Proc. of the Eighth Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2019

ISBN: 978-1-63248-165-8 DOI : 10.15224/978-1-63248-165-8-13

Case Study of Peer-to-Peer Network Environment in a Domestic Network

Jungkee Kim

***Abstract*— The P2P network is widely used in the Internet world. Many people share resources through the P2P network. However, domestic network connections are not stable and we need to consider their own network environment from the design. This paper presents a survey of measuring flow level information of a group. We can utilize the analysis of the information to design a customized P2P overlay network efficiently in our country in the future.**

***Keywords*— P2P, network environemnt, Overlay Network**

I. Introduction

The initial research on P2P systems focused on designing an overlay network on current networks without additional network protocols or network facilities. P2P file sharing systems allow nodes to collaborate each other so that very large files can be distributed from one server node to several client nodes – gossiping [1]. The P2P system randomly selects a peer node to connect to another node using random gossiping.

A P2P system has common characteristics such as equality, autonomy, decentralization, self-organization, and sharing resources. All the peers are equal and there is no central control or services. There is no coordination from outside and peers can share the resources provided by other peers.

Measuring the response times for a potential peer communication group can be collected and the data can be utilized for a proper design of the P2P network. Even if we use the existing P2P protocols, the collected response time data can be useful for the simulation to pick up the best candidate type of the P2P networks.

The response time between two peers can be measured by the active method or the passive method. The active measurement is accompanied by generating traffic between two peers that would not be sent otherwise. The round trip time between two peers is considered as an active measurement. The passive measurement just observes the traffic between peers. The passive method provides good generality and we adopt the method to measure a group of network users in our country. We plan to propose a proper P2P network in the future.

Jungkee Kim
Sungkonghoe University
Korea

II. Peer to Peer Networks

Peer-to-peer (P2P) technology emerged as a model to organize distributed systems for file sharing, distributed computing, system integration, or information search. However, P2P is not a new idea for network communication. In an earlier age of the Internet, many network systems depended on P2P technology. Usenet and the Domain Name System (DNS) were early examples of P2P based systems. However, recent Usenet departs from pure P2P by providing only selective Newsgroups and messages, because the Internet Service Provider (ISP) does not serve all Newsgroups, due to the relatively large volume of News messages. The newer Freenet restores the original P2P architecture. It is designed to protect itself from censorship using encrypted files and "route-through" data communication. It serves a full list and the server cannot block a particular Newsgroup. DNS is a mixed form of P2P and a hierarchical model. Searching a particular name is referred from lower level to higher level name servers. The name server has the role of server as well as client.

In the early years of the P2P overlay network, Napster was the most famous P2P file sharing system. In Napster, the metadata of the shared files are indexed on a centralized server. All the requests for locating files are served through this server. Only the actual file transfer occurs between peers. When a user joins the system, the user connects to the server and sends a list of possessed sharable files. To obtain target files from Napster, a "wanted" list is sent to the server. The result of the query returns the IP addresses of peers possessing the wanted files. The user can select one of the returned IP addresses and download the file. When a user disconnects from the server, the list of sharing files possessed by that user is deleted from the server. Recently, we call Direct Connect (DC) for this type.

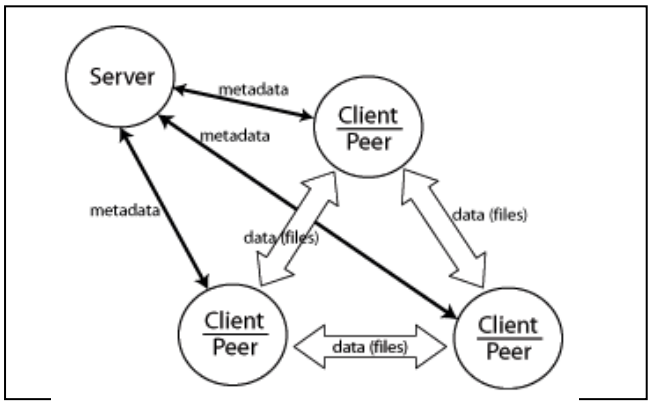

Figure 1. Napster Architecture

Proc. of the Eighth Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2019

ISBN: 978-1-63248-165-8 DOI : 10.15224/978-1-63248-165-8-13

Gnutella is a pure P2P network protocol. The initial list of hosts is usually obtained from a transitory Web lookup. A servant (node or peer) broadcasts a Ping message to find the active hosts forming the initial network. Those hosts are neighbors and the actual query is broadcast to the neighbor hosts. The neighbor servants send the query to their own neighbors again, even when they have the target file. All the messages are forwarded to the neighbors within the limited number of hops defined by the Time to Live (TTL) in the message header. If the desired files were found, the servant sends back the matched result set to the neighbor through which it received the query. The request servant selects the file from the result set and downloads the target file directly from the possessing host in the same way as in HTTP download. Due to the Breadth-First-Search (BFS) mechanism of query in the Gnutella protocol, Gnutella may cause network traffic to significantly increased. A number of studies have been focused on reducing such inefficient network usage. Distributed Hash Tables (DHTs) is one approach that reduces network communication. In DHTs, a key is mapped onto a node, which is assigned through a hash table.

