**Mobile P2P Files Sharing**

**A Term Paper**

**Presented to**

**Dr. Terry Griffin**

**CMPS 5373: Native IOS App**

**Department of Computer Science**

**Midwestern State University**

**By**

**Kotiyala, Surekha**

**Term Paper**

**Spring 2015**

**Abstract**

P2P files sharing via mobile devices has introduced several discussions and challenges with various technologies and methods in today’s mobile territory. This paper describes the variety of ways to utilize the P2P (here on referred as P2P) networks which caused an increase of mobile devices with security. The evolution has started from Internet connection allotted by traditional mobile cellular telecommunication networks to free Internet connection through Wi-Fi technology, further extended by using Bluetooth. However, smart phones are assumed to be equipped with a ZigBee modem for allotting control functionality for personal wireless sensor networks. Furthermore, a systematic review with various approaches like unstructured and structured P2P system, mobile-to-mobile technique, and tree-structured based are discussed. Besides, it takes a look at the system stability when frequent disconnections occur and on different types of applications that are used for sharing the files with less delay time. Moreover, for rapid development of the mobile P2P communications hierarchical architecture is developed. This architecture uses clustering for obtaining peer communications with three main aspects such as maximum connection time, minimum hop count, and number of connected peers. These connections between the peers are intent by their communication ranges, velocity vector and also by their locations. Hence, the network between the peers will be stable and cost is reduced with good success in content searching. Security and privacy also plays an important role while sharing files between trusted and untrusted networks like Wi-Fi and Bluetooth. For flexible and power efficient mechanisms a system is developed, which is known as Smokescreen.

**Contents**

1. Introduction
2. Purpose
3. Overview
4. P2P Networking
5. Mobile P2P Methods
6. Unstructured-based P2P method
7. Structured-based P2P method
8. Direct mobile to mobile technique
9. Distributed hash table and Tree Structure method
10. Mobile P2P Technologies
11. Communication with Bluetooth and BlueTorrent
12. Communication with ZigBee
13. Communication with wireless Ad hoc networks
14. Security
15. Conclusion
16. References
17. **Introduction**

P2P file sharing is the process of sharing different files like audio, video, images, documents etc. over different devices. Now a days, users are moving towards a mobile connected world, one way of increasing of mobile users is by using P2P file sharing which is introduced with various technologies with different methods in today’s mobile territory.

**1.1. Purpose**

A file is shared with a group of people who make a request on central server; this server is linked with all the people who request a file. The file would be transferred between two devices. The P2P networking technology is used for file sharing like sharing between groups of people, sending and receiving digital media using mobile devices.

**1.2. Overview**

The overview of the paper is organized by sections: Section 2 describes about how files can be shared on a P2P network. Section 3 discusses different methods involved in mobile P2P communication. Section 4 explains various technologies used on mobile devices. Section 5, includes how security is provided by using P2P network on mobile devices. Finally, Section 6 concludes of the paper.

1. **P2P Networking**

The P2P networking is created between two or more devices for sharing the resources. P2P communication is possible in both wired and wireless internet, but for mobile devices wireless internet is only possible through subscribed cellular radio services. The P2P helps all the devices to spread and maintain the load with good networking. To provide security in P2P networking, authorization and authentication are needed.

Another way to use P2P service is by using Fon. Fon provides a system, which is a dual access wireless network and has the largest Wi-Fi networking in the world with more than 14 million hotspots as claimed in March 2015. This is for the customers who do not want to share the internet connection but want to buy the Wi-Fi access from Fon.

1. **Mobile P2P methods**

P2P describes different ways of communication between two devices with same protocol. Mobile Ad-hoc Network (MANET) is used for decentralized and dynamic exchanging of information. Mobile P2P communication is through wireless internet, based on the proximity. There are several protocols with different technologies and methods.

**3.1. Unstructured based P2P method**

The unstructured based P2P method provides unaware resources to their adjacent peers. This method describes about the total number of messages that are pinged and ponged between two connected devices.

The process of this method for finding and downloading a file from the requested peer is as follows. Firstly, peer1 sends a query to find a file; peer2 receives the message sent from peer1 and tries to find the file; if file is not found peer2 replies “the file does not exist”. And the query is sent to next peer; if it is found it starts downloading. This is the process of unstructured based P2P method.

**3.2. Structured based P2P method**

The structured-based P2P method provides information about resources offered by the adjacent peers. This method provides low latency and load balancing with high signal overheads. The system depends on distributed hash table (DHT) which includes hash function, this helps in sharing contact information and locations.

This method is similar to unstructured based with some additional feature like peer1 and peer2 are communicated securely. That is, peers uses peer ID and predecessor ID in the network for communicating.

**3.3. Distributed hash table and Tree Structure method**

Distributed hash table and Tree Structure method uses topology of network for storing and maintaining the peers information for example locations and routing, which works for MANET. This method performs various tasks like detecting the nodes, communicating with the nodes within the range, notifying its failure. It is same as unstructured-based for maintaining information about the shared file with its location.

