An Overview of P2P

Vijayakumar C M, Kumudavalli.M.V, Bipradip Roy, Rohit Kumar Singh

Dept. of Computer Applications,
Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.

Abstract: *P2P is a decentralized means of communication with peers involved as the means of interaction. P2P here is having great potential. We represent P2P as an effective setup for the IOT and as well as other fields where P2P would be considered effective. The future of networks will rely on P2P increasing security as well as efficiency and performance.*

Keywords: IoT, P2P, Cloud, UDP.

INTRODUCTION

P2P (Peer to Peer), as the name says, is a direct client access network protocol where the network interaction is client to client based. The users in the network layer are interconnected to each other and everyone has equal rights and can initiate communication.

Internet as proposed by Tim Berners Lee was a p2p model where computers were supposed to interact with each other (client to client) to share information. P2P works by creating a network layer on top of an existing network where the application may request a piece of information from the systems connected. It can also receive a set of information from multiple clients reducing the load on a particular system.

Peers are the system users which are active on the network. They contribute to the cycle that completes p2p. They are both receivers and givers of resources. In grid computing, all the systems are equally sharing the hardware resources among the various active peers. In file sharing systems, users are divided into leechers and seeders. Leechers download the
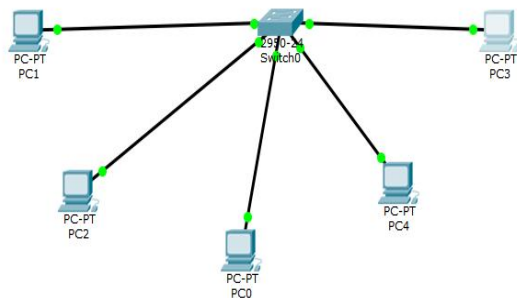
file and seeders upload the file.

Fig 1: An example of basic P2P network.

Peer to peer systems have a great potential and are advancing with the existing technologies. One example being Bit torrent, it is considering itself to use the UDP protocol over the TCP protocol where the network relies least on any protocol mechanism and it increases the privacy of the downloader.

DISRUPTIVE TECHNOLOGY

Disruptive technology is altering the way a technology worked into something that is much more advanced and reliable. It changes the way the business work, it alters one's lifestyle. An existing technology may be replaced or modified in a way that the previous technology may be out of the market. Prof. Clayton Christensen coined the term, where new products come in with better features and much newer technology where it takes over the previous generation of products.

EXAMPLES OF DISRUPTIVE TECHNOLOGIES.

Touch screen – Touch screen technology is almost half a century old, but that was not so innovative and was mostly used for air traffic controls. Not until 2007, where phones were having just few extra features such as GPS, Music Player, and required hardware keys to be pressed to be controlled, Apple[1] released its first Smartphone that revolutionized the mobile industry by releasing a fully touch based interface in a phone, the iPhone.

Modern computers – Mainframe systems that were bulky and not available for personal use, they had high power requirements, low memory and could only perform certain set of tasks. They advanced into high powered computers which currently do almost 3 billion calculations per second and most of them have the Graphical User Interface.

The Internet - With internet spreading all over the world, nearly everyone would be connected. Internet has the ability advance to an extent where it is our primary means of communication. Here, internet is a disruptive technology because Internet has not reached its entire potential. With cloud computing emerging in the market, Internet makes it possible to work directly on the servers at low costs. It does not require high end resources to perform large computation; everything is done remotely in the cloud servers.

Next-generation Genomics - Use of computers for treatment purpose is not something new. The next era of advancement in the field of genomics combine the science for imaging nucleotide base pairs with rapidly advancing computational and analytic capabilities. It will be possible to manipulate genes and improve diagnostics and treatments with an improved understanding of genes in the human body. In coming future, the biggest disruption is probably going to happen in the genetics area. The ability to have personal genetics records and the ability to start gathering all of the gene sequencing into places will be helpful in cancer treatment and other diagnostics over the period of time.

WHAT ARE PEERS

Peers are the system users which are active on the network. They contribute to the cycle that completes p2p. They are both receivers and givers of resources. In grid computing, all the systems are equally sharing the hardware resources among the various active peers. In file sharing systems, users are divided into leechers and seeders. Leechers download the file and seeders upload the file.