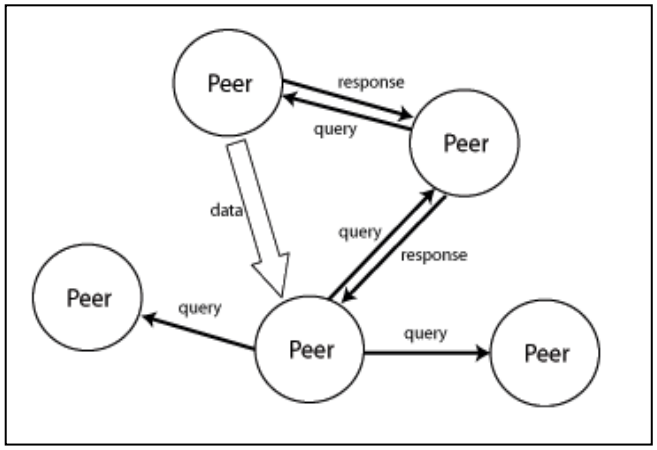

Figure 2. Gnutella Architecture

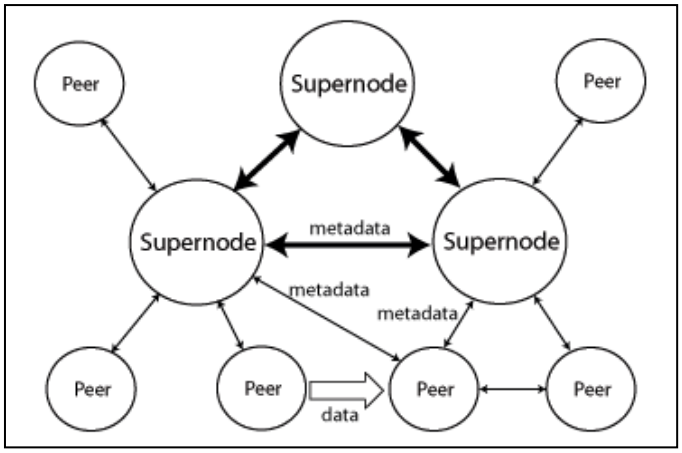

Figure 3. FastTrack Architecture

The Supernode (Hub) architecture is introduced to the unstructured peer-to-peer network for better performance. FastTrack organizes a hybrid – centralized and decentralized -form of network topology as in Figure3. Instead of centralized control, a peer node that has enough bandwidth and storage is voluntarily selected as a supernode. The supernode has a larger number of connections than ordinary nodes. Most peers act the same way as in Gnutella and also query the supernode to find target data. The large amount of cached metadata in supernodes dramatically reduces the network traffic. From the list of target data from peers including supernodes, the selected target files can be downloaded through the simplified HTTP protocol.

JXTA is the first open, platform and language independent protocol for general P2P communication and collaboration between network devices. JXTA makes it possible to organize a virtual network in which heterogeneous peers can share files, communicate with each other, and collaborate on top of the JXTA protocol.

A unique JXTA ID is allocated to each network resource. The JXTA ID is not related to the Internet Protocol (IP) address, and the ID is not changed even if IP addresses are dynamically allocated. Any network entity that executes the JXTA protocols is called a peer. Peers may be not only computers but also network devices. Each peer has network functionalities that are "independent and asynchronous" from other peers. A peer endpoint links a peer. Several peer endpoints, which represent various network connections, can reach the same peer. A group of peers that are interested in the same category can form a peer group. A peer group is identified with an ID for the group. Peers in the different domains, possibly separated by a firewall or Network Address Translation (NAT), can belong to the same group. A peer is allowed to have membership of multiple peer groups.

Messages are used to communicate between JXTA peers. An ordered sequence of named and typed elements forms a message. There are two formats for the message – XML and binary – but only a binary format is used for the physical transfer. The messages are transferred through pipes, which is the JXTA virtual abstraction for a network connection. There are three kinds of pipe connections – a point-to-point pipe, a propagate pipe, and a secure unicast pipe. A point-to-point pipe is a one-to-one connection. A propagate pipe provides one-to-many connections. A secure pipe is a point-to-point communication through a secure network channel. All the pipe operations are based on "asynchronous and unidirectional" communications. Bi-directional communications are provided on top of the pipe service. Multicasting may be used in the propagate pipe.

