ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Filtering False Evidence Sequentially and Distributed By Extending Bayesian Malware Detection to DTNS

Mahmoud Saeed Al-Jabari
Master of Science (Information System),
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

T. Ramdas Naik
Assistant Professor Dept, Computer Science (PG)
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

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 behavioural 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), Detection, Wi-Fi.

INTRODUCTION:

The popularity of mobile consumer electronics, like laptop computers, PDAs, and more recently and prominently, smartphones, 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.A later example is the iOS-based Ikee worm, which exploited the default SSH password on iPhones to propagate through IP-based Wi-Fi connections. 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 attacks. With the adoption of new short-range communication technologies such as NFC and Wi-Fi Direct that facilitate.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 delaytolerant 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 mode.

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 longrun. 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.

LITERATURE SURVEY:

"Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs"Message delivery in sparse mobile ad hoc networks (MANETs) is difficult due to the fact that the network graph is rarely (if ever) connected. A key challenge is to find a route that can provide good delivery performance and low end-to-end delay in a disconnected network graph where nodes may move freely. We cast this challenge as an information flow problem in a social network. This paper presents social network analysis metrics that may

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

be used to support a novel and practical forwarding solution to provide efficient message delivery in disconnected delay-tolerant MANETs. These metrics are based on social analysis of a node's past interactions and consists of three locally evaluated components: a node's "betweenness" centrality (calculated using ego networks) and a node's social 'similarity' to the destination node and a node's tie strength relationship with the destination node. We present simulations using three real trace data sets to demonstrate that by combining these metrics delivery performance may be achieved close to epidemic routing but with significantly reduced overhead. Additionally, we show improved performance when compared to PRoPHET routing.

"Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)"Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. We propose a protocol, called CONFIDANT, for making misbehavior unattractive; it is based on selective altruism 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 forti- fied 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.

"DRBTS: Distributed Reputation-based Beacon Trust System"Wireless sensor networks (WSNs) have critical applications in diverse domains like environmental monitoring and military operations where accurate location of sensors is vital. One common method of location discovery uses a set of specialty nodes known as beacon nodes (BNs) that assist other sensor nodes (SNs) to determine their location. This paper proposes a novel reputation-based scheme called distributed reputation-based beacon trust system (DRBTS) for excluding malicious BNs that provide false location information.

To the best of our knowledge, DRBTS is the first model to use the concept of reputation for excluding BNs. In DRBTS, every BN monitors its 1-hop neighborhood for misbehaving BNs and accordingly updates the reputation of the corresponding BN in the neighbor-reputation-table (NRT). The BNs then publish their NRT in their 1-hop neighborhood. BNs use this second-hand information published in NRT for updating the reputation of their neighbors after it qualifies a deviation test.

On the other hand, the SNs use the NRT information to determine whether or not to use a given beacon's location information, based on a simple majority voting scheme When Gossip is Good: Distributed Probabilistic Inference for Detection of Slow Network Intrusions. Intrusion attempts due to self-propagating code are becoming an increasingly urgent problem, in part due to the homogeneous makeup of the internet. Recent advances in anomalybased intrusion detection systems (IDSs) have made use of the quickly spreading nature of these attacks to identify them with high sensitivity and at low false positive (FP) rates.

However, slowly propagating attacks are much more difficult to detect because they are cloaked under the veil of normal network traffic, yet can be just as dangerous due to their exponential spread pattern. We extend the idea of using collaborative IDSs to corroborate the likelihood of attack by imbuing end hosts with probabilistic graphical models and using random messaging to gossip state among peer detectors. We show that such a system is able to boost a weak anomaly detector D to detect an order-of-magnitude slower worm, at false positive rates less than a few per week, than would be possible using D alone at the end-host or on a network aggregation point.

