Volume 2, No. 4, April 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICLE

Available Online at www.jgrcs.info

SECURITY THREATS IN PEER TO PEER NETWORKS

Chander Diwakar[1], Sandeep Kumar*[2], Amit Chaudhary[3]

[1]C.S.E. department, U.I.E.T, Kurukshetra University,
Kurukshetra, India
chander_cd@rediffmail.com
[2]C.S.E. department, U.I.E.T, Kurukshetra University,
Kurukshetra, India
sandeep167@gmail.com
[3]C.S.E. department, U.I.E.T, Kurukshetra University,
Kurukshetra, India
amitch115@gmail.com

Abstract: Peer-to-peer networks break the dominant networking concept of client-server relationships in information exchange when we use heterogeneous multipurpose machines for interaction and sharing functionality. Peer-to-peer (P2P) networks are the popular networks for certain applications and deployments for many reasons, such as fault tolerance, economics, and legal issues. In this paper we try to collect information about various attacks on P2P networks and try to categories these attacks. In this paper we describe some of the known security issues found in common P2P networks.

Keywords: P2P Network, security issues and attacks.

INTRODUCTION

Computer network is an accumulation of computers and devices interlinked by communications channels that provide communications among users and permit users to employ resources. Fundamentally network configuration is of two types i.e. Client/Server networks and Peer-to-Peer networks. In a client server configuration, servers are dedicated machines that execute particular task in the network. A server may be file server, database server,mail server, print server and security server where every component has a prespecified function in the network. Still, there is a scalability problem in a client-server approach as the performance of the server will decreases as the number of communicating clients requesting services from the server increase. To beat out the above problem of traditional client-server network, there is an alternative network model called Peer-to-Peer (P2P) network where all nodes are equal. P2P networks act as a decentralized model where each device classified as a peer and simultaneously it may be client or server peer[1]. Thus, a peer may requests services to other peers, and provide sevices to other incoming requests from other peers at the same time on the network. Todays time, Peer-to-Peer technologies have become very common as P2P employ their personal hardware resources like storage capacity, processing power and network bandwidth in a cost-effective manner. The service rendered by the peer network is reachable by other peers directly without using intermediate entities. A pure P2P networks consists of only peers whereas other P2P networks depends on centralized servers for finding other peers or depends upon concepts such as special peers termed as super nodes. Some Peer To Peer network are overlay networks[2] as the peer themselves inform address of other partcipating peers. This is because searches and sometimes transfers adopt a route routed among the peers, and usually do not require an intermediate server for its general function. However, these systems depends on the mechanism that permit new peers into the P2P network for the first time. This mechanism can be as simple as sending the IP address of a site-peer network

PEER TO PEER ARCHITECTURE

There are various ways to classify P2P networks where first approach assumes that a P2P network is used for applications such as file sharing, telephony, media streaming etc. The second approach gives the degree of centralization and differentiate between pure P2P without central server and networks with central server stores information on peers. Therefore, the following terminologies are used in P2P network: centralized, or decentralized P2P networks, structured, unstructured, or hybrid P2P networks[3].

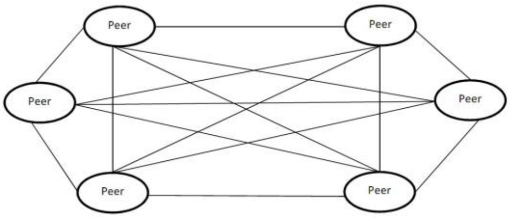

Figure: Architecture of Peer to Peer network

Centralized P2P Architecture: It depends on a centralized entity to place data items within the network. The first apperance of the P2P paradigm in general public cognition was Napster[4]. This popular file-sharing system elegantly find out the lookup problem by using P2P architecture where a centralized device gives a directory service to all employed peers ,therefore forming a star network. All peers combining the system have to register their data with the centralized server therefore allowing a easiest or convinient way to other peers in the network for locating any data in the network by occurence of a physically centralized directory. Instead of the actual data only pointers to decentralized peers are kept at the centralized server therefore lessens the load at the central entity. After finding the applicable data with the help of directory, each peer could communicate directly with other peers that keep data in a deconcentrate manner[3]. But in a pure P2P system, it should be possible to remove any device from the network without loss of functionality.Despite, a peer should play roles of both server and client, such that the functioing of the system is distributed equally over all the employed peers in the network. Therefore according to this definition, Napster can not be represented as a P2P system. Shutting down of Napster centralized server by the judicial authorities allowed easy closure of the entire system.

