International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:4, 2012

Taxonomy of Structured P2P Overlay Networks Security Attacks

Zied Trifa, Maher Khemakhem

***Abstract*—**The survey and classification of the different security attacks in structured peer-to-peer (P2P) overlay networks can be useful to computer system designers, programmers, administrators, and users. In this paper, we attempt to provide a taxonomy of structured P2P overlay networks security attacks. We have specially focused on the way these attacks can arise at each level of the network. Moreover, we observed that most of the existing systems such as Content Addressable Network (CAN), Chord, Pastry, Tapestry, Kademlia, and Viceroy suffer from threats and vulnerability which lead to disrupt and corrupt their functioning. We hope that our survey constitutes a good help for who's working on this area of research.

***Keywords*—**P2P, Structured P2P Overlay Networks, DHT, Security, classification

I. Introduction

P2P networks systems have generated substantial interest in the last few years because the emergent of global scale phenomena. As more and more users own powerful processors, large storage spaces and fast network connections, P2P networks represent an attractive way to mobilize these resources. They were designed to provide many services such as creating large scale data sharing, distributed computing, instant messages communication, collaborative applications, multi players games, and ad-hoc network. These popular services make P2P networks an attractive target for attackers.

Knowing how systems have failed can help us build systems that resist failure [1]. This paper collects and organizes a number of current security attacks that have caused failure in structured P2P overlay networks, so computer system designer, programmers, administrators, and users may do their work with a precise knowledge of what has gone before.

Based on the overlay topology and the organization of the network connection different types of P2P networks have been defined as hierarchical P2P network, and flat P2P network. In this paper, we will focus on hierarchical P2P network, more precisely on structured P2P overlay networks.

Security attacks of structured P2P overlay network are any condition or circumstance that can threaten the best functioning of the system.

To evaluate these attacks, an analyst must do a deeply research, understand the system fluently, and recognize that attacks may exist anywhere in the system.

Zied Trifa is with the Faculty of Economics and Management, Sfax, CP 3013 TUN (e-mail: trifa.zied@ gmail.com).

Maher Khemakhem, was with Faculty of Economics and Management, Sfax, CP 3072 TUN. He is now with the Department of Computer Science, higher institute of business administration, Sfax, CP 3072 TUN (e-mail: maher.khemakhem@fsegs. rnu.tn).

Thus, the security attacks of such systems are considered as a serious topic that should be considered carefully. The reminder of the paper is organized as follow. Section 2 presents an overview of P2P networks including definitions, benefits, their characteristics, and types. Section 3 focuses on structured P2P overlay network and summarizes the taxonomy of security attacks at each level of the network. Section 4 analyzes and makes a clarification of the different links between attacks. Finally, section 5 provides conclusions.

II. P2P Overlay Networks

Peer-to-Peer overlay networks are distributed systems consisting of interconnected nodes able to be self-organized into network topologies with purpose of sharing resources such as content, CPU cycles, storage and bandwidth, and accommodating transient populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority [2].

P2P networks are virtual overlay networks built on an underlay network. That means each entity in the underlay network has a corresponding identity in the overlay networks. Different types have been defined as hierarchical P2P network and flat P2P network. The main difference between them is based on how many levels the network topology is utilizing. In this paper, we will just focus on the first type. Hierarchical P2P network utilizes multiple levels of hierarchy to distribute the overlay node and it can also be classified into three categories: unstructured, structured and hybrid networks as shown in Fig. 1.

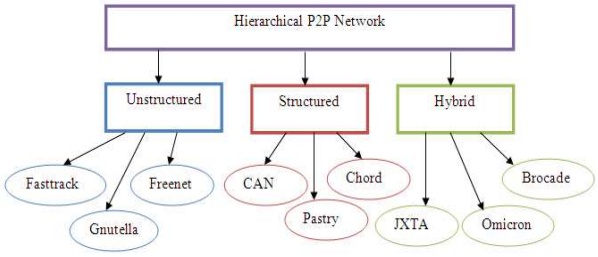

Fig. 1 Hierarchical P2P networks

A. Unstructured P2P networks

In this category, the P2P overlay network organizes peers in a random graph which means that the links between nodes are established arbitrary so there is no correlation between a peer and the content managed by it.