SOME USAGES OF P2P

Instant Messaging - A p2p network makes IM (instant messaging) easier and faster. In UNIX[6], the write command issued to a particular user on the network is a simple messaging feature that works under p2p network. A P2P network does not process request from a centralized server, thus, the connection between two clients is direct in nature. If a server is used for IM, the server will not be able to handle the load on large number of requests. Larger request will slow down the process making the messages delivered extremely slow and affecting the performance on every system communicating through IM. A p2p network connects to the users through opening ports allowing direct access and equal load balance.

File Sharing - The file sharing of p2p works by directly receiving files without going through a server. A local system requests for a file to be searched over the network. The clients receive the request and check if the file exist if not the message is passed over to the next client and it happens until the file is found. This reduces the load on the server and distributes the load across the computer systems.

VoIP - Just like IM, P2P can be used for VoIP services. Skype, Viber provides these services. In a simple manner, the voice over the protocol is encrypted making it secure and it is a non-server based communication making it faster. Not only VoIP but video calling feature is implemented too. To initiate a p2p connection a client server connection is required and then the connection is forwarded to the client.

EXAMPLES OF P2P APPLICATIONS

Bit Torrent, Napster, Gnutella, LimeWire, Skype, and KaZaA are some examples of P2P applications

Napster[2] - In Napster, unlike other mp3 sharing websites, songs are present on various user machines. When a song is downloaded, the mp3 file is not copied from the server system; instead the song is downloaded from another user's machine. Individuals make all sorts of copyrighted songs available to the world from their personal machines, which violate the copyright laws. Piracy was the main reason behind shutting down of Napster.

Gnutella[3] - Currently, the most popular system for sharing files is another peer-to-peer network called Gnutella. There are two main similarities between Gnutella and

Napster –
• Users place the files they want to share on their hard disks and make them available to everyone else for downloading in peer-to-peer fashion.
• Users run a piece of Gnutella software to connect to the Gnutella network.

There are also two big differences between Gnutella and Napster:
• There is no central database that knows all of the files available on the Gnutella network.
• There are many different client applications available to access the Gnutella network.

Bit Torrent[4] - Bit torrent is a communication protocol used for sharing of files across the network. The working of bit torrent is based on p2p communication. Because of the p2p network that bit torrent use, it shares large files very efficiently and at lightning fast speed. A file that is ready to be shared is made available on a host computer as a torrent file. The system that hosts the original file is called a seed and it splits the entire file into lots of pieces. If any user of bit torrent wants the file, then it uses a bit torrent client to request it from the seed. The client receives one of the pieces of information from the seeders and the remaining pieces from other user's computer through P2P communication. Hence, at a given moment, a computer is simultaneously downloading some parts of the file from some peers and uploading some other parts of the file to other peers. A system can start sharing files before even downloading the entire file because bit torrent divides the file into several small parts.

SKYPE AS P2P

Skype[5] is an IM, Voice, Video Chatting application. Skype in general has a server that stores the user information such as the user id, contacts linked with the id and peer information. Skype cannot host all its calls on the server, doing that so will require high speed cable and high bandwidth, lots of storage space and of course, high costs. Skype uses a much more efficient method to implement its calling feature. There is a central server that is active when the user is active on Skype, it has all the contact information. When a user wants to initiate a call, the skype server receives a request to initiate a call on the other end, to the person called. Once the connection is established, the server looks for open ports in the system and creates a connection between those two users.

Skype uses an overlay p2p network for the communication process. The Skype network contains three types of entities: super nodes, ordinary nodes, and the login server. The Skype application that is installed in the user system is an ordinary node that is used to place voice calls and send text messages. The ordinary node (Skype application) is used to connect the user to a super node and authenticate itself with the Skype login server. The Skype login server is

important in completing the Skype network as user name and passwords are stored in the server. This server ensures that every Skype user has a unique username and password.

Any system with a public IP addresses and having sufficient CPU, memory and network bandwidth can become a super node. A super node is a system that has IPs to all other available peers in the network that can be routed through an open firewall, and also consist of systems with high bandwidth and more resources. A normal client can also be a super node. In super node p2p system one can rely on the users of the network rather than its own server to handle the majority of the traffic. Super node are standard computers which are selected by the Skype application to serve as the traffic cops for their entire network.

