International Journal of Research in Advent Technology, Vol.2, No.9, September 2014
E-ISSN: 2321-9637

Design and Development of Hybrid Malware Detection Technique Using Delay Tolerant Network

Nithya.K[1], Dr.A.Malathi[2]
[1]*M.Phil Scholar, Government Arts College, Coimbatore.*
[2]*Assistant Professor of Computer Science, Government Arts College, Coimbatore.*
nithya18k@gmail.com, malathi.arunachalam@yahoo.com

Abstract: In modern network the malware is one of the serious issues where it can be identified by many roles such as email spam, Denial of service and Trojan like viruses. DTN (Delay Tolerant Network) suffered from the above malware related problems. The proposed System introduces a novel malware detection technique in DTN. It deals with the evidence collection risk, false report identification and distribution problem. The system also identifies the misbehaving nodes by collecting and validating their evidence. The proposed system introduces a backtracking method which is used to track the previous behaviors and analysis and combinatorial optimization algorithm, which is a method that consists of finding optimal evidence and object from a finite set of objects and evidences. The method HMD is proposed to reduce the time.

Keywords: Delay tolerant network; malware detection and backtracking method.

1. INTRODUCTION

The Delay or Disruption tolerant protocols that govern the way nodes communicate on the Internet largely assumes that there are reliable low latency connections between any two points on the net. In real time several applications where we'd like to get the benefits of computer networking, the following example help to know more about DTN, NASA sends an instruction to a Mars Rover, there are both latency (speed of light delay) and disruption problems. Another example is the challenge of getting the benefits of the Internet to a village in a developing nation. Traditional telecommunications technology cannot reach it cost-effectively.

DTN System is based on complex technology; we may experience unexpected delays while communicate in the network development, improving the performance, deploying it on the network. Any modification in the DTN System entails similar development risks. At any given time, various new product introductions and enhancements to our DTN System are in the development phase and are not yet ready for commercial manufacturing or deployment. In addition, unexpected intellectual property disputes, failure of critical design elements, and a host of other execution risks may delay or even prevent the introduction of enhancements to our DTN System.

2. RELATED WORK

There are several common malware detection method [3] currently in practice is pattern matching, which is a supervised data matching technique. The existing pattern matching suffers from the following drawbacks 1.Processing overhead the lack of generality,2. High false positive rate in one round of analysis make it unsuitable for DTN applications in real-time. Proximity malware and mitigation [4][5] schemes has been proposed which helps to collect Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations.Some existing developed Bluetooth malware model.[6], which showed that Bluetooth can enhance malware, propagation rate over SMS/MMS.

Additionally some technique enhanced malware propagation through proximity channels in social networks and wide-area wireless networks. Late some techniques discussed optimal malware signature distribution in heterogeneous, resource-constrained mobile networks. In traditional, non-DTN, networks proposed to detect malware with learned behavioral model, in terms of system call and program flow. The final implementation extends the Naive Bayesian model[10], which has been applied in filtering email spam's, detecting botnets and designing IDSs and address DTN-specific, malware-related, problems.Random waypoint method has been applied,recent finding on these techniques these models may not be realistic.[7],[8]. optimal malware signature

distribution in heterogeneous, resource-constrained mobile networks. In traditional, non-DTN, networks proposed to detect malware with learned behavioral model, in terms of system call and program flow [9].

3. EXISTING SYSTEM

There are many different technologies available to detect malwares. Most of which rely on the internal structure rather than the behavior of the malware. Although the behavior of each of the transformation of a hidden malicious code is the same, the structure is different which means they can become difficult to detect depending on the amount of variation. There are some detection methods [2] which detect suspicious ability or behavior within a program, such as heuristic analysis; however these methods are rarely used as a sole means of virus protection as they are normally prone to false-positives.

Proximity malware based [1] 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) [11][12] 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) [13] usually exhibit repetitive motions. Several recently proposed DTN routing algorithms have utilized the DTNs' cyclic properties for predicting future forwarding. Opportunistic data forwarding [14] 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 [15].

4. PROBLEM DEFINITION

Although many schemes have been proposed to defend against malware attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. The packets injected by outsider attackers can be easily filtered with authentication techniques. However, authentication alone does not work when insider attackers inject packets and replicas with valid signatures. Thus, it is still an open problem is to address inject attacks in DTNs.

Most existing malware detection schemes are not a DTN specific; several existing failed to identify the malware exactly within the DTN. And several techniques suffered from several trust management problems. This also suffers from the insufficient evidence versus evidence collection risk and Sequential and distributed online evidence filtering is very complicated.

5. PROPOSED SYSTEM

Protecting a victim (host or network) from malicious traffic is a hard problem that requires the coordination of several complementary components, including nontechnical and technical solutions. The implementing malware detection and access control rules are very tedious because the network has so many vulnerabilities and security issues. The proposed system introduces a new protocol which is named as COMPACT (**C**ombinatorial Optimal **M**alware **P**roclamation And**C**ontent **T**racking**).** The

decentralized approach provides effective rule matching and verification process in the network while data transmission. Access Control List has also applied in order to maintain black and white list of users and nodes for effective data restriction. The importance of the COMPACT protocol is facilitating a solution against filter selection problem. Detection Applies invisible watermarking technique to track the spam initiator

- COMPACT protocol for fast malware node filter
- Malicious data detection before sending
- Rule based Malware detection filtering method
- Identifies the compromised machines

Algorithm: evidence collection process in COMPACT

Steps:

1. Get acknowledgement A from Node N.
2. If(N is a new user and acknowledgment is valid) then
3. Create node n in the evidence collection
4. Locate the evidence in the log
5. Verify the acknowledgement s with the signature P
    a. For each ack(si verifies P)
    b. If the parameter P valid
    c. Calculate age P for Node N in log T.
6. For all acknowledgement A containing p do
    a. If s is the last acknowledgement in T then

b. Append s in T based on the priority P.