Unstructured P2P Architecture: In contrary to centralized approaches, non-centralized or decentralized P2P architectures do not depend on any centralized device to find out data items within the network. More particularly, unstructured P2P approaches is a specialization of the decentralized architectures where peers recursively transmit received request to their neighboring peers (also called neighbors) in an attempt to locate all important points in the network. To avoid missing peers in the network, each peer transmit messages to all other known peers, whether those neighboring peers record the relevant data or not. This message forwarding approach uses breadth-first search strategy which is called as message flooding approach. For avoiding infinite loops and controlling the number of messages produced by single request, each message alloted time-to-live (TTL) value. Every peer forwarding this TTL message decrement there value by one, and those messages get forwarded having positive TTL values. The advantage of unstructured P2P networks is that it doesnot require to maintain a network structure proactively. Peers sustain pointers to an upper- bounded number of direct neighbors and they can be placed anywhere in the netwok as there is no enforcement of a particular storage location for data items[5].

Structured P2P Architecture: In a centralized architecture, complexity of the linear storage central directory entity is restricted and its suffers from scalability which prevent an unlimited number of employed peers. In an unstructured architecture, the communication overhead caused by flooding message is an important deficit. Thus, an efficient and scalable method requires sub-linear increase in the complexity of storage and retrieval, as more peers added in the network.

Structured P2P architectures utilize particular overlay structures to map peers and data items having similar address space, enabling a unique mapping from data items to peers given the current state of the network[6]. To guarantee balanced storage and retrieval loads among the peers, the responsibilities for data items have to be distributed as uniformly as possible. To understand the function of routing, a distributed data structure rely on hash table is used to permit the insertion and retrieval of key/value pairs.Thus, to insert or remove a key / value pair, peer answerable for a key in the network as defined by the structured P2P network is used. The peer stores and maintains all relevant key / value pairs for a key to the whole library. Unlike the unstructured P2P architectures, the placement of data is not arbitrary, the distribution is accurately determined by the recovery of the underlying architecture, which provides a guarantee to find data items indexed by the network.

The expression distributed hash table stands for such a functionality in a P2P network and DHT is commonly used as a similar meaning for structured P2P architectures in general. But, there is also the strict distinction between structured P2P routing primitives and the DHT interfaces of inserting and retrieving data as upper layer for functionality on the other side.

Super-Peer Architectures: Super-peer architectures employ the fact that the performance characteristics of the peers i.e. processing power, bandwidth, availability, etc is not evenly spread to all the peers in the network. Thus, the advantage of a perfect decentralization are declining. In super-peer architecture, a small group of peers takes the particular responsibilities in the network, e.g., routing tasks or aggregation task. Thus, the super-peers can be viewed as the distributed extensions of the centralized entity in the Napster architecture. Conceptually, only the super-peers build-up the P2P network; all other peers connect to this backbone by communicating to one super-peer, which acts in the spirit of database mediators aggregating the content of downstream peers.

Routing in super-peer architectures is conducted in a two-phase mode. A request is routed within the super-peer backbone at first, and is then distributed to the peers connected via the super-peers. While dedicating specific peers potentially limits the self-organizing capabilities of a P2P network, super-peer architectures have been proven a way to alleviate the performance issues of pure unstructured topologies[7].

ATTACKS ON P2P NETWORK

As with software implementations today most P2P software is insecure. It is well known that the installation of this software create new methods for malicious users to cause damage. Although some of these weaknesses are relatively unknown by users, developers, others are known and could easily have been avoided if the developers consider the problem during development.

