Improve Accurate Functionality of Delay Tolerant Networks

Mr. Ashwani Kumar
MCA 3rd Year, II Sem,
CMR College of Engineering & Technology,
Hyderabad.

Ch.Dayakar Reddy
MCA, M-Tech, MPhil, Ph.D,
Professor and HOD,
CMR College of Engineering & Technology,
Hyderabad.

ABSTRACT:

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 (“in sufficient 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.

INTRODUCTION:

The popularity of mobile consumer electronics, like laptop computers, PDAs, and more recently and prominently, smart phones, 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 jailbroken 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 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 system, 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. 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. Instead of assuming a sophisticated malware containment capability, such as patching or self-healing, 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 system, 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 Naïve Bayesian model, which has been applied in filtering email spams, detecting botnets, and designing IDSs, 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. Our contributions are summarized below.

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" problem.

3. We consider the benefits of sharing assessments among nodes, and address challenges derived from the DTN model: liars (i.e., bad-mouthing and false praising malicious nodes) and defectors (i.e., good nodes that have turned rogue due to malware infections). We present two alternative techniques, dogmatic filtering and adaptive look-ahead, that naturally extend look-ahead to consolidate evidence provided by others, while containing the negative effect of false evidence.

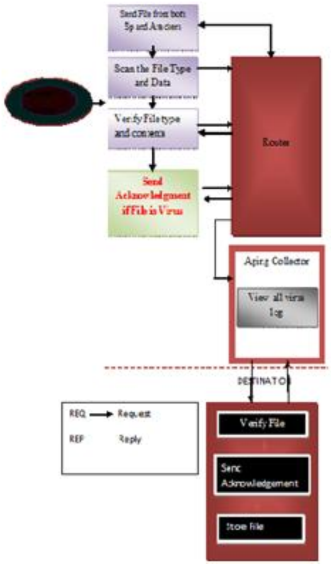
EXISTING SYSTEM:

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.

PROPOSED SYSTEM:

We introduce a proposal for inter-region routing based on both probabilistic and deterministic forwarding mechanisms, embedded in an architectural frame-work 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.

SYSTEM ARCHITECTURE:


Send File from both Sp and Anders
Scan the File Type and Data
Verify File type and contents
Send Acknowledgment if File is Virus
Router
Aging Collector
View all virus log
DESTINATOR
REQ → Request
REP Reply
Verify File
Send Acknowledgement
Store File

IMPLEMENTATION

Service Provider

In this module, the Service Provider browses the required file and uploads to the particular end user (End User A, End User B, End User C, End User D) via Delay Tolerant Router.

DTN Router

The Delay Tolerant Network Router consists of Warm Filter, which is responsible for forwarding file for destination (End User A, End User B, End User C, End User D). The Warm Filter scans each and every file in the router and then forwards to dedicated destination, If found any malware in the scan then it forwards to the Evidence Aging collector. In Router can view the files scanned and transmitted with their tags File Name, Destination node details.

Malware Files

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.

Evidence Aging Collector

The Evidence aging collector is responsible to scan and block the malicious infected file. 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 solve the problem of outdated assessments, old assessments are discarded and to save the end user by infected malware file in a process called evidence aging.EAC can view the Virus Name, attacker IP, attacked time, Result.

End User

In this module, the End user can Recieve the data file from the Service Provider and end user who will receive file contents scanned by the warm filter in the Delay Tolerant Network Router.

Attacker:

In this module, the Attacker browses the malicious file and uploads to the particular end user (End User A, End User B, End User C, End User D). The malicious nodes those are able to transmit malware to the destination.

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.

REFERENCES:

Trend Micro Inc. (2004) SYMBOS CABIR.A. [Online]. Available: http://goo.gl/aHcES

Trend Micro Inc. (2009) IOS IKEE.A. [Online]. Available: http://goo.gl/z0j56

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.

A. Lee. (2012) FBI warns: New malware threat targets travelers, infects via hotel Wi-Fi. [Online]. Available: http://goo.gl/D8vNU
NFC Forum. About NFC. [Online]. Available: http: //goo.gl/zSJqb

Wi-Fi Alliance. Wi-Fi Direct. [Online]. Available: http: //goo.gl/fZuyE

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.

U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering," in Proc. IEEE NDSS, 2009.

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.

G. Zyba, G. Voelker, M. Liljenstam, A. M´ehes, and P. Johansson, "Defending mobile phones from proximity malware," in Proc. IEEE INFOCOM, 2009.

F. Li, Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in smartphone-based mobile networks," in Proc. IEEE INFOCOM, 2010.

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.

P. Graham. Better Bayesian filtering. [Online]. Available: http://goo.gl/AgHkB

J. Zdziarski, Ending spam: Bayesian content filtering and the art of statistical language classification. No Starch Press,2005.