ISSN NO: 9726-001X
Volume 03 Issue3, July 2015

JOURNAL OF CURRENT SCIENCE

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

Ashwini

RSCOE, Pune, India

Abstract

the difficulty of sending and receiving messages inside the same network
With the proliferation of short-range communication technologies like Bluetooth, NFC, and Wi-Fi Direct in today's mobile consumer electronics, the delay-tolerant-network (DTN) model is emerging as a practical communication alternative to the conventional infrastructure paradigm. Malware belonging to the category of "proximity" takes advantage of the accidental interactions and decentralized structure of DTNs to spread. We highlight two distinct obstacles ("insufficient evidence vs. evidence gathering risk" and "filtering false evidence sequentially and distributedly") to bringing Bayesian malware detection to DTNs, and we offer a simple yet effective solution: look-ahead. The efficiency of the suggested approaches is tested using real mobile network traces.

Bayesian filtering; delay-tolerant networks; proximity malware; characterisation of malware's behavioral patterns;

1.INTRODUCTION

Almost all the existing work on routingin delay tolerant networks has focused on theinfrastructure 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. THE CURRENT SETUP

Routing in delay-tolerant networks has hitherto only seen work on infrastructure and naming. However, in many deployment scenarios, especially in developing regions, it will be necessary to route between regions composed of several heterogeneous types of network domains, such as satellite networks and ad hoc networks composed of short-range radio enabled devices, such as mobile phones with Bluetooth interface.

The widespread use of portable devices like laptops, PDAs, and most recently, smartphones, has resuscitated the delay-tolerant- network (DTN) concept as an alternative to conventional infrastructure.

1.1 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 theopen research problems.

2.Equations

ISSN NO: 9726-001X
Volume 03 Issue3, July 2015

JOURNAL OF CURRENT SCIENCE

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

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

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

and

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

5.Conclusion:

If you're trying to identify polymorphic or obfuscated malware, you may want to try behavioral characterisation instead of relying just on pattern matching. In order to tackle two distinct difficulties in bringing Bayesian filtering to DTNs, we provide look-ahead coupled with dogmatic filtering and adaptive look-ahead. These difficulties are "insufficient evidence vs. evidence collecting risk" and "filtering false evidence sequentially and distributedly," respectively. To account for strategic malware detection evasion using game theory is a tough but intriguing future topic that might be accomplished by extending the behavioral definition of proximity malware

.References Journal papers:

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

Books:

According to "On modeling malware spread in generalized social networks," published in IEEE Comm. Lett., volume 15, issue 1, pages 25-27, by authors S. Cheng, W. Ao, P. Chen, and K. Chen in 2011.

Book Sections:

Social network analysis for information flow in disconnected delay-tolerant MANETs, E. Daly and M. Haahr, IEEE Transactions on Mobile Computing, volume 8, issue 5, pages 606-621, 2009.

Theses:

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