An Optimal Distributed Malware Defense System For Mobile Networks With Heterogeneous Devices

S.Mabjan , S.Rajiya sulthana

CSE,BCETW,KADAPA , AP, INDIA

CSE,BCETW,KADAPA , AP, INDIA

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. 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. Real mobile network traces are used to verify the effectiveness of the proposed methods.

Keywords: delay-tolerant networks; proximity malware; behavioral malware characterization; Bayesian filtering

1.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 infrastructuremodel. An early example of proximity malware is theSymbian-based *Cabir* worm, which propagated as a SymbianSoftware Installation Script. Proximity malware based on the DTN model brings unique security challenges that are not present in theinfrastructure model.Individua lobservations maybe *imperfect*, but abnormal behaviors of infected nodesare *identifiable* in the long-run. Real contact traces are used to verify the effectiveness of the methods.

2.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.

2.1 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.

3.Equations

$$S_i = \lim_{N \to \infty} \frac{s_N}{N}.$$

By Equation (1), Si [0, 1]. A number Le (0, 1) ischosen as the *line between good and evil*.

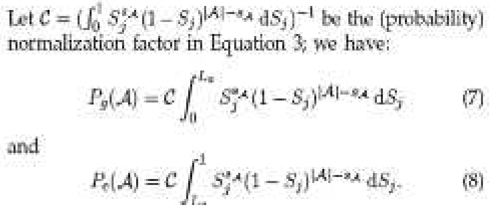
$$P(S_j|\mathcal{A}) \propto P(\mathcal{A}|S_j) \times P(S_j).$$

P(Sj) encodes our prior belief on j's suspiciousness Sj ;P(A|Sj) is the likelihood of observing the assessment sequenceA given Sj.

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

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

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



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

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

and

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

5.Conclusion:

Behavioral characterization of malware is an effectivealternative to pattern matching in detecting malware,especially when dealing with polymorphic or obfuscatedmalware. We present *look-ahead*, along with *dogmatic fil-tering* and *adaptive look-ahead*, to address two uniquechallenging 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 characterizationof proximity malware to account for strategic malwaredetection evasion with game theory is a challenging yetinteresting future work.

References

Journal papers:

[G. Yan, H. Flores, L. Cuellar, N. Hengartner, S. Eidenbenz,and V. Vu, “Bluetooth worm propagation: mobility pattern matters!” in *Proc. ACM ASIACCS*, 2007.

Books:

S. Cheng, W. Ao, P. Chen, and K. Chen, “On modeling malware propagation in generalized social networks,”*IEEE Comm. Lett.*, vol. 15, no. 1, pp. 25–27, 2011.

Chapters in Books:

E. Daly and M. Haahr, “Social network analysis for informationflow in disconnected delay-tolerant MANETs,”*IEEE TMC*, vol. 8, no. 5, pp. 606–621, 2009.

Theses:

A. Srinivasan, J. Teitelbaum, and J. Wu, “*DRBTS: Distributedreputation-based beacon trust system*,” in *Proc.IEEE DASC*, 2006