International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.1, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

SOCIAL NETWORK ANALYSIS FOR INFORMATION FLOW IN DISCONNECTED DELAY–TOLERANT NETWORK

Nivethitha.L, Akshaya.R, Thiripurasundari.V, Mrs.D.Anuradha
Department of Computer Science and Engineering, Panimalar Engineering College, Chennai

Article Received: 16/02/2015 | Article Revised on:21/02/2015 | Article Accepted on:27/02/2015

ABSTRACT
The delay-tolerant-network (DTN) model is becoming a viable communication for 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. 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. It used to need to identify two unique challenges for extending Bayesian malware detection to DTNs In this paper additionally 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.

Indexed Terms— Malware, Bayesian methods, Bluetooth, dogmatic filtering, Delay-tolerant networks, proximity malware, behavioral malware characterization.


Nivethitha.L


Akshaya.R


Thiripurasundari.V


Mrs.D.Anuradha

INTRODUCTION

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 [6] and Wi-Fi Direct[7]. 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 [8], 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 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. The popularity of mobile consumer electronics, like laptop computers and more recently and prominently, smart phones, revives the delay-tolerant network (DTN) model as an alternative to the traditional infrastructure model. 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. So 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. 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[6] that facilitate spontaneous bulk data transfer between spatially proximate mobile devices, the threat of proximity malware is becoming more realistic and relevant than ever. The main problems in existing are a Proximity malware is based on the DTN model brings unique security challenges that are not present in the model. The two DTN specific, malware-related, problems:

1. Insufficient evidence versus evidence collection risk 2.Filtering false evidence sequentially and distributedly.

MODELS

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.

METHODLOGY

We present a general behavioral characterization of proximity malware, which captures the functional but imperfect nature in detecting proximity malware which has been previously proposed as an effective alternative to pattern matching for malware detection. The advantage of this method is that real mobile network traces are used to verify the effectiveness of the proposed methods. The proposed evidence consolidation enables 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. The disadvantage of existing is that Central monitoring and resource limits are absent in the DTN model. Very risk in collecting evidence and also has insufficient evidence. In our model, we assume that each node is capable of assessing the

Other party for suspicious actions after each encounter, resulting in a binary assessment. A node is either evil or good, based on if it is or is not infected by the malware. It may occasionally assess an evil node's actions as non suspicious or a good node's actions as suspicious, but most suspicious actions are correctly attributed to evil nodes.

MODULES

DTN (Delay-Tolerant-Network)
Look Ahead: Distribution versus Maximizer
Look Ahead
Evidence Consolidation

DTN (Delay-Tolerant-Network):

It approaches the computer networks architecture that address the technical issue of heterogeneous networks that may continuous network connectivity. In our model, we assume that each node is capable of assessing the other party for suspicious actions after each encounter, resulting in a binary assessment. For example, a node can assess a Bluetooth connection or an SSH session for potential

Cabir or Ikee infection [19][20]. In the previous works on malicious behavior detection in mantes and distributed reputation systems are other examples, a node is either evil or good, based on if it is or is not infected by the malware.

Figure 1: DTN (Delay-Tolerant-Network)

LOOK AHEAD DISTRIBUTION VERSUS MAXIMIZER

We compare the two alternative approaches, distribution and maximize, to the look-ahead strategy. In both data sets, the detection-rate and false-positive rate are comparable for the distribution and maximizer approach, with the distribution approach having a slightly higher detection rate and false-positive rate.

LOOK HEAD

We compare Bayesian-based strategies with, and without, the look-ahead extension under the household-watch model. The Bayesian strategy does not look ahead and proceeds with cutting-off once the evidence becomes unfavorable to the neighbor. In the Bayesian strategy has the highest detection and false-positive rate. Both rates drop with an increasing look-ahead parameter.

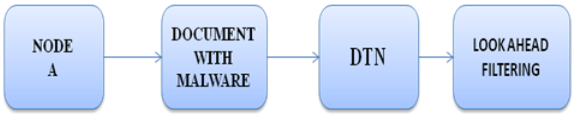

Figure 2: Look ahead approach

EVIDENCE CONSOLIDATION

We also evaluate the benefits of sharing assessments among nodes, and the effect of the proposed evidence consolidation strategies in minimizing the negative impact of liars on the shared evidence's quality. We compare the dogmatic filtering and adaptive look-ahead evidence consolidation methods with two other (naive) evidence consolidation methods taking no indirect evidence, i.e., look ahead with no evidence consolidation and taking all the indirect evidence without filtering

In this paper 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. 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 consider the benefits of sharing assessments among nodes, and address challenges derived from the DTN model.

