International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 616-620
 https://dx.doi.org/10.37622/IJAER/11.1.2016.616-620

Survey on the Present State-of-the-Art of P2P Networks, Their Security Issues and Counter Measures

Gera Jaideep[1]
Research Scholar, Dept .of Computer Science and Engineering,
Acharya Nagarjuna University, Guntur, India.

Dr. Bhanu Prakash Battula[2]
Associate Professor, Department of Computer Science and Engineering,
Vignan College, Guntur, India.

Abstract
Peer-to-Peer (P2P) networks are quite different from traditional client-server networks. In P2P systems, all nodes are equal or peers and they can either act as client or server. All the nodes have similar capabilities. These networks became ubiquitous for file sharing and performing operations in distributed fashion. P2P networks are overlays on top of Internet or wide area network. P2P networks such as Gnutella, Napster, BitTorrent, and Freenet are some of the existing applications that allow sharing resources and searching for resources. Direct exchange of resources is made possible with P2P networks provided there are certain mechanisms such as directory service, distributed hash table, and flooding to discover services. P2P networks have the potential to enhance the capabilities of networks with sharing of music, video, and other services. Nevertheless, the P2P networks throw security challenges as the nodes are vulnerable to various attacks. In this paper we review the P2P networks, their security issues and counter measures. The attacks include DoS, DDoS, Man-in-the-Middle, Worm Propagation, Pollution Attack, Rational Attack, Sybil Attack and Index Poisoning Attack. This paper also provides counter measures of these attacks as available in the literature. The insights in this paper provide broad overview of P2P network issues and solutions.

Keywords: Networks, peer-to-peer networks, file sharing, resource discovery, security attacks, counter measures

Introduction

Peer-to-peer (P2P) network is different from traditional computer network. In traditional networks one or more servers are dedicated to provide services to clients [10]. Plenty of File Transfer Protocol (FTP) and Hyper Text Transfer Protocol (HTTP) servers are examples over Internet to provide file, download and other services. In contrast to the traditional Client-Server (C/S) model, P2P distributes the burden of services to many nodes that are interconnected [27]. Such nodes can act as either client or server and are known as peers. This kind of network that can spread across the world as an overlay network is known as P2P network. Stated differently P2P network is one of the computer networks that exhibits characteristics like distributed control, symmetric communication and self-organization. Basically there is not centralization of resources in P2P network. The link capacity and resources to be shared are truly distributed and thus the control is distributed. In this way P2P is in contrast with traditional model. The client-server model needs centralized resources to serve clients while the P2P model has decentralized services that are pooled for common good. Nevertheless, P2P networks are susceptible to attacks due to their decentralized and pee-relying nature. Before exploring security issues and possible solutions, we provide more details on P2P networks here. The notion of P2P was first conceived in 1969 with first RFC on such network. The idea was to build host-to-host connectivity which is in contrast with client-server. Usenet was the first ever implementation of a P2P network in 1979. In this network peers can communicate with each other and also there are servers connected like peers for provisioning resources. The surge of popularity of P2P began in 1990s for sharing and exchanging multimedia files. With respect to file sharing, some of the popular protocols include BitTorrent, eDonkey2000, Gnutella, Direct Connect, Napster, and Freenet as shown in Table 1. With the emergence of these networks, it became easier to have files shared across the globe.

Table 1: Popular P2P Protocols

P2P Protocol	First Released
Freenet	July 1999
Napster	September 1999
Direct Connect	November 1999
Gnutella	March 2000
BitTorrent	April 2001

Interestingly, the P2P application Napster was started like a directory service prior to improving P2P services. It also led the show to other applications like Gnutella and eDonkey and currently the most popular file sharing protocol BitTorrent. Discovering peers and resources in such networks is the major issue. As there are no centralized servers, peers need to identify other peer that can provide resources or files. The basic approach of file sharing is to

have a centralized directory that indexes the resources available with peers. After making lookup into this directory, the peers can locate resources with other peers. Napster and BitTorrent employ this approach in one way or other. Though it is P2P network, the resource lookup part remains client-server. This type of network is shown in Figure 1.

