The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 4 || Pages || PP.01-04|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Behavioral Malware Detection in Dtn Using Intrusion Detection System

[1]R.Sankari Devi, [2]R.Dinesh Kumar
[1]*PG Scholar, Department of Computer Science and Engineering , Bharathiyar College Of Engineering And Technology, Karaikal*
[2]*Assistant Professor , Department of Computer Science and Engineering, Bharathiyar College Of Engineering and technology.karaikal*

----------**ABSTRACT**----------
The delay-tolerant-network (DTN) model is becoming a viable communication to communicate with short-range technologies such as Bluetooth, NFC and Wi-Fi Direct. Proximity malware is a malicious program that spreads critically. 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 frequency based method to detect the malware in delay tolerant network. We identify the challenges in frequency based model such as frequency coexistence, non location aware and hidden duplicate source. We propose effective technique such as location based model, intrusion detection system and random routing procedure to address the challenges.

Keywords *– frequency coexistence ,hidden duplicate source ,nonlocation aware ,pattern matching*

------Date of Submission: 31-March-2015 Date of Accepted: 20-April-2015

I. INTRODUCTION

1.1SCOPE OF PROJECT

1.1.1 Distance Based Detection

The distance-based redeployment detection is based on the following insight: without node redeployment attack, the monitee's location will not change and the distance measurements at its neighboring nodes should be consistent, respectively. Thus, if the monitee is redeployed into a different location, a monitor can detect the redeployment by noticing the inconsistency in the distance measurements. In other words, the distributions of the distance measurements before and after redeployment are different. More specifically, if a monitor makes before and after distance measurements on the monitee, it can calculate the difference between the before and after distance-measurement pairs and determine whether that monitee has been redeployed or not. The before measurement, which consists of a set of distance measurements, is collected right after the initial deployment, and we denote the set of data in before measurement as the reference-set. The after measurement is done at sometime thereafter and we denote the collected data set at this time as the testing-set.

1.1.2 Re-Routing

Rerouting, sometimes known as chaining or parent/child, allows you to route Helix Universal Rerouting requests through other Helix Universal Rerouting. The rerouting routing feature instructs Helix Universal Rerouting to look at the address of the requested material, and to send it either to a specific Helix Universal Rerouting, or to send it directly to the Helix Universal Server that hosts the content. The main Helix Universal Rerouting which handles requests bound for the Internet is called the parent Helix Universal Rerouting; the Helix Universal Rerouting located closest to the clients are called child Helix Universal Rerouting. Typical uses for this feature include routing all requests for locally-served material directly to the Helix Universal Server, and forwarding all other requests through a gateway Helix Universal Rerouting.

1.1.3 Localization System

We have developed a general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy-to-plug-in localization algorithms. It is built around four

logical components are Transmitter, Landmark, Server, Solver. Transmitter: Any device that transmits packets can be localized. Oftentimes, the application code does not need to be altered on a sensor node to localize it.

Landmark: The Landmark component listens to the packet traffic and extracts the RSS reading for each transmitter. It then forwards the RSS information to the Server component. The Landmark component is stateless and is usually deployed on each landmark or AP with known locations.Server: A centralized server collects RSS information from all the Landmark components. The identity-based detection is performed at the Server component. The Server component summarizes RSS information such as averaging or clustering and then forwards the information to the Solver component for localization estimation.

1.2 OVERVIEW OF PROJECT

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 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.

II. LITERATURE SURVEY

2. MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks

MASK and D-ANODR have problems in meeting the un-indentify ability and un-link ability. The node IDs in a neighborhood and along a route are possibly exposed in SDAR and Anon-DSR, respectively. The plain node IDs are used in the route request of MASK and D-ANODR. In this work, we use the node's pseudonym instead of its real ID, to avoid the information leakage during RREQ and RREP processes.

Some of the protocols adopt additional authentication schemes to sign the routing packets, including A3RP, RAODR, USOR, and PRISM. Although MASK provides neighborhood authentication, it cannot sign the routing packets. RAODR deploys a master key mechanism, which cannot provide the anonymity, traceability, and enforceability that are supported by a group signature. The drawbacks are Each protocol is active against different attacks,Collective approach is not feasible, Coverage changes is not possible for a dynamic environment.

EXITING SYSTEM

Consider a DTN consisting of 'n' nodes. The neighbors of a node are the nodes it has (opportunistic) contact opportunities with. 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. 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. For example, a node can assess a Bluetooth connection or a SSH session for potential Cabir or Ikee infection. The watchdog components in previous works on malicious behavior detection in MANETs and distributed reputation systems are other examples. A node is either evil or good, based on if it is or is not infected by the malware. The suspicious-action assessment is assumed to be an imperfect but functional indicator of malware infections: 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. A previous work on distributed IDS presents an example for such imperfect but functional binary classifier on nodes' behaviors.

2.1.1 Neighborhood Watch

Besides using own assessments, incorporate other neighbors' assessments in the cut-off decision against another node. This extension to the evidence collection process is inspired by the real-life neighborhood (crime) watch program, which encourages residents to report suspicious criminal activities in their neighborhood. Similarly, i shares assessments on j with its neighbors, and receive their assessments on 'j' in return. In the neighborhood-watch model, the malicious nodes that are able to transmit malware (we will see next that there may be malicious nodes whose objective is other than transmitting malware) are assumed to be consistent over space and time. These are common assumptions in distributed trust management systems, which incorporate neighboring nodes' opinions in estimating a local trust value. By being consistent over space, we

mean that evil nodes' suspicious actions are observable to all their neighbors, rather than only a few. If this is not the case, the evidence provided by neighbors, even if truthful, will contradict local evidence and, hence, cause confusions.

