Published in the Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security, 2007 (ICCIIS, 07), pp:132-138.

A Taxonomy of Attack Methods on Peer-to-Peer Network

Md. Sadek Ferdous[1], Farida Chowdhury[2] and Md. Moniruzzaman[3]

Abstract—**In the recent years we've seen a tremendous growth in peer-to-peer network development. Such rapid development has drawn the attention of many types of attackers. They either choose peer-to-peer network as their ultimate target or they use peer-to-peer network as an intermediate tool to generate more sophisticated attack against another target. There are many papers contributed by many researchers targeting different types of attack model found in peer-to-peer network. But a single paper classifying all known types of attacks peer-to-peer network is scarce. This paper fills in that gap by proposing a complete taxonomy of popular known attack methods found in peer-to-peer network.**

Key Words: Peer-to-Peer, Peer-to-Peer Security, Taxonomy.

I. Introduction

Peer to Peer, shortly known as P2P is one of the two architectures in communication network by which two or more entities in a networked environment communicate with each other. The other architecture is Client/Server. In client/server architecture, there is usually a Server entity and one or more Client entities. Communication between any two entities has to be done through server. Traditionally Server is the service provider and the client(s) are the service consumer. But Peer to Peer architecture is a server-less architecture. Every entity in the network is altogether Server and Client, that is, every entity is at a time service provider and service consumer. A network based on Peer to Peer architecture can be loosely said as Peer to Peer Network. A formal definition can be stated as [26]: Peer to Peer Networks are those that exhibit three characteristics: self organization, symmetric communication and distributed control. A self organizing P2P network "automatically adapts to the arrival, departure and failure of nodes" [27]. P2P system and P2P computing sometimes are used by the researchers to loosely define the P2P network. In this paper, those three terms will be used interchangeably.

Before 1999 P2P was a topic of research interest among only the researchers. But the inception of Napster in 1999 changed the whole scenario of P2P research [2]. Since then researchers around the world deployed P2P network in many different applications which include Communication Application like IM (Instant Messaging), Distributed Computation Project like Seti@Home, gnome@home, etc, Distributed Database System, Content Distribution System for sharing mostly digital media [29]. Due to the immense interest of the researchers and the active participation of mass peoples many P2P network like Gnutella, Pastry, Tapestry, Chord, Content Addressable Network (CAN), Kazaa, Freenet, FastTrack, Overnet, eDonkey, BitTorrent have come into existence [26, 29]. Such popularity drew attention of many "bad peoples" or hackers. With a scalable rate of attack success, P2P network has been a potential target for them. Outlook magazine ranked P2P applications on the list of top 20 vulnerabilities of the recent time [8]. That's why, security in the P2P network has been one of the most sought after factors among the researchers.

Following this introduction, this paper is organized as follows: Section 2 describes the related works in P2P attack model. Section 3 proposes the complete taxonomy of different attack methods found in P2P network. Section 4 suggests future work. We conclude in Section 5.

II. Related Works

Numerous papers have been published in this field either illustrating different P2P attack model or exemplifying different defense mechanisms in certain aspect. In this section we'll cite some of those papers. In [10, 13, 16, 19, 31], impact of worm propagation in P2P network been analyzed. [3] discusses how a P2P system can be used to generate DDoS attack. In [11], Sybil, one of the major types of attacks in P2P network, has been analyzed. [5] examine another virulent attack of P2P network named Eclipse. [21] examines attacks based on content availability in P2P network. [28] provides a taxonomy of rational attack found in P2P network. [17] illustrates different types of P2P attack methods and their solutions. [23] proposes a distributed recovery method if a P2P network is under violent attack. In [18] an attack resistant P2P system has been proposed. Though there are many papers in this respective field, but almost each of them is confined to different aspect of a single attack entity. But to the best of our knowledge we've not seen any paper which proposes a comprehensive taxonomy of all known attack methods in P2P network. If such paper exists in reality, we've been completely unaware of it during the writing of this paper.

