ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Behavioral Characterization of Proximity Malware Detection Approach Which Based on Bayesian Model

J.Sairam Reddy
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. kirthikumar
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

B.Jaya laxmi
Assistant Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

Abstract:

Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.The Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware. The viable communication with mobile consumer electronics equipped with short range communication technologies such as Bluetooth, Wi-Fi Direct is DTN. There exists a general behavior characterization of proximity malware based on Naive Bayesian model, It was identified with two unique challenges for extending Bayesian malware detection to DTNs. We examine and implement a simple and effective method look ahead, to address the challenges with two extensions to look ahead, dogmatic filtering, and adaptive look ahead, they address the challenge of "malicious nodes sharing false evidence."

Keywords:

DTNs, Malware, Detection, Communications, Bayesian, behavioral malware characterization.

Introduction:

Abbreviated as DTN, Delay/Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications.

It is an experimental protocol developed by the Delay & Disruption Tolerant Networking Research Group, which operates under the Internet Research Task Force.DTN works using different kind of approach than TCP/IP for packet delivery that is more resilient to disruption than TCP/IP. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). The Bundle Protocol (BP) sits at the application layer of some number of constituent internets, forming a store-and-forward overlay network.

BP operates as an overlay protocol that links together multiple subnets (such as Ethernet-based LANs) into a single network. The basic idea behind DTN network is that endpoints aren't always continuously connected. In order to facilitate data transfer, DTN uses a store-and-forward approach across routers that is more disruption-tolerant than TCP/IP. However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity.

Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices.

Solutions have typically been modified from mobile ad hoc network and distributed security research, such as the use of distributed certificate authorities and PKI schemes. Original solutions from the delay-tolerant research community include: 1) the use of identity-based encryption, which allows nodes to receive information encrypted with their public identifier; and 2) the use of tamper-evident tables with a gossiping protocol.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is often disguised as, or embedded in, non-malicious files. As of 2011 the majority of active malware threats were worms or trojans rather than viruses.

EXISTING SYSTEM:

Existing worms, spam, and phishing exploit gaps in traditional threat models that usually revolve around preventing unauthorized access and information disclosure. The new threat landscape requires security researchers to consider a wider range of attacks: opportunistic attacks in addition to targeted ones; attacks coming not just from malicious users, but also from subverted (yet otherwise benign) hosts; coordinated/distributed attacks in addition to isolated, single-source methods; and attacks blending flaws across layers, rather than exploiting a single vulnerability. Some of the largest security lapses in the last decade are due to designers ignoring the complexity of the threat landscape.The increasing penetration of wireless networking, and more specifically wifi, may soon reach critical mass, making it necessary to examine whether the current state of wireless security is adequate for fending off likely attacks. Three types of threats that seem insufficiently addressed by existing technology and deployment techniques. The first threat is wildfire worms, a class of worms that spreads contagiously between hosts on neighboring APs.

We show that such worms can spread to a large fraction of hosts in a dense urban setting, and that the propagation speed can be such that most existing defenses cannot react in a timely fashion. Worse, such worms can penetrate through networks protected by WEP and other security mechanisms. The second threat we discuss is large-scale spoofing attacks that can be used for massive phishing and spam campaigns. We show how an attacker can easily use a botnet by acquiring access to wifi-capable zombie hosts, and can use these zombies to target not just the local wireless LAN, but any LAN within range, greatly increasing his reach across heterogeneous networks.

2.2 DISADVANTAGES:

* Viruses can cause many problems on your computer. Usually, they display pop-up ads on your desktop or steal your information. Some of the more nasty ones can even crash your computer or delete your files.

* Your computer gets slowed down. Many "hackers" get jobs with software firms by finding and exploiting problems with software.

* Some the applications won't start (ex: I hate mozilla virus won't let you start the mozilla) you cannot see some of the settings in your OS. (Ex one kind of virus disables hide folder options and you will never be able to set it).

To quantify these threats, we rely on real-world data extracted from wifi maps of large metropolitan areas in the country. Existing results suggest that a carefully crafted wireless worm can infect up to 80% of all wifi connected hosts in some metropolitan areas within 20 minutes, and that an attacker can launch phishing attacks or build a tracking system to monitor the location of 10-50% of wireless users in these metropolitan areas with just 1,000 zombies under his control.

2.3 PROPOSED SYSTEM:

In this paper, 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 naive Bayesian model, which

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

has been applied in filtering email, spams detecting botnets, and designing IDSs.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 versus evidence collection risk" 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.