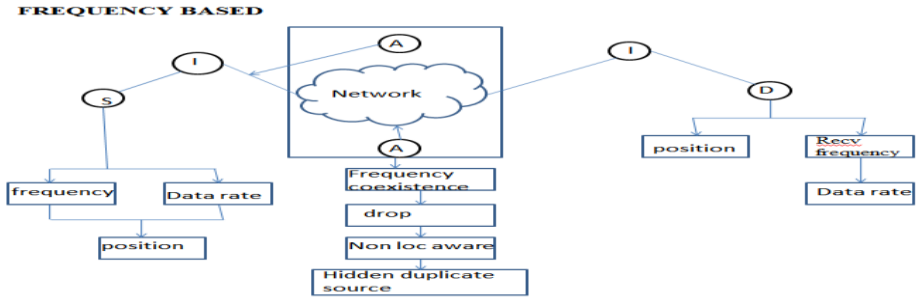
PROPOSED SYSTEM

Using location based system the malware is detected using distance based calculation.To address the challenges we use a simple yet effective techniques such as intrusion detection system and random routing procedure.

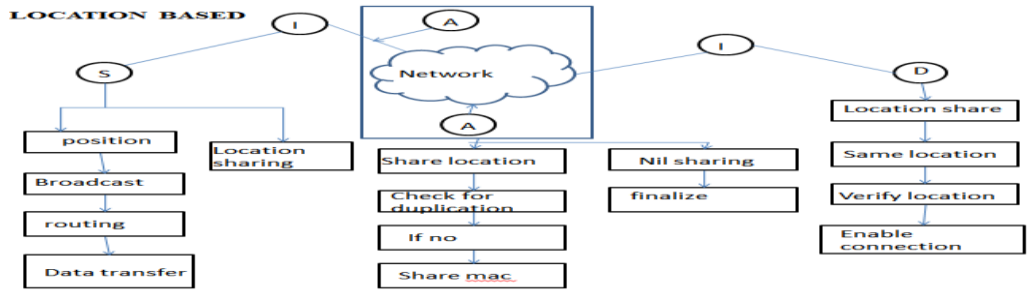
III. SYSTEM ARCHITECTURE DESIGN

3.1 Network Diagram

3.1.1 frequency based



3.1.2 Location based



IV SYSTEM IMPLEMENTATION

4.1 Modules with description

4.1.1 Distance based node detection

Recent technological advances have made it possible to deploy large scale sensor networks consisting of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate in short distances through wireless links. Such networks have a wide range of applications in civilian and military operations such as target tracking and battlefield surveillance. Many researchers have been attracted to develop protocols that can fulfill the requirements of these applications.

Sensors' locations play a critical role in many sensor network applications. Not only do applications such as environment monitoring and target tracking require sensors' locations to accomplish their tasks, but several fundamental techniques in wireless sensor networks also require sensors' locations. For example, in geographical routing (e.g., GPSR), sensor nodes make routing decisions at least partially based on their own and their neighbors' locations. However, due to the cost reasons, it is not practical to have a GPS receiver on every sensor node. In the past several years, many location discovery protocols have been proposed to reduce or completely remove the dependence on GPS in wireless sensor networks.

4.2.2 Location aware routing

The advancement in wireless communication and economical, portable computing devices has made mobile computing possible. One research issue that has attracted a lot of attention recently is the design of mobile ad hoc network (MANET). A MANET is one consisting of a set of mobile hosts which can communicate with one another and roam around at their will. No base stations are supported in such an environment. Due to considerations such as radio power limitation, power consumption, and channel utilization, a mobile host may not be able to communicate directly with other hosts in a single-hop fashion. In this case, a multi-hop scenario occurs, where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host. Applications of MANETs occur in situations like battlefields or major disaster areas, where networks need to be deployed immediately but base stations or fixed network infrastructures are not available. A

working group called "manet" has been formed by the Internet Engineering Task Force (IETF) to study the related issues and stimulate research in MANET.

V. CONCLUSION AND FUTURE WORK

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

[1] Chun-jen Chung, jeogkeun Lee and Dijiang Huang,"NICE:Network Intrusion Detection and Countermeasure Selection in Virtual Network System", IEEE trans.Dependable And Secure Computing, vol. 610,no.4, July/August2013.

[2] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security RiskManagement Using Bayesian Attack Graphs," IEEE Trans.Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb. 2012.

[3] L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts,"Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[4] R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Frameworkand Techniques," Proc. ACM Int'l Conf. Privacy, Security andTrust: Bridge the Gap between PST Technologies and Business Services (PST '06), pp. 37:1-37:10, 2006.

[5] S. Roschke, F. Cheng, and C. Meinel,"A New Alert CorrelationAlgorithm Based on Attack Graph," Proc. Fourth Int'l Conf.Computational Intelligence in Security for Information Systems, pp. 58-67 2011.

[6] A. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), June 2012.

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

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

[10] 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.

[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.

[13] I. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos, "An experimental comparison of naive bayesian and keyword-based anti-spam filtering with personal e-mail messages," in Proc. ACM SIGIR, 2000.

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

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

[16] R. Villamar´ın-Salom´on and J. Brustoloni, "Bayesian bot detection based on DNS traffic similarity," in Proc. ACM SAC.