Unstructured P2P network uses flooding, random walks or expanding Time-to-Live (TTL) search on the graph to query

content stored by overlay peers [3]. If a peer wants to find desired pieces of data from the network, the query has to be flooded through the network to find as many peers as possible that share the data. In such systems the network can be easily constructed. If a new peer wants to join the network, it could just copy existing links of another node and then form its own links over time. Moreover, these systems suffer from a lot of weaknesses such as:

- Queries for content that are not widely replicated must be sent to a large fraction of peers;
- There is no coupling between topology and data items location so there is no guarantee that flooding will find a peer that has the desired data;
- Flooding also causes a high amount of signaling traffic in the network.

B. Structured P2P overlay networks

In contrast to the unstructured P2P networks, structured P2P overlay networks provide a topology that is tightly controlled, which mean that content in such systems is not placed at random peers but rather at specified location. The overlay network assigns a key to data items and organizes it peers into a graph that map each data key to a peer. This enables efficient discovery of data items using the key of a data element [4].

These systems are usually based on distributed hash table (DHT), which are decentralized and distributed systems providing a lookup service similar to a hash table. By using the DHT algorithm, the peers can map the keys to node easily and can guarantee that any data object can be located in small overlay hops. Structured P2P overlay networks provide a cooperative, stable, and robust mechanism for storing and retrieving content. But, these good proprieties are maintained only when their algorithms are executed correctly. Such system provides a powerful platform for the construction of a variety of services such as network storage, content distribution, web caching, searching and indexing. But, the major problem with such systems, they do not support complex queries and it is necessary to store a copy or a pointer to each data object at the peer responsible for the data object's key. Also, most of them deploy a security mechanism which is minimalist or pervasive; this makes the network an attractive target of attackers.

C. Hybrid P2P networks

Hybrid P2P systems combine unstructured and structured overlay topology in its hierarchy and they can utilize structured overlay topology at its upper level while utilizing unstructured overlay topology at its lower level, or vice versa. Such system defines several super peers. Each super peer acts as a server to a small portion of the network. Moreover, each super peer stores a list of index files information that is available to the peers that it manages. They use the similar query mechanism as centralized P2P network [5].These systems reduce the signaling traffic, save the bandwidth and they provide a robust and scalable system since there is no single point of failure. However, they are very difficult to adapt to physical network due to the hierarchical structure and also available content might not be found.

III. Security Attacks In Structured P2p Overlay Networks

Structured P2P overlay network was based on providing efficient search of data items, robust wide area routing architecture, redundant storage, scalability, and fault tolerance. These characteristics can be used to build more complex system. Several structured P2P overlay networks were emerged such as Content Addressable Network (CAN) [6], Chord [7], Pastry [8], Tapestry [9], Kademlia [10], and Viceroy [11]. Moreover, these systems use the Distributed Hash Table (DHT) as a substrate, in which data object location information is placed at the peers with identifiers corresponding to the data object unique key [3]. Early work in structured P2P overlay networks security attacks was based on providing an overview of individual attack; researchers searched for security attacks and attempted to remove them. Unfortunately, that task was in most cases unending, more attacks always seemed to appear. In this section, we describe and provide reasonably detailed actual attacks found in two main groups: general network and specific structured P2P network as shown in Fig. 2. Our goals are more ambitious than previous works [12]–[13]–[14]–[15], we seek to provide an understandable organization of security attacks that have occurred and help who have attention to build a safer structured P2P overlay networks. Security attacks in this report are classified into two categories: General network attacks and Specific structured P2P overlay network attacks. In the first categories, we try to provide the most damaged attacks threatening the network in general since structured P2P network are virtual overlay networks built on an underlay network. Therefore, in the second categories, we present the specified structured P2P networks attacks through three levels: network level, application level, and user level.

A. General Network Attacks

1) DoS and DDoS

With time and as the internet gets more and more used as a communication channel, Denial of Service (DoS) and Distributed Denial of Service (DDos) become more popular than ever. A DoS attack and DDoS attack are characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service, in other words, this is an attack which causes a service to stop functioning or an attack that causes the loss of service. In DoS attack, attacker utilizes reasonable service requests to drain the resources of a target host. However, in DDoS attack attacker exploits considerable amount of distributed hosts to launch the attack to the target.

