A Survey of Peer-to-Peer Attacks and Counter Attacks

Yu Yang and Lan Yang
Computer Science Department
California State Polytechnic University, Pomona
3801 W. Temple Ave., Pomona, CA 91768, USA

Abstract--*Peer-to-Peer (P2P) network is a distributed network architecture that partitions tasks or workloads among peers (nodes). Similar to traditional Internet, P2P networks are open to many attacks. In this research work we survey the defensive measures against general attacks as well as P2P specific attacks. We take BitTorrent (a P2P communications protocol for file sharing) as an example to illustrate defense strategies for Rational attack and Index Poisoning attack, present an algorithm named Self-Registration to defend against Sybil attack, and clarify terminologies for defending Eclipse attack. We summarize and classify the various possible defense mechanisms for both general and P2P specific attacks.*

Keywords: Peer-to-Peer (P2P); attack; defense; general attacks; specific attacks

1 Introduction

Peer-to-Peer (P2P) technology implements peers (nodes) of equal standing with other peers (nodes) in a P2P network. Each node not only accepts the service, but also provides the service, and nodes can exchange information directly. P2P networks make good use of network resources by utilizing the idle resource of the nodes to develop an efficient information sharing platform. At present, P2P technology is widely used in file sharing protocols such as BitTorrent and Dropbox, as well as in instance message communication systems such as Skype. Similar to traditional Internet, P2P networks are open to many general attacks, such as Denial-of-Service (DoS) attack, Distributed Denial-of-Service (DDoS) attack [9], Man-in-the-middle attack [9], Worm propagation [3], and Pollution attack [4]. To defend these general attacks, technologies and mechanisms for ensuring network safety usually come from security companies (for example, the Verizon Business [13]) and the common network knowledge, such as encryption mechanisms and authentication technologies. Also, some well-known safety measures, such as firewall, anti-virus software, and security operating systems, provide the relative defensive strategies. P2P networks can also be the victim of some P2P specific attacks. Rational attack [7], Index Poisoning attack [4], Sybil attack [14], and Eclipse attack [14] are P2P specific attacks. The secure mechanisms for defending these P2P specific attacks are from a variety of sources. In this research work, we survey general attacks as well as P2P specific attacks and analyze defense strategies for each attack surveyed. In particular, we use BitTorrent as an example to illustrate the defensive measures against Rational attack and Index Poisoning attack. We present an algorithm called Self-Registration [2] to defend against Sybil attack, and clarify terminologies that are used to defend Eclipse attack. The rest of the paper is organized as follows. In section 2, five types of general network attacks and their defense mechanisms are presented. In section 3, P2P specific attacks and their corresponding defensive strategies are described. Finally, summary and classification of attacks and defenses including analysis of attack behaviors, defense strategies, risk analysis and level of defense are presented.

2 General Attacks and Defenses

2.1 Denial-of-Service (DoS) Attack

DoS attack is an attack on a computer or a network, attempting to make a computer resource unavailable to its intended users. In P2P networks, the most common form of DoS attack is an attempt to flood the network with bogus packets, thereby preventing legitimate network traffic. Another method is to drown the victim node with fastidious computation so that the node becomes too busy to answer any other queries [9].

Defenses:

A widely used technique to hinder DoS attacks is “pricing” [9]. In this technique, the host will submit puzzles to its clients before continuing the requested computation. When an attacker attempts to flood his victim, he has to solve a puzzle first, thus it becomes more difficult for the attacker to launch a successful DoS attack.

2.2 Distributed Denial-of-Service (DDoS) Attack

DDoS attack is an attacking technique based on the DoS attack [9]. The system of DDoS attack includes four parts as Figure 1 shows.

