ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Reliable Data Transmission in P2P Networks by Preventing Malware Propagation

Arun Prasath. Y[1], Malathy. M[2]

PG Student, Department of IT, Sri Venkateswara College of Engineering, Sriperumbudhur, India [1]

PG Student, Department of IT, Sri Manakula Vinayagar College of Engineering, Puducherry, India [2]

Abstract: Internet plays a vital role with its technology which it holds inherently. It possesses enormous applications and also the impact behind it. Attack of malicious programs poses major threats into the internet. The P2P system holds rich connectivity through internet to provide endless service for its users. The propagation of worms and virus in the network may exploit and leave a path for malicious attack. This issue is carried out by dealing with both offline and online P2P based services and preventing them from malicious attack by implementing the containment strategy. This would provide a platform where endless services can be done with any compromises and also the ability to perform in small cell phone network.

Keywords: Peer to Peer Networks, Reliable Data Transmission, Worms and Virus Propagation

I. INTRODUCTION

Network security is an important task of ensuring management of network. A threat to security of network is malware propagation. There are specific types of malware which perform scanning of the entire network topology and spread the network information. An analytic model to understand the dynamics of malware spread in P2P networks is developed. The need for a statistical framework incorporating user identities and communication patterns was put forth by quantifying their influence on the basic deployment ratio. A decentralized network has no central authority, which means that it can operate with freely running nodes alone .The first major project to delve into decentralized file sharing was Gnutella. The publication of protocol is proved to be extremely useful, as distinct developers were able to contribute their own Gnutella-compliant software that could inter-operate.

Another prominent decentralized file sharing system is Freenet, an open source implementation described by authors. Freenet varies from Gnutella in that its basic purpose is to create an unsensorable and secure global information storage system. The Freenet architecture is designed with special consideration for anonymity and fault-tolerance. Modern worm spreads events show that active worms can propagate in an automated fashion and flood the Internet in a very short period of time.P2P systems can be a potential vehicle for the active worms in the Internet.

This implementation addresses of active worm propagation on top of P2P systems effects. A P2P system based active worm attack model and study two attack strategies (an off-line and on-line strategy) under the defined model is defined. An analytical approach to analyze the propagation of active worm under the defined attack model and conduct an extensive study to the impacts of P2P system parameters, such as size, topology degree, and the structured/unstructured properties on active worm propagation is defined.

II. RELATIONSHIP WITH THE PRIOR WORK

The focus of work is on modeling the spread of topological malwares. Model is motivated by probabilistic graphs .Use of a graphical representation to abstract the propagation of malwares that employ different scanning methods. Then use a spatial-temporal random process to describe the statistical dependence of malware propagation in topologies. As the spatial relies is particularly difficult to characterize, the problem becomes how to use simple models to approximate the spatially dependent process. The simple model is to study the performance of BitTorrent, a second generation peer-to-peer (P2P) application. A simple fluid model and study the scalability, working and reliability of such a file-sharing mechanism. We then consider the default or constant incentive mechanism of BitTorrent and study its effect on network performance . The numerical results based on both simulations and real traces obtained from the Internet.

Every time a Gnutella user searches for media files in the affected computer, the virus always response to the request by heading the user to believe that it is the file the user searched for. The plan of the search technique has the following implications: first, the worms can spread much faster, and second, the rate of failed connection is less. A comprehensive model for malware spread in Gnutella type P2P networks that address the above shortcomings. The strategy is followed by two stages: first, the average number of peers within TTL hops from any given peer is quantified and in the second stage incorporates the neighborhood information into the final model for malware spread.

.

III. WORM PROPAGATION

An active worm is a program that propagates across hosts in a network by exploiting their security issues. Active worms are same as biological viruses in their self-replicating and propagating behavior. In general, there are two stages in active worm attack: (1) scanning the network

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

to select victim hosts; (2) infecting the victim after discovering its deprecacy. Affected hosts proceeds and propagate the worm to other vulnerable victims and so on. In the above two stages there are three key factors that decide worm propagation speed: (1) how fast the worm can scan other hosts in the network; (2) the probability of the worm to scan a real host; and (3) vulnerability of the scanned host.

The first factor is modelled as the scan rate R, which is the number of hosts per unit time that a worm infected host can scan. The scan rate R is a asset of the worm itself, and is be individual the victims it attacks. However, the second and third factors are victim. We ignore that not all addresses in the Internet are applicable. Recent studies have shown that only 24% of addresses in the Internet space are used by active hosts. Thus, a significant number of scans launched by worm actually hit many such non-existent hosts. Nevertheless, when propagating on P2P systems, scans can be more precise, since P2P systems have a large number of real and active hosts with rich connectivity to other P2P hosts. The factor, namely vulnerable of victim hosts is quite high in the case of P2P systems as most P2P hosts are untrusted and invalidated during the entry into the P2P system.

