Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.304 – 309

RESEARCH ARTICLE

Secure Message Passing and Content Sharing in Smart-Phones Using Wi-Fi

Nivedita S. Deshmukh

Student, M.E. Computer Engineering, Pune Institute of Computer Technology, Savitribi Phule Pune University, India
nivedita.malik@gmail.com

Abstract— ***Along with the rapid growth of Wi-Fi-enabled smartphone devices, the need for efficient content sharing techniques for smartphones in Wi-Fi environment has increased. There are many methods recently presented by various researchers for efficient content sharing in Smartphones However existing methods are suffered from the various limitations. Hence, this area of research is still thought provoking problem for researchers. This paper present secure approach for message passing and content sharing in smartphones using Wi-Fi (WCS), which gives better speed and range over Bluetooth and no internet connection or heavy centralized servers, are required in this process. Each smartphone can work as client and server at the same time .Message passing is done securely by using encryption decryption technique. Users can also share files with large numbers of other users in the network following Peer-to-Peer(P2P) protocol. Based on the analysis done for secure message passing scheme, it is observed that with little difference in time secure message passing is done using encryption.***

Keywords— Wi-Fi, Peer-to-Peer Protocol, Bluetooth, Encryption

I. INTRODUCTION

Smartphones have become very popular and commonplace in the last few years. They have become highly capable multimedia devices that can share various types of user generated contents and messages by making use of data plans over the internet. Messaging is another important feature and application in mobiles. Messaging is possible over the internet and off the internet (through SMS service).One traditional technique of sharing on mobile phones is done through MMS (Multimedia Messaging Service), but it has a size limitation. A sophisticated data exchange model Bluetooth standard that we use today is allowing wireless communication between enabled devices. However sending data using Bluetooth in the real world is not easy. Devices should follow the Bluetooth standard[3] to discover devices via Bluetooth and connect to them. According to some researchers, Bluetooth is not an appropriate solution to some situations [4][5].

Following issues are there in P2P file sharing application for mobile devices in ad-hoc environments:

(1) how to organize the shareable contents for a mobile device?
(2) how a mobile device can discover the content of users interest in proximity?
(3) how efficient transmission of content from one/more mobile devices to one/more other mobile devices can be ensured?
(4) how energy consumption in mobile devices is minimized to save battery power?

Solution to above problem is peer-to-peer sharing among smartphones, by using W-Fi instead of using expensive packet data networks for sharing files.

II. LITERATURE SURVEY

Some mobile P2P file sharing applications like Mobile Mule ,Symella, mbit have been developed [6][7]. For all these applications: (1). Devices need to be connected with internet and (2).It is assumed that created network is stable and infrastructure based. Another real time problem with these applications is internet connectivity is not always very reliable, and even if it is available, it incurs high usage cost. To avoid this cost, a mobile user can use the Wi-Fi interface of the mobile phone to connect to the Internet.

Mobile P2P content sharing using ad-hoc environments is a popular area of study [9],[10], [11], [12]. These studies are promising, but they focus on routing technique and assume that the underlying network is multi-hop. In such case ,smart- phones (peers) that are within reach of each other can form a mobile ad-hoc network using Wi-Fi(IEEE 802.11), and find efficient way to discover and download contents generated by other peers in the network. 802.11 supports an ad-hoc mode of operation, provides longer communication range as compared to Bluetooth, and now a day all smartphones are equipped with the Wi-Fi feature.

This paper includes the proposal of a system for providing the above features of content sharing and messaging over the Wi-Fi. ANDROID platform is used for deployment of an application that provides secure messaging and content distribution using Wi-Fi without using the internet or costly centralized servers.

III.DESIGN OVERVIEW

A. System Architecture.

The Goal is to implement the secure message passing and content sharing scheme for smart phones using wireless network. Messages are transmitted by sender and stored on server database in encrypted form. From server database they are delivered to receiver's smartphone if he is online otherwise delivery of message is delayed till user is not online. Contents to be stored are kept in sharable folder with each smart phone user and . Metadata of all these files is kept with server .Actual file is not present with server. Any file from sharable folder can be downloaded by requester.

