Proximity Malware Detection in Delay Tolerant Networks

M. Srikanth
M.Tech, Software Engineering
S.R. Engineering College, Warangal
E. Raju
Associate Professor, Department of CSE
S.R. Engineering College, Warangal

Abstract: *With the universal presence of short-range property technologies (e.g., Bluetooth and, a lot of recently, Wi-Fi Direct) within the shopper physical science market, the delay tolerant network (DTN) model is changing into a viable various to the standard infrastructural model. During this paper, we have a tendency to address the proximity malware detection and containment drawback with express thought for the distinctive characteristics of DTNs. we have a tendency to formulate the malware detection method as a call drawback underneath a general behavioural malware characterization framework. we have a tendency to analyze the chance related to the choice drawback and style a straightforward nevertheless effective malware containment strategy, look-ahead, that is distributed naturally and reflects a private node's intrinsic trade-off between staying connected (with different nodes) and staying safe (from malware). moreover, we have a tendency to think about the advantages of sharing assessments among directly connected nodes and address the challenges derived from the DTN model to such sharing within the presence of liars (i.e., malicious nodes sharing false assessments) and defectors (i.e., smart nodes that have turned malicious thanks to malware infection).*

Index Terms: Delay-tolerant networks, Proximity malware, and Behavioral malware characterization.

1. INTRODUCTION

Mobile shopper natural philosophy permeate our lives. laptop computer computers, PDAs, and additional recently and conspicuously, smart-phones, are getting indispensable tools for our educational, skilled, 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 combined exacerbate the malware problem in DTNs. Malware could be a piece of malicious code that disrupts the host node's practicality and duplicates and propagates itself to different nodes via contact opportunities. within the ancient infrastructural model, the carrier is a gatekeeper UN agency will centrally monitor network abnormalities and inhibit malware propagation; what is more, the resource bottleneck for individual nodes naturally limits the impact of the malware. However, the central gatekeeper and natural limitations ar absent within the DTN model. Proximity malware, that exploits the temporal dimension and distributed nature of DTNs in self-propagation, poses serious threats to users of latest technologies and challenges to the networking and security analysis community. a typical malware detection technique presently in apply is pattern matching. additional concretely, a sample of malware is 1st according by associate degree infected user. The sample is analyzed by security specialists, and a pattern that (hopefully) unambiguously identifies the malware is extracted; the pattern are often either code or knowledge, binary or matter. The pattern is then used for the detection of malware. 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. During 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 suspects another node j of being infected with the malware, i could stop to attach within the future. we wish to explore however so much such a straightforward technique will take United States of America. Our focus is on however individual nodes build such cut-off choices supported direct and indirect observations.

Due to the temporal dimension and distributed nature of DTNs, the key challenge visaged by the proximity malware behavioural detection and containment mechanism could be a call problem: once to cut-off? This challenge are often compared with a remarkable example in reality. once someone smells one thing burning, he or she is facing with 2 decisions. One is to decision the fireplace emergency service immediately; the opposite is to gather additional proof and to form a additional wise to call later. the primary selection is related to a high value for a attainable false fireplace alarm, whereas the second selection is related to the danger of losing the first chance of containing the fireplace. we have a tendency to face an identical perplexity within the context of proximity malware in DTNs. Hyper-sensitivity results in high false positive whereas hypo-sensitivity results in high false negative. In this paper, we have a tendency to gift a straightforward nonetheless effective resolution that reflects a private node's intrinsic trade-off between staying connected with different nodes and staying safe from the malware. we have a tendency to additionally take into account the advantages of sharing observations among nodes and address the challenges of liars and defectors derived from the DTN model.