III. Taxonomy of Attacks on P2P

Various forms of attacks in the P2P network can be roughly categorized into two broad categories (Figure 1): Active attack and Passive attack. Active attack can be defined as the attack which mainly targets node or nodes in the P2P network. The main motif behind active attack is to cause damage to a node or nodes. Whereas, passive attack includes those attacks whose ultimate target is the P2P network itself, not the node of the P2P network. The main motif behind

[1]Dept. of Information & Communication Technology, Metropolitan University, Sylhet, Bangladesh. E-mail: sferdous@metrouni.edu.bd

[2]Dept. of Computer Science & Engineering, Shah Jalal University of Science & Technology, Sylhet, Bangladesh. E-mail: farida-cse@sust.edu

[3]Dept. of Computer Science & Engineering, Primeasia University, Dhaka, Bangladesh. E-mail: mzn_munna@yahoo.com

passive network is to disrupt or damage the P2P network service so that participants are restrained to use the particular service.

A. Active Attack

Active attack can again be subdivided into two other categories (Figure 2a): Targeted attack and Opportunistic Attack. A targeted attack is launched by the attacker with a definite target or targets in mind. Before initiating such attack, attacker fixes a particular target(s) and gathers as much knowledge as possible about the possible target(s). Whereas in the Opportunistic attack, an attack is launched aiming no particular node. Intention behind such attack is to exploit as much node as possible and then take advantage of the vulnerabilities found on those nodes. So the number of affected nodes in the targeted attack is almost much lesser than those of opportunistic attack.

1. *Targeted Attack*: There are several types of attack in the P2P network that can be classified into some form of Targeted attack. Those attacks include (Figure 2a): MiTM (Man in The Middle) attack, DoS/DDoS Attack, Short Circuit Attack, Resource Exhaustion Attack and Identity Attack.

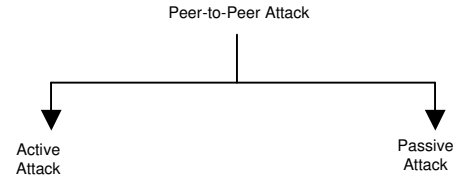

Fig. 1: Taxonomy of P2P attack

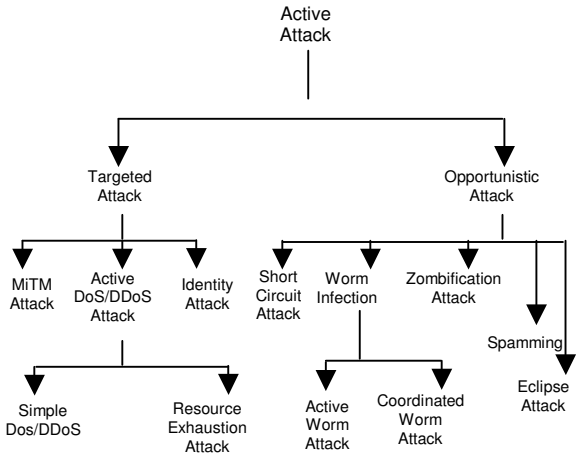

Fig. 2a: Taxonomy of active attack

MiTM: Man in The Middle (MiTM) is a very infamous attack which prevails in almost every form network communication, both in wired and wireless communication. According to [22], a MiTM can be defined as: "An attack in which the attacker impersonates both ends of a secure communication channel. The attacker eavesdrops on a secure/non-secure communication session to gain information that enables the attacker to impersonate both parties' communicating". In the network communication, an attacker, by using some crafty method, places himself between two nodes exchanging data. So that, every data that should pass only between two original hosts passes through the attacking host. Such attack can remain undetected if the attacker remains passive. In the active attack method, the attacker can choose to modify the data that passes through him. These nodes can be either in wired or wireless network and either in P2P network or Client/Server network. In a non-P2P environment, this crafty method is usually done with the help of ARP cache poisoning [20]. In a P2P network this task is extremely simple [17] as there is no control over node placement in the P2P network. That is, a node can be placed any where in the network. Most current P2P networks such as pastry, chord, etc support this. The above mentioned P2P networks are extremely vulnerable to this level of attack.

Identity Attack: An identity attack in P2P network can be defined as: "An attack on which the identity of participating nodes in the P2P network is not protected and can be easily tracked down by the attacker with the intention to harass or actively and legally attack them" [1, 25]. In two very popular P2P networks such as BitTorrent and eMule, list and identities of participating nodes can be traced with some queries [1]. After revealing the identities, other forms of attack such as DoS, DDoS, State Exhaustion Attack, etc can be initiated against those nodes or they can be legally harassed in many forms.