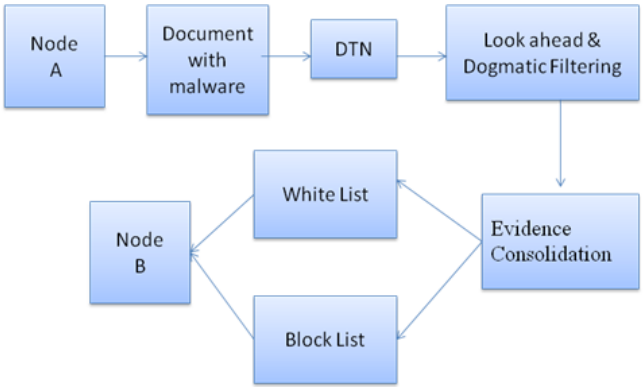

Figure 3: Evidence Consolidation

ARCHITECTURE DIAGRAM

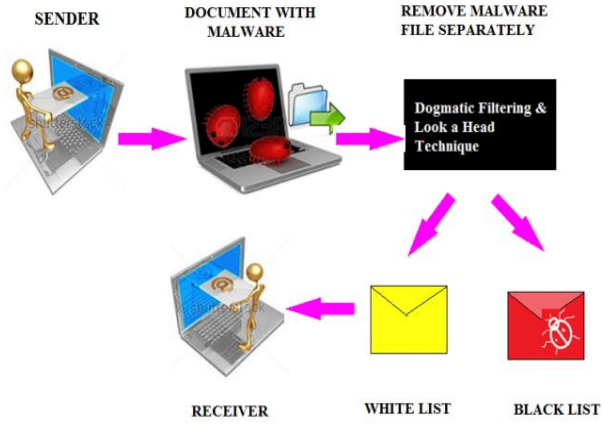

Figure 4: Architecture diagram

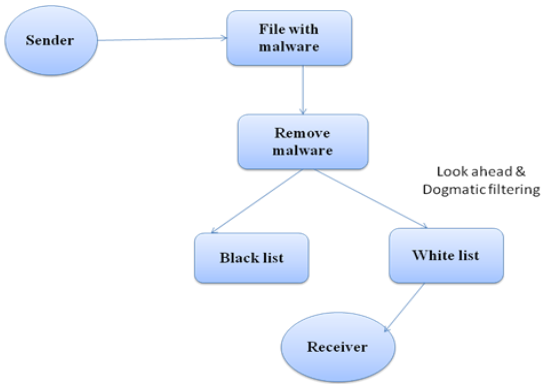

Figure 5: Data Flow Diagram

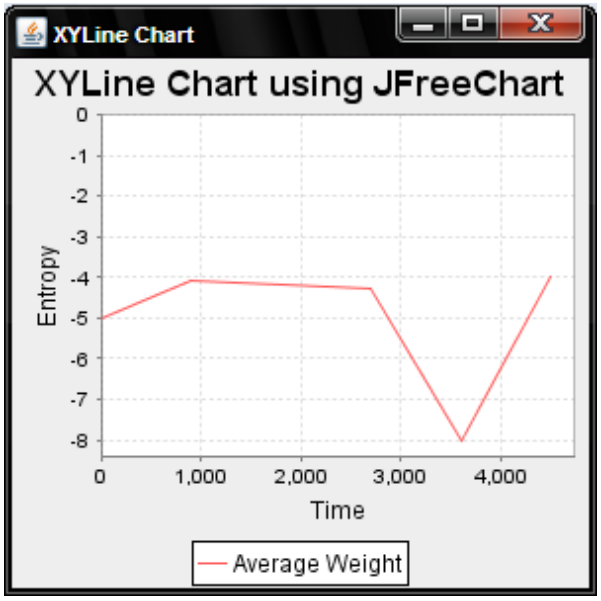

Figure 6: Output

CONCLUSION

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 behavioral characterization of DTN-based proximity malware. We present look ahead, along with dogmatic filtering and adaptive look ahead. 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]. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM Mobi Com, 2000.

[2]. I. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos, "An Experimental Comparison of Naive Bayesian and Keyword-Based Anti-Spam Filtering with Personal E-Mail Messages," Proc. 23rd Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), 2000.

[3]. S. Buchegger and J. Boudec, "Performance Analysis of theconfidant Protocol," Proc. ACM mobihoc, 2002.

[4]. A. Vahdat and D. Becker, "Epidemic Routing for partiallyconnected Ad Hoc Networks," technical report, Duke Univ., 2002.

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

[6]. S. Buchegger and J. Le Boudee, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems," IEEE Comm. Magazine, vol. 43, no. 7, pp. 101-107, July 2005.

[7]. 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," Proc. 21st Nat'l Conf. Artificial Intelligence (AAAI), 2006.

[8]. A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-Based Beacon Trust System," Proc. IEEE Second Int'l Symp. Dependable, Autonomic and Secure Computing (DASC), 2006

[9]. 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," Proc. Fourth ACM Workshop Recurring Malcode (WORM), 2006

[10]. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[11]. G. Yan, H. Flores, L. Cuellar, N. Hengartner, S. Eidenbenz, and V. Vu, "Bluetooth Worm Propagation: Mobility Pattern Matters!," Proc. Second ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2007.

[12]. P. Akritidis, W. Chin, V. Lam, S. Sidiroglou, and K. Anagnostakis,"Proximity Breeds Danger: Emerging Threats in Metro-areawireless Networks," Proc. 16th USENIX Security Symp., 2007.

[13]. 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," Proc. 21st Nat'l Conf. Artificial Intelligence (AAAI), 2006.

[14]. J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau,"CRAWDAD Data Set Cambridge/Haggle (v. 2006-09-15),"http://goo.gl/rjrkn, Sept. 2006.

[15]. U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda,"Scalable, Behavior-Based Malware Clustering," Proc. 16th Ann.Network and Distributed System Security Symp. (NDSS), 2009.

[16]. G. Zyba, G. Voelker, M. Liljenstam, A. Me´hes, and P. Johansson,"Defending Mobile Phones from Proximity Malware," Proc. IEEE INFOCOM, 2009.

[17]. E. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant manets," IEEE Trans. Mobile Computing, vol. 8, no. 5, pp. 606-621, May 2009.

[18]. F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, 2010.

[19]. S. Cheng, W. Ao, P. Chen, and K. Chen, "On Modeling Malware Propagation in Generalized Social Networks," IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.

[20]. R. Villamarı´n-Salomo´ n and J. Brustoloni, "Bayesian Bot Detection Based on DNS Traffic Similarity," Proc. Acmymp. Applied Computing (SAC), 2013.