International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Centeralized Mechanism For Passive Worm Detection And Throttling In P2P Networks

Gokul K[1], Karthik L P. [2], Mohan S. [3], Femila Goldy R. [4]

[1], [2], [3] U.G. Scholar, [4] Assistant Professor Department of Computer Science Anand Institute Of Higher Technology Chennai, TN, India.

[1] gokuldotk@gmail.com[2] karthikselvam11@gmail.com,[3] mohanscse58@gmail.com,[4] femilajoyrobert@gmail.com

Abstract — **Over the years, worms have emerged as a main source of trouble in P2P networks. If worm enters the system it immediately starts affecting the system activities. Also the system gets slower. If it is a distributed system and many systems are connected in peer to peer format then the systems that are connected to the infected system may also get affected. In order to prevent the system from worm, passive worm detection method is used. In this method, one system in a network acts as guardian system and other system in the network acts as child system. If any system is affected by worm, the request is given to the guardian system. The guardian system sends an alert message to other systems in the network. By using patch framework the guardian system rectifies the worm problem from the system which has been affected by worm. Hence the systems in the network were protected from worms.**

Index Terms — ***P2P; Passive worm.***

I. INTRODUCTION

Peer to Peer (P2P) applications as we know them today inform of contribute the major chunk of the Internet traffic. Being technically categorized as unstructured and structured, the P2P networks have diversified applications like file sharing, collaborations, process sharing (e.g. Distributed.net and Adhoc Networks) and distributed computing. Decentralized nature of P2P networks benefits through the properties like scalability, reliability, fault tolerance and load balancing, while in presence of no centralized authority, these networks are prone to many security threats in respect to breaches of confidentiality, integrity, authentication, access control and non-repudiation.

Over the years, worms have emerged as a main source of trouble in P2P networks. Worms can be categorized mainly as scanning and non-scanning. Scanning worms always keep on probing addresses for new victims. They do waste time in probing unused addresses and may potentially have a high rate of failed connections. Moreover, they do not blend with the normal P2P traffic. Due to the circumstances discussed, the non scanning worm could sometimes be more dangerous than the scanning ones as they chose the vulnerable nodes through the neighbor lists and are hence more successful in acquiring precise and fast knowledge of their prey. we focus on passive worms that hide themselves in popular P2P resources by embedding malicious code in executable files. This strategy of selecting the targets has made passive worms unpopular & less attended in history because most of the files shared in the early P2P networks were non-executable files like MP3 or some other media files.

However, more recent popular P2P systems, like Bit Torrent, Kazaa, eDonkey2000 & others provide the users with much easier access to executable files, and make passive worms become a major threat yet again to the safety of the P2P networks. The passive worms operate in a purely epidemic manner to spread in the network. Firstly they embed themselves in the popular executable files in the P2P network and make a few copies in the sharing folder of the infected user. Once another user downloads the files and executes them, the worms duplicate themselves and create a few new copies in the sharing folder, which increases their possibility of being downloaded by the other vulnerable users. Since the user can only be infected after the file is executed, the downloading of the passive worms are, most of the time, treated as legitimate P2P network behavior and this actually makes it quite difficult to detect. Some researchers define the passive worms as the ones that attach to files and propagate with user activities as viruses. We would use terms “worms” and “viruses” alternatively for the passive worms.

There have been lot of efforts to study propagation of

P2P active worms and defaces against them but a little has been done in regards to passive worms. Although such worms may propagate in a slower passion, the P2P networks are themselves the vehicles for fast passive worm propagation.. The P2P worms propagate as a part of legitimate network activity and hence are difficult to detect than scanning worms. Many studies are underway to analysing the patterns of virus propagation in P2P networks to better understand worm behaviour. For this article, we mainly focused on unstructured file sharing P2P networks such as Kazaa and BitTorrent because most of the existing P2P worms target these kinds of systems.

II. EXISTING SYSTEM

In the existing system, there is no centralized security mechanisms for networks only the antivirus software are used for detecting and removing the worms. This system is applicable only to the standalone and not applicable for networks. This system is more costly since each unique copy of software is needed for each and every system. Absence of centralized security system makes the network more prone towards the worms..

III. PROPOSED SYSTEM

In the proposed system, a centralized security mechanism is introduced by keeping one of the peers as guardian system and if any system in the network gets affected by worm, the request is given to the guardian system. The patch framework is given to the affected system by the guardian system and with the help the patch framework, the worm in the affected system is cleared. A centralized security mechanism is introduced hence the systems in the entire network is secured. This system is extremely cost effective compared with existing system. This method is also time consuming since the patch is available within the system for same type of worms.

A. Worm Creation and Propagation

In this phase three different types of worms were created namely Shutdown worm, Folder Replication worm and DLL file creation worm. These worms were propagated towards the peers through data sharing.

B. Detection Phase

As an integral part of the framework, the guardian node is equipped with observation software to identify any malicious behaviour. The guardian node detects some malicious code, it would request the worm definition database to look for the worm definition and confirm it. Besides detection of attacks, locating the nodes responsible for vulnerability in the networks is important to make this activity rather efficient in identifying the threats.

C. Analysis & Confirmation of Threat

The guardian node, by looking at the virus definitions confirms the threat, it would generate the alert to the entire

P2P network. This alert generation would have different meanings for the peers and other guardian nodes in the network. The guardian nodes would get the patch ready and they could simply push the patch to other devices or wait for this patch to be pulled by the devices.