7. End for
8. End

The aim of the system is to effectively and efficiently detect malicious code at every hop and host. The proposed system is an enhanced and optimal malware detection and elimination using content tracking and incorporates a prioriknowledge about a particular malware group in the network. The attacker can add malicious code while transmitting the data in the network. This is a challenging problem when end to end data verification. To overcome the problem, the system generates and verifies node behavior by generating detection models based on the observation of the node and malware programs. The system executes and monitors a anti malware program in a controlled analysis environment. Based on this observation it extracts the behavior that characterizes the execution of this program and node. The behavior is then automatically translated into detection and removal models that operate at very host in the network.

6. RESULT AND ANALYSIS

To evaluate the efficiency, four measures were used to evaluate the effectiveness. One is the number of modified entries, indicating how much the content of the original database is preserved. The other measures are defined as follows:

The following graph represents the time comparison between the existing and proposed systems.

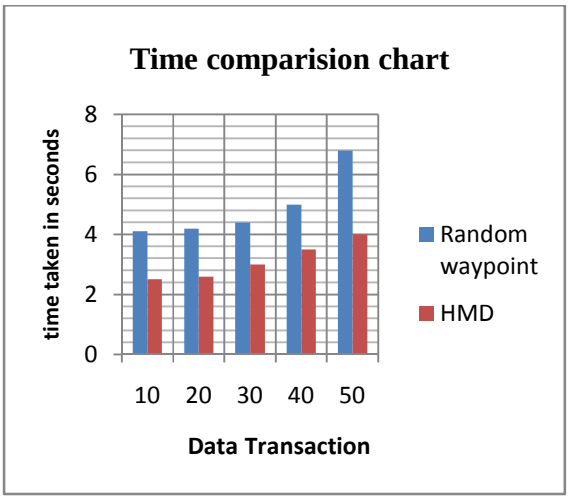

Fig 6.1Comparison chart based on the time

The above Figure 6.1 represents time comparison graph between existing random waypoint technique and proposed HMD protocol. In this graph the existing technique takes 6.2 seconds to complete this process, and HMD completes by 4 seconds. Comparing with several existing technique the process of HMD technique is high, so that the processing time is reduced.

7. CONCLUSION

The system overcomes the main three issues which are evidence collection risk and fake evidence identification and malicious code removal problem. The system also focused on the performance enhancement with two major metrics such as accuracy and detection time. To detection it use request - transmit and check scheme each node itself checks the number malicious code exists, and node carry the acknowledgement when they move, and cross-check if their carried claims are inconsistent when they contact. If node exceed the rate limit then declare the network contain flood attack**.**In this paper Comparing with several existing technique the process of HMD techniques is high, so that the processing time is reduced. This proves that HMD techniques are best of other techniques.

REFERENCES

[1] Peng, Wei, et al. "Behavioral Malware Detection in Delay Tolerant Networks."Parallel andDistributed Systems, IEEE Transactions on 25.1 (2014).

[2] Govindaraju, Aditya. "Exhaustive statistical analysis for detection of metamorphic malware." (2010).

[3] Tahan, Gil, LiorRokach, and Yuval Shahar. "Mal-id: Automatic malware detection using common segment analysis and meta-features." The Journal of Machine Learning Research 13.1 (2012).

[4] Mohaisen, Aziz, Omar Alrawi, and M. Larson. AMAL: Highfidelity, behavior-based automated malware analysis and classification. Verisign Labs, Tech. Rep, 2013.

[5] Ramu, Srikanth. "Mobile Malware Evolution, Detection and Defense." EECE 571B, TERM SURVEY PAPER (2012).

[6] Channakeshava, Karthik, et al. "High performance scalable and expressive modeling environment to study mobile malware in large dynamic networks."Parallel& Distributed Processing Symposium (IPDPS), 2011 IEEE International.IEEE, 2011.

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

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

[9] Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng, "An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices," Proc. IEEE Eighth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2011.

[10] 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.

[11] Ren, Yanzhi, et al. "Detecting wormhole attacks in delay-tolerant networks [Security and Privacy in Emerging Wireless Networks]." Wireless Communications, IEEE 17.5 (2010)

[12] Zhang, Zhensheng. "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges." Communications Surveys & Tutorials, IEEE 8.1 (2006):

[13] Li, Feng, Jie Wu, and AnandSrinivasan. "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets." INFOCOM 2009, IEEE.IEEE, 2009.

[14]Ansa, Godwin, Haitham S. Cruickshank, and Zhili Sun. "An Energy-Efficient Technique to Combat DOS Attacks in Delay Tolerant Networks." EAI Endorsed Trans. Ubiquitous Environments 1 (2012): e6.

[15] Kate, Aniket, Gregory M. Zaverucha, and UrsHengartner. "Anonymity and security in delay tolerant networks." Security and Privacy in Communications Networks and the Workshops, 2007.SecureComm 2007.Third International Conference on.IEEE, 2007.