Active DoS/DDoS: Denial of Service (DoS) is a specialized form of attack, in which the attacker tries to prevent legitimate users to access to a system or network by several possible means, including: Flooding the network with so much traffic that traffic from legitimate clients is overwhelmed, flooding the network with so many requests for a network service that the host providing the service cannot receive similar requests from legitimate clients and thus disrupting communications between hosts and legitimate clients by various means, including alteration of system configuration information or even physical destruction of network servers and components [22].

As defined by the World Wide Web Security FAQ [14]: "A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms". That is in a DDoS, attacker, by using some crafty methods, compromises as many as host as possible in the network. Such compromised host is known as Zombies. Then using these zombies, the attacker launches DDoS attack against a particular target where each zombie launches its own forms of DoS attack against that node. In DoS attack, the attacking node actively participates in the attack so that attacking node can easily tracked down, whereas in DDoS attack, the main attacker seldom participates in the attack. He mainly coordinates the attack among the zombies and upon his order,

the zombies participates in the active attack. So it is very difficult to track down the main attacker.

DoS and DDoS attack in the P2P is very likely to occur. In a P2P network, there are a huge number of participants and the traffic generated by them is huger. So it is very difficult to predict traffic between nodes. This makes very very hard to detect compromise of P2P nodes from the outside. Attack traffic of DoS and DDoS and attack control traffic of DDoS can be hidden in normal P2P traffic. In this way, a compromised P2P system may offer enough security for an attacker [3]. DoS and DDoS attack in the P2P network can be targeted against any particular node or against the P2P network system. The former is a form of active attack while the later is a form of passive attack. So here we're discussing the DoS attack that can be initiated against the node and we'll discuss the later in the paragraph of the passive attack.

Resource Exhaustion Attack: In [22] this attack is defined as: "A resource exhaustion (or resource starvation) is a form of DoS attack in which the attacker uses up a resource on the target system, with the result that no resources are available for legitimate users trying to access the system. Examples of types of resources that can be "starved" include Central Processing Unit (CPU) cycles, memory (physical or virtual), network bandwidth, disk space, disk quota, file handles, processes, and thread". In a P2P network a modified version of such attack is initiated against the nodes in which information related to a network query is stored [18]. In such attack, the attacker launches a huge amount of queries at a very rapid rate on those nodes to tire out the buffers of those nodes so that those nodes can't serve any query and thus creating disruption of service. Recursive overlay network is much susceptible to this kind of attack [18].

2. *Opportunitistic Attack*: There are several types of attack in the P2P network that can be classified into some form of Opportunistic attack. Those attacks include (Figure 2b): Worm Infection, Zombification Attack and Eclipse Attack.

Short Circuit Attack: In a recursive overlay network, query may reach a node more than one time. In the usual sense, the node will detect and drop those queries. However, if responses are lost due to some factors such network error, node failure or malicious nodes, the querying node may be unable to find an object even though there exists a path to the node where it resides. When a node drops such response with the intention that node drop will lead to the possibility of disruption of availability of a node for the querying node, then this malicious event can be considered as Short Circuit Attack [18]. This is a particular event of opportunistic attack as this attack succeeds if and only if other path of the response also somehow becomes unavailable.

Worm Infection: In [22], Worm has been defined as "Autonomous code that propagates across a network". Computer virus is a malicious code that infects files on a system, whereas worm is one form of a computer virus which can infect a local system and spread to other systems on the network as well. Like all other network system, worm infection imposes a great threat toward P2P system. Recent surge in the P2P system also makes it a potential lucrative target for worm infection. Wei Yu, Corey Boyer, Dong Xuan in [31] stated three reasons which explained the justification for P2P system to be as one of the major targets for worm infection. Those reasons are: "1) compromising P2P systems with a large number of registered active hosts can easily accelerate Internet worm propagation, as hosts in P2P systems are real and active; 2) some hosts in P2P systems may have vulnerable network and system environments, i.e., home networks; 3) as hosts in P2P systems maintain a certain number of neighbors for P2P routing purposes, worm infected hosts in the P2P system can easily propagate the worm to its P2P neighbors, which continue the worm propagation to other hosts". Their statements were justified when one of the vicious recent worms known as MyDoom spread themselves over the Kazaa P2P system [31]. P2P worm can be of two types: 1) Active worm or Scanning worm and 2) Coordinated worm or Overlay Topological worm.

