International Journal of Science Engineering and Advance Technology

Detection of Behavioral Malware in Delay Tolerant Networks

Kolanu Venkata Krishna Sasikanth[1], K.Satyanarayana Raju[2]
[1] M.Tech (IT), S.R.K.R.Engineering College, A.P., India.
[2]Assistant Professor, Dept. of Information Technology, S.R.K.R.Engineering College, A.P., India.

***Abstract* — Disruption-tolerant networking has gained currency in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise. 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.**

K*eywords* — delay-tolerant networks; proximity malware; behavioral malware characterization; Bayesian filtering

I. Introduction

Computer network architecture that seeks to address the technical issues in heterogeneous network that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space [1]. The popularity of mobile consumer electronics, like laptop computers, PDAs, and more recently and prominently, Smartphone's, 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.

An early example of proximity malware is the Symbian-based Cabir worm, which propagated as a Symbian Software Installation Script (.sis) package through the Bluetooth link between two spatially proximate devices [1]. A later example is the iOS-based Ikee worm, which exploited the default SSH password on jailbroken [2] iPhones to propagate through IP-based Wi-Fi connections [3]. Previous researches [4] 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 attacks [5]. With the adoption of new short-range communication technologies such as NFC [6] and Wi-Fi Direct [7] 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 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. For example, the installation package in Cabir and the SSH session in Ikee, which were used for malware propagation, cannot be detected by the cellular carrier. However, such central monitoring and resource limits are absent in the DTN model. Proximity malware exploits the opportunistic contacts and distributed nature of DTNs for propagation.

A prerequisite to defending against proximity malware is to detect it. In this paper, we consider a general behavioral characterization of proximity malware. Behavioral characterization, in terms of system call and program flow,

has been previously proposed as an effective alternative to pattern matching for malware detection [8],[9]. 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. For example, a single suspicious Bluetooth connection or SSH session request during one encounter does not confirm a Cabir or Ikee infection, but repetitive suspicious requests spanning multiple encounters is a strong indication for malware infection. The imperfection of a single, local observation was previously in the context of distributed IDS against slowly propagating worms [10].

Instead of assuming a sophisticated malware containment capability, such as patching or self-healing [11, 12], we consider a simple "cut-off" strategy: If a node i suspects another node j of being infected with the malware, i simply ceases to connect with j in the future to avoid being infected by j. Our focus is on how individual nodes shall make such cut-off decisions against potentially malware-infected nodes, based on direct and indirect observations. A comparable example from everyday experience is fire emergency. An early indication, like dark smoke, prompts two choices. One is to report fire emergency immediately; the other is to collect further evidence to make a better informed decision later. The first choice bears the cost of a false alarm, while the second choice risks missing the early window to contain the fire.

In the context of DTNs, we face a similar dilemma when trying to detect proximity malware: Hypersensitivity leads to false positives, while hypo-sensitivity leads to false negatives. In this paper, we present a simple, yet effective solution, look-ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection, to balance between these two extremes. Essentially, we extend the Naive Bayesian model, which has been applied in filtering email spams [13, 14, 15], detecting botnets [16], and designing IDSs [10, 17], and address two DTN-specific, malware-related, problems. 1. Insufficient evidence vs. evidence collection risk. In DTNs, evidence (such as Bluetooth connection or SSH session requests) is collected only when nodes come into contact. But contacting malware-infected nodes carries the risk of being infected. Thus, nodes must make decisions (such as whether to cut off other nodes and, if yes, when) online based on potentially insufficient evidence. 2. Filtering false evidence sequentially and distributedly. Sharing evidence among opportunistic acquaintances helps alleviating the aforementioned insufficient evidence problem; however, false evidence shared by malicious nodes (the liars) may negate the benefits of sharing. In DTNs, nodes must decide whether to accept received evidence sequentially and distributedly.