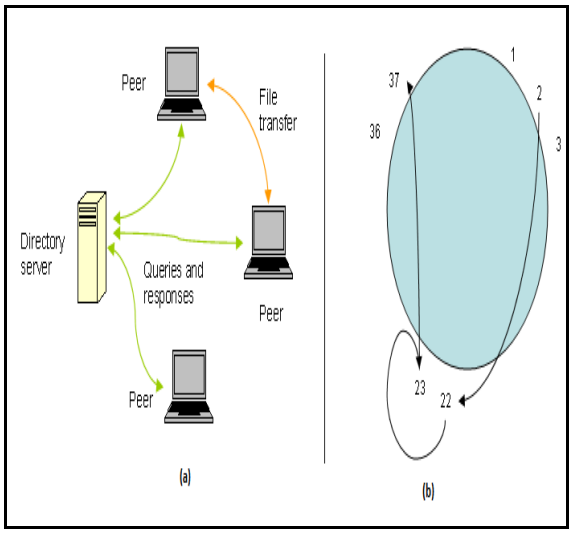

Figure 1: Resource discovery with centralized directory server (a) and the same with DHT (b) [16]

There is another approach to discover resources in P2P as used in Gnutella. Instead of looking up for resources in a centralized server, peers broadcast a request to other peers for discovering resources. This concept is known as query flooding. This mechanism does not encounter central point of failure for discovering resources. However, the flooding process causes overhead in terms of bandwidth. Sometimes even it can lead to an unintended Distributed Denial-of-Service (DDoS) attack which is popularly known as network storm. A variant of flooding approach is to choose some nodes as super nods that are characterized by high-capacity and high availability. These super nodes are distributed across network and they are given responsibility of maintaining index of resources in their respective domains and respond to lookups appropriately. Moreover, the super nodes can query other super nodes and allow other super nodes to query them in turn. This approach can avoid bandwidth problem to a great extent but it cannot completely eliminate inherent issues caused by flooding. Service discovery protocols were found in [21]. Distributed Hash Table (DHT) is another approach (see Figure 1) for discovering resources in P2P networks. This was introduced in 2001 in the projects like Tapestry, Pastry, Kademlia and Chord. The DHT contains indexing of resources and located in peers. This will help in efficient lookup for resources. DHT follows centralized approach but eliminates single point of failure. Most recent P2P protocols including BitTorrent (trackerless) were switched to DHT lookups. To sum it up, in P2P networks, there are three different means of discovering resources such as lookup on centralized directory, flooding and DHT. Though these approaches are different, the common thread among all P2P networks is that resource transmission is in P2P fashion. P2P systems can be used for e-business [1]. P2P nodes can also participate in overlay networks [11]. Gong [12] explored JXTA which is one of the P2P systems. Opportunistic networks were explored in [13], [15]. Maximum Likelihood Estimation technique was employed in [14] for assessing performance of peers. Li [16] explored security issues in P2P networks while Parno & Perrig [17] does the same in vehicular networks. Private P2P networks were explored in [18]. Such network is nothing but Internet overlay but owned by an organization. Shared sensing is possible in the real world with P2P approach [2] [19]. Caching mechanism in P2P systems can improve performance of network [22]. Distributed resource management is possible with P2P systems [23]. Fortunately for P2P networks TCP protocols can also be used [24].

Lee and Kim [3] proposed a reputation based protocol for adaptive authentication in P2P networks for securing communications. Similar kind of work was in [4]. To reduce selfish behaviour of nodes in P2P networks, Wu [5] proposed differentiated admissions based on incentives. Freedman & Zin [6] investigated social networks to solve information problems pertaining to P2P networks. The study was related to P2P lending instead of traditional banking. Their results were encouraging. Yan [7] investigated social networks and trust modelling which concludes the significance of trust in digital information exchange. Similar kind of work was done in [26]. Ramasubramanian and Sirer [8] proposed a proactive replication framework that could exploit power law query distributions for improving lookup performance in P2P systems. Threat categories in Gnutella [9] include hijacking queries, flooding, and content authentication. The threat solutions include Distributed Hash Table (DHT), authentication, FFTs and encryption. Unfortunately P2P networks are vulnerable to attacks [20], [25] that can disable or disrupt these networks. The rest of the paper focuses on security issues in P2P networks and their counter measures. Our contributions in this paper include the study and review of P2P systems, their service models, security challenges, attacks and prevention mechanisms. The remainder of the paper is structured as follows.