Active Worm: Active worm or scanning worm is one particular type of worm which randomly probe IP addresses for their propagation [31]. Actually this is the type of worm that is usually found in any network including P2P network. This type of worm is implemented using Pure Random-based Scan or PRS [31]: In this strategy, worm-infected hosts do not have any prior knowledge of the hosts. The worm host randomly selects the IP addresses of victim targets from the global IP address space and launches the worm attack and tries to find some vulnerability to be exploited among them.

Coordinated Worm: Coordinated worm, also known as Overlay Topological Worm, is a particular type of worm which is designed specially for any particular P2P network. It never randomly scans for any target like the scanning worm, rather it uses some kind of coordinating information found in the Overlay topology of the P2P network. This type of worm is more deadly than the scanning worm in three ways which include [31]: First, they spread much faster. Second, the rates of failed connections they generate are not high. Finally, their traffic patterns can be blended into the normal traffic patterns of the P2P network which makes them very difficult to be detected. One of the main sources of coordinated information is Distributed Hash Table (DHT) of many P2P networks [10]. The other sources might be the software itself by which any user connects to the P2P network as many nodes in the P2P networks will be running the same software. So a vulnerability in that software (such as a buffer overflow), all of the nodes in the network are also vulnerable. In this case a P2P worm need only look at the P2P routing tables and infect the hosts neighbor set and thus has the capability to spread exponentially (by the average degree of nodes) through the network [17].

Zombification Attack: Zombie is a compromised system used as an intermediary in a Distributed Denial of Service (DDoS) attack [22]. Such compromised hosts generally are poorly secured systems connected to the Internet, which the attacker

compromises and on which the attacker installs special DDoS agent software. Using large numbers of zombies is the key to a DDoS attack and provides the amplification factor that makes them so much more effective than traditional DoS attacks.

The process of finding poorly secured system can be defined as Zombification Attack and it is a form of opportunistic attack as the attacker has no specific target in mind. He will try to zombiefy as many nodes as possible by exploiting different vulnerabilities found on different node. The step of Zombification is quite simple. The attacker will run automated tools to find vulnerable hosts on other networks connected to the Internet. Popular tools for launching such DDoS attacks include TFN, TFN2K, Trinoo, and Stachel-draht, all of which are readily available on the Internet [22].

Spamming: According to [22], the more formal way of defining spam is any form of e-mail that tries to hide its originating e-mail address to make it hard to trace the sender or that uses deception in the subject line to try to induce the recipient to open the message. It has become the curse of the Internet. Though spamming is not directly related to the security of the system, but it can create disturbances for the participants of the P2P network. As in some P2P network identity of the user can be revealed, attacker can target them for spamming and thus harass them.

Eclipse Attack: Eclipse attack [15] in P2P network is defined as an attack in which a large number of malicious nodes with some methods compel the legitimate nodes to adopt the malicious nodes as their neighbors so that they can dominate the sets of legitimate nodes. If successful, an Eclipse attack enables the attacker to mediate most overlay traffic [5]. In the extreme, an Eclipse attack allows the attacker to control all overlay traffic that means, a successful Eclipse attack partition the network into two or more partitions and then all communication that passes the partition is forwarded by the malicious node [17]. It's one large form of MiTM attack. A successful eclipse attack, combined with creating fake nodes, can bring most networks entirely down [17]. Castro et al. identify the Eclipse attack as a threat in structured overlay networks [15].

B. Passive Attack

There are many different forms of passive attack which include (Figure 2b): Cached Data Attack, Sybil Attack, Bootstrapping Attack, Spamming, ID Mapping Attack, Routing Table Attack, Rational Attack, Passive Dos/DDoS attack and Content Availability Depletion Attack.