P2P networks are composed by large number and anonymous concurrently running hosts. Thus, one or more malicious nodes in the network can easily perform DoS or DDoS attacks [14].

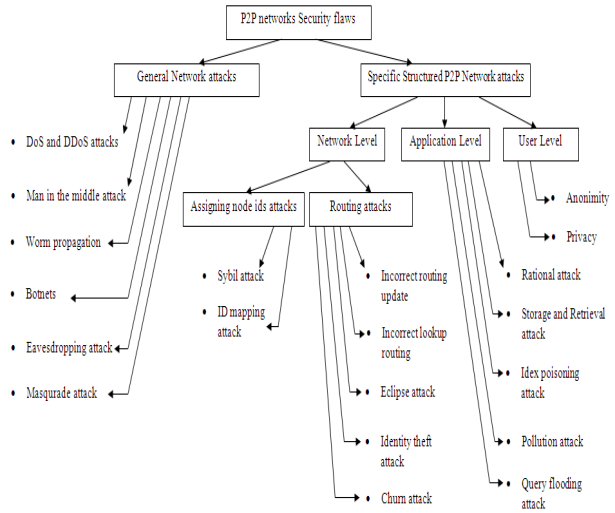

Fig. 2 P2P networks security attacks

The first problem with defending against such attacks is detecting them. There are several approaches in counteracting these attacks [15]–[16]. But, the most widely used technique to hinder DoS attack is pricing. The host will submit puzzles to his clients before continuing the requested computation, thus ensuring that the client go through an equally expensive computation.

2) Worm propagation

Worms pose one of the biggest threats to the internet. Currently, worms such as Code Red or Nimda are capable of infecting hundreds of thousands of hosts within hours and no doubt that better engineered worms would be able to infect to reach the same result in a matter of seconds.

As P2P networks facilitate transfer and sharing file, malicious code can exploit this channel to propagate to other peers. Worm can be a large piece of complex software which is capable of much more complicated attacks such as collection of all sorts of information (credit cards, passwords, etc), corrupt or modify files, denial of service, and massive distributed denial of service attacks.

Worms are spread by exploiting vulnerabilities in operating systems. To decrease the efficiency of these attacks, we must always supply regular security updates and if these updates are installed to a machine then the majority of warms are unable to spread to it. Furthermore, one suggestion that was given was to write P2P clients in strongly typed language such as java and c sharp (C#), which could avoid many security flaws [17].

3) Man in the middle

The man in the middle attack is a form of active eavesdropping [18] in which an attacker inserts himself between two other nodes in the network, makes independent connections, and relays messages between them. The attacker makes the two nodes believes that they are talking directly to each other when in fact all communication passes through him. He can achieve this by inserting, dropping, or retransmitting previous messages in the data stream. In this case, the attacker can modify messages, insert fake information, and in the worst case assume the identity of either node or both to launch a denial of service.

All P2P systems which have no control over node placement are extremely vulnerable to this attack. Without a central trusted authority, it is not possible to detect a man in the middle attack. The main defense against this attack is the use of digital signatures based on public key cryptography.

4) Botnets

One of the most significant threats to the internet today is the threat of botnets, which are networks of compromised machines under the control of an attacker [19]. A botnet produces very significant threats to structured P2P networks. Compared to other internet malware, botnets are different from traditional discrete infections in that they act as a coordinated attacking group. Machines participating in botnet frequently have numerous heterogeneous infections such as viruses, worms, and trojans. The cloud of victims can be used to create redundant, highly resilient networks form attacks.

Today, a number of ad hoc methods exist to detect and stop botnets, and these methods continue to mature such as splitting high-degree nodes to avoid targeted responses, and designing sets of turing tests like puzzles that users must solve to access overtaxed resources. As techniques for botnet detection and mitigation advance, the robustness and resiliency of botnets will also advance [20].

5) Eavesdropping attack

Eavesdropping is another type of attack on networks. Attackers can gain access to data within a network and eavesdrop the traffic. One of the biggest security problems faced by users is the ability of attackers (eavesdroppers) to monitor networks, that is leads to several problems such as sniff passwords and keys, get MAC address, get IP address, and capture data to eventually cause the network to crash or even become corrupted.