However, there can be security issues regarding such usage as p2p is an open connection and gives out the user address to the client, increasing security risks. Hence, Skype encrypts the connection from one end to another end, making it hard for an attacker to intercept the traffic and act as a middle man. The encryption is a standard AES 256-bit.Connection between the Skype client sides to a network provider, i.e. normal calls is encrypted, but the connection from the PSTN is not.
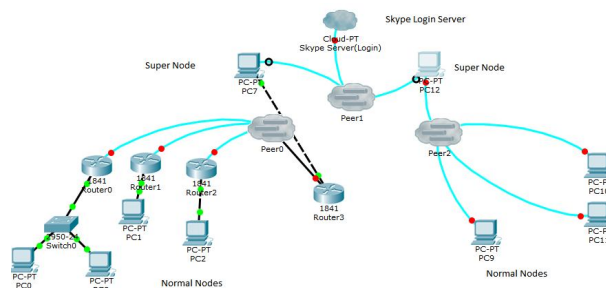
SECURITY CONCERNS REGARDING P2P

Open Ports: The p2p network relies on open ports to receive or send pieces of information from peers. If the port is blocked it makes p2p sharing impossible. The open port here may lead to an exploit of the system. Each port that is being opened may give the exploiter a chance to hack into the system. As open ports have no restriction in incoming/outgoing traffic, they are more vulnerable.

DDoS attacks: Poisoning of other devices in a p2p network will make the devices target a particular device in a network by sending large number of requests to the system, increasing its workload and making it crash. This cannot be stopped as the traffic cannot be filtered. The only option remains is to shut down the client being attacked[7][8].

Malware Spreading: The files shared in p2p are not one whole piece but is divided into pieces. Unlike a pure p2p system where a file may not be divided into pieces, the chances of spreading a malware is more. A user may corrupt the file with a malware making the receiver more vulnerable. Extending this to hybrid p2p systems, the pieces of

information can be corrupted making the file unusable, or if the file that is corrupted is downloaded from the same source with all the pieces intact, the file will be attacked with malware.

IOT MEETS P2P

Internet being a disruptive technology, is gaining its potential through the emerging topic of IOT (Internet of Things). Basically, IOT is just every device being connected to internet, from usual devices like Phones, TVs and Computers to unusual devices like ACs, microwave, refrigerator etc. This also involves everything being connected to each other, communicating with each other, cooperating and providing more power to the user in an efficient manner.

Things are always connected to each other in a suitable network, collecting and receiving data constantly and updating the information. They are real time, require good network and are error free making it usable to public. A smart watch is a device that can be linked to the smartphone with a Bluetooth, constantly syncing data with the phone and updating data to the phone. This can be upgraded as IOT by adding few more sensors to the watch such as a heart rate monitor, gyroscope, and ambient light sensors etc. (which are already present in the current smart watches). They keep in sync with the phone about the whereabouts of the user and the data is synced with the smartphone and then uploaded to the cloud. The data is now available to all the devices linked to the same account in the cloud. This data can now be used to switch on the geyser if the user is located 5 minutes away from home, ensuring he gets hot water when he bathes or the AC turned on way before he reaches the home, ensuring efficient cooling. Many other features of IOT are available and is being implemented.

Considering IOT as a huge advancement in connected technologies, it needs the right resource to be connected with each other. IOT has been designed to efficiently work with the internet as the name says, but that's not a real efficient solution towards things linked in small area. Most devices within a small area, like office or home or small industries connected through the same network, like a router or a switch need not communicate each other through cloud. Cloud is unreliable in terms of unreliable internet connection. Other failures include broken communication hardware, or network congestion.

This technology can be implemented over a small area where the devices are in close proximity(Wi-Fi range, or LAN range) can be better implemented using a Pure P2P mechanism, unlike the standard cloud mechanism where devices need to be constantly in sync with the cloud.

Possible implementation using Cloud:

All devices are connected to a single source (Router) that receives the data and transmits data to the cloud where there is a signal from the cloud server sent to the device to respond and then further instructions are performed by the listening device[9].

Ex: Devices gather data from sensors, send the processed data to the cloud. The cloud server then stores the data into the server. The data is now processed by the cloud to decide

what operations are to be performed, the cloud sends a signal to the device that will perform the instruction and the device listens to it and then performs its instruction.

Possible implementation using P2P:

All devices are connected to each other signaling the respective device/devices in the network range and performing operations (Direct access) and simultaneously uploading data to the server[10].

Ex: All devices are having their ports open and are constantly listening. The devices are constantly processing data and signaling respective devices to perform operation without any server in as a central source.