Cached Data Attack: Caching has been a major way to improve performance in the P2P network. An excellent description of caching in peer-to-peer systems can be obtained in [24], [30]. Though caches offer a performance boost, it opens up a new security loophole in the system. The attacker may exploit the cache of the nodes. Such exploitation may create down-gradable performance for the network [18].

Sybil Attack: Sybil attack is defined as an attack on uniqueness on identity in which a node dominates the P2P network by obtaining a large number of node identifiers and thus imitating a large number of nodes [11]. This dominance can be used to control the whole P2P network by only one node. The network becomes more vulnerable to this attack if the attacker can place the new nodes anywhere in the network by manually influencing in the ID space. This enables the attacker to use a minimum number of nodes and impose a large amount of damage to the network. When the attacker gains enough nodes in that segment compared to the legitimate nodes, the attacker can control all messages that pass through the segment. This attack can be used as gateway to execute large scale attacks of other types such as Eclipse. Sybil attack is one of those attacks in the P2P network which are very difficult to detect [18].

Bootstrapping Attack: When a new node joins the system, it must contact at least one existing node of the system. This process is known as bootstrapping and this can be accomplished in two ways: either using a centralized bootstrapping service through a bootstrap server or maintaining a list of nodes in which the program runs. The later method is very popular as it diminishes the need of contacting a bootstrap server [18]. This bootstrapping can be source of another form of attack known as bootstrapping attack. It is not exactly a direct attack over the P2P network, rather an outcome of different types of P2P attack such Sybil or Eclipse Attack. In any of the above attacks, when a network is partitioned, the Bootstrapping Attack can be formalized. If there is a subnet of malicious nodes around the new node and the new node just bootstraps using one of them then that new node will be effectively a part of the malicious node and be partitioned from the actual network. The attacker then can use this node as one of his attacking nodes.

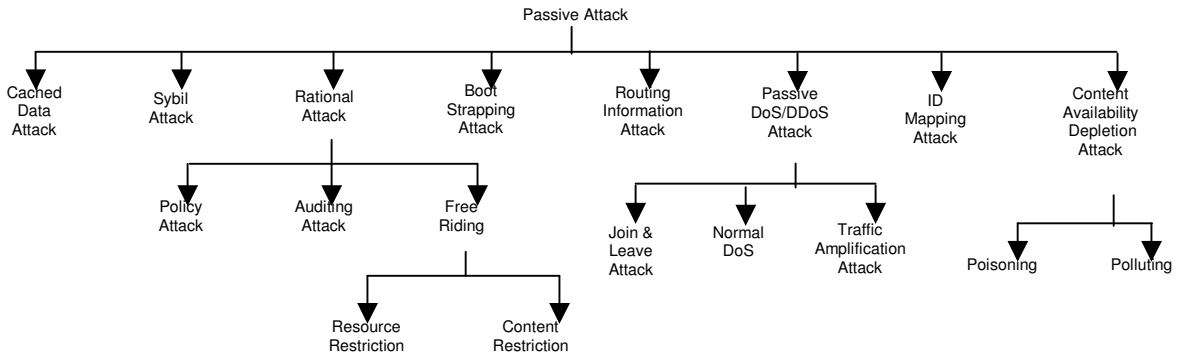

Fig. 2b: Taxonomy of passive attack

ID Mapping Attack: In this attack, an attacker may obtain a particular node identifier and thus a particular position on the overlay network. Having got a particular identifier, the attacker gains control over nearby resources [6]. The outcome of this type of attack can be illustrated with an example: Node A contacts a malicious node B. Node B knows that node A will contact the set of neighbors such as Node C. B sends A the list of its neighbors including C. Then B pretends to be node C by the IP mapping attack and sends the answer to node A. If A has no mean to verify the origin of the message then it could be deceived into believing that false message that it obtained from B was indeed the actual message from C.

Routing Information Attack: Nodes in the P2P network preserve some sort routing information to route queries in the system. Those routing information can be a potential target. Routing information attack in the P2P network involves either Incorrect Lookup Routing or Incorrect Routing Update [12]. In the incorrect lookup routing, malicious node forwards queries to incorrect or non-existence node and then the original node may never find the destination node. In the incorrect routing update, a malicious node could corrupt the routing table with incorrect updates to neighbors so that the non-malicious nodes may then start pointing to incorrect nodes or to nonexistent nodes. Structured P2P network that has the freedom to choose between multiple routes is more vulnerable to such attack [12, 18].

