Survey on Behavioral Malware Detection in Delay Tolerant Networks

Khadijah Mukhtar[1], Sharmin Nishad[2], Shailaja Patel[3], Nitya Gupta[4] , Latha N.R.[5]
Computer Science and Engineering, BMS College of Engineering,Bangalore

Abstract - **Delay Tolerant Networks (DTNs) are networks that are caused due to any delay in communication networks. Earlier, Delay Tolerant Networks were only used for long term communication; however, more recently, DTNs are also being used for short term communication such as those of mobile to mobile, laptop, Bluetooth and NFC. Malware detection in such short range communication networks is still unexplored. In this paper, we analyse different techniques by which malware can be detected in Delay Tolerant Networks and the various approaches of the same.**

Index Terms— **Malware, Malware Detection, Behavioral Methods, Signature Methods, Routing.**

I. INTRODUCTION

The term malicious software is what has been shortened to malware. An example of malware is a program installed on a computer or any other digital device without the knowledge of the user. This threatens the security of data stored on the device or the device's operation. The risk of such compromises taking place is clear to see since computers are used in almost every aspect of day-to-day life nowadays such as transportation, education, and communication, healthcare, finance, entertainment and so on. A multitude of tried and tested techniques are used to detect and defend against malware. A few of them are antivirus scanners (AVS), firewalls, etc. But today, the sort of people who create malware are, in many cases, one step ahead of the methods employed to root out malware.

A Delay Tolerant Network (DTN) is a general-purpose overlay network that operates on top of varying regional networks that includes the internet. DTNs permit regional networks with varying delay characteristics to operate together by providing mechanisms to translate between their respective network parameters. Therefore, the underlying protocols and technologies for these regional networks may differ significantly, but the flexibility of the DTN architecture allows them to be connected to each other.

II. LITERATURE SURVEY

Dolly Uppal et al [1] explained the various types of malware and their classification. The types of malware that exist broadly classified as are Virus, Worms, Trojans, Root kit, Spyware and Key loggers. The two main methods used to detect malware are: Signature Based, in which the malware detector searches for a pattern or a signature; and Anomaly Based, in which the malware detector searches for commands or instructions. To check for any malware, the detector searches for previously specified signatures or commands.

Jayalakshmi S. and M. Jeba Kumari [2] proposed a system which is based on behavioral detection technique. The aforementioned technique uses a game-theory approach which allows Delay Tolerant Networks to make strategic security decisions. Hence, the behavioral malware detection method effectively replaces the signature based malware detection technique. This technique also has low energy consumption and provides a high detection rate.

Zhu Kenan and Yin Baolin [3] analyzed the methodology based on the concept of the Naive Bayesian model. The Naive Bayesian model increases the efficiency, accuracy, and effectiveness of malware detection. In the primitive methods of malware detection, the focus was on what the system does and not on what was present in the program. The program is not checked for any errors but instead, the performance of the system is observe, making this model is the most practical model present. Behavioral characterization using the Naive Bayesian model is done in two steps. First, the expected normal behavior of the system is learnt. Secondly, the acquired knowledge about the system behavior is used in detecting malware. The behavior of the system plays an important role in the entire process.

Vineeth.S and Shiva Ranjani [4] described Delay Tolerant Networks (DTNs) as networks that are designed to provide communications in stressed and unstable environments. DTNs use store and forward message switching which have indefinite storage capacity. It is not necessary that all the nodes in a DTN have to have large storage capacity in order to maintain complete end to end integrity. DTNs are very vulnerable to malware attacks. They introduce a technique called HMD (Hybrid Malware Detection) which combines signature and behavior based techniques to help in accurate detection of malware.

Zahra Bazrafshan et al [5] described Malware as malicious code that is introduced to harm a computer or network. Based on their research there are many categories of malware.

- A Virus is a malicious code that copies itself onto other programs thus disrupting the normal functioning of the malware.
- A Worm is an independent program and does not need any other program for execution. It does not require an interface for its functioning.
- A Spyware is a program that is installed on the computer that controls the computer without the user's permission.