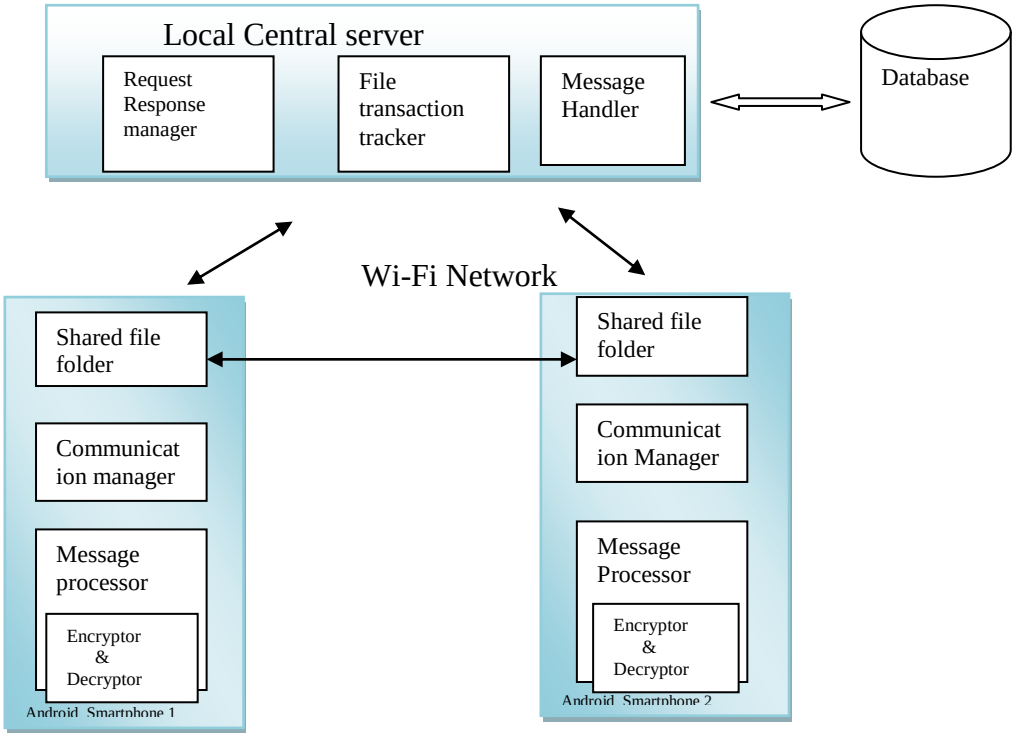

Fig. 1 system architecture of secure message passing and content sharing system

In System we are having wireless Adhoc network, inside of that handsets are communicating with each other through peer to peer connection. Central server having database of smart phone users which have already done their registration. Central server has GUI, Request Response Manager and File Transaction Tracker. Android Mobile Handsets have Communication Manager, Shared File Folder and message processor.

Client Side

1. Communication Manager: It is responsible for handling the connectivity of the system, both It deals with sending request to the server for searching contents and receiving list of peers containing required contents.
2. Shared File Folder: It allows user to make content available to other peers.
3. Message processor: At sender side it does the work of encrypting message and at receivers end it decrypts message.

Server Side

The server handles registering the users into the network, validating users and searching and showing the list of files available in the network to a user.

1. File Transaction Tracker: It keeps the track of transactions carried out by users.
2. Request Response Manager: It handles request from user and provides response accordingly.
3. GUI : It provides interaction to administrator.
4. Massage Handler: Stores and retrieves encrypted messages from database.

*B. **File and Message Sharing Technique***

Each user has folder of sharable files .When user log into the system his IP address and list of shared files is updated on server. Any user can get the list of shared files with owner's IP address by sending request to server.

For sharing message user asks server for list of network users and then selecting User_id of peer user can share chat message with it. If user clicks on to User_id of any peer all previous communications with that user can be viewed. If user is offline then messages intended for him will get stored on server database in encrypted form and once he is offline all stored messages will get delivered to him and decrypted messages can be viewed at receivers end.

C. ***Algorithmic Design***

For secure message passing new encryption and decryption algorithm is design. Procedure followed for encrypting and decrypting message are briefly given here.

Encrypting Message:

1. Before sending string S to server do

Ascii(S[i]) is processed as $E_k(S[i])$= Encrypted S[i] endfor

2. Provide this encrypted string (E_s) to huffman algorithm to encode E(S) in the form of 1 and 0 .

3. Resulting String H(E_s) is stored in server database.

Decrypting Message:

1.H(E_s) is processed with Huffman decoding technique to get E_s.

2.Decypt E_s by using D_k to get S again. $D_k(E_s)$= S

3.Resulting plain text S is displayed on users device.

IV. PERFORMANCE EVALUATION

Performance of the system is evaluated based on different parameters like, transmission speed, variable file length, variable message length, distance etc.

a) Comparison of message passing time with and without decryption.