**3.4. Direct mobile to mobile technique**

Direct mobile to mobile technique is an improvement over unstructured-based method. This method provides stable communication with direct mobile to mobile with availability of UMTS channels and its network. This uses mesh architecture with Frequency Division Duplex.

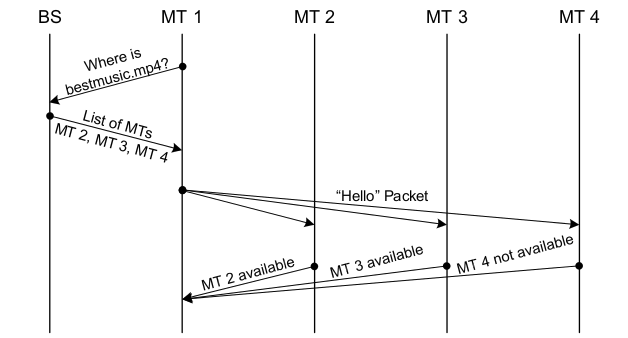


Figure 1: Unstructured-based on M2MT [5].

1. **Mobile P2P Techniques**

The mobile devices uses various techniques with variety of services, different P2P techniques supports the energy efficiency within the network for sending and receiving the information between the peers. The energy efficiency is maintained by mobile battery, which is focused on energy reserving. There are different technologies like Wi-Fi, Bluetooth, ZigBee, RFID etc. they are used in the world for transferring the data between the peers. Some of the technologies are explained below:

**4.1. Communication with Bluetooth and BlueTorrent**

Bluetooth enables connectivity between two devices within small range that is around 1 Mbps to 10 meters, for free of cost. It follows star network topology. This interface communicates with the mobile device for sharing information among close proximity. If either of the communicating device is out of the range for sharing the file, then the receiving file will be paused and stops till it again reaches the range for sharing or till it finds the same file with exact time frame. BlueTorrent, this enables for sharing audios and videos contents. BlueTorrent is based on pervasive Bluetooth.

**4.2. Communication with ZigBee**

ZigBee is also known as Wi-Zi cloud, it uses a dual WiFi-ZigBee radio on mobile devices and access point. This provides high energy efficiency with low power, low cost and higher bandwidth. This technology is introduced on android devices like smartphones and tablets with different versions of platforms such as JellyBean, ICS.This works on cluster tree and mesh networking. ZigBee motes are used for connecting directly to the devices for enabling the flow of information from a device to other. This motes look like USB, so they are called as USB dongles. It enables the device and allows communicating through ZigBee modem for sending and receiving files. The main role of these dongles are controlling and monitoring while collecting and transferring information.



Figure 2: USB dongle and packet sniffer [4].

The sharing of file has a process for sending and receiving the files. That is, for sharing a file; a file is need to select, then, this file is converted into byte array before it is sent to USB dongle. Again, while receiving the byte array is converted to file form. Users can also use broadcast messaging by connecting to internet and send messages directly by using an application called ZigBeeComm. The packet sniffer is used for testing and sending packet to the devices. This device is reliable to use and it’s a robust technology which runs on primary battery for long years.

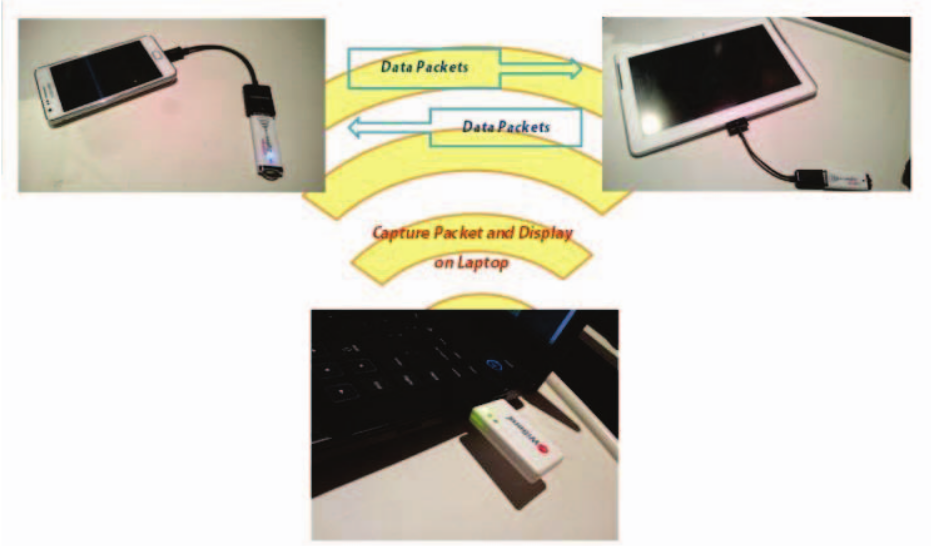


Figure 3: USB dongles and packet sniffer is connected to PC, tablet and mobile devices [4].