Implementation of IOT requires each device to interpret the given data and generate a response that has to be sent to respective devices. The data sent over the network should have the device information to be signaled and the listening devices should receive the data and perform the instruction. This is similar to M2M (Machine to Machine) but since all devices are interconnected it brings in the challenge of coding the device data to be understood by other devices. P2P fails in a large complex system of devices working on different kinds of data. A better option is to implement IOT using hybrid P2P[12].

Possible implementation of Hybrid P2P in IoT:

The devices within small proximity are connected to a local network in P2P fashion, where similar devices communicate with each other, non – similar devices will have to upload the data onto a machine that can process the data, if the data is clear enough to the machine it'll signal the device required to perform operations. If the data is not interpretable, the data is uploaded to the cloud from the machine.

Why choose hybrid P2P over a direct cloud communication?

Hybrid P2P unlike usual cloud network does not require every device to be connected to the internet. This reduces the addressing issue where each device will be communicated through a common machine that is connected to the cloud. This will keep the standard ipv4 addressing rather than having to upgrade to IPv6.

Hybrid P2P will reduce internet traffic and reduce the requirement for lower pings. Since the machine is the only device interacting with the cloud, each device need not constantly ping the server increasing the load. This will also help reduce data redundancy and increase consistency.

Does not always depend on internet connections. Basic IoT functions can be done by the machines locally.

Greater security since everything from the server goes into the machine that decodes the instruction and not directly to the devices.

Many more advantages like, debugging a device failure with the local machine, constant updates of its function, improved privacy protection.

Disadvantages of P2P over a cloud connection:

IOT running will have complex system architecture to run across in a parallel mode with other devices. They should understand the message passing structure, where the communication is direct (One device to another) or indirect (Device to an interpreter then to the device to whom the message is for).

P2P systems are limited to the Big Data access where they are not stand alone on nature, they depend on structures around to complete their processes.

P2P systems require more resource power since they are working together they may be crowded with data rather than a central server[11].

If the centralized processor is malfunctioning, the entire network structure may fail. Whereas in cloud, they are standalone and are communicating on their own. Individual device failure will just result in no message passing from that device itself, the rest of them may be intact.

Security concerns with p2p as IoT:

Security is not a big issue with the p2p foundation of IOT because the implementation is decentralized and the data transmission is encrypted, making it much secure.

No device can be misconfigured or taken control of by any unauthorized source as they are directly communicating with each other or with a central machine. The only way they can be taken control of is by knowing the instructions passed by the machine or taking the control over the machine.

CONCLUSION

P2P does have broader applications than it is currently in use today. Prototyping IoT with hybrid P2P modes of communication will enhance the flow of packets, reduce the IP addressing issue, and uplift the security compared to a Cloud model. The P2P system works on any system connected to any device, regardless of the platform and has very easy implementation. There are many ways of implementing this technology, one way is by decentralizing the network and encrypting the data transmitted. P2P can grow into a large network of things being connected to each other.

REFERENCES

[1]   K. Aberer, M. Hauswirth, M. Punceva, and R. Schmidt. Improving Data Access in P2P Systems. IEEE Internet Computing, 6(1), Jan./Feb. 2002.

[2]   E. Adar and B.A. Huberman. Free Riding on Gnutella. First Monday, 5(10), 2000. http://firstmonday.org/issues/issue5 10/adar/index.html.

[3]   W. J. Bolosky, J. R. Douceur, D. Ely, and M. Theimer. Feasibility of a Serverless Distributed File System Deployed on an Existing Set of Desktop PCs. In Proceedings of the International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2000), pages 34–43, 2000.

[4]   I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B.Wiley. Protecting Free Expression Online with Freenet. IEEE Internet Computing, 6(1), Jan./Feb. 2002.

[5]   I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. Freenet: A Distributed Anonymous Information Storage and Retrieval System. In H. Federrath, editor, Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymit y and Unobservability, number 2009 in Lecture Notes in Computer Science. Springer Verlag, Berlin, 2001.

[6]   Clip2. The Gnutella Protocol Specification v0.4 (Document Revision 1.2). http://www.clip2.com/GnutellaProtocol04.pdf.

[7]   http://www.apple.com/in/

[8]   https://en.wikipedia.org/wiki/Napster

[9]   https://en.wikipedia.org/wiki/Gnutella

[10] http://www.bittorrent.com/

[11] http://www.skype.com/en/about/]

[12] https://en.wikipedia.org/wiki/Unix