Rational Attack: It will be reasonable if we assume that most of the participating nodes in the P2P network will be rational, that is they will try to maximize their consumption of system resources while lowering the use of their own. If such behavior breaches the system policy then it can be defined as a rational attack. According to the [28], a formal definition has been defined as: "In most P2P systems, self-interested behavior at the expense of the system can be classified as a rational manipulation failure or, from a different perspective, a rational attack". Rational attack takes different disguise which include:

Free Riding: Free riding in the P2P network is defined as a process when a Peer consumes resources mostly while producing very few. For example, in a file sharing P2P system, when the users only download resources and never upload/share any their resources then they are defined as a free rider. Free riding is a very common phenomenon for any P2P network. Adar and Huberman [7] analyzed free-riding in the Gnutella. The authors found that almost 70% of Gnutella users were free-riders and the top 1% of sharing hosts returns 50% of all responses. Nearly 50% of the shared files came from just 1% of hosts. In more recent research, Asvanund et al [4] found that 42% of Gnutella v0.6 users were free-riders. Though free riding is not directly related to the security of P2P network but greater involvement of the free riding- peers will certainly decrease the network performance. Free riding is of two types: Content Restriction & Resource Restriction.

Content Restriction: Content restriction is defined as a particular type of free riding in which participating nodes are not sharing any of their contents (e.g. files) on the network [17].

Resource Restriction: Resource restriction is defined as a particular type of free riding in which participating nodes are not contributing any of their resources on the network [17].

Policy Attack: Some P2P networks implement some sorts of auditing policies to diminish the possibility of free riding. A policy attack is defined as an attack in which a node in the P2P network exploits any loophole that is found in those auditing policies [28].

Auditing Attack: Auditing attack in the P2P network is defined as an attack in which any auditory system, that is present in the network, is interrupted by some methods so that they can't detect the misbehavior of the irrational nodes [28].

Passive Dos/DDoS Attack: In the passive DoS/DDoS attack, the target is not any particular node(s). Its main motif is to disrupt the service of the respective P2P network. Such passive DoS/DDoS can take different forms which include: Join & Leave Attack, Simple DoS Attack and Traffic Amplification Attack.

Join & Leave Attack: In the P2P systems, nodes join and leave in dynamic fashion. Most of existing structured systems need some amount of routing information to handle such dynamism. There are two different types of DoS attacks possible based on such dynamic join and leave of nodes: (a) DoS against the network using rapid joins and leaves and (b) DoS against the network using network stabilization protocols [18]. If a significant number of nodes join and leave the network at an extremely rapid rate the overhead associated with such dynamic join and leave can become significant and thus degrading the performance of the system. The attacker can initiate such attack in two different ways (a) By being a participant in rapid leave and join itself (b) By exploiting a set of victim nodes by attacking malicious nodes.

Simple DoS Attack: The main motif of such attack is to disrupt the service the network offers. As for example, lookup (key), store (key) of a distributed hash table offers can be thwarted. This can be accomplished by increasing the false traffic in the system more than its limit. In this case no more legitimate users will be able to take that particular P2P service. Both recursive and iterative overlay network are vulnerable to such attack.

Traffic Amplification Attack: Traffic amplification attack is defined as any type of attack that magnifies the effect of a single attacking host. Traffic amplification attack works by having one packet generate multiple responses. The resulting effect is that a single attacking host appears as multiple hosts, with the goal of intensifying the effect of the attack to bring down entire networks. Distributed Denial-of-Service (DDoS) attacks are classic examples of amplification attacks in which

intermediary compromised hosts are used to multiply the malicious intent of a single intruder [22].

Content Availability Depletion Attack: Content availability depletion attack in the P2P network can be defined as an attack in which availability of the resources in the network will be depleted with some crafty methods so that legitimate users find it difficult to avail a particular resource. Copyright Holders are here the potential attackers who try to deplete the copyrighted materials in the P2P file-sharing network so that the copyrighted materials can't be easily availed. There are two popular techniques by which such attack can be generated: Poisoning and Pollutioning. A study provides empirical evidence that a considerable amount of the files found in the KaZaA/FastTrack network are unusable, due to either pollution or poisoning [9].