General Network Attacks

A. *Denial of Service (DoS) Attack:*

DoS attack is an attempt to make a computer or network resource unavailable to its legitimate users. Thus it is able to deny service to intended users. In case of P2P networks, this attacks causes flood of bogus packets to be flown in the network thus preventing legitimate network traffic. There is another approach in which DoS attack is made. In this approach a victim node is drown with fastidious computation to make the node too busy to answer genuine queries. The widely used defence mechanism for such attack is “pricing” [36] where a puzzle is sent to client before it is allowed in computations. Before an attacker floods his victim with false traffic, he needs to solve the puzzle which make difficult to launch DoS attack successfully.

B. *Distributed Denial-of-Service (DDoS) Attack:*

DDoS attack is an extension to DoS attack. Stated differently it follows the technique of DoS. It is an attack that occurs in distributed network environment. In this attack an attacker

cannot directly launch attack on victim nodes. Instead, an attacker takes a PC which is connected though broadband into his control. The compromised PC is known as zombie. This Zombie is used to launch attack in large scale. Therefore this zombie is known as controlling zombie. This zombie makes use of many other zombies that are known as attacking zombies. The attacking zombies actually launch DDoS attack on victim. As the attacker is not directly involved, it is difficult to trace the actual attacker. The impact of DDoS attack is very vast and the whole network of an enterprise might be denied from serving its clients [36]. Defence for DDoS attacks is very hard as there are plethora of nodes involved and the source of attack is hidden. However there are certain counter measures for such attacks. Filtering malicious information, security teams monitoring such attacks, employing mitigation plans, maintenance of blacklist or whitelist, and so on are some precautions for countering DDoS attacks [40].

C. *Man-in-the-middle Attack:*
It is an indirect intrusion attack where an attacker positions his computing device between two nodes [36]. This way the middle node is able to intercept and modify messages flown between two legitimate users without the knowledge of actual sender and receiver of messages. As defence mechanism encryption methods can be used for transmitting data. In order to detect such attacks, authentication mechanisms can help. The authentication process [35], [37] can identify the legitimate users from attacker.

D. *Worm Propagation:*
Worm is a malicious program that can copy itself to other nodes through network or infected storage media. The propagation of worm can be done through web server, email, file and so on [30]. There are defence strategies as described here. The counter measures provided by networks in general can be used. For instance, firewall can be used. Anti-Virus is another defence mechanism that makes use of virus signatures in order to detect and isolate malicious content [38], [39]. Operating systems also offer defence mechanisms. For instance OpenBSD OS have protection from propagation of malicious content through integer overflows and buffer overflows [36].

E. *Pollution Attack:*
This attack can effectively replace a file in the network with a fake file but the polluted file is not useful to the users of network [31]. Moreover, the attacker spoils original file and makes the duplicate one available to network users for sharing. The polluted content disguises itself as original file or content in order to attract people. From the perspective of users, the polluted file may not be harmful but it causes waste of time to users as it is of no use for them. Thus the users of P2P are disturbed with such files and they might lose interest in using such networks for file sharing. Simply users need to delete such files.

Attacks Pertaining To P2P Networks

A. *Rational Attack:*
In P2P networks, a node might indulge into self-interested behaviour that does not fall into the expected behaviour as per the underlying protocol. Such behaviour is classified into Rational attack [34]. When a node is supposed to participate in data transfer and do not do that whole heartedly to save its resources, this behaviour can be called Rational attack. When many nodes behave so, it causes to destabilize the whole network [34]. This situation cannot let the network to give any guarantee of quality uploads and downloads. BitTorrent has counter measure for Rational attack. It makes use of Choking algorithm [28], [32] that ensures that peers do follow protocol and involve in upload and downloads as expected.

