International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

A NEW MECHANISAM IN PROXIMITY MALWARE IN DELAY TOLERANT NETWORKS

NAGOORVALI SHAIK[#1], GUNTAPALLI MINNI [*2]and SAYEED YASIN[*3]

[#] *Student, M.Tech (C.S.E), Nimra College of Engineering & Technology, A.P., India.*

[*2]*Assistant professor , Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

[*3]*Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— Mobile consumer electronics permeate our lives. Laptop computers, PDAs, and more recently and prominently, smart phones, are becoming indispensable tools for our academic, professional, and entertainment needs. With the universal presence of these short-range connectivity technologies, the communication paradigm, identified by the networking research community under the umbrella term Delay-tolerant Networks (DTNs), is becoming a viable alternative to the traditional infrastructural paradigm.The delay-tolerant-network (DTN) model is becoming a viable 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 matching 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, which has been successfully applied in non-DTN settings such as filtering email spams and detecting bonnets. We identify two unique challenges for extending Bayesian malware detection to DTNs ("insufficient evidence vs. evidence collection risk" and "filtering false evidence sequentially and distributedly"), 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.**

***Index Terms*— proximity malware, behavioral malware characterization, Bayesian filtering, delay-tolerant networks.**

I. INTRODUCTION

The popularity of new mobile devices (e.g., smart phones), the adoption of common platforms (e.g., Android),and the economic incentive to spread malware (e.g., spam) combinedly exacerbate the malware problem in DTNs. Malware is a piece of malicious code which disrupts the host node's functionality and duplicates and propagates itself to other nodes via contact opportunities. In the traditional infrastructural model, the carrier serves as a gatekeeper who can centrally monitor network abnormalities and inhibit malware propagation; moreover, the resource bottleneck for individual nodes naturally limits the impact of the malware. However, the central gatekeeper and natural limitations are absent in the DTN model. Proximity malware, which exploits the temporal dimension and distributed nature of DTNs in self-propagation, poses serious threats to users of new technologies and challenges to the networking and security research community. A common malware detection method currently in practice is pattern matching. More concretely, a sample of malware is first reported by an infected user. The sample is analyzed by security specialists, and a pattern which(hopefully) uniquely identifies the malware is extracted; the pattern can be either code or data, binary or textual. The pattern is then used for the detection of malware1. The extension to Naïve Bayesian model has been applied in filtering email spams, detecting botnets and address two DTN specific malware related problems. 1. Insufficient evidence versus evidence collection risk: In DTNs, when nodes come into contact, then only evidence such as Bluetooth connection or SSH session requests is collected. But there is always a risk of infection because of carriage of contacting malware infected nodes. Hence, nodes must take decisions whether to cut off the communication with other nodes and, if so, when. 2. Filtering false evidence sequentially and distributedly: Sharing evidence with opportunistic cognizant helps in reducing the above mentioned problem of insufficient evidence; ho wever, untrue evidence shared by malicious nodes may negate the benefits of sharing. In DTNs, nodes are supposed to decide whether to accept received evidence sequentially and distributedly. The following are the contributions: 1. The characterization of general behavior of proximity malware, which captures the functional but imperfect nature in detection of proximity malware 2. The malware detection process is formulated as a distributed decision problem based on a simple cutoff malware containment strategy. DTN consisting of n nodes where the nearby nodes are the nodes it has contact opportunities with.