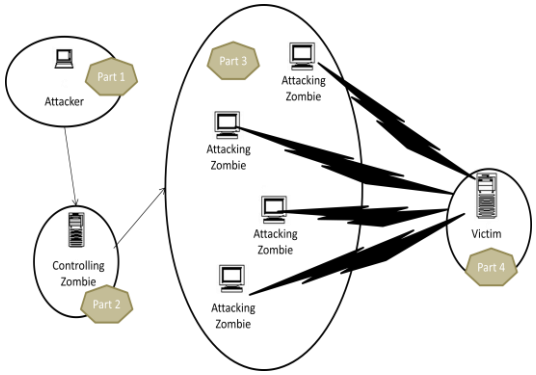

Figure 1. DDoS Attack

The first part is the actual attacker, who controls the part 2 and part 3. Part 2 and part 3 are often personal computers with broadband connections that have been compromised by a virus or Trojan. The difference between part 2 and part 3 is: from the point of view of part 4, the victim, the attacking comes from part 3, the attacking zombies while part 2 only issues an attacking order from the actual attacker without actually attending an attack. The detailed parts of DDoS attack can also be developed as shown in Figure 2.

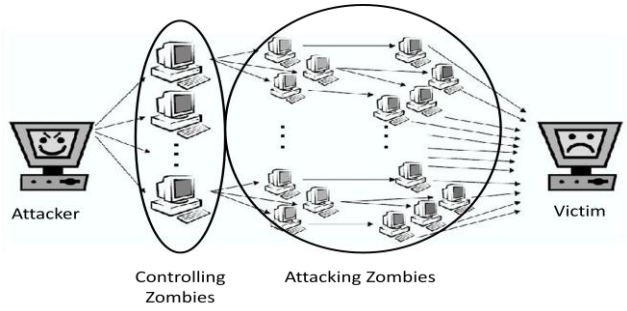

Figure 2. Developed DDoS Attack

In the developed DDoS attack, the hacker controls more than one controlling zombies, and each controlling zombie also controls a lot of attacking zombies and so on [9]. So, in DDoS attack it is hard to trace the actual attacker, because the attacker is often indirectly involved.

Defenses:

DDoS attacks are extremely hard to block due to the enormous numbers and diversity of machines involved in the attack. However, there are still many companies proposing countermeasures to defend against DDoS attack. Take Verizon business security team for example [13]. In the online broker's business, when hackers use DDoS attack to launch some attacks, the companies will lose revenue, productivity and reputation. The attacks will cause the broker's clients to experience timed-out pages, slow loading times, and overall non-responsiveness to user inquiries. And the company will receive the notice to demand an extortion in order to stop the crippling attacks or prevent the coming attacks.

There are three steps to prevent DDoS attacks:

First, let the broker company's Internet traffic through Verizon business, which will help the clients to filter a series of malicious information. Second, security team offers a monitoring and detection capability that constantly searches incoming DDoS attack. This warning system also gives the broker the ability to determine the extent of an attack and respond with the proper level of mitigation that could help protect against losses. Finally, the brokers can have their own blacklist or whitelist, which allow the brokers to terminate blacklisted traffic before it reached the brokers' Internet site while allowing whitelisted traffic to always be permitted [13].

2.3 Man-in-the-middle Attack

Man-in-the-middle attack is an indirect intrusion, and the attacker inserts his computer undetected between two nodes [9].

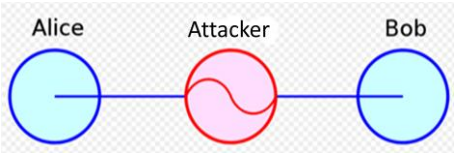

Figure 3. Man-in-the-middle Attack

In Figure 3, Alice and Bob are normal users. The attacker in the middle can intercept data, modify data and send data without being detected by Alice and Bob.