B. *Index Poisoning Attack :*
Indexing is used by more of the file sharing systems to speedup discovery of files. Index poisoning is an attack that causes problems in finding correct content in P2P network. The attackers inject huge number of invalid peer data that will be put into index that will prevent users from finding correct resources [31]. For instance, BitTorrent was subjected to index poisoning attacks. Before describing how attack is made, we provide the usage of indexing in BitTorrent. First, a file downloaded with .torrent extension is known as seed. This file contains information such as name of file, its size, and a tracker. The tracker is something from which peers can get information pertaining to other peers that are involved in downloading the same file. When any peer initiates a BitTorrent task, it is supposed to advertise its information into tracker and obtains other peers' information through tracker. The problem with tracker is that it does not authenticate any advertisement and does not verify it. This is exploited by attacker who can deliberately advertise large quantity of false data that can cause index poisoning attack. There is high probability of genuine peers trying to connect to invalid peers [31]. There are two specific measures that can be used against index poisoning attack. First, authenticating versions and advertisements can prevent the attack [33]. Second, it is useful to rate sources so that it is possible to avoid taking advertisements from bad sources. When bad sources are identified, they can be blacklisted.

C. *Sybil Attack :*
This attack is related to identities of entities. Generally P2P systems employ frequent backup mechanisms in order to ensure privacy and integrity. The network is supposed to ensure that each entity in the network has ID and that indicates only one entity. When an entity has multiple identifies, it can have significant control over the network. This kind of attack is known as Sybil attack which can destroy redundancy in such systems [41]. When the malicious entities with multiple identities are involved, the backup processes will never succeed. The defence against Sybil attack is the identity registration procedure known as "Self-Registration" [29]. A new node needs to follow registration process. While registration a new node hashes its port and IP address and computes an identifier. Then its identifier needs to be registered with other nodes. Thus the

new node is able to join the network. At the same time, the other nodes also are responsible and can identify other nodes.

D. *Eclipse Attack:*
It is an attack in which attacker is able to control the neighbours of a genuine node in P2P network. The compromised nodes will work together and fool the genuine node by adding the addresses of them to the genuine node's neighbour list. This kind of attack is known as Eclipse attack. Sybil attack is one kind of Eclipse attack when the attack is able to have multiple identities that appear as neighbours of genuine node [41]. The defences against Eclipse attack are described here. Even before doing that two terms such as indegree and outdegree are defined here. Number of incoming routes and outgoing routes of a particular node are termed as indegree and outdegree respectively. The counter measure of Sybil attack can help to an Eclipse attack based on Sybil attack. Then the indegree and outdegree of attacker nodes is dealt with. Since peers maintain neighbour nodes' list, the count of indegree and outdegree nodes can provide some clue pertaining to Eclipse attack. The size of inbound and outbound degree is bound to determine Eclipse attack [41].

Summary

This section summarises findings in the research. The summary is made in terms of attacks, their behaviour, defence strategy, severity of impact, and level of defence. DoS attack is characterized by flooding network with false packets and drowning the victim in fastidious computation. Pricing is its defence strategy. Its impact on the network is medium while the level of defence is easy. DDoS attack is characterized by attacker controlling zombies and in turn attacking zombies to launch massive DoS attack on victims. Its defence mechanism includes trusted server, warning system and provision for blacklist and whitelist. The impact of the attack is high while the defence level is hard. Man-in-the-middle attack is characterized by an attacker intruding between two genuine nodes and intercept and modify traffic. Authentication and encryption are defences. The impact on the network is medium while the level of defence is also medium. Worm propagation attack is characterized by worm copying itself to other nodes. Defence strategies include safety mechanisms of OS, anti VIRUS and firewall. The impact of the attack is medium and the level of defence is medium. Pollution attack is characterized by the sharing of files which are of no use. The defence mechanism is to remove such files. The impact of this attack is low and level of defence is easy. Rational attack is characterized by the selfish behaviour of a node which downloads files but do not involve in uploading files for resource conservation. Choking algorithm as used in BitTorrent is the defence against it. Its impact on the network is medium and the level of defence is also medium. Index poison is the attack that poisons indexing information to hinder genuine search. Authenticating advertisements and versions besides using rating is the defence against the attack. Its impact is high and the defence level is medium. Sybil attack is to use multiple identities illegally which can be defended using self-registration algorithm. The impact of this attack is high and level of defence is hard. Eclipse attack is characterized by the fact that the malicious neighbour nodes fool the genuine node which can be prevented using indegree and outdegree of nodes. The impact of the attack is high and it is hard to have counter measure to prevent it.