There are three main methods by which malware can be detected. They are Signature based, Behavior based and Heuristic methods. The diagram below [5] shows the classification of malware into signature based, Behavior based and Heuristic based.

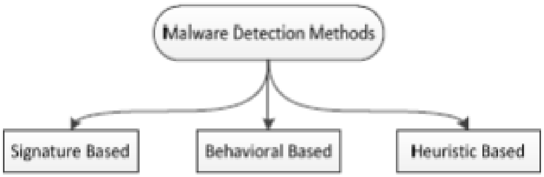

Fig 1 : Malware Detection Methods [5]

- Signature Based methods: A Signature is unique for each file. All the signatures are recorded and the detector checks the signature of the existing file with the pre existing signatures.
- Behavior Based methods: They concentrate on what the malware does rather than what it says. This was mainly used to overcome the shortcomings of signature based methods.
- Heuristic methods: These methods use data mining and machine learning to gather information about the file. Overcomes the disadvantages of Signature and Behavior based methods.

Vinod P., V.Lama, M.S Gore [6] analyzed the different malware detection techniques and their merits and demerits are discussed. These traditional methods are slow, inaccurate and inefficient. Due to quickly growing technology, many different types of malware are created. These traditional methods cannot cope with the malware of today. A technique is required which can deal with such malware. This method should be accurate and efficient. Hence, Behavioral Malware technique can be used for malware detection instead of the older and more traditional techniques.

Dr Farad Farah [7] presents Delay Tolerant Networks (DTNs) and their applications. These are networks that are designed to withstand a large amount of delay in them. A few examples of Delay Tolerant Networks are the Interplanetary Network and Military Tactical Network. Typically, Delay Tolerant Networks are used in long distance communication but now, their application is used even for short range communication networks. This feature also allows communication between two different networks (Inter Region Networks).

Moa Coho Chua et al [8] in their paper list the various schemes of routing in intra region domain of delay tolerant networks. Since, delay tolerant networks remain only periodically connected, the performance of each routing schemes vary. Routing schemes enable the ferrying of messages and backhaul links and their role in improving the efficiency of message transmission in delay tolerant networks. A detailed description of store and forward mechanism is given and how it is the most beneficial in inter region routing is explained.

Hemal Shah, Yogeshwar P. Kosta [9] list the different routing techniques, their efficiencies and the protocols for Delay Tolerant Networks. The techniques discussed in this paper are:

- Direct Delivery: Source waits until it comes into direct contact with the destination.
- Message Ferries: These are members of the network which are responsible for carrying the message along the right link and delivering it, unlike the other network members
- Forwarding Approach: The message is transmitted across to node in the route to the destination node and duplication is prevented.
- Mobile Vehicle Routing: The message is forwarded to the node which has the maximum probability of being a part of the route to the destination.

Wei Peng, Feng Li, Xukai Zou, Jie Wu [10] have published a paper through which it is explained that malware is a piece of malicious code that installs itself in a digital device and disrupts the functionality of the host computer .It duplicates itself and propagates to adjacent nodes with the help of contact opportunities. In traditional infrastructure models, where network abnormalities can be easily detected by gatekeepers and hence preventing any malicious node from entering the device, while in DTN's where nodes are directly connected prior to sending any information, malware can be easily installed. So DTN's are more prone to malware threats which now a days are being extensively used in short range communications such as mobile to mobile, Bluetooth, NFC's etc.the traditional practice that is being used till date is pattern matching which requires the analysis and extraction and an overhead of manual expertise labour.

Tao Young and Wang Xiao-Fang [11] give us an insight about another interesting routing technique called adaptive clustering hierarchy routing. This method combines single hop and multi hop along with hop by hop and multi hop techniques which is excellent for Delay Tolerant Networks because of their opportunistic nature. Another advantage of this technique is that it is fast and reliable.