Defenses:

So far from our literature survey we haven't yet found any effective defense strategies for this type of attack. However, deriving from the common network knowledge we propose the following defense strategies. First, encryption mechanism should be used to protect the information to be transmitted. The information is encrypted with some encryption methods before being transmitted. Even though the intruder intercepts the information, he is unable to decrypt the message without knowing how to decrypt the message [12]. Also, authentication technologies should be used to detect Man-in-the-middle attack. The authenticator includes redundant information about the message contents, such as who created the authenticator, who is the sender of the messages. In other words, authentication is used to verify and distinguish the authenticity and validity of a user [8] [10]. The purpose of this technique is to distinguish legal users from illegal users.

2.4 Worm Propagation

Worm transits the copies of itself from one node to others through the network communication, and starts by itself. Worm can be propagated through file, email, web server, and so on [3].

Defenses:

The defense strategies we recommend here are to use some common network measures that have already been widely used in many computer systems. The first one is using firewall. Most of the time, worm scans a certain port in the computer to infect, and firewalls can block the port that worm needs. Also, we can use some anti-virus software to protect our computers. The anti-virus software includes the virus signature, if some attributes of the file correspond to the attributes in virus signature, the anti-virus software can delete or isolate that file [11]. The last defense has been offered by security measures from operating system developers. For example, OpenBSD operating system concentrates on the aspect of security and possesses many security features such as protecting the operating system from buffer overflows or integer overflows, which makes an attacker without any ideas of what data segment he should overwrite [9].

2.5 Pollution Attack

The practice of this attack is to replace a file in the network by a false one, and this polluted file is of no use to the clients [4]. The attacker makes the target content unusable by changing the contents or part of it into another irrespective content, and then makes this polluted content available for sharing. In order to attract people to download the polluted content, the polluted content needs to disguise itself as the target content, such as having the same format and similar size. It also needs to keep high-bandwidth connections.

Defenses:

From the user's side, the downloaded file that has been polluted is not harmful to our computers, but it is just of no use. Therefore, in our opinion, once a user finds out that the downloaded files are polluted files, the user should remove the files from the P2P system.

3 P2P Specific Attacks and Defenses

3.1 Rational Attack

In most P2P systems, self-interested behavior at the expense of the system can be classified as a Rational attack [7]. For instance, Figure 4 shows a possible scenario of Rational attack.

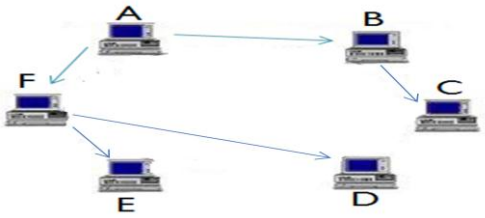

Figure 4. Rational Attack

In the P2P system shown in Figure 4, node A wants to distribute content. To decrease the upload bandwidth burden on the node A, only a small number of nodes such as node B and node F are directly connected to it. The content is then propagated from node B and node F to additional peers such as node C, D and E. Because of the self-interested behavior in most P2P systems, a self-interested node may realize that it can save expensive upload bandwidth if it chooses not to share. If a large number of nodes are self-interested and refuse to contribute, the system may destabilize [7]. In this case, if enough nodes such as B and F become self-interested, the system cannot guarantee a reasonable level of uploads and downloads.

Defenses:

Here we take BitTorrent as an example to illustrate the countermeasure of Rational attack. BitTorrent is popularly used for file distribution. In BitTorrent, there is an algorithm called Choking algorithm [1] [5], which can guarantee a reasonable level of upload and download reciprocation. If peers just download, and never upload, they should be penalized.

Terminology in Choking algorithm:

Pieces and Blocks: transmission unit on the network.

Interested and Choked: peer A is interested in peer B when peer B has pieces that peer A does not have. Otherwise, peer A is not interested in peer B. Peer A chokes peer B when peer A decides not to send data to peer B. Otherwise, peer A unchokes peer B.

Planned optimistic unchoked peer: a random peer that is choked and interested.

Active peer: a peer has sent at least one block in the last 30 seconds.

The flowchart is shown in Figure 5 describes details of the Choking algorithm.