The first step in preventing eavesdropping attack is to use a strong physical security, and the next step is to use strong encryption services that are based on cryptography.

6) Masquerade attack

Masquerade attack is a type of attack in which one system entity illegitimately poses as another entity to gain access to confidential systems. This means to hide one's true identity on the network to create a spoofed identity. Masquerade attacks are extremely serious; they can occur in several different ways, they may get access to a legitimate user's account either by stealing a victim's password, or through IP address.

A common method to limit this type of attack is to filter incoming packets that appear to come from an internal IP address and filter outgoing packets that appear to originate from an invalid local IP address.

B. Specific Structured P2P network attacks

1) Network level attacks

At the network level an adversary may try to break the routing system, or block access to information by impeding the routing process, or obtain some particular identifiers. We try to split attacks in this level into two sub-categories: assigning node Ids attacks and routing attacks.

a) Assigning node IDs attack

Before joining the network, every peer must usually generate a user identifier. These user identifiers uniquely identify node in a P2P networks. However, the assignment of IDs is usually not controlled enough. This allows malicious users to perform different types of attacks such as Sybil attack and Id mapping attack.

-Sybil attack

Due to the open nature of the Structured P2P network a single malicious user can create multiple fake identities and pretend to be multiple, distinct physical node in the system. Such attack is known as Sybil attack [21]. In this case, malicious node can compromise the network by generating and controlling large numbers of fake identities. It can attack several protocols such as distributed storage to defeat replication and fragmentation mechanisms, and routing protocol to defeat routing algorithms.

To defend the Sybil attack the system must ensure that distinct identities refer to distinct entities and limit the ability of an entity to determine identity. Unfortunately, these two conditions are currently solved only by relying on centralized authority. But, this is impossible to ensure since P2P networks are scalable and decentralized. Several other approaches have been developed to prevent this attack and overcome the lack of decentralization. We categorize these approaches based on the cost involved in the creation of identities. This cost may be computational, when a node wishes to join a network it is challenged by the other nodes of the network with a cryptographic puzzle [22], also material, identities are linked to smartcards [23], charging a fee [13], use static IP address [24], finally the cost may be social, when a node joins a network it obtains identity through social relationships [25]–[26].

-ID mapping Attack

In structured P2P overlay networks; there is a uniform random distribution of node identities (Ids). This random distribution allows an attacker to obtain some particular identifier and gain a strategic position on the overlay network to eventually gain control over certain resources. This attack is closely related to the Sybil attack. But, the main difference is that the Sybil attack is used to generate a large number of random identifiers, while Identity mapping attack is used to obtain some particular ones.

Previous approaches to node Id assignment have assumed that node Ids are chosen randomly by the new node [27]. However, this is not enough to prevent a user from choosing its identifiers. The best solution to avoid Id mapping attack is to use centralized authority which distributes the identifiers but this is impractical since P2P networks are scalable and decentralized. The Id mapping attack can be protected only if the identifier depends on some piece of information outside of the control of a node [28]. For example force a node to derivate its identifier from IP address and port number and hashing the outcome.

b) Routing attack

According to the function of DHT algorithm each node in the overlay maintains a routing table which guarantee the look up and mapping of the keys. Routing attacks are performed by exploiting the weaknesses in the routing mechanisms. In this section, we describe the most important routing level attacks faced in structured P2P networks.

-Incorrect routing update

The major issue of the DHT based networks such as Chord, Pastery, and Tapestry was the creation of the routing table. Each node creates their routing table by consulting other nodes. A malicious user could corrupt the routing tables of others nodes by sending them invalid updates to cause misdirect queries to inappropriate nodes, or to non-existent nodes.

Different solutions are developed for this kind of problem such as impose certain requirements. For example CAN [6], it takes into account the round-trip-time in order to favor lower latency paths in routing updates, however, in Pastry [8] each entry in the tables must be preceded by a correct prefix, which cannot be reproduced by malicious nodes.