The final factors are the reasons, why the attacks of worm propagate on P2P systems attains significance. In the following, we exhibit our P2P-based worm attack models. We first present a normal attack model namely Pure Random Scan (PRS), where the worm randomly scans the network to identify victims. We then present two P2P-based attack models that propagate on P2P systems to achieve very rapid propagation. The worm will affect the computer and also the softwares

IV. ONLINE AND OFFLINE P2P HIT LIST SCAN

In this model, the large population of users in P2P systems is the first target for the attacker. This model proposes that the attacker collects IP address information of the P2P system offline and online. We denote this as the hit-list of the attacker. Gaining the hit-list can be retained by various methods, such as using P2P-based Crawler tools . In this attack model, there are two phases: in the first phase (called the P2P system attack phase), recently infected hosts vigorously attack the hit-list until all hosts in the hit-list have been scanned.

Algorithm 1: OPHLS – offline, online P2P-based hit-list scan

Require: node i is the worm infected host in the P2P system with scan rate R, and hit-list L

1: ***while*** L is not empty ***do***
2: Select a set V consisted of R victims from L and launches the attack to all victims in V
3: L = L – V
4: ***end while***
5: Attack the rest of the Internet via Pure Random Scan

In the second phase , the detected worms are cleared by using the automatic worm containment strategy.
.

V. CONTAINMENT STRATEGY

The worms and virus are detected and cleared by using automatic worm containment strategy. The containment works on the process of at first it detects all the worms whichever spread over the network. The spread virus will attack the files in the network and also the systems connected to the network. To avoid these kinds of problems the worms has to be governed and removed at the initial stage. To propose this system the automatic worm containment strategy is used. This strategy will remove the malicious programs whichever wanted into the network by removing it at the initial stage or stop progressing it even after it entered into the network. The major benefit is that the hit ate of hosts can be reduced by using the containment strategy.

Once the data propagation is initiated, the containment will possess the worms and viruses in the networks, which are collected from several sources. This collection will lead to validation of the several nodes to identify whether they are infected or not. And hence, it is necessary to preserve the containment up-to-date. Once the containment is ready, each node in the network will be able to access it, irrespective of the internet connectivity. Thus, our proposed algorithm and strategy enables the reliable data transmission over the peer-to-peer networks, by preventing the malware propagation. It also ensures that the overall network is made reliable for every node that access it from both inside and outside the network.

VI. CONCLUSION

The model provides a better path to enforce the avoidance of malicious programs over the P2P network.. It also proves that it can overcome the attack of malicious program in both offline and online. The P2P network comprises of many challenges , one among them is worms and virus attack. Those problems are focused and a best solution is obtained by automatic worm containment strategy for the betterment and future work focuses on topology in network regarding worm containment

REFERENCES

[1] F. Freitas, R. Rodrigues, C. Ribeiro, P. Ferreira, L. Rodrigues, Tverme: worm containment in peer-to-peer overlays, in: Proceedings of the 6th International Workshop on Peer-to-Peer Systems, Sellevae, WA, February 2007.

[2] X. Ding, W. Yu, Y. Pan, A dynamic trust management scheme to mitigate Malware proliferation in p2p networks, in: Proceedings of IEEE International Conference on Communication (ICC), Beijing, PR China, May 2008.

[3] J. Luo, B. Xiao, G. Liu, Q. Xiao, and S. Zhou, "Modeling and Analysis of Self-Stopping BT Worms Using Dynamic Hit List in P2P Networks," Proc. IEEE Int"l Symp. Parallel and Distributed Processing (IPDPS "09), May 2009.

[4] F. Wang, Y. Dong, J. Song, and J. Gu, "On the Performance of Passive Worms over Unstructured P2P Networks," Proc. Int"l Conf. Intelligent Networks and Intelligent Systems (ICINIS), pp. 164-167, Nov. 2009.

[5] X. Yang and G. de Veciana, "Service Capacity in Peer-to-Peer Networks,"Proc. IEEE INFOCOM '04, pp. 1-11, Mar. 2010

[6] D. Qiu and R. Srikant, "Modeling and Performance Analysis of BitTorrent-Like Peer-to-Peer Networks," Proc. ACM SIGCOMM, Aug. 2011

[7] J. Mundinger, R. Weber, and G.Weiss, "Optimal Scheduling of Peer-to-Peer File Dissemination," J. Scheduling, vol. 11, pp. 105-120, 2012

[8] A. Bose and K. Shin, "On Capturing Malware Dynamics in Mobile Power-Law Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm.Networks (SecureComm), pp. 1-10, Sept. 2013

[9] L. P. Cox and B. D. Noble. Honor among thieves in peer-to-peer storage. In Proceedings of the 19th ACM Symposium on Operating Systems Principles, pages 120–132, Bolton Landing, NY, USA,. ACM SIGOPS, ACM Press.

BIOGRAPHIES

Arun Prasath .Y, currently pursuing M.E (Computer & Communication). Interested over areas such as, Networks, Web service and Data handling.

Malathy .M, currently pursuing M.Tech (Networking). Interested over areas such as, Networks, Cloud and web security.