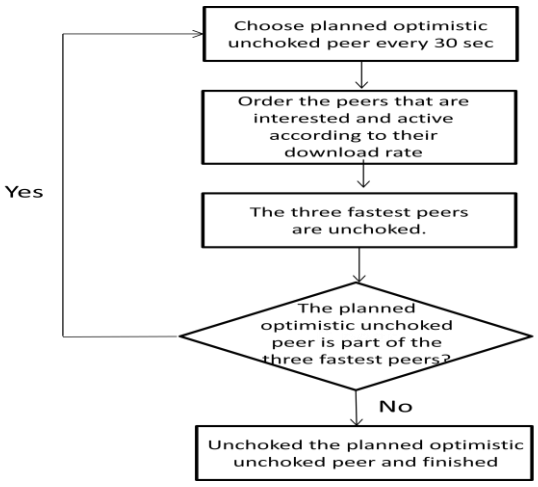

Figure 5. Flowchart of Choking Algorithm

3.2 Index Poisoning Attack

Most P2P file sharing systems have indexes, allowing users to discover locations of desired content. Index poisoning aims at the index querying process of users and makes it hard to find correct content in P2P network. The attackers simply insert large numbers of invalid peer information into the index to hinder the users from finding correct resource [4]. For example, BitTorrent is easy to be attacked by Index poisoning. In BitTorrent, first, we need to download a complete file known as a seed with the extension .torrent. The .torrent contains information about the file, such as its length, name, and a tracker. The tracker acts as an information exchange center from which peers obtain necessary information about other peers, which are downloading the same file. When a peer starts a BitTorrent task, it first advertises its information into the tracker, and then the peer contacts the tracker and gets a list of other peers' information. When a tracker receives an advertisement for a task from a peer, it does not authenticate the advertisement and does not verify whether the content is truly available with the advertised information or not. The attacker deliberately advertises large quantity of invalid peer information of the targeted content. So, when a user attempts to download the content corresponding to the task, his BitTorrent client always fails to establish connection with the other peers, due to the high probability of connecting to invalid peers [4].

Defenses:

There are two measures to defend against the Index poisoning attack. The first one is to authenticate versions and advertisements [6]. Like some rating websites and forums, the content has been initiated with a moderator to manage disputes. The second method is rating sources [6]. If these are good sources, which advertise and upload files they actually have, the corresponding peers will get high rating scores. If these are bad sources, whose index poison and pollute the system, the corresponding peers will be blacklisted.

3.3 Sybil Attack

Many P2P systems introduce a redundant backup mechanism to protect integrity and privacy. A P2P system must ensure that each network entity ID indicates only one entity. If an entity acts as a number of multiple identities, this entity can control a significant part of networks. Such attack is defined as Sybil attack. Sybil attack will destroy the redundancy in P2P network [14].

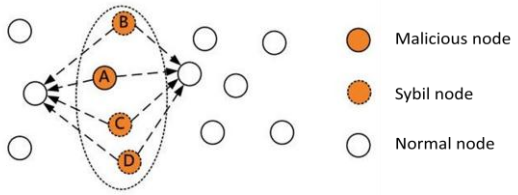

Figure 6. Sybil Attack

In Figure 6, when a normal node makes redundant backup, it selects a group of entities such as node A, B, C and D that have different IDs. But in fact, node B, C and D actually do not exist, as they are the malicious nodes created by the attacker, so the backup cannot finish.

Defenses:

The countermeasure is an identity registration procedure called "Self-Registration" [2], which is shown in Figure 7 and explained below:

A new node hashes its IP address and port to calculate its identifier, and then register its identifier at already registered nodes, which are the registration process of the new node. After that, the new node requests to join P2P network. Other registered nodes have the ability and responsibility to identify whether the new node is real or not. If the new node is not fake, it will be accepted by the P2P network.