D. Patch Selection

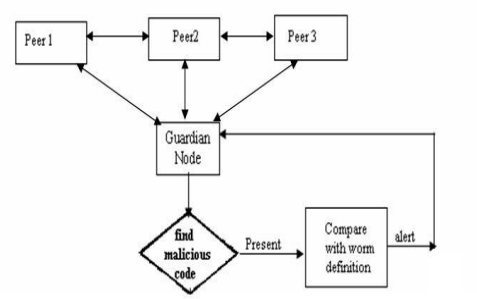
Selection of a proper patch from the patch reservoir is a key task when we look at the worm throttling process. Prompt and proper patch availability could let the network recover quickly from the attack.

E. Patch Propagation

A better strategy is required to be deployed to make the patch dissemination process fast to an extent that it could take over the worms in the network. Hence when the patch is ready, it could either be propagated straightaway to the peers or the guardian node would wait for the peers to download it in response to the alert.

IV. IMPLEMENTATION

As an integral part of the framework, the guardian node is equipped with observation software to analyze the traffic patterns and to identify any malicious behaviour. In our case the guardian node detects some malicious code, it would request the worm definition database to look for the worm definition and confirm it. Besides the content, the threat could also be detected through the behaviour of the network or traffic suppose by an alarmingly increased number of connections. This activity may be traced by the firewalls and reported to the guardian nodes for the remedy.



A. Analysis & Confirmation of Threat

In this phase, if the guardian node, by looking at the virus definitions confirms the threat, I would generate the alert to the entire P2P network. This alert generation would have different meanings for the peers and other guardian nodes in the network. The guardian nodes would get the patch ready and they could simply push the patch to other devices or wait for this patch to be pulled by the devices. Selection of a proper patch from the patch reservoir is a key task when we look at the worm throttling process. Prompt and proper patch availability could let the network recover quickly from the attack.

While the definitions for some worms are not there, techniques used to deploy to convert the worm into anti-worm. Failure to which could require a human intervention prevents the further propagation of the virus from that infected machine. Hence the addresses from which the worm attack is being generated could be blocked for some duration to at least contain this epidemic while the recovery process would be underway in parallel. The alert messages could be made more effective if they also carry the information that could result in probing all the peers to block the traffic from some particular addresses. Doing so, these alerts could play a vital part in worm containment process. Meanwhile the major recovery process through patch propagation and worm scans on the individual peers is done.

A better strategy is required to be deployed to make the patch dissemination process fast to an extent that it could take over the worms in the network. As described by, the speed of epidemiological behaviour of worms has always been a hard question. Hence when the patch is ready, it could either be propagated straightaway to the peers or the guardian node would wait for the peers to download it in response to the alert. An important phase in this regard is the communication between guardian nodes upon receiving the patch. When a guardian node detects a threat directly or through any peer, in an alert message, it is assumed that it would also announce the identity of the worm so that the peers that may already have the patch could start taking care of the worm. The guardian nodes receiving the alert would make the patch available in their shared folders or even reactively flood the patch into the network

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we briefly analysed the worm and patch modeling work and a considerable review of worm detection mechanisms. we conclude that worm detection could be very effective if done in a distributed manner. We argue that for the scalable P2P networks, the distributed or technically hybrid detection mechanisms could prove even more effective than conventional centralized detection. We proposed a distributed threat detection and worm throttling framework and deducing from the previous work in the field we could safely say that the performance of this framework would depend on the prompt and intelligent threat detection, efficiency in sharing the threat information with the entities that matter, and a very strong recovery strategy.

In the future, the same project can be extended to detect many type of worms. Thus Worm detection could be very effective if done in a distributed manner for all type of worm

ACKNOWLEDGEMENT

The authors would like to thank R.Femila Goldy for assisting with the experimental setup, and D.Rajini Girinath,HOD/CSE for helpful discussions.

REFERENCES

Yini Wang, Sheng Wen, Yang Xiang, and Wanlei "Modeling the propagation of Worms in Networks: A Survey", vol. 16,no. 2, second quarter 2014.

[2] Napster homepage, http://www.napster.com/

[3] Gnutella homepage, http://www.gnutella.com/

[4] Eric Chien, "Malicious Threats of Peer-to-Peer Networking", Symantec White Paper, 2003.

[5] www.cim.mcgill.ca/~sveta/COMP102/P2P.pdf

[6] William Stallings, "Cryptography and Network Security, Principles and Practice", Second Edition, Prentice Hall Publishing, ISBN-13: 9780130914293, 2001.

[7] Lidong Zhou et al., "A First Look at Peer-to-Peer Worms: Threats and Defenses", Book Chapter, Peer-to-Peer Systems IV, Springer Publishing, 2005.

[8] Bo Zhan et al., "Defense against Passive Worms in P2P Networks", Proceedings of Networking & Electronic Commerce Research Conference (NAEC 2008), 2008.

[9] Guanling Chen et al., "Simulating Non-Scanning Worms on Peer-to- Peer Networks", Proceedings of INFOSCALE '06, Hong Kong, 2006.

[10] Zhiguang Qin , "Propagation Models of Passive Worms in P2P Networks", IEEE International Conference on Machine Learning and Cybernetics (ICMLC), 2008

[11] S. Staniford et al., "How to Own the Internet in Your Spare Time", Proceedings of the 11th USENIX Security Symposium, San Francisco, 2002