Robiah Y. et al [12] address the current norms for malware detection techniques and the methods by which each method can be improved. A new method for classification of malware detection has been proposed which is a combination of Anomaly based methods and Signature based methods to overcome the shortcomings of the contemporary malware detection methods in detecting malware attacks.

Ulrich Bayer et al [13] explained the process of detecting the malware. Traditionally, it was done manually in which each sample was analyzed. This paper introduces a method for dynamically analyzing the malware. The system calls on Windows and the API are recorded. The code is then run through an emulated operating system to monitor it.

Konrad Rieck et al [14] explained how different types of short range communications have been affected by malware. Malware can effectively propagate via blue tooth by collecting scanner traces and simulations. Rather than assuming a sophisticated malware containment capability such as patching or self-healing in previous works. Their designs are based on a decision mechanism developed using direct and indirect observations to deal with proximity malware. In mobile networks, intermittently connected smart phones are one of the most feasible and cost effective way to route packets. While early work in mobile networks used a variety of simplistic random i.i.d.models, such as random waypoint, recent work shows that these models may not be realistic. Furthermore, many recent studies based on real mobile traces, revealed that nodes' mobility showed certain social network properties. Two real mobile network traces are used in the study.

Idika, Nwokedi and Aditya P Mathur [15] in their paper explain proximity malware. In proximity malware, malware propagates through opportunistic contacts in delay tolerant networks while in traditional networks there is a gatekeeper who protects the virus from entering into the system. The neighborhood model is used to cut off the malicious node from the non affected ones. The malicious nodes are identified by closely observing the behavior of each of the nodes in the system.

Vinod P., V.Lama and M.S.Gore [16] in their paper use phylogenetic trees to assess the difference between malicious and non malicious nodes. This is one of the several malware analysis techniques where disassembled piece of malicious code is not available and the whole execution takes place in a virtualized environment. In this method, behavior of the nodes is distinguished and, based on the information, a phylogenetic tree is created which brings out even minute differences between the behaviors of the nodes so as to get the best accuracy.

Kevin Fall [17] explained about the architecture of Delay Tolerant Networks. Some networks have bad end-to-end connectivity. These networks can take part in inter region communication only through Delay tolerant networks. A description of Linux based implementation of a DTN is also included.

Ramu and Srikanth [18] in their paper explain that the use of smart phones has increased widely among different types of users. Nearly everything from paying bills to managing accounts to the storage of private data is mobile based, which creates an even larger platform for attackers to perform mobile malware attacks. Hence, malware detectors are required to be installed in every smartphone or other malware detection techniques need to be employed in order to prevent malware attacks. New kinds of malware are being developed that are airborne and stealth malware which affected all the iphones, gathering all the confidential data and hence hindering the security. Hence there is a sheer need for preventing malware attacks. Based on their study there are several prevention as well as detection based techniques to avoid malware attacks by stakeholders at every level, be it application level or service level, and before installing the application or programme software, a user should also be self-educated to identify all kinds of threats so that he/she can take preventive measures.

V. Cerf [19] explains the advantages of Delay Tolerant Networks and areas in which they have been used. The said areas include sensor based networks, terrestrial wireless networks that cannot main end to end connectivity, satellite networks that have moderate delays, etc. The DTN architecture allows the interconnection of homogeneous gateways and employs store and forward message routing to overcome delays and disruptions in the network. This architecture also protects the network from unauthorized access.

Sushant Jain [20] explained different routing techniques. The performance of each technique is measured by using simulations and its dependence on the amount of prior knowledge required about the topology of the network. The end result gives us the conclusion that store and forward mechanism is the best.

III. CONCLUSION

This paper is an in depth survey on malware detection techniques in Delay Tolerant Networks. Behaviour based malware characterization is an effective and viable alternative to pattern matching malware detection, particularly when dealing with polymorphic malware. Malware is a worldwide epidemic that can affect any device on any platform. Studying malware detection techniques in detail and choosing the most efficient type will reduce the potential effects of malware on mobile users, lower the chances of mobile devices deteriorating, and minimize large scale network breakdowns which are the result of malware outbreaks. Inter-region networking in Delay Tolerant Networks will bridge the gaps that currently exist between communication devices.