-Incorrect lookup routing

Lookups for keys in Structured P2P overlay networks are performed by routing queries through a series of nodes. Each of these nodes uses a local routing table to forward the query toward the node responsible for the key. This mechanism is used to store, retrieve, replicate, and authenticate the data. Since the malicious node could corrupt this mechanism through routing updates system; it could forward messages to an incorrect or non-existent node.

The routing portion of a lookup protocol involves maintaining routing tables and then dispatching requests to the nodes in the same protocol. It is critical that routing is correct in a distributed hash table [4]. This can be fixed with two steps. First, the requester should ensure that the destination itself agrees that it is a correct termination point for the query. Second, the system should assign keys to nodes in a verifiable way.

-Eclipse attack

Due to the fact that each node in the network maintains overlay links to a set of neighbor nodes and each node uses these links to perform a lookup from its neighbors, an attacker

can control a significant part of overlay network by controlling a large part of the neighbors of correct nodes. This attack is known as Eclipse attack. It is closely related to the Sybil attack described above. If an attacker is able to generate a large number of fake identities and place those identities in the overlay network, he could mediate most overlay traffic and eclipse correct nodes from each other (i.e. separate the network into two or more partitions).

We can perceive that eclipse attack basically represent a large scale man in the middle attack so the key to defending an eclipse attack is the same as defending a man in the middle attack, digital signatures and public key cryptography. Some other countermeasures for this problem have been developed such as an optimized routing table and verified routing table [27], and induced churn method [30].

-Identity theft attack

In P2P overlay networks, each node of the structured P2P overlay network knows only a small fraction of other nodes. A node wanting to deliver a message to the root node of some key just had to trust that the other nodes will route the message to the correct root node [31]. However, malicious user can exploit this trust to launch identity theft attack. When a malicious node in the path of a message claims that it is the desired destination node, so, it can hijack route and lookup requests to forge and destroy data to corrupt applications.

To defend this attack Puttaswamy et al have proposed in [31] a method in which they use proofs, blacklists and malice-aware routing and it was shown to effectively detect, mark and redirect traffic away from malicious user.

-Churn attack

Structured P2P overlay networks are widely used to deploy services. This characteristic makes such system attractive to thousands or millions of users and at the same time vulnerable to the phenomena of churn. The independent arrival and departure of thousands or millions of peers creates a collective effect called churn. An attacker could exploit this attack by generation peer joining and leaving the network fast enough to corrupt the best function of the network.

To cope with churn, Stutzbach and Rejaie pointed out that P2P networks should be designed to be able to efficiently handle the large number of peers joining the system for just a few minutes [32].

2) Application level attacks

At the application level an adversary can attempt to corrupt or delete data stored in the system. We try to present and describe the most common attacks in this level such as rational attack, storage and retrieval attack, index poisoning attack, pollution attack, and query flooding attack.

a) Rational attack

A significant challenge in structured P2P overlay networks is the problem of cooperation. These systems can only scale if nodes are willing to cooperate. Unfortunately, the human nature is always contradictory with this; a self-interested node will attempt to maximize their consumption of system resources while minimizing the use of their ones. This is known as rational attack. A rational node aims to achieve maximal utility; it will attempt to generate either content restriction or resource restriction or both of them and this goal is achieved over their current knowledge of the P2P system.

Rational attack remains poorly study, but few of P2P system attempt to solve it. For example, Napster tried to solve this problem by giving people a title for the level at which they shared. Bit Torrent implements a system for bartering for chunks of data, the more a node shares with others, the more it will get back. So, more a node is willing to upload to others, the faster download it gets. Samsara ensures that a node may only use as much space on another node as it is giving up to the network [17].

b) Storage and retrieval attack

Storage and retrieval attack is closely related to rational attack since malicious users refuse to provide services to the other nodes or deny the existence of data which was responsible for. This attack can be dangerous in a system that does not assign nodes verifiable identifiers. In such a system a node can choose to become responsible for data that it wishes to hide.

In order to prevent this attack, the system must ensure replication. Replication must be handled in a way so that no single node is responsible for replication or facilitating access to the replicas [4].

c) Index poisoning attack

P2P systems store the index of files, which users search to find locations of desired data. Index poisoning means the insertion of massive number of bogus information into the index. As a result, when a user attempts to download a file with a randomly generated identifier, the file sharing system fails to locate associated file.