Conclusions and Future Work

Peer-to-Peer (P2P) networks became ubiquitous for file sharing and performing operations in distributed fashion. P2P networks are overlays on top of Internet or wide area network. P2P networks such as Gnutella, Napster, BitTorrent, and Freenet are some of the existing applications that allow sharing resources and searching for resources. These networks are vulnerable to various attacks such as DoS, DDoS, Man-in-the-Middle, Worm Propagation, Pollution Attack, Rational Attack, Sybil Attack and Index Poisoning Attack. Awareness of these attacks can help in making well informed decisions. Towards this end, this paper throws light into the P2P networks, security issues and counter measures. This research can be extended further to develop mechanisms that can prevent attacks on such networks.

References

[1] Diomidis Spinellis and Vassilios Karakoidas. (2004). Performing Peer-To-Peer E-Business Transactions: A Requirements analysis and preliminary design proposal1. *iadis*. p399–404.
[2] Pekka Nikander, Jukka Ylitalo, and Jorma Wall. (2001). Integrating Security, Mobility, and Multi-homing in a HIP Way. *Ericsson Research NomadicLab*.p1-14.
[3] Hyunrok Lee. (2003). An Adaptive Authentication Protocol based on Reputation for Peer-to-Peer System. *SCIS*. 26 (29), p305-732.
[4] Zheng Yan, Peng Zhang, Teemupekka Virtanen. (1999). Trust Evaluation Based Security Solution in Ad Hoc Networks, *Nokia*,p1-14.
[5] Chun-Hsin Wu. (2003). Differentiated Admission for Peer-to-Peer Systems: Incentivizing Peers to Contribute Their Resources,p2-18.
[6] Seth Freedman. (2008). Do Social Networks Solve Information Problems for Peer-to-Peer Lending? Evidence from Prosper.com. *NBER*. 19, p1-63.
[7] Zheng Yan. (2007). Trust Modeling and Management: from Social Trust to Digital Trust. *IGI Global*, p2-27.
[8] Venugopalan Ramasubramanian and Emin G¨un Sirer. (2001). Beehive: Exploiting Power Law Query Distributions for O(1) Lookup Performance in Peer to Peer Overlays, p1-14.
[9] Dimitri DeFigueired, Antonio Garcia, and Bill Kramer. (2001). Analysis of Peer-to- Peer Network Security using Gnutella. *Nature*, p1-20.
[10] Dejan S. Milojicic, Vana Kalogeraki, Rajan Lukose,. (2002). Peer-to-Peer Computing. *HP Laboratories*, p1-52.