Poisoning: A popular technique to reduce the availability of a specific resource such movie, song or software in a P2P network is to inject a huge number of decoys into the network The decoys can be defined as "the files whose name and metadata information (e.g., artist name, genre, length) match those of the item, but whose actual content is unreadable, corrupted, or altogether different from what the user expects [21]". Such intentional injection of decoys is regarded as poisoning. Decoy can be inserted either by random decoy injection, replicated decoy injection or replicated transient decoy injection [21].

Polluting: Polluting can be defined as accidental insertion of poorly encoded or truncated chunks/packets into an otherwise valid file on the network [22]. It has the effect of reducing the amount of usable resource in the network.

IV. Future Works

In this paper, we've presented a complete taxonomy of all the attack methods that are found in the P2P network currently. This work can be extended in future by proposing another complete taxonomy of the mitigation methods of these attack methods.

V. Conclusion

There is no doubt that P2P network will enjoy much more popularity day by day. Such increasing popularity will draw attention of many more attackers. So the rate and amount of the attacks in P2P network is surely to amplify. To fight back such attack and their upcoming variants, a comprehensive understanding on those attack methods are crucial. This paper serves this purpose by providing a complete taxonomy of almost all known types of attack methods in P2P network. This understating can then be used to investigate new countermeasures and comprehensive solutions against any type of attacks in P2P network.

References

[1] Nash, Andre L., "Attacking P2P Networks", ECS 235—Hao Chen - Fall 2005, December, 2005.

[2] Oram, Andy, "Peer to Peer: Harnessing the Power of Disruptive Technologies", O'Reilly, 2001.

[3] Wagner, Arno and Plattner, Bernhard, "Peer to Peer Systems as attack platform for Distributed Denial of Service", ACM SACT Workshop 2002, Washington D.C., USA, 2002.

[4] Atip, Asvanund, Clay, Karen, Krishnan, Ramayya and Michael Smith, "An Empirical Analysis of Network Externalities in Peer-To-Peer Music Sharing Networks", In Proceedings of the 23rd International Conference on Information Systems (ICIS), Barcelona, Spain, December, 2002.

[5] Singh, R. Atul, Castro, Miguel, Druschel, Peter and Rowstron, Antony, "Defending against Eclipse attacks on overlay networks", In the Proceedings of the 11th ACM SIGOPS European Workshop, Leuven, Belgium, September 2004.

[6] Cerri, Davide, Ghioni, Alessandro, Paraboschi, Stefano and Tiraboschi, Simone, "ID Mapping Attacks in P2P Networks", In IEEE GLOBECOM 2005.

[7] Adar, Eytan and Huberman, Bernardo A., "Free riding on Gnutella", http://www.firstmonday.dk/issues/issue5_10/adar/

[8] Gross, Grant, "What Are the Worst Security Problems?", Outlook, IDG News Service, October, 2003.

[9] Liang, J., Kumar, R., Xi, Y., and Ross, K., "Pollution in P2P file sharing systems", In Proceedings of IEEE INFOCOM'05, Miami, FL, March, 2005.

[10] Kannan, Jayanthkumar and Lakshminarayanan, Karthik, "Implications of Peer-to-Peer Networks on Worm Attacks and Defenses", CS294-4 Project, Fall 2003, For Computer Science Dept. of Berkley University. http://www.cs.berkeley.edu/~kubitron/courses/cs294-4-F03/ projects /karthik_jayanth.pdf.

[11] Douceur, John R., "The Sybil Attack", In Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), Cambridge, Massachusetts, USA, March. 2002.

[12] Shanmugasundaram, Kulesh, "Peer-to-Peer Systems Security Issues" http://isis.poly.edu/kulesh/stuff/talks/p2psecurity.ppt.

[13] Zhou, Lidong, Zhang, Lintao, McSherry, Frank, Immorlica, Nicole, Costa, Manuel and Chien, Steve, "A First Look at Peer-to-Peer Worms: Threats and Defenses", In Proceedings of the 4th International Workshop on Peer-To-Peer Systems (IPTPS 2005), Ithaca, New York, February, 2005.