We show that this general architecture is scalable in the sense that a fixed absolute false positive rate can be achieved as the network size grows, spreads communication bandwidth uniformly throughout the network, and makes use of the increased computation power of a distributed system. We argue that using probabilistic models provides more robust detections than previous collaborative counting schemes and allows the system to account for heterogeneous detectors in a principled fashion.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

"Scalable, Behavior-Based Malware Clustering"Anti-malware companies receive thousands of malware samples every day. To process this large quantity, a number of automated analysis tools were developed. These tools execute a malicious program in a controlled environment and produce reports that summarize the program's actions. Of course, the problem of analyzing the reports still remains. Recently, researchers have started to explore automated clustering techniques that help to identify samples that exhibit similar behavior. This allows an analyst to discard reports of samples that have been seen before, while focusing on novel, interesting threats. Unfortunately, previous techniques do not scale well and frequently fail to generalize the observed activity well enough to recognize related malware.

PROBLEM DEFINITION:

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.

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.

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.

Drawbacks:

We present an adaptive end-host anomaly detector where a supervised classifier trained as a traffic predictor is used to control a time-varying detection threshold. Using real enterprise traffic traces for both training and testing, we show that our detector outperforms a fixed-threshold detector.

This comparison is robust to the choice of off-the shelf classifier and to a variety of performance criteria, i.e., the predictor's error rate, the reduction in the "threshold gap," and the ability to detect incremental worm traffic that is added to real life traces. Our adaptive-threshold detector is intended as a part of a distributed worm detection system.

This distributed system infers system-wide threats from end-host detections, thereby avoiding the sensing and resource limitations of conventional centralized systems. The system places a constraint on this end-host detector to appear consistent over time and host variability.

PROBLEM STATEMENT:

We introduce a proposal for inter-region routing based on both probabilistic and deterministic forwarding mechanisms, embedded in an architectural framework able to support it. We also compare our solution to existing approaches in delay tolerant networking, discussing the main requirements and possible solutions, and outlining the open research problems.

1. We present a general behavioral characterization of proximity malware, which captures the functional but imperfect nature in detecting proximity malware.

2. 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 vs. evidence collection risk.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Advantages:

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.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.

IMPLEMENTATION :
Store and forward message switching:

Hold data until it has a scheduled transfer in network storage. Suppose not view the message means delivery status is not received otherwise receives status.

Delay-tolerant networking:

A Delay-Tolerant Network (DTN) is a general-purpose overlay network that operates on top of varying regional networks, including the Internet. DTNs allow regional networks with varying delay characteristics to interoperate by providing mechanisms to translate between their respective network parameters. Therefore, the underlying protocols and technologies for these regional networks may differ considerably, but the flexibility of the DTN architecture allows them to be connected to each other.

Gateway:

Gateway is designed to forward bundles between two or more DTN region networks and may optionally act as a host. The bundle overlay of gateways must have persistent storage and allow custody transfers. Gateways link together networks that operate on different lower-layer protocols.

Router:

Router works within a single DTN region and is responsible for forwarding bundles.Such user requires persistent storage to queue and keep bundles until outbound.

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, 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.

FUTURE WORK:

In this model, we define communities that are visited often by the nodes to capture skewed location visiting preferences, and use time periods with different mobility parameters to create periodical re-appearance of nodes at the same location. We have clearly observed these two properties based on analysis of empirical WLAN traces. In addition to the proposal of a realistic mobility model, we derive analytical expressions to highlight the impact on the hitting time and meeting times if these mobility characteristics are incorporated. These quantities in turn determine the packet delivery delay in mobility-assisted routing settings.

REFERENCE:

[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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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 detectionat the end host," in Proc. USENIX Security, 2009.

[9] U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, andE. Kirda, "Scalable, behavior-based malware clustering,"in Proc. IEEE NDSS, 2009.

[10] D. Dash, B. Kveton, J. Agosta, E. Schooler, J. handrashekar, 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.

AUTHORS BIOGRAPHY:

Mahmoud Saeed Al-Jabari,pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.

T. Ramdas Naik ,Assistant Professor Dept, Computer Science (PG), Qualifications : B.E, MCA,M.Tech,(Ph.D) Nizam College (Autonomous),O.U, Basheer Bagh, Hyderabad, India.