An advertisement is an XML-based metadata script, which describes JXTA network resources – peer, peer group, pipe, service, and other core resources. The JXTA resolver is a generic object discovery to resolve any kind of information used in typical distributed systems. All actions of resolution are integrated into the discovery of advertisements. The advertisement search mechanism depends on the policy of the application, though JXTA protocol provides a substitutable protocol framework for resolution. The resolver service includes query send and response, query propagation, and security functions – authentication and verification of credentials. Each advertisement has an expiration time, which is extensible.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2019

ISBN: 978-1-63248-165-8 DOI : 10.15224/978-1-63248-165-8-13

The Rendezvous super-peer is the optional but default policy model for resolution in a JXTA network. The Rendezvous peer is the same as other peers but has an additional cache of advertisement indexes. Through the Shared Resource Distributed Index (SRDI) service, non-rendezvous (edge) peers can publish their advertisement indexes on the rendezvous peers. The physical location of a peer does not affect the qualification of a rendezvous peer. When a peer queries an advertisement, it sends a request to its rendezvous peer. If the rendezvous peer does not have the index of the query, it propagates the query to the next rendezvous. However, from 2011 Oracle officially withdrew the JXTA project and does not continue to update it.

III. An Outline of P2P Network Measurement

First, we will recruit a group of volunteers who are willing to participate in the network measurement experiment with their own computing facilities in their resident. The passive method for measuring response time is adopted due to its good generality. The measurement starts from bandwidth between IP addresses. IP level response time should be useful because it provides fine grained aspect of the load distribution in the network of the group. Some of the group members may use the Network Address Translation (NAT) for the dynamic IP addresses, and separate identification should be strongly considered. But the overall bandwidth pattern and daily basis network activities are more interesting factors.

The next level of analysis focuses on the routing prefix. The prefix denotes the routing at the IP layer, and it is important to understand traffic for the group of the overlay networks. This layer gives clues on how they are close each other in a network routing viewpoint. Autonomous system (AS) also means in the level of similarity of their ISP administrations. It usually presents a common routing policy to the Internet.

We consider two points – not only a signaling between nodes but also actual download time between them. It is because many P2P networks are used for resource sharing with large sizes especially in video format. An excellent style manual for science writers is [7].

From the statistics of the flow records, we can consider three typical P2P systems – Direct Connect (DC), Gnutella, and FastTrack. A number of simulations on the three systems can give a clue to select an effective P2P system for the particular group under the local network environment.

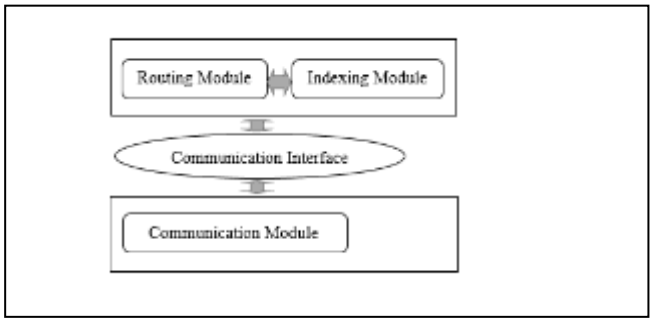

Figure 4. The Network Measurer Architecture

The structure of the P2P network measurer has two layers presented in Figure 4.

Communication: The communication layer presents a communication infrastructure to measure bandwidth between peers. For generality, we will provide a common interface that provides basic communication functionalities.

Application: Application layer includes the indexing, and routing modules. The indexing module is responsible for recording the location information. The routing module presents to locate in the P2P network peers.

IV. Conclusion

We briefly describe the P2P networks and illustrate the system structure for measuring the response times in a group of P2P network. In the future work, we can use those collected data to analyze and utilize to search a proper type of a given P2P network.

References

[1] A. Demers et al., "Epidemic algorithms for replicated database maintenance," *ACM SIGOPS Operating Systems Review*, vol. 22, pp.i-32, 1988.

[2] I. Clarke, T. Matthew, and O. Sandberg, "The Free Network Project," WWW, http://freenet.sourceforge.net/, 2008.

[3] I. Clarke, O. Sandberg, B. Wiley, and T. Hong, "Freenet: A Distributed Anonymous Information Storage and Retreival System," *In Designing privacy enhancing technologies*, pp. 46-66, Springer, 2001.

[4] Napster, L. L. C. "Napster," WWW, http://www.napster.com/, 2001.

[5] The Gnutella protocol specification, WWW, http://gnutell.wego.com/.

[6] I. Stoica, R. Morris, D. Karger, M. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, pp.149-160, 2001.

[7] A. Rowstron, and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," *In IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing*, pp. 329-350, Springer, 2001.