Attacks on unstructured P2P systems

i) Attacks by self-replication

Most P2P systems today assigned a user ID, regardless of their IP address. This allows malicious users to run without problem because they can easily get a new identity when they need it. A malicious user can respond positively to all requests, which shows he has the necessary resources. If he discovered new identity he could easily switch to another identity and continue to disrupt the network. Furthermore, honest peers who ignore the modified content, continues to share and contribute to the spread[8].

ii) Man in the middle attack

This type of attack takes advantage of the application level routing in the P2P network. By placing itself between two peers a malicious user can intercept traffic between them. By altering the IP address and port number in a "Query Hit" message (contains confirmation on the requested resources) a malicious node can deceive the querying peer and make it connect and download altered content from the malicious node [8][9].

Attacks on structured P2P systems

i) Routing attacks

Routing attacks are aimed at exploiting weaknesses in the routing protocol used by the different P2P overlays. There are several variants of routing attacks:

- Incorrect lookup routing: A malicious node can search route requests to non-existent nodes. The network performance will deteriorate if it can be obtained in a large scale.
- Incorrect routing update: Each node in the routing table search system is based on routing information, asking other peers. This could allow attackers to corrupt the peer routing table of the other (innocent) peers, providing them with the incorrect updates. A more subtle approach would be to provide information to the peers, that lead to unreliable, that high-latency or other malicious peers.
- Partition attacks: These attacks attempt to form a parallel network running the same protocol as the legitimate network. By using the bootstrap method malicious users can deceive innocent peers into connecting to this illegitimate network.

ii) **Storage and retrieval attacks**

A corrupted node can connect the network and participate in the lookup protocol correctly, but when other peers wish to download from this malicious node it would deny them access to the data or deny the existence of such data.

iii) **Node joins and leaves**

A malicious node can reduce network performance continuously by entering and leaving the network. Events such as a join require that the network update its routing tables and rebalance the distribution of shared data by moving data to the newly joined node(s). If nodes join and leave at a high rate this will create a large overhead of traffic and processing, thus helps in reducing the network performance.

Structured P2P overlays can be effective when used in data retrieval, load balancing and distribution of resources. Overlays can remedy some of the weaknesses that exist in unstructured P2P networks, but they are away from being secure systems [10].

General Attacks and Defenses

i) **DOS Attacks**

A DOS (Denial of service) attack on a computer network is responsible for the loss of a service. There are several ways or methods to commit a DOS attack in the P2P network. The most common form of DOS attack is to flood the network with fake packets and preventing legitimate network traffic. Another method for overwhelm the victim is to perform the meticulous computation so that it become busy to do answer any other queries.

DOS attacks are much more effective if multiple providers are involved in the attack. During a DDOS attack, malicious computers are personal computers with broadband connections which have been endangered by a virus or Trojan. The author remotely controls these machines (called zombies or slaves) and directing an attack on any host or network. Finally, by using non-malicious hosts as amplifiers a DDOS attack can be further intensify [11]. The zombies transmit requests to the non-malicious hosts and deceive the zombies IP addresses to the victim's IP. The non-malicious hosts respond, by sending the answering packets to the victim. This is known as a reflection attack.

ii) Worm Propagation

Worms are becoming a major threat to the Internet. Today, worms like Code Red or Nimda can infect hundreds of thousands of hosts within hours and there is no doubt that the improvement of engineering to infect achieve the same result in seconds. Worms spread via P2P applications would be a disaster: it is probably the most serious threat.

Specific P2P Attacks and Defenses

There will be two different planes of attack in this section: data plane and control plane. The data plan attack means to attack the data used by the P2P application itself, for e.g. by poisoning or do not in any way inaccessible whereas the control plane attack directly challenges the functionality of the P2P program that attempts to slow or ineffective as possible[12]. This is usually done by the weakness of the routing protocol. Depending on the sake of the attacker, he will choose to attack in a plane or the other or both.

i) **Rational Attacks**

For making the P2P services effective, participating peers must collaborate with each other, but in most cases a node stands for a self-interested party and collaborate cannot be expected nor compelled. A reasonable presumption is that a large part of P2P nodes are rational and seek to maximize the use of system resources and minimize the use of its own [13][14].

