IISRC International Industrial Scientific Research Corporation
International Conference on Industrial Scientific Research Engineering
www.worldconferences.org

# Containment of Proximity Malware Behavioral Detection in Delay Tolerant Networks

**S.IRAFANA BEGUM[1], S.G.NAWAZ[2]**
[1]PG Scholar, Dept of CSE, Sri Krishna Devaraya Engineering College, Gooty, AP, India,
E-mail: irfanahifi@yahoo.com.
[2]HOD, Dept of CSE, Sri Krishna Devaraya Engineering College, Gooty, AP, India.

**Abstract:** With the universal presence of short-range connectivity technologies (e.g., Bluetooth and, more recently, Wi- Fi Direct) in the consumer electronics market, the delay tolerant- network (DTN) model is becoming a viable alternative to the traditional infrastructural model. Proximity malware, which exploits the temporal dimension and distributed nature of DTNs in self-propagation, poses threats to users of new technologies. In this paper, we address the proximity malware detection and containment problem with explicit consideration for the unique characteristics of DTNs. We formulate the malware detection process as a decision problem under a general behavioral malware characterization framework. We analyze the risk associated with the decision problem and design a simple yet effective malware containment strategy, look-ahead, which is distributed by nature and reflects an individual node's intrinsic trade-off between staying connected (with other nodes) and staying safe (from malware). Furthermore, we consider the benefits of sharing assessments among directly connected nodes and address the challenges derived from the DTN model to such sharing in the presence of liars (i.e., malicious nodes sharing false assessments) and defectors (i.e., good nodes that have turned malicious due to malware infection).

**Keywords:** Delay-Tolerant Networks (DTNS), SSH Session Requests, Wi-Fi.

## I. INTRODUCTION

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. These new devices are often equipped with a diverse set of non-infrastructural connectivity technologies, e.g., Infra-red, Bluetooth, and more recently, Wi-Fi Direct. 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. Because of users' natural mobility, new information distribution applications, based on peer-to-peer contact opportunities instead of persistent connection channels among nodes, are considered to be the game changer for future network applications. 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 analysis and extraction often involve extensive manual labor and expertise. The overhead, the lack of generality, and high false positive rate in one round of analysis make it unsuitable for promising DTN applications on smart devices. The quest for a better malware detection method comes to the very question of how to characterize proximity malware in DTNs.

In this paper, we consider an approach to characterize proximity malware by the behaviors of an infected node observed by other nodes in multiple rounds. The

individual observation can be imperfect for one round, but infected nodes' abnormal behavior will be distinguishable in the long-run. Methods like pattern matching can be used in one round of observation for the behavioral characterization of proximity malware. Instead of assuming a sophisticated malware containment capability, such as patching or self-healing , we consider the simple capability of "cutting off communication". In other words, if a node i suspects another node j of being infected with the malware, i may cease to connect with j in the future. We want to explore how far such a simple technique can take us. Our focus is on how individual nodes make such cut-off decisions 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 hyposensitivity 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, detecting botnets and designing IDSs and address two DTN specific, malware-related, problems:

- Insufficient evidence versus 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.
- Filtering false evidence sequentially and distributed. 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 distributed.

Our contributions are summarized as follows:

- 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. Look ahead extends the naive Bayesian model, and addresses the DTN specific, malware-related, "insufficient evidence versus evidence collection risk" problem.

## II. NEIGHBORHOOD WATCH

Besides using i's own assessments, i may incorporate other neighbors' assessments in the cut-off decision against j. This extension to the evidence collection process is inspired by the real-life neighborhood (crime) watch program, which encourages residents to report suspicious criminal activities in their neighborhood. Similarly, i shares assessments on j with its neighbors, and receives their assessments on j in return. 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. These are common assumptions in distributed trust management systems (summarized in Section 5), which incorporate neighboring nodes' opinions in estimating a local trust value. 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 cannot 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.

## III. EVIDENCE AGING

The presence of defectors breaks the assumption when we characterize a node's nature by suspiciousness. A defector starts as a good node but turns evil due to malware infections; the assessments collected before the defector's change of nature, even truthful, are misleading. To alleviate the problem of outdated

assessments, old assessments are discarded in a process called evidence aging. Each assessment is associated with a timestamp. Only assessments with timestamps less than a specific aging window TE from now are included in the cut-off decision. To see that the aging window TE alleviates the defector problem, consider a node that is infected at time T. Without evidence aging, all evidence before T mounts to testify that the node is good; if the amount of this prior evidence is large, it may take a long time for its neighbors to find out about the change in its nature. In comparison, with evidence aging, at time T þ TE, all prior evidence expires and only those assessments after the infection are considered, which collectively testify against the node. However, in practice, the choice of the aging window TE depends on the context. While a small TE may speed up the detection of defectors by reducing the impact of stale information, TE must be large enough to accommodate enough assessments to make a sound cut-off decision. If TE is too small, a node will not have enough assessments to make robust cut-off decision.