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. In this model, it is assumed that, after each encounter each node is capable of assessing the other party for suspicious actions, resulting in a binary assessment. A node is either evil or good, based on it's infection by the malware. The assessment of suspicious action is assumed to be an imperfect but functional indicator of malware infections: It may sometimes judge an evil node's actions as "non suspicious" or agood node's actions as "suspicious," but most suspicious actions are correctly attributed to evil nodes. The functional assumption characterizes a malware infected node by the assessments of its neighbors. If node i has N (pairwise) encounters with its neighbors and sN of them are assessed as suspicious by the neighbors, its suspiciousness Si is defined as Si = By equation, Si [0,1]. A number Le (0,1) is chosen as the line between good and evil. Node i is good if Si ≤ Le , orevil if Si > Le :

II. PROBLEM STATEMENT

Almost all the existing work on routing in delay tolerant networks has focused on the problem of delivery of messages inside a single region, characterized by the same network infrastructure and namespace. However, many deployment scenarios, especially in developing regions, will probably involve routing among different regions composed of several heterogeneous types of network domains such as satellite networks and ad hoc networks composed of short- range radio enabled devices, like mobile phones with Bluetooth interface.

III. LITERATURE SURVEY

A. S. Buchegger and J. Boudec, "Performance Analysis of the CONFIDANT Protocol," Proc. ACM MobiHoc, 2002.

In this paper Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding. How-ever, it may be advantageous for individual nodes not to cooperate. We propose a protocol, called CONFIDANT, for making misbehavior unattractive; it is based on selecaltruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. The detailed implementation of CONFIDANT in this paper assumes that the network layer is based on the Dynamic Source Routing (DSR) protocol. We present a performance analysis of DSR fortied by CONFIDANT and compare it to regular defenseless DSR. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in sharp contrast to a defenseless network. All simulations have been implemented and performed in GloMoSim .

B. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigen trust Algorithm for Reputation Management in P2P Networks," Proc. ACM 12th Int'l Conf. World Wide Web (WWW), 2003.

In this paper Peer-to-peer file-sharing networks are currently receiving much attention as a means of sharing and distributing information. How-ever, as recent experience shows, the anonymous, open nature of these networks offers an almost ideal environment for the spread of self-replicating inauthentic files. We describe an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that as-signs each peer a unique global trust value, based on the peer's history of uploads. We present a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network. In simulations, this reputation system, called Eigen Trust, has been shown to significantly decrease the number of in authentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately subvert the system.

C. Wei Peng, Xukai Zou, "Behavioral Malware Detection in Delay Tolerant Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014.

In this paper The delay-tolerant-network (DTN) model is becoming a viable 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 matching 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, which has been successfully applied in non-DTN settings such as filtering email spams and detecting botnets. We identify two unique challenges for extending Bayesian malware detection to DTNs ("insufficient evidence versus evidence collection risk" and "filtering false evidence sequentially and distributedly"), and propose a simple yet effective method, look ahead, to address the challenges.

IV. RELATED WORK

Proximity malware and mitigation schemes. Su et al. collected Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations. Yan et al developed a Bluetooth malware model. Bose and Shin showed that Bluetooth can enhance malware propagation rate over SMS/MMS. Cheng et al. analyzed malware propagation through proximity channels in social networks. Akritidis et al. quantified the threat of proximity malware in wide-area wireless networks. Li et al. discussed optimal malware signature distribution in heterogeneous, resource-constrained mobile networks. In traditional, nonDTN, networks, Kolbitsch et al. and Bayer et al. proposed to detect malware with learned behavioral model, in terms of system call and program flow. We extend the Naive Bayesian model, which

has been applied in filtering email spams detecting botnets and designing IDSs and address DTNspecific, malware-related, problems. In the context of detecting slowly propagating Internet worm, Dash et al. presented a distributed IDS architecture of local/global detector that resembles the neighborhood-watch model, with the assumption of attested/honest evidence, i.e., without liars. Mobile network models and traces. In mobile networks, one cost-effective way to route packets is via the short-range channels of intermittently connected smart phones. Two real mobile network traces were used in our study. Reputation and trust in networking systems. In the neighborhood watch model, suspiciousness, defined in (1),can be seen as nodes' reputation; to cut a node off is to decide that the node is not trustworthy. Thus, our work can be viewed from the perspective of reputation/trust systems. Three schools of thoughts emerge from previous studies. The first one uses a central authority, which by convention is called the trusted third party. In the second school, one global trust value is drawn and published for each node, based on other nodes' opinions of it; eigen Trust is an example. The last school of thoughts includes the trust management systems that allow each node to have its own view of other nodes. Our work differs from previous trust management work in addressing two DTN specific, malware related, trust management problems:1) insufficient evidence versus evidence collection risk and2) sequential and distributed online evidence filtering.