Registration nodes: in this procedure nodes are verified that they are not fake nodes.

New nodes: In this procedure, a node is checked that its ID and Registration ID are one-to-one mapping.

The Self-Registration algorithm consists of two parts, the "Registration node" and the "New node". The functionality of both parts is described in Figure 7.

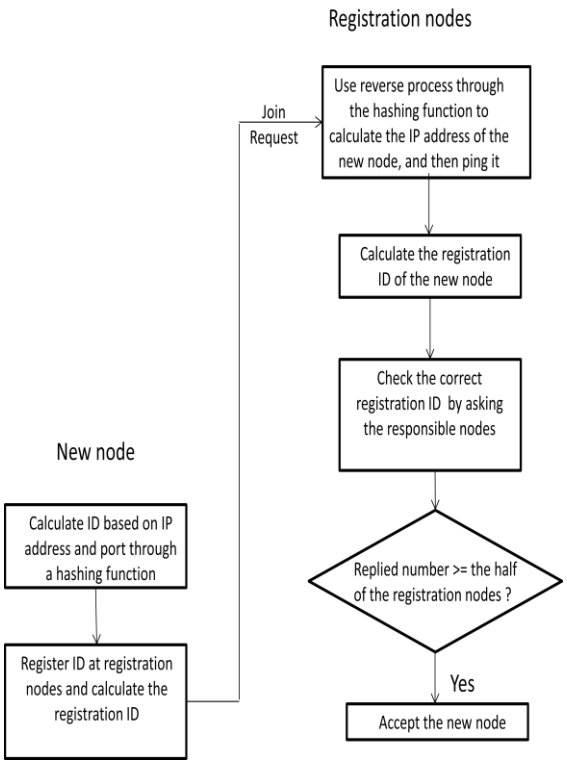

Figure 7. Self-Registration Algorithm

3.4 Eclipse Attack

In an Eclipse attack, an attacker controls a large part of a good node's neighbors. In this situation, the union of malicious nodes works together to fool a good node by writing their addresses into the neighbor list of a good node. By using Eclipse attack, an attacker can control the significant part of a network, even the entire network. Thus, nodes cannot forward message correctly and the whole network cannot be managed. A Sybil attack can be considered as a specific Eclipse attack, if the attacker generates great amount of identifications to act as neighbors of a good node [14]. For instance, a scenario of an Eclipse attack is shown in Figure 8.

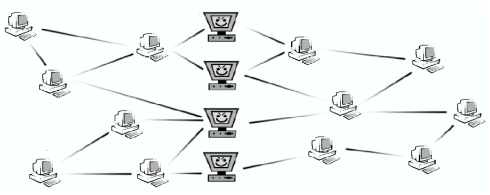

Figure 8. Eclipse Attack

In Figure 8, the malicious nodes separate the network into two subnetworks. No matter what methods are used to communicate within two subnetworks, the normal nodes cannot avoid connecting with one of the malicious nodes. So, the entire network has been controlled by malicious nodes.

Defenses:

Before introducing the countermeasure to against an Eclipse attack, we need to clarify two terminologies, which are indegree and outdegree. Indegree means the number of direct routes coming into a node and outdegree means the number of direct routes going out of a node. The idea to defend against Eclipse attack is to bound both indegree and outdegree of the attacker nodes. This method can be described as follows. First, we apply the countermeasure to the Sybil attack. This process assures there is no possibility of Eclipse attack based on a Sybil attack. Then we concentrate on how to deal with the indegree and outdegree of the attacker nodes. Each node in P2P networks maintains a list of its neighbors. We make a node periodically query the neighbor lists of its neighbor peers. If the items on the replied neighbor list are greater than the indegree bound, or that node is not on its neighbor's list or the size of returned neighbors is greater than the outdegree bound, it means an Eclipse attack happened [14].

