is important. Here we discuss some methods for the detection of malware.

2. EXISTING SYSTEM

Previous researches quantify the threat of proximity malware attack and demonstrate the possibility of launching such an attack, which is confirmed by recent reports on hijacking hotel Wi-Fi hotspots for drive-by malware attack.

With the adoption of new short-range communication technologies such as NFC and Wi-Fi Direct that facilitate spontaneous bulk data transfer between spatially proximate mobile devices, the threat of proximity malware is becoming more realistic and relevant than ever. Proximity malware based on the DTN model brings unique security challenges that are not present in the model.

2.1. EXISTING SYSTEM DISADVANTAGES

- Central monitoring and resource limits are absent in the DTN model.
- Very risk to collecting evidence and also having insufficient evidence.
- It is filter the false evidence in sequentially and distributed.

3. PROPOSED SYSTEM

Behavioral characterization, in terms of system call and program flow, has been previously proposed as an effective alternative to pattern matching for malware detection. In our model, malware-infected nodes' behaviors are observed by others during their multiple opportunistic encounters: Individual observations may be imperfect, but abnormal behaviors of infected nodes are identifiable in the long-run. We identify challenges for extending Bayesian malware detection to DTNs, and propose a simple yet effective method, look-ahead, to address the challenges. Furthermore, we propose two extensions to look-ahead, dogmatic filtering and adaptive look-ahead, to address the challenge of "malicious nodes sharing false evidence".

3.1. PROPOSED SYSTEM ADVANTAGES

- Real mobile network traces are used to verify the effectiveness of the proposed methods.
- The proposed evidence consolidation strategies in minimizing the negative impact of liars on the shared evidence's quality.
- It is used to identify the abnormal behaviors of infected nodes in the long-run.

3.2.PROPOSED TECHINQUES

Proximity malware is a malicious program that disrupts the host node's normal function and has a chance of duplicating itself to other nodes during (opportunistic) contact opportunities between nodes in the DTN. When duplication occurs, the other node is infected with the malware. We present a general behavioral characterization of proximity malware, which captures the functional but imperfect nature in detecting proximity malware.

Under the behavioral malware characterization, and with a simple cut-off malware containment strategy, we formulate the malware detection process as a distributed decision problem. We analyze the risk associated with the decision, and design a simple, yet effective, strategy, look-ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection.

We present two alternative techniques, dogmatic filtering and adaptive look-ahead, that naturally extend look-ahead to consolidate evidence provided by others, while containing the negative effect of false evidence. A nice property of the proposed evidence consolidation methods is that the results will not worsen even if liars are the majority in the neighborhood

3. METHODOLOGIES

Methodologies are the process of analyzing the principles or procedure for behavioral characterizing of node with two methods, dogmatic filtering and adaptive look-ahead, for consolidating evidence provided by other nodes, while containing the negative impact of liars in delay tolerant network.

3.1.ADVANTAGES

- Real mobile network traces are used to verify the effectiveness of the proposed methods.
- The proposed evidence consolidation strategies in minimizing the negative impact of liars on the shared evidence's quality.
- It is used to identify the abnormal behaviors of infected nodes in the long-run.

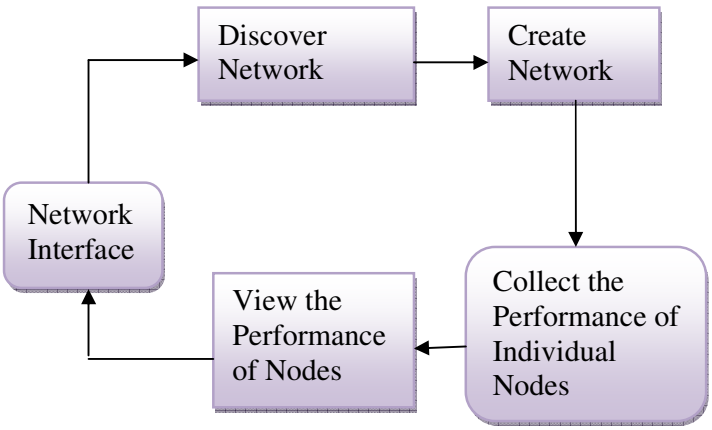
MODULES

I.Authentication
II.Network Nodes
III.Malware Detection
IV.Evidence Analysis
V.Evil Node Revocation

3.2.MODULE DESCRIPTION

Authentication

If you are the new user going to consume the service then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself..



Network Nodes

Under this module, the network nodes which are interconnected by local area network, that node ip address will be fetched in order to share the resources among the network. As well as the performance of individual system have been analyzed to assess the behavior

Malware Detection

Malware detection module helps to identify the evil node which is affected by malware program

Evidence Analysis

This module used to investigate about evidences of nodes by collecting assessments before a normal node get affected by malware program. Evidence aging process helps to discard outdated assessments of a node and evidence consolidation helps to filter negative assessments of a node provided by the other nodes.

Evil Node Revocation

After detection of evil node, we need to drop the communication with that in order to prevent from malware spreading and the evil node details are transferred to database for further reference. Finally evil node gets revoked from the network computer list.

4.CONCLUSION

Our system proposes a general behavioral characterization of DTN-based proximity malware. We present dogmatic filtering and adaptive look-ahead technique to address two unique problems "insufficient evidence vs. evidence collection risk" and "filtering false evidence sequentially and distributed".

5.REFERENCES

1.Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng, "An optimal distributed malware defense system for mobile networks with heterogeneous devices," in Proc. IEEE SECON, 2011.

2. D. Dash, B. Kveton, J. Agosta, E. Schooler, J. Chandrashekar, A. Bachrach, and A. Newman, "When gossip is good: Distributed probabilistic

inference for detection of slow network intrusions," in Proc. AI, 2006.

3. F. Li, Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in Smartphone-based mobile networks," in Proc. IEEE INFOCOM, 2010.

4. U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering," in Proc. IEEE NDSS, 2009.

5. J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, and A. Goel, "A preliminary investigation of worm infections in a bluetooth environment," in Proc. ACM WORM, 2006.

6. S. Cheng, W. Ao, P. Chen, and K. Chen, "On modeling malware propagation in generalized social networks," IEEE Comm. Lett., vol. 15, no. 1, pp. 25–27, 2011.

7. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks." in Proc. ACM WWW, 2003.

8. A. Bose and K. Shin, "On mobile viruses exploiting messaging and bluetooth services," in Proc. IEEE SecureComm, 2006.