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 .RELATED WORK

Proximity malware and mitigation schemes. Su et al. collected
Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations [14]. Yan et al. developed a Bluetooth malware model [15]. Bose and Shin showed that Bluetooth can enhance malware propagation rate over SMS/MMS [16]. Cheng et al. analyzed malware propagation through proximity channels in social networks [17]. Akritidis et al. quantified the threat of proximity malware in wide-area wireless networks [4]. Li et al. Discussed optimal malware signature distribution in heterogeneous, resource-constrained mobile networks [18]. In traditional, non-DTN, networks, Kolbitsch et al. [8] and Bayer et al. [9] 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 [13, 14, 15], detecting botnets [16], and designing IDSs [10, 17], and address DTN-specific, 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 neighborhoodwatch model, with the assumption of attested/honest evidence, i.e., without liars [10]. Mobile network models and traces. In mobile networks, one cost-effective way to route packets is via the short-range channels of intermittently connected smartphones [9, 10, 11]. While early work in mobile networks used a variety of simplistic random i.i.d. models, such as random waypoint, recent findings [12] show that these models may not be realistic. Moreover, many recent studies [3], based on real mobile traces, revealed that a node's mobility shows certain social network properties. Two real mobile network traces were used in our study. Reputation and trust in networking systems. In the neighbourhood watch model, suspiciousness, defined in Equation (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; eigenTrust [4] 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 [15, 16]. Our work differs from previous trust management work in addressing two DTNspecific, malware-related, trust management problems: 1) insufficient evidence vs. evidence collection risk and 2) sequential and distributed online evidence filtering.

Consider the case in which i bases the cut-off decision against j only on i's own assessments on j. Since only direct assessments are involved, we call this model household watch (the naming will become more evident by the beginning. Let A = (a1, a2, . . . , aA) be the assessment sequence (ai is either 0 for "non-suspicious" or 1 for "suspicious") in chronological order, i.e., a1 is the oldest assessment, and aA is the newest one Bayes' theorem tells us: P(Sj |A) P(A|Sj) × P(Sj). P(Sj) encodes our prior belief on j's suspiciousness Sj ; P(A|Sj) is the likelihood of observing the assessment sequence A given Sj ; P(Sj |A) is the posterior probability, representing the plausibility of j having a suspiciousness of Sj given the observed assessment sequence A. Since the evidence P(A) does not involve Sj and serves as a normalization factor in the computation, we omit it and write the quantitative relationship in the less cluttered proportional form1. Figure 1 shows the normalized posterior distributions P(Sj |A) for assessment samples with different sizes, given by Equation 3. In each case, the ratio between suspicious and non-suspicious assessments is the same, i.e., 1:3; by Equation 4, Sj = 1 1+3 = 0.25 is the maximizer of P(Sj |A), which is clearly shown in Figure 1. The distribution becomes sharper with a larger sample, which accords to the intuition of the increasing certainty on the suspiciousness Sj .

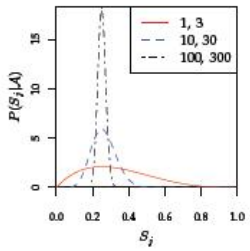

Fig. 1: The normalized posterior distribution $P(S_j|\mathcal{A})$ for assessment samples with different sizes. The two numbers for each line in the legend show the number of suspicious and non-suspicious assessments, respectively. In each case, the ratio between suspicious and non-suspicious assessments is 1 : 3. All distributions have a maximal value at $S_j = \frac{1}{1+3} = 0.25$. However, the distribution becomes shaper with a larger sample, which corresponds to a sense of increasing certainty regarding the suspiciousness S_j.