IV. ACKNOWLEDGMENT

We would like to thank TEQIP (Technical Education Quality Improvement Programme) for giving us an opportunity to carry out our survey.

REFERENCES

[1] Dolly Uppal, Vishakha Mehra and Vinod Verma, "Basic survey on Malware Analysis, Tools and Techniques", International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[2] Jayalekshmi S. , M. Jeba Kumari, "Efficient Game-Theoretic Approach for Malware Detection in Delay-Tolerant Networks", The International Journal of Science & Technoledge Vol. 2 Issue 11, October 2014.

[3] Zhu Kenan, Yin Baolin, "Malware Behaviour Classification Approach Based on Naive Bayes", State Key Laboratory of Software Development Environment, School of Computer Science and Engineering, BeiHang University.

[4] Vineetha.S, Shiva Ranjani.P, “A Hybrid Scheme for Malware Detection in Delay Tolerant Networks", International Journal Of Engineering Sciences & Research Technology, October 2014

[5] Zahra Bazrafshan, Hashed Has hemi, Seed Midi Hastate Far, Ali Haze, " A Survey on Heuristic Malware Detection Techniques", 5th Conference on Information and Knowledge Technology (IKT), 2013.

[6] Vinod P., V. Lama, M.S. Gore, "Survey on Malware Detection Methods", Malaria National Institute of Technology, Raipur, Rajasthan.

[7] Dr Farad Farah and, " Delay Tolerant Networks: Challenges and Application", Central Connecticut State University.

[8] Moa Coho Chua, Pang Yang, Brian D. Davison, Liang Cheng," Performance Comparison of Uncast Routing Schemes in DTNs ", Lehigh University.

[9] Hemal Shah, Yogeshwar P. Kosta, " Evolution of Routing Techniques, Routing Protocols and Routing Efficiencies for Delay Tolerant Network ", IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.

[10] Wei Peng, Feng Li, Xukai Zou, Jie Wu, " Behavioral Detection and Containment of Proximity Malware in Delay Tolerant Networks", Issue No.01 vol.25, January 2014.

[11] Tao Yong, Wang Xiao-fang, "Adaptive clustering hierarchy routing for delay tolerant network", Central South University Press and Springer-Verlag Berlin Heidelberg 2012. http://link.springer.com/article/10.1007%2Fs11771-012-1179-y#page-2

[12] Robiah Y, Siti Rahayu S., Mohd Zaki M, Shahrin S., Faizal M. A., Marliza R.," A New Generic Taxonomy on Hybrid Malware Detection Technique", International Journal of Computer Science and Information Security, Vol. 5 No. 1, 2009.

[13] Ulrich Bayer, Andreas Moser, Christopher Kruegel, Engin Kirda, "Dynamic analysis of malicious code", Journal in Computer Virology, 2006.

[14] Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick Dussel, Pavel Laskov, "Learning and Classification of Malware Behaviour", In 5th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, June. 2008

[15] Idika, Nwokedi, and Aditya P. Mathur, "A survey of malware detection techniques" Purdue University 48, 2007.

[16] Gerard Wagener, Radu State, Alexandre Dulaunoy, "Malware Behaviour Analysis",Springer-Verlag France 2007. http://www.researchgate.net/publication/220673433_Malware_behaviour_analysis

[17] Kevin Fall, " A Delay-Tolerant Network Architecture for Challenged Internets ", Intel Research, Berkeley , 2003.

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

[19] V. Cerf et al, “Delay-Tolerant Network Architecture”, Internet Draft, draft-irtf-dtnrg-arch-06.txt, March 2006.

[20] Sushant Jain: University of Washington, Kevin Fall: Intel Research, Berkeley, Rabin Patra: University of California, Berkeley, " Routing in a Delay Tolerant Network", 2004.