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. A nice property of the proposed evidence consolidation methods is that the results will not worsen even if liars are the majority in the neighborhood traces are used to verify the effectiveness of the methods.

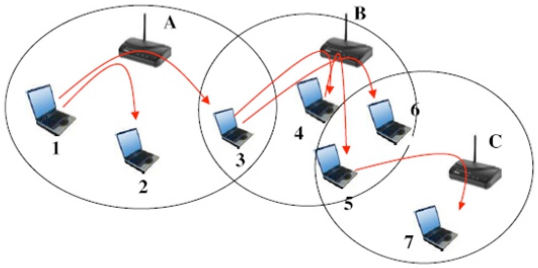
2.4 ADVANTAGES:

Two DTN specific, malware-related:

1. Insufficient evidence versus 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.

ARCHITECTURE DIAGRAM:



Modules:

1.Network Formation

2.Send Files from source to destination

3.Behavioral Malware Detection

4.Receive Files

Network Formation:

• Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.

• First create a delay tolerant network router frame then create many nodes.

• Without loss of generality, it will choose Le = 0.5 to be the linebetween good and evil. This network randomly pick10 percent of the nodes to be the evil nodes and assign themwith suspiciousness greater than 0.5; the rest of the nodes aregood nodes and are assigned suspiciousness less than 0.5.

Send Files from source to destination:

• File transfer is a generic term for the act of transmitting files over a computer networklike the Internet. There are numerous ways and protocols to transfer files over a network. Computers which provide a file transfer service are often called file servers. Depending on the client's perspective the data transfer is called uploading or downloading. File transfer for the enterprise now increasingly is done with Managed file transfer.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

• Here the source node wants to send a file to server. The source node wants to know about the destination behavior. So it used behavioral malware detection.
Behavioral Malware Detection:

• It will determine if a node is infected with malware through observing and assessing its behaviors in multiple rounds.

• Source node has N (pair wise) encounters with its neighbors and sN of them are assessed as suspicious by the other party.

• Assessments come from two models. 1. Household watch 2. Neighborhood watch. The Household watch source node's own assessments only. The Neighborhood watch source node own assessments with its neighbors'.

• In Household watch: Pg(A) >= Pe(A) Evidence A is favorable to j. Pg(A) <Pe(A) Evidence A is unfavorable to j. Instead of making the cut-j-off decision right away when Pg(A) <Pe(A), source node looks ahead to confirm its decision.

• In the Neighborhood watch, two cases are complicated:1. Liarsand 2. Defectors.

• Liars: Evil nodes whose purpose is to confuse other nodes bysharing false assessments.

• Defectors: Nodes which change their nature due to malware infection.

• The Evidence Consolidation propose two alternative methods, dogmatic filtering andadaptive look ahead , for consolidating evidence provided byother nodes, while containing the negative impact of liars.

Receive Files:

• If Pg(A) >= Pe(A) Evidence is favorable to destination else Pg(A) <Pe(A) Evidence is unfavorable to destination.

• If evidence is unfavorable, malware attack detected. It will break the file transfer.

• Else the source node files are sent to the destination successfully.

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. 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]Wei Peng, Feng Li , XukaiZou&Jie Wu, Behavioral Malware Detection in Delay Tolerant Networks, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014

[2] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, "Effective and Efficient Malware Detection at the End Host," Proc. 18th Conf. USENIX Security Symp.

[3] U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, Behavior-Based Malware Clustering," Proc. 16th Ann. Network and Distributed System Security Symp. (NDSS), 2009.

[4] 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," Proc. 21st Nat'l Conf. Artificial Intelligence (AAAI), 2006.

[5] G. Zyba, G. Voelker, M. Liljenstam, A. Me´hes, and P. Johansson, "Defending Mobile Phones from Proximity Malware," Proc. IEEE INFOCOM, 2009.

[6] F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based-Mobile Networks," Proc.IEEE INFOCOM, 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[7] 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," Proc. 23rd Ann.Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), 2000.

[8] P. Graham, "Better Bayesian Filtering," http://goo.gl/AgHkB, 2013.

[9] J. Zdziarski, Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification. No Starch Press, 2005.

[10] R. Villamarı´n-Salomo´ n and J. Brustoloni, "Bayesian Bot Detection Based on DNS Traffic Similarity," Proc. Acmymp. Applied Computing (SAC), 2013.

About Author's:

J.Sairam Reddy
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. kirthikumar
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

B.Jaya laxmi
Assistant Professor,
Depatment of CSE,
TKR College of Engineering & Technology.