The uncertainty over j's suspiciousness Sj (and, hence, the risk of losing a good neighbor) holds i back from cutting j off immediately, based on insufficient evidence. In the following discussion, we consider two alternative approaches, distribution and maximizer, to handle the insufficient-evidence problem, based on Equations (3) and (4), respectively. In the distribution approach, i consider the whole posterior suspiciousness distribution (Equation (3)) in making the cut-off decision against j. From i's perspective, after observing an assessment sequence A, the probability Pg(A) that j is good is:

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 (with dogmatism of 0.0001, 0.01, and 1, respectively) and adaptive look-ahead evidence consolidation methods with two other (naive) evidence consolidation methods: 1) taking no indirect evidence,i.e., look-ahead with no evidence consolidation, and 2) taking all indirect evidence without filtering.

The structure of the behavioral malware characterization model (specifically, a single threshold Le is used to distinguish the nature of a node) gives rise to a subtlety concerning i's prejudice against j in the distribution approach. Similarly, i can look multiple steps ahead. In fact, the number of steps i is willing to look ahead is a parameter of the decision process rather than a result of it. This parameter shows i's willingness to be exposed to a higher infection risk in exchange for a higher certainty about the nature of j and a lower risk of cutting off a good neighbor; in other words, it reflects i's intrinsic risk inclination against malware infection.

In the neighborhood-watch model, the malicious nodes that are able to transmit malware (we will see next that there may be malicious nodes whose objective is other than transmitting malware) are assumed to be consistent over space and time.

$$P_g(\mathcal{A}) = \int_0^{L_e} P(S_j|\mathcal{A})\,\mathrm{d}S_j; \quad (5)$$

the probability $P_e(\mathcal{A})$ that j is evil is:

$$P_e(\mathcal{A}) = 1 - P_g(\mathcal{A}) = \int_{L_e}^{1} P(S_j|\mathcal{A})\,\mathrm{d}S_j. \quad (6)$$

Let $\mathcal{C} = (\int_0^1 S_j^{s_\mathcal{A}}(1-S_j)^{|\mathcal{A}|-s_\mathcal{A}}\,\mathrm{d}S_j)^{-1}$ be the (probability) normalization factor in Equation 3; we have:

$$P_g(\mathcal{A}) = \mathcal{C}\int_0^{L_e} S_j^{s_\mathcal{A}}(1-S_j)^{|\mathcal{A}|-s_\mathcal{A}}\,\mathrm{d}S_j \quad (7)$$

and

$$P_e(\mathcal{A}) = \mathcal{C}\int_{L_e}^{1} S_j^{s_\mathcal{A}}(1-S_j)^{|\mathcal{A}|-s_\mathcal{A}}\,\mathrm{d}S_j. \quad (8)$$

When $P_g(\mathcal{A}) \geq P_e(\mathcal{A})$, the evidence collected so far (i.e., $\mathcal{A}$) is favorable to j. However, when $P_g(\mathcal{A}) < P_e(\mathcal{A})$, the evidence is unfavorable to j and suggests that j might be an evil node. i needs to *decide whether to cut j off*.

By being consistent over space, we mean that evil nodes' suspicious actions are observable to all their neighbors, rather than only a few. If this is not the case, the evidence provided by neighbors, even if truthful, will contradict local evidence and, hence, cause confusions:

Nodes shall discard received evidence and fall back to the household watch model. By being consistent over time, we mean that evil nodes can not play strategies to fool the assessment mechanism. This is equivalent to the functional assumption in characterizing the nature of nodes by suspiciousness. The case in which the evil nodes can circumvent the suspiciousness characterization (such as by first accumulating good assessments, and then launch an attack through a short burst of concentrated suspicious actions) calls for game-theoretic analysis and design, and is beyond the scope of this paper. Instead, we propose a behavioral characterization of proximity malware; further game- theoretic analysis and design could base on this foundation. Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices.[8][9] Solutions have typically been modified from mobile ad hoc network and distributed security research, such as the use of distributed certificate authorities[10] and PKI schemes. Original solutions from the delay-tolerant research community include: 1) the use of identity-based encryption, which allows nodes to receive information encrypted with their public identifier;[11] and 2) the use of tamper-evident tables with a gossiping protocol.

IV Conclusion

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 filtering 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.