**4.3. Communication with wireless Ad hoc networks**

P2P mobile communication with wireless Ad hoc networks helps in sharing and receiving content information among various devices like mobile phones. It provides an efficient searching with low cost in a wide network by using distributed hash table method, since each contact is assigned with key that has a unique value for hashing which stores by the receiver. The receiver has a range to store the keys. The peers are classified into Super peer and Sub peer, to manage the peers for sending and receiving the information. Super peer maintains data and routing of sub peers in mobile environment. But, this needs high updates in connecting peers again and again because it disconnects easily. For this, clustering architecture is been introduced, which has three major roles, connecting the peers for long time, maximum hop count with super peer and number of connected peers of super peer.

This architecture works with normal and super peers. A cluster consists of similar velocity vector with nearer physical locations which disable the thought of disconnecting between the peers. When information is searched efficiently by managing cost of the network, the hop count is significant between normal and super peers with maximum connecting time and minimum hop count. This can balance the super peer by threshold values which gives the total number of connected peers of individual super peer. Normal peer are communicated to super peer with intermediate peers and Communication is possible between super peers through boundary peers.

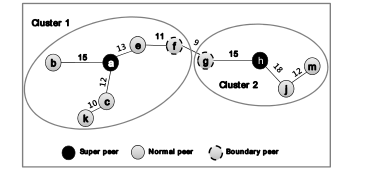


Figure 4: Communication cluster with Super peer, normal peer and boundary peer [3].

In cluster, if a new peer requests to add to a network, it needs to send a “hello” message to enter a cluster. If the new peer gets response it joins the cluster and if it receives more than one response from different clusters it can decide which one to join. But, if it doesn’t get any response it will be called as new super peer and forms a new cluster by its own.

In cluster, if a peer leaves a network. This can happen in either of the ways, leaving the networking without informing due to loss of battery or sending a leaving message before leaving. The sending a leaving message can be notified by normal peers, super peers or by intermediate peers. If the leaving message is sent by normal peer there won’t be any affect but, if it is a super or intermediate the rest of the peers need to get notified for reorganizing the network with new super peer.

These connections between the peers are intent by their communication ranges, velocity vector and also by their locations. Hence, the network between the peers will be stable and cost is reduced with good success in content searching.

1. **Security**

When various technologies are used to access the information in different platforms, privacy plays a vital role to maintain information in secure way. Privacy control’s provides flexibility to share between trusted and untrusted social relations. For flexible and power efficient mechanisms a system is developed, which is known as Smokescreen. This system broadcasts clique signals which can accessed only by trusted users that is sharing between social relations and on other side some opaque identifiers are used for trusted broker that is sharing between strangers.

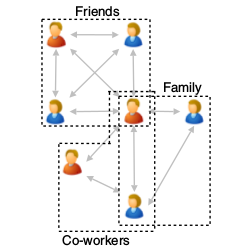


Figure 5: Trusted social network [1].

The clique signals have a unique key, for providing access to trusted group of people. This is applicable on social networks like Facebook, What app, twitter etc. for sharing the required information like sharing location with interested people and disclosed some information from others. Privacy is concerned with controlling, dispersion, disclosure, Isolating information from others.

1. **Conclusion**

In this paper, it described about variety of ways to utilize the P2P networks which caused an increase of mobile devices with security and low cost for transferring the files. Efficient methods had been used for establishing maximum connectivity between the devices. Moreover, message transferring mechanism is clearly discussed by using different methods and technologies. Also, an application of android device that is ZigBee communication is mentioned for file sharing and message broadcasts via USB dongles which is detected by the android devices and alerts the user to start the application. Furthermore, privacy can be regulated by using low cost clique signals with unique key between trusted social relations while using Wi-Fi and Bluetooth. Despite of growing mobile usage, the cost of Wi-Fi is increasing. For this, Fon Company has developed a system which provides dual access wireless networking (it’s a router). This networking brought for the customer who doesn’t want to share Internet connection but want to have the Wi-Fi access with less cost.

1. **References**
2. Cox, L P., Dalton, A., M, Varun., “*SmokeScreen: Flexible Privacy Controls for Presence- Sharing*.” Proceedings of the 5th international conference on Mobile systems, applications and services.
3. Hartley, J., “*Peer-to-Peer Networking: A Mobile Coming of Age*.” Intel Corporation, November 2007.
4. Li, H., Bok, K., Yoo, J., “*A Cluster based Mobile P2P Architecture in Wireless Ad Hoc Networks*”. Proceedings of the 20th ACM international conference on Information and knowledge management, New York, NY, USA, 2011, Pages 2393-2396.
5. Rahman, A N A., Habaebi, M H., Ismail, M., “*Android-based P2P File Sharing Over ZigBee Radios*.” 2014 Fifth International Conference on Intelligent Systems, Modelling and Simulation.
6. Yasin, W., Ibrahim, H., Hamid, N A W A., Udzir, N I., “*A Systematic Review of File Sharing in Mobile Devices Using Peer-To-Peer Systems.*” Computer and Information Science, Vol 4, No 1, 2011.