The countermeasure of the index poisoning attack is difficult to find. So, to estimate poisoning the straightforward approach is to query the file sharing system, sample copy advertisements, attempt to download versions from those advertisements, and then attempt to determine if the download versions are clean or poisoned [33].

d) Pollution attack

The best way to corrupt P2P file sharing is to deposit into the file sharing system some junk pieces of data known as polluted files. In this way, attacker corrupts the content of shared file, rendering it unusable, and forwards the corrupted file to other peers. As a result, polluted files spread through the network and users become unable to distinguish polluted files from unpolluted file.

To fight against polluted files, Dhungel et al [34] propose four possible defenses: blacklisting, traffic encryption, hash

verification, and chunk signing. Other mechanisms presented by Liang et al [35]: Detection without downloading, after receiving search results the mechanism attempt to determine whether the files in the results are polluted. Detection with downloading, for this class, the mechanism detects whether a file is polluted by first downloading portion of the file.

e) Query flooding attack

A structured P2P network consists of a large number of nodes each connected not to all other nodes. If a node wants to find a resource on the network, it could simply broadcast its search query to its immediate neighbors. If neighbors do not have the resource, it then asks its neighbors to forward the query to their neighbors. Malicious users can exploit this mechanism to generate a query flooding attack. This attack is handled when a malicious node generate as much queries as possible to flood the network. As a result, the downloading session cannot be established and the whole P2P network does not work.

Gnutella was the first system to tackle this problem because each node in Gnutella knows a maximum number of queries of a maximum node. Therefore, a node can accept at most the maximum queries from a request peer. After getting the maximum number of queries from a request node, it just drops the rest requests from that incoming link [36].

3) User level attacks

Users themselves can be the subject of attacks if an adversary goes after anonymity and privacy protection.

a) Anonymity

In the context of Structured P2P overlay networks, each peer has a routing table containing a set of peers responsible for certain keys, and each step in the lookup process brings the query closer to the destination peer. This ability to reach the peer responsible for a key by combining information from routing tables of various peers is in contrast to the goal of anonymity, which demands that it should not be possible to identify a peer responsible for any query item. An attacker can monitor all information passing through him to gain a good knowledge of other peers surrounding him. In this case, the attacker can know most of files that legitimate node is detaining and manage them to break anonymity. The problem of anonymity reduces to protecting the identities of the peer issuing the query and the peer responsible for that particular key.

b) Privacy

Nowadays, the P2P networks have become increasingly popular in a short time, they are designed to share resources and provide services. These characteristics make it attractive to several users and in the same time vulnerable. Thus, the privacy of users is a serious problem that should be considered. Users can accidentally or unknowingly allow their private or personal files to be shared. In this situation they risk disclosing their private information to other users on the network. So, privacy within P2P networks requires attention from the user. The user has to know how to use software and what kind of information is being shared. It is quite possible to share the entire hard drive, including sensitive information such as mailbox and private documents [36]. Malicious users with intermediate hacking skills can exploit this misuse of such environment and launch several attacks.

IV. Attack Connection

These attacks describes above as we can see are not just theoretical, but some of them can be used to significantly amplify the effects of other attacks to perform in real life Structured P2P network. Thus, in this section we try to give an overview of the different links between attacks.

A. Identity assignment attacks to routing attacks

Malicious users can create multiple fake identities (Sybil attack) and they can obtain some particular identifiers (ID mapping attack), hence they can launch several other attacks such as eclipse attack, in which an attacker can control a large part of the neighbors of a good node, identity theft attack, in which an attacker exploit the fact that that each node see a small fraction of other nodes to claim to be the root node, intercept application request, and turn data of its own choosing, and churn attack, in which an attacker generate peers joining and leaving the network fast enough to destabilize the overlay.

A malicious user mounts a Sybil attack by obtaining a large numbers of identities. These identities horn in the routing paths and thus permitting it to confuse the process of routing update and lookup routing. Moreover, when an entity can run a large numbers of nodes and obtain a large numbers of nodes identifiers, the whole network can be dominated by this entity. This dominance can be used to undermine replication mechanisms, which results in subvert content storage and retrieval.