[14] Stein, Lincoln and Stuart, John N., "The World Wide Web Security FAQ", Version 3.1.2, February 4, 2002. http://www.w3.org/Security/ faq/wwwsf6.html#DOS-Q2

[15] Castro, M., Druschel, P., Ganesh, A., Rowstron, A. and Wallach, D.S., "Secure routing for structured peer-to-peer overlay networks", In Proceedings of USENIX Operating System Design and Implementation(OSDI), Boston, MA, Dec. 2002.

[16] Costa, Manuel, Crowcroft, Jon, Castro, Miguel, Rowstron, Antony, Zhou, Lidong, Zhang, Lintao and Barham, Paul, "Vigilante: End-to-End Containment of Internet Worms", In Proceedings of the 20th ACM Symposium on Operating Systems Principles (SOSP 2005), Brighton, United Kingdom, October, 2005.

[17] Engle, Marling, "Vulnerabilities of P2P Systems and a Critical look at Their Solutions", April, 2006. http://medianet.kent.edu/surveys/ IAD06S-P2PVulnerabilities-marling/index.html.

[18] Mishra, Mayank, "Cascade: an attack resistant peer-to-peer system", http://mnl.cs.stonybrook.edu/home/mayank/CascadeReport.pdf.

[19] Collins, Michael, Gates, Carrie and Kataria, Gaurav, "A Model for Opportunistic Network Exploits : The Case of P2P Worms", In Fifth Workshop on the Economics of Information Security, Cambridge, UK, 2006. http://weis2006.econinfosec.org/docs/30.pdf.

[20] Tulloch, Mitch, Microsoft Encyclopedia of Security, Microsoft Press, 2003.

[21] Christin, Nicolas, Weigend, Andreas S. and Chuang, John, "Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks", In Proceedings of the 6th ACM conference on Electronic commerce, Vancouver, BC, Canada, Pages: 68–77, 2005.

[22] Peer-to-Peer information from wikipedia. http://en.wikipedia.org/wiki/Peer-to-peer.

[23] Keyani, Pedram, Larson, Brian and Senthil, Muthukumar, "Peer Pressure: Distributed Recovery from Attacks in Peer-to-Peer Systems", In IFIP Peer-to-Peer Computing, 2002.

[24] Yolum, Pinar, Singh and Munindar P., "Flexible Caching in Peer-to-Peer Information Systems", In Proceedings of the 4th International Bi-Conference Workshop on Agent-Oriented Information Systems (AOIS), Bologna, July 2002.

[25] Wagner, Robert, "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks", Practical Assignment GSEC Version 1.2f, August, 2001. http://www.phlak.org/docs/arp/address.pdf.

[26] Roussopoulos, M., Baker, M., Rosenthal, D., Guili, T., Maniatis, P. and Mogul, J., "2 P2P or Not 2 P2P?", In The 3rd International Workshop on peer to peer systems, San diego, CA, USA, February, 2004.

[27] Rowstron, A. and Druschel, P. "Pastry: Scalable, distributed objection location and routing for large scale peer-to-peer systems", In IFIP/ACM Middleware, Heidelberg, Germany, November, 2001.

[28] Nielson, Seth James, Crosby, Scott A. and Wallach, Dan S., "A Taxonomy of Rational Attacks", In The 4th International Workshop on Peer-to-Peer Systems (IPTPS'05), Ithaca, New York, USA, February, 2005.

[29] Androutsellis-Theotokis, Stephanos and Spinellis, Diomidis, "A survey of peer-to-peer content distribution technologies", In ACM Computing Surveys, 36(4):335–371, December 2004.

[30] Stading, Tyron, Maniatis, Petros and Baker, Mary, "Peer-to-Peer Caching Schemes to Address Flash Crowds (2002)", In 1st International Peer To Peer Systems Workshop (IPTPS 2002).

[31] Yu, Wei, Boyer, Corey, Chellappan, Sriram and Xuan, Dong, "Peer-to-Peer System-based Active Worm Attacks: Modeling and Analysis", In Proc. of IEEE International Conference on Communications (ICC), pp. 295-300, May 2005.