2. RELATED WORK

Consider a DTN consisting of n nodes. The neighbors of a node ar the nodes it's contact opportunities with. every node keeps a log, chronologically recording the neighbors it had contact with, and uses this log to estimate its contact pattern with them. A proximity malware could be a piece of malicious code that disrupts the host node's practicality and encompasses a likelihood of duplicating itself to different nodes throughout inter-nodal communication; once duplication happens, we are saying the opposite node is infected by the malware. Suppose every node is capable of assessing the opposite party for suspicious actions when every encounter, leading to a binary assessment of either suspicious or non-suspicious. An example of a suspicious action is sending a self-signed program which modifies system configurations. At any particular time, we say a node's nature is either evil or good based on if it is or is not infected by the malware. We assume that the suspicious-action assessment is an imperfect, but functional indicator of malware infection: it may assess an evil node's actions as "non-suspicious" (or a good node's actions as "suspicious") at times, but most suspicious actions are correctly attributed to evil nodes. Before proceeding to further discussions, we make explicit the assumptions in the neighborhood-watch model: an evil node's behavior is consistent and non-targeted.

- **Consistency:** This rephrases the functional assumption in characterizing a node's nature by the suspiciousness (Equation 1). Only those nodes with suspiciousness higher than the threshold Le are capable of transmitting the malware. In other words, a node cannot do the evil (transmitting the malware) and pretend to be good (maintaining a low suspiciousness).
- **Non-targetedness:** An evil node j's suspicious actions should be observable to all of its neighbors rather than a specific few. Otherwise, if j targets at i, i's other neighbors' opinions, even faithful ones, only confuse i. This assumption is vital to all evidence collecting methods which incorporate neighbors' observations.

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. The Delay Tolerant Networks (DTNs) are especially useful in providing mission critical services including emergency scenarios and battlefield applications. However, DTNs are vulnerable to wormhole attacks, in which a malicious node records the packets at one location and tunnels them to another colluding node, which replays them locally into the network. Nodes in disruption tolerant networks (DTNs) usually exhibit repetitive motions. Several recently proposed DTN routing algorithms have utilized the DTNs' cyclic properties for predicting future forwarding. Opportunistic data forwarding can be abused by an adversary by injecting spurious packets in order to waste the resources of the network. Security and privacy are critical for DTNs.

DTN NETWORK MODEL:

The DTN graph is a directed multi-graph, in that a lot of than one edge (also referred to as link) might exist between a combine of nodes (see Figure 2). the explanation for employing a impress is straightforward: it's going to be doable to pick between 2 distinct (physical) association varieties to maneuver knowledge between a similar combine of nodes. what is more, the link capacities (and to a lesser extent, propagation delay) ar time-dependent (capacity is zero now and then once the link is unavailable). Thus, the set of edges within the graph should capture each time-varying capability and propagation delay further as multiple parallel edges. a straightforward example of a foothold captured by this description involves a ground station and a LEO satellite rising, passing directly overhead, and setting at the alternative horizon. because it rises, its data rate can usually increase till it's directly overhead and can decrease for the remaining time of the pass. this is often as a result of noise is negligible once the satellite is directly overhead however will increase at lower elevations.

Another example would be a bus (carrying a wireless access point) passing by a village. The outturn of the wireless link would rely on the gap of the bus from the village. once no communication is feasible, the sting is assigned zero capability. whereas DTN applications ar expected to be tolerant of delay, this doesn't mean that they'd not to a lower place from cut delay. what is more, we tend to believe this metric is Associate in Nursing acceptable live to use in exploring the differential analysis of many routing algorithms in Associate in Nursing application-independent manner. Minimizing delay lowers the time messages pay within the network, reducing competition for resources (in a qualitative sense). Therefore, lowering delay indirectly improves the likelihood of message delivery.

3. IMPLEMENTATION

Proximity malware and existing interference schemes. variety of studies demonstrate the severe threat of proximity malware propagation. Su et al. collected Bluetooth scanner traces and used simulations to point out that malware will effectively propagate via Bluetooth. Yan et al. developed a Bluetooth malware model. Satyendra N. Bose and Shin showed that malware that uses each SMS/MMS and Bluetooth will propagate quicker than by electronic messaging alone. instead of assumptive a complicated malware containment capability, like repair or self-healing in previous works, we tend to base our style on quarantine and develop a choice mechanism mistreatment direct and indirect observations to upset proximity malware. Packet forwarding in mobile networks. In mobile networks, one cost-efficient thanks to route packets is via shortrange communication capabilities of intermittently connected good phones. whereas early add mobile networks used a range of oversimplified random id. models, like random waypoint, recent findings show that these models might not be realistic. Moreover, several recent studies, supported real mobile traces, disclosed that nodes' quality showed sure social network properties. we tend to use 2 real mobile network traces in our study.