## IV. 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 (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. In our study, 10 percent of the evil nodes play the dual roles of evil-doers and liars. There are many possible liar strategies. Based on our observations we adopt an exaggerated false praise/accusation liar strategy. More specifically, a liar (falsely) accuses good nodes of suspicious actions and (falsely) praises other evil nodes for non suspicious actions. Besides, to exert a significant influence on the public opinion, they exaggerate the false praises/ accusations by 10 times (since they are only 10 percent of the whole population).

The results on the performance of various evidence consolidation strategies under this setting are shown in Fig. 1. Clearly shows the negative impact of liars on malware detection if evidence is not filtered: Under the influence of liars, the naive "all" strategy has a low detection rate and a high false-positive rate. This calls for a nontrivial evidence consolidation strategy to deal with the liars. Both dogmatic filtering and adaptive look ahead show significant increases in detection rate and modest increases in false positive rate over the baseline 3-robust look-ahead strategy with no evidence filtering. Together, the results indicate that the 3-robust look ahead, with either dogmatic filtering or adaptive look ahead, is comparable in detection rate and, even in the presence of liars, shows a significantly lower false positive rate in comparison with both the Bayesian and 1-robust strategies.

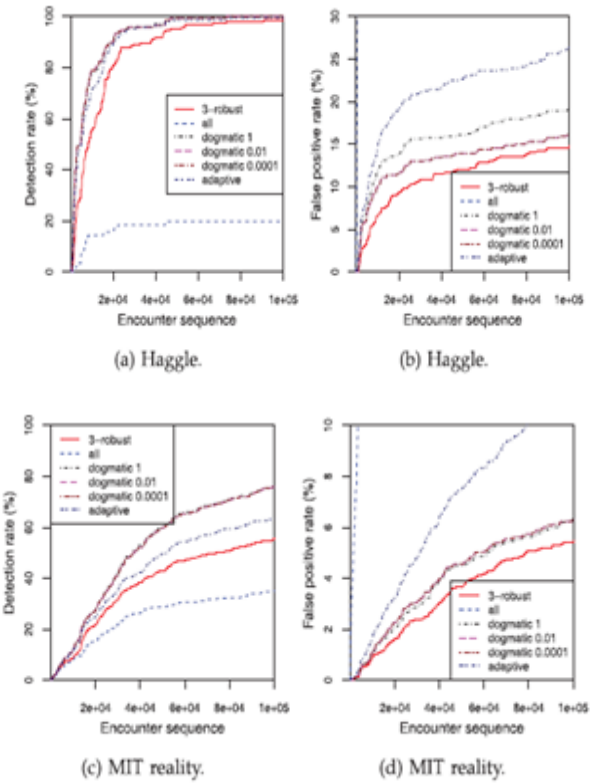


**Fig.1. Performance impact of various evidence consolidation methods on the look-ahead cut-off strategy.**

## V. 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, non-DTN, 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 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 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 and 2) sequential and distributed online evidence filtering.

## VI. CONCLUDING REMARKS

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, to address two unique challenging in extending Bayesian filtering to DTNs: "insufficient evidence versus 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.

## VII. REFERENCES

[1] Trend Micro Inc. SYMBOS_CABIR.A., http://goo.gl/aHcES, 2004.
[2] http://goo.gl/iqk7, 2013.
[3] Trend Micro Inc. IOS_IKEE.A., http://goo.gl/z0j56, 2009.
[4] P. Akritidis, W. Chin, V. Lam, S. Sidiroglou, and K. Anagnostakis, "Proximity Breeds Danger: Emerging Threats in Metro-Area Wireless Networks," Proc. 16th USENIX Security Symp., 2007.
[5] A. Lee, "FBI Warns: New Malware Threat Targets Travelers, Infects via Hotel Wi-Fi," http://goo.gl/D8vNU, 2012.
[6] NFC Forum. about NFC, http://goo.gl/zSJqb, 2013.
[7] Wi-Fi Alliance. Wi-Fi Direct, http://goo.gl/fZuyE. 2013.
[8] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, "Effective and Efficient Malware Detection at the End Host," Proc. 18th Conf. USENIX Security Symp., 2009.