[11] Steven lim, microsoft asia. (2005). A survey and comparison of peer-to-peer overlay network schemes. *Ieee*. 7 (2), p73-93.
[12] Li Gong. (2001). Project JXTA: A Technology Overview. *Sun Microsystems, Inc*.. 25, p1-12.
[13] Leszek Lilien, Zille Huma Kamal, Vijay Bhuse,and Ajay Gupta. (2002). Opportunistic Networks: The Concept And Research Challenges In Privacy And Security. *WiSe (Wireless Sensornet) Lab*, p1-36.
[14] Zoran Despotovic, Karl Aberer. (2001). Maximum Likelihood Estimation of Peers' Performance in P2P Networks. *EPFL*, p1-6.
[15] Marco Conti. (2010). Opportunities In Opportunistic Computing. *ieee*, p42-50.
[16] Jamesli. (2008). A Survey . *A Survey of Peer-to-Peer Network Security Issues*. , p1-8.
[17] Bryan Parno. (1999). Challenges in Securing Vehicular Networks.*phasical layer*, p1-6.
[18] Michael Rogers and Saleem Bhatti. (2004). How to Disappear Completely: A Survey of Private Peer-to-Peer Networks. *andrews*, p1-10.
[19]. Aman Kansal, Suman Nath, Jie Liu, and Feng Zhao. (2007). SenseWeb: An Infrastructure for Shared Sensing. *IEEE*, p1-6.
[20] Mike Chen. (2000). Security and Deployment Issues in a Sensor Network. *edu*, p2-11.
[21] Choonhwa Lee and Sumi Helal. (2002). PROTOCOLS FOR SERVICE DISCOVERY IN DYNAMIC AND. *ISSN*. 11 (1), p1-12.
[22] Weisong Shi, Kandarp Shah, Yonggen Mao, and Vipin Chaudhary. (1990). Tuxedo: A Peer-to-Peer Caching System. *edu*, p1-17.
[23] Prem Uppuluri, Narendranadh Jabisetti, Uday Joshi, Yugyung Lee. (2001). P2P Grid: Service Oriented Framework for Distributed Resource Management. *edu*, p1-4.
[24] Jeffrey L. Eppinger. (2005). TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem. *CMS*, p1-9.
[25] Dr. Roger Wattenhofer. (2005). Attacks on Peer-to-Peer Networks.*ETH*, p1-36.
[26] Huaizhi Li and Mukesh Singhal. (2007). Trust Management in Distributed Systems. *IEEE*, p45-53.
[27] Karl Aberer, Manfred Hauswirth. (2008). An Overview on Peer-to-Peer Information Systems. *EPFL*, p1-14.
[28] B, Cohen, Incentives Build Robustness in BitTorrent. In 1st International Workshop on Economics of P2P Systems, pp. 1-5, June 2003
[29] J. Dinger, and H. Hartenstein, Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration. In Proceedings of the First International Conference on Availability, Reliability and Security. Institut fur Telematik, Universitat Karlsruhe (TH), Germany, 2006.
[30] X. Fan, and Y. Xiang, Propagation Modeling of Peer-toPeer Worms. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications. Central Queensland University, Rockhampton, Australia,2010, pp. 1128-1135.
[31] J. Kong, W. Cai, and L.Wang, The Evaluation of Index Poisoning in BitTorrent. In 2010 Second International Conference on Communication Sofware and Networks. Northewestern Polytechnical University, Xi'an, China, 2010, pp. 382-386.
[32] A. Legout, U. Guillaume, and M. Pietro, Understanding BitTorrent: An Experimental Perspective. In IEEE/INFOCOM'05, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Institut Eurecom, Sophia Antipolis, France, 2005, pp. 2235-2245.
[33] J. Liang, N. Naoumov, and K.W. Ross, The Index Poisoning Attack in P2P File Sharing Systems. In 25th IEEE International Conference on Computer Communications. Polytechnic Univerisy, Brooklyn, NY, 2006, pp. 1-12.
[34] S. J. Nielson, S. A. Crosby, and D. S. Wallach, A Taxonomy of Rational Attacks. Department of Computer Science, Rice University, Houston, Texas, 2005.
[35] L. L. Peterson, and B.S. Davie, Computer Networks: A Systems Approach. Elsevier, Inc. San Francisco, CA 2007
[36] B. Pretre, Attacks on Peer-to-Peer Networks. Department of Computer Science, Swiss Federal Institute of Technology (ETH) Zurich, Swiss, 2005, pp. 6-15.
[37] W. Stallings, Cryptography and Network Security: Principles and Practices. Prentice Hall, Upper Saddle River, NJ, 2005.
[38] F. Su, Z. Lin, and Y. Ma, Effects of Firewall on Worm Propagation. Proceedings of ICCTA 2009. Research Institute of Networking Technology, Beijing University of Posts and Telecommunications, Beijing, China, 2009, pp.880-884
[39] A.S. Tanenbaum, Computer Networks. Prentice Hall PTR, Upper Saddle River, NJ, 2003.
[40] Verizon business, Major Online Stock Broker Turns to Verizon Business to Help Stop a Potentially Devastating DDoS Attack. Verizon business, 2008.
[41] L. Wang, Attacks Against Peer-to-Peer Networks and Countermeasures. TKK T-110.5290 Seminar on Network Security. Helsinki University of Technology, Finland, 2006