B. Identity assignment attacks to application level attacks

If an adversary is able to obtain some particular identifiers, it can allocate itself a collection of identifiers closer to some object's key than any existing node in the system [25]. This would allow the malicious user to exploit this to censor or corrupt the object by poisoning the index or polluting the whole object.

C. Specific structured P2P attack to Denial of Service (DoS) and Distributed Denial of Service (DDoS)

At network level current assignment schemes and routing mechanisms allow an adversary to carefully select user IDs (ID mapping attack), simultaneously obtain many pseudo identities (Sybil attack), control sufficient fraction of the neighbors of a good node (Eclipse attack), and generate peers joining and leaving fast enough to destabilize the overlay (Churn attack). These attacks lead to distort or disconnect a part of the network from the rest. At application level, these attacks

generate a lot of flaws such as index poisoning, pollution data, storage and retrieval bugs, and query flooding attack to attempt to control and distort the anonymity and privacy of users. In the worst case, an adversary might eventually be able to gain full control over the whole network and launch a denial of service attack or a distributed denial of service.

V. Conclusion

The idea of this survey was conceived when we were considering how to secure structured P2P overlay networks from security attacks without a central coordination. We are convinced that knowing how systems have failed can help us to build systems that resist to failure.

This paper provides an overview of different categories of hierarchical P2P systems and took a major security attacks threatening the function of structured P2P overlay networks. We classified these attacks into two main groups: general network attacks and specific structured P2P network attacks.

Finally, we close this survey with a discussion of the different links between attacks and we confirm that ensuring that a structured P2P overlay network will be sufficient and suitable involves the balancing of many factors such as trust, privacy and security.

In light of this study, we can affirm that existing structured P2P overlay networks are still a way from a safe utilization. Thus, the development of appropriate security measures seems to be a mandatory.