V. CONCLUSION & FUTURE WORK

Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical In Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware. Naive Bayesian model has been successfully applied in non-DTN settings, such as filtering email spams and detecting botnets. We propose a general behavioural characterization of DTN-based proximity malware. We present look-ahead, along with dogmatic fil-tering and adaptive look-ahead, to address two unique challenging in extending Bayesian filtering to DTNs: "insufficient evidence vs. evidence collection risk" and "filtering false evidence sequentially and distributedly". In prospect, extension of the behavioral characterization of proximity malware to account for strategic malware detection evasion with game theory is a challenging yet interesting future work.

.

REFERENCES

[1] Trend Micro Inc. (2004) SYMBOS CABIR.A. [Online]. Available: http://goo.gl/aHcES
[2] [Online]. Available: http://goo.gl/iqk7
[3] Trend Micro Inc. (2009) IOS IKEE.A. [Online]. Available: http://goo.gl/z0j56
[4] P. Akritidis, W. Chin, V. Lam, S. Sidiroglou, and K. Anagnostakis, "Proximity breeds danger: emerging threats in metro-area wireless networks," in Proc. USENIX Security, 2007.
[5] A. Lee. (2012) FBI warns: New malware threat targets travelers, infects via hotel Wi-Fi. [Online]. Available: http://goo.gl/D8vNU
[6] NFC Forum. About NFC. [Online]. Available: http: //goo.gl/zSJqb
[7] Wi-Fi Alliance. Wi-Fi Direct. [Online]. Available: http: //goo.gl/fZuyE
[8] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, "Effective and efficient malware detection at the end host," in Proc. USENIX Security, 2009.
[9] U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering," in Proc. IEEE NDSS, 2009.
[10] 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. AAAI, 2006.
[11] G. Zyba, G. Voelker, M. Liljenstam, A. M´ehes, and P. Johansson, "Defending mobile phones from proximity malware," in Proc. IEEE INFOCOM, 2009.
[12] F. Li, Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in smartphone-based mobile networks," in Proc. IEEE INFOCOM, 2010.
[13] I. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos, "An experimental comparison of naïve bayesian and keyword-based anti-spam filtering with personal e-mail messages," in Proc. ACM SIGIR, 2000.
[14] P. Graham. Better Bayesian filtering. [Online]. Available: http://goo.gl/AgHkB
[15] J. Zdziarski, Ending spam: Bayesian content filtering and the art of statistical language classification. No Starch Press, 200 5.
[16] R. Villamar´ın-Salom´on and J. Brustoloni, "Bayesian bot detection based on DNS traffic similarity," in Proc. ACM SAC.
[17] J. Agosta, C. Diuk-Wasser, J. Chandrashekar, and C. Livadas, "An adaptive anomaly detector for worm detection," in Proc. USENIX SysML, 2007.
[18] S. Marti, T. Giuli, K. Lai, M. Baker et al., "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000.

Mr NAGOORVALI SHAIK is a student of NIMRA College of Engineering and Technology, IBRAHIMPATNAM, VIJAYAWADA. He is presently pursuing her M.Tech degree from JNTU, Kakinada.

G.MINNI is presently working as Assistant professor in CSE department in Nimra college of Engineering and Technology, Jupudi, Nimra Nagar,VIJAYAWADA. She has obtained M.Tech degree from JNTU, Kakinada. She is pursuing Ph.D., in A.N.U, GUNTUR. She has published several research papers in various national and international Journals. She has more than Ten years of experience in teaching field, her area of interests are networks & Web Designing.

SAYEED YASIN received his MTECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.