ii) File Poisoning

File poisoning attacks working with the data Plane, and has become very common in Peer- to-peer networks. The intend of this attack is to replace the wrong file system. As the infected file is obviously not useful[13].

iii) Sybil Attack

The idea behind this Sybil attack is that a single fake node can present multiple identities, and thus acquire the control over the whole network [14]. Once this has been carried out, the attacker can misuse the protocol in any way possible. For example, he could derive the responsibility for certain files and choose to pollute them. If the attacker can place their identities strategically, the damage can be considerable. He could choose to continue in an eclipse attack, or slow down the network by redirecting all queries in the wrong direction[13].

iv) Eclipse Attack

In an eclipse attack, an attacker can establish control over a certain number of nodes along with strategic routing paths. After attaining the control he can divide the network the network in different subnets[14]. Therefore, if one node wants to communicate with another node from the other subnet, his message must have certain point to be directed through one of the attacker's nodes. The attacker thus "eclipses" each subnet from the other. In a way, an eclipse attacks also known as high-scale man-in-the-middle attacks.

CONCLUSION

In peer-to-peer networks nodes may be work as resource providers and resource consumers at the same time. In this concept services offered by a Peer to Peer network totally based on resource sharing among their peers. For this purpose we need higher security. Here we discuss the various types of attacks on peer to peer networks. In this paper, we also describe the various security issues presents in Peer to Peer network.

REFERENCES

[1] Riidiger Schollmeier "A Definition of *Peer-to-Peer* Networking for the Classification of *Peer-to-Peer* Architectures and Applications" IEEE, 2002

[2] Hyojin Park, Jinhong Yang, Juyoung Park, Shin Gak Kang, Jun Kyun Choi "A Survey on Peer-to-Peer Overlay Network Scheme" Feb. 17-20, 2008 ICACT 2008

[3] Zupeng Li, Daoying Huang, inmg Liu, Jianhua Huang " Research of Peer-to-Peer Network Architecture" proceedings of ICcT2003

[4] Yunfei ZHANG, Changjia CHEN , Xiaoping WANG "Recent Advances in Research on P2P Networks" Proceedings of the Seventh International Conference on Parallel and Distributed Computing,Applications and Technologies (PDCAT'06) IEEE 2006

[5] Asad Awan , Ronaldo A. Ferreira, Suresh Jagannathan, Ananth Grama "Unstructured peer-to-peer networks for sharing processor cycles" Parallel Computing 32 (2006) pp. 115–135 www.sciencedirect.com

[6] Wolfgang Kellerer, Gerald Kunzmannb, Rüdiger Schollmeier, Stefan Zöls "Structured peer-to-peer systems for telecommunications and mobile Environments" Int. J. Electron. Commun. (AEÜ) 60 (2006) pp. 25 – 29, www.sciencedirect.com

[7] J.Schäfer K. Malinka P. Hanáček "Peer-to-Peer Networks Security" IEEE 2008

[8] John Risson, Tim Moors "Survey of research towards robust peer-to-peer networks: Search methods" Computer Networks 50 (2006) pp. 3485–3521 www.sciencedirect.com

[9] Man Qi "P2P Network-Targeted DDoS Attacks" IEEE 2009

[10] Xiaowen Yue, Xiaofeng Qiu, Yang Ji, Chunhong Zhang "P2P Attack Taxonomy and relationship Analysis" Feb. 15-18, 20091CACT 2009

[11] J. Liang, R. Kumar, Y. Xi, and K. Ross : Pollution in p2p file sharing Systems In IEEE INFOCOM, 2005.

[12] Ziyao Xu, Yeping He, Lingli Deng "A Multilevel Reputation System for Peer-to-Peer Networks" The Sixth International Conference on Grid and Cooperative Computing(GCC 2007) IEEE 2007

[13] Ruichuan Chen, Eng Keong Lua, Jon Crowcroft, Wenjia Guo, Liyong Tang, Zhong Chen "Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks" Eighth International Conference on Peer-to-Peer Computing (P2P'08) IEEE 2008

[14] Prashant Dewan and Partha Dasgupta "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22, NO. 7, JULY 2010