References

[1] Petroski: To Engineer is Human: The role of failure in successful design. Vintage Books, New York 1992.
[2] S. Androutsellis-Theotokis and D. Spinellis: A survey of peer-to-peer content distribution technologies. ACM Computing Surveys 36(4): 335–371 2004.
[3] E.K. lua, J. Crowcroft, and M. PIAS: A survey and comparaison of Peer-to-Peer Overlay Networks Schemes. IEEE Communication Survey and Tutorial, 2005
[4] Emil Sit and Robert Morris: Security Considerations for Peer-to-Peer Distributed Hash Tables. Workshop on Peer-to-Peer Systems,March 2002
[5] MS. Artigas, PG. López, and A.F. Skarmeta: A comparative study of hierarchical DHT systems. Proceedings of the 32nd IEEE Conference on Local Computer Networks 325–333 2007
[6] Ratnasamy, S., Francis, P., Handley, M., Karp, R., and Shenker: A scalable content-addressable network. In Proceedings of ACM SIGCOMM San Diego, California, Aug. 2001.
[7] I. Stoica, R. Morris et al., "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications," IEEE/ACM Trans. Net., vol. 11, no. 1, 2003, pp. 17–32.
[8] A. Rowstron and P. Druschel, "Pastry: Scalable, Distributed Object Location and Routing for Large-scale Peer-to-peer Systems," Proc. Middleware, 2001.
[9] B. Y. Zhao et al., "Tapestry: A Resilient Global-Scale Overlay for Service Deployment," IEEE JSAC, vol. 22, no. 1, Jan. 2004, pp. 41-53.
[10] P. Maymounkov and D. Mazieres, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," Proc. IPTPS, Cambridge, MA, USA, Feb. 2002, pp. 53–65.
[11] D. Malkhi, M. Naor, and D. Ratajczak, "Viceroy: A Scalable and Dynamic Emulation of the Butterfly," Proc. ACM PODC 2002, Monterey, CA, USA, July 2002, pp. 183–92.
[12] X. Yue, X. Qiu, Y. Ji, and C. Zhang: P2P attack taxonomy and relationship analysis. In ICACT'09: Proceedings of the 11th international conference on Advanced Communication Technology, pages 1207–1210. IEEE Press, 2009.
[13] D. S.Wallach: A survey of peer-to-peer security issues. In International Symposium on Software Security, pages 42–57, 2002.
[14] L. Wang: Attacks against peer-to-peer networks and countermeasures. Paper on the course T II0.5290 Seminar on Network Security at TKK, 2006.
[15] Conner W, Nahrstedt K, Gupta I: Preventing DoS attacks in peer-to-peer media streaming systems. In: Proc of the 13th annual conference on multimedia computing and networking (MMCN'06), San Jose
[16] Yang J, Li Y, Huang B, Ming J: Preventing DDoS attacks based on credit model for P2P streaming system. In: ATC '08: Proc of the 5th international conference on autonomic and trusted computing. Springer, Berlin, pp 13–20
[17] M. Engle and J. I. Khan: Vulnerabilities of P2P Systems and a Critical Look at their Solutions Technical Report 2006: http://medianet.kent.edu/technicalreport.htm
[18] http://en.wikipedia.org/wiki/Man-in-the-middle_attack
[19] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proceedings of SRUTI: Steps to Reducing Unwanted Traffic on the Internet, July 2005.
[20] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon: Peer-to-peer botnets: Overview and case study. In USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07), 2007.
[21] J.Douceur: The Sybil Attack. Proceedings of the First International Workshop on Peer-to-peer Systems. Springer, March 2002.
[22] H. Rowaihy, W. Enck, P. McDaniel, and T. La Porta: Limiting Sybil attacks in structured P2P networks. pages 2596 –2600,May 2007.
[23] P. Druschel and A. I. T. Rowstron. PAST: A large-scale, persistent peer-to-peer storage utility. In Proceedings of the 8th IEEE Workshop on Hot Topics in Operating Systems. IEEE Computer Society, 2001.
[24] J. Dinger and H. Hartenstein. Defending the Sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration. Apr. 2006.
[25] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. Sybilguard: defending against sybil attacks via social networks. In Proceedings of the ACM SIGCOMM Conference (SIGCOMM). ACM Press, 2006.
[26] H. Yu, P. B. Gibbons,M. Kaminsky, and F. Xiao. Sybil-Limit: A near-optimal social network defense against Sybil attacks. Networking, IEEE/ACM Transactions on, PP(99):1 –14, 2009.
[27] M. Castro, P. Druschel, A. J. Ganesh, A. I. T. Rowstron, and D. S. Wallach. Secure routing for structured peer-to-peer overlay networks. In Proceedings of the 5th ACM Symposium on Operating System Design and Implementation (OSDI), Operating Systems Review, pages 299–314. ACM Press, 2002.
[28] D. Cerri, A. Ghioni, S. Paraboschi, and S. Tiraboschi: ID mapping attacks in P2P networks. In Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE, volume 3, Dec. 2005.
[29] T. Condie, V. Kacholia, S. Sankararaman, J. M. Hellerstein, and P. Maniatis: Induced churn as shelter from routing-table poisoning. In In Proc. 13th Annual Network and Distributed System Security Symposium (NDSS), 2006.
[30] K. Puttaswamy, H. Zheng, and B. Zhao: Securing structured overlays against identity attacks. Parallel and Distributed Systems, IEEE Transactions on, 20(10):1487–1498, Oct. 2009.
[31] D. Stutzbach and R. Rejaie: Understanding churn in peer-to-peer networks. In IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, pages 189–202. ACM, 2006.
[32] Jian Liang, Naoum Naoumov, and Keith W. Ross: The Index Poisoning Attack in P2P File Sharing Systems. In IEEE Conference on Computer Communication, Barcelona, Spain, April 2006.
[33] Dhungel P, Hei X, Ross KW, Saxena N: The pollution attack in P2P live video streaming: measurement results and defenses. In: Proc of the 2007 workshop on peer-to-peer streaming and IP-TV (P2P-TV'07). ACM, New York, pp 323–328
[34] J. Liang, R. Kumar, Y. Xi and K. Ross, Pollution in P2P File Sharing Systems, In Proc. Of INFOCOM'05, May 2005.
[35] Neil Daswani and Hector Garcia-molina: Query-Flood DoS Attacks in Gnutella. InACM CCS, 2002
[36] N.S. Good, A. Krekelberg: Usability and privacy: a study of KaZaA P2P file-sharing. CHI 2003, April 5-10, 2003, Ft. Lauderdale, Florida, USA in ACM, Volume No. 5, Issue No 1