4 Conclusions and Future Improvement

In this paper, we describe a list of network attacks that are common in current P2P networks. Some of these attacks are general attacks occurring over the traditional Internet that also applies to P2P networks, while others are specific attacks against P2P networks. General attacks described in this paper include DoS attack, DDoS attack, Man-in-the-middle attack, Worm propagation, and Pollution attack. P2P specific attacks include Rational attack, Index Poisoning attack, Sybil attack, and Eclipse attack. Countermeasures to defend each of the general and specific attacks in P2P networks are discussed and analyzed. BitTorrent is used to illustrate the defensive measures against Rational attack and Index Poisoning attack. Examples are used to illustrate various attacks in P2P network. In the following Table 1, we clarify the defense measures and the behaviors of the attacks. Table 1 also summarizes the risk analysis and the level of defense. The summary is derived from the information we collected and analyzed from the above described attacks and defense strategies on P2P networks.

Future will includes more in-depth study of effective defense strategies for various attacks on P2P networks, and survey multiple attacks on one Peer-to-Peer network.

Table 1: Summary of Attacks and Defense Strategies

Name of Attack	Behavior	Defense strategy	Extent of Danger	Level of Defense
Denial-of-Service (DoS)	1. Flood the network with bogus packets. 2. Drown the victim in fastidious computation.	Pricing	Medium	Easy
Distributed Denial-of-Service (DDoS)	Hacker controls the controlling zombies, through the controlling zombies to control attacking zombies to launch the attack.	Through the trusted server, provide warning system, and created blacklist and whitelist for trusted visits.	High	Hard
Man-in-the-middle	An attacker inserts himself undetected between two nodes, and intercept, modify and send data between those two nodes.	Encryption mechanism and authentication technology	Medium	Medium
Worm Propagation	Transits the copies of itself from one node to others automatically.	Firewall, anti-virus and some safety operating system	Medium	Medium
Pollution	Share a file, which is unused.	Remove it	Low	Easy
Rational	Download the resource and refuse to upload.	Choking algorithm	Medium	Medium
Index Poison	Poison the index information to make the node hard to find correct content.	Authenticate versions and advertisements, rating sources	High	Medium
Sybil	An attack controls a number of identities	Self-Registration algorithm	High	Hard
Eclipse	The malicious nodes work together to fool the good nodes.	Indegree and Outdegree method	High	Hard

5 References

[1] B, Cohen, Incentives Build Robustness in BitTorrent. In 1st International Workshop on Economics of P2P Systems, pp. 1-5, June 2003.

[2] 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.

[3]X. Fan, and Y. Xiang, Propagation Modeling of Peer-to-Peer Worms. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications. Central Queensland University, Rockhampton, Australia,2010, pp. 1128-1135.

[4] 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.

[5] 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.

[6] 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.

[7] S. J. Nielson, S. A. Crosby, and D. S. Wallach, A Taxonomy of Rational Attacks. Department of Computer Science, Rice University, Houston, Texas, 2005.

[8] L. L. Peterson, and B.S. Davie, Computer Networks: A Systems Approach. Elsevier, Inc. San Francisco, CA 2007.

[9] B. Pretre, Attacks on Peer-to-Peer Networks. Department of Computer Science, Swiss Federal Institute of Technology (ETH) Zurich, Swiss, 2005, pp. 6-15.

[10] W. Stallings, Cryptography and Network Security: Principles and Practices. Prentice Hall, Upper Saddle River, NJ, 2005.

[11] 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.

[12] A.S. Tanenbaum, Computer Networks. Prentice Hall PTR, Upper Saddle River, NJ, 2003.

[13] Verizon business, Major Online Stock Broker Turns to Verizon Business to Help Stop a Potentially Devastating DDoS Attack. Verizon business, 2008.

[14] L. Wang, Attacks Against Peer-to-Peer Networks and Countermeasures. TKK T-110.5290 Seminar on Network Security. Helsinki University of Technology, Finland, 2006.