Trust analysis schemes. we tend to base our style on the observation that trust evaluations will link past experiences with future predictions. numerous frameworks are designed to model trust relationships. 3 faculties of thoughts emerge from studies. the primary one uses a central authority, that by convention is named the trusty third party. within the second college, one international trust worth is drawn and printed for every node, supported different nodes' opinions of it. EigenTrust is Associate in Nursing example. The last college includes the trust management systems that enable every node to own its own read of different nodes. not like these works, we tend to judge trait on items of proof instead of on individual nodes; this permits America to promptly deal with dynamical nature of nodes with minimum overhead.

Protecting a victim (host or network) from malicious traffic could be a arduous drawback that needs the coordination of many complementary elements, as well as untechnical and technical solutions. The implementing malware detection and access management rules area unit terribly tedious as a result of the network has such a lot of vulnerabilities and security problems. The projected system introduces a replacement protocol that is known as as COMPACT (Combinatorial optimum Malware Proclamation And Content Tracking). The decentralized approach provides effective rule matching and verification method within the network whereas information transmission. Access management List has additionally applied so as to take care of black and white list of users and nodes for effective information restriction. The importance of the COMPACT protocol is facilitating an answer against filter choice drawback.

CONCLUSION

In this paper, we tend to address the proximity malware detection and containment drawback with express thought for the characteristics of DTNs. instead of counting on a selected malware detection technique (e.g., infectious agent pattern matching), we tend to propose a general activity characterization of malware infection, that permits for useful however imperfect assessments on malware presence. beneath this framework, we tend to formulate the malware detection method as a call drawback, analyze the danger related to the choice drawback, and style an easy however effective malware containment strategy, lookahead, that is distributed naturally and reflects a private node's intrinsic trade-off between staying connected (with alternative nodes) and staying safe (from malware). what is more, we tend to contemplate the advantages of sharing assessments among directly connected nodes and address the challenges derived from the DTN model within the presence of liars (i.e., malicious nodes sharing false assessments) and defectors (i.e., sensible nodes that have turned malicious because of malware infection). Real mobile network traces area unit accustomed verify our analysis. In prospect, the projected activity malware characterization and therefore the bestowed malware detection and containment technique give clearer understanding on the bar of proximity malware in DTNs and function a foundation for future work on this line.

REFERENCES:

[1] NFC Forum. about NFC, http://goo.gl/zSJqb, 2013.

[2] Wi-Fi Alliance. Wi-Fi Direct, http://goo.gl/fZuyE. 2013.

[3] CPLEX: Linear Programming Solver. http://www.ilog.com/.

[4] DTN Research Group. http://www.dtnrg.org/.

[5] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. In ACM SIGCOMM, Aug. 2003.

[6] L. R. Ford and D. R. Fulkerson. Flows in Networks. Princeton University Press, 1962.

[7] V. Erramilli, M. Crovella, A. Chaintreau, and C. Diot, "Delegation forwarding," in Proc. of MobiHoc. ACM, 2008.

[8] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling time-variant user mobility in wireless mobile networks," in Proc. of INFOCOM. IEEE, 2007.

[9] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in Proc. of MobiHoc. ACM, 2007.

[10] N. Djukic, M. Piorkowski, and M. Grossglauser, "Island hopping: Efficient mobility-assisted

forwarding in partitioned networks," in Proc. of SECON. IEEE, 2006.

[11] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618–644, 2007.

[12] Trend Micro Inc. SYMBOS_CABIR.A., http://goo.gl/aHcES, 2004.

[13] http://goo.gl/iqk7, 2013.

[14] Trend Micro Inc. IOS_IKEE.A., http://goo.gl/z0j56, 2009.