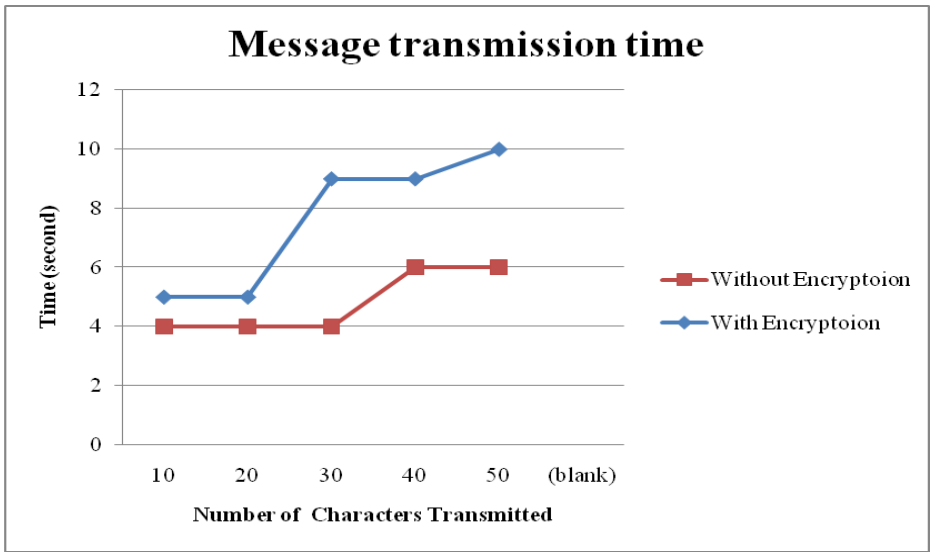

Fig. 2 Comparison of message passing time with and without decryption

Above graph shows transmission time of message in the communication system. Messages of variable lengths are passed between users in indoor environment with and without encryption. Based on analysis of above graph it is observed that message security is obtained using encryption with little extra transmission time.

b) Comparison of Bluetooth and WCS based on transmission speed.

Considering, 1.File size=3.1MB 2.Number of users are fixed 3.distance is varying

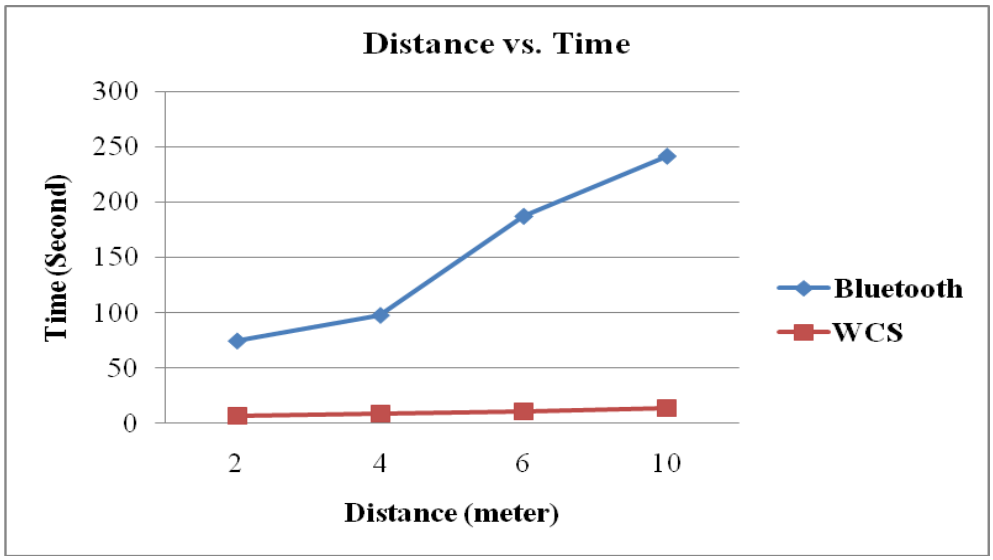

Fig. 3 Bluetooth vs. WCS file transmission speed

From above graph it can be analysed that if distance increases then transmission time increases significantly in Bluetooth but in WCS it remains almost stable. With calculations based on actual readings 93% improvement in transmission speed is observed in WCS over Bluetooth.

c) Comparison between Bluetooth and WCS for varying file size

Considering,

1. Fix distance 2.Fix no of users 3.varying file size(from 3MB to 60 MB)

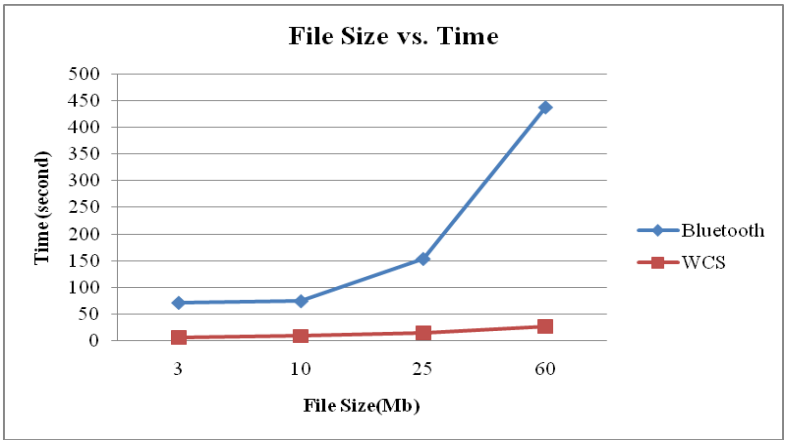

Figure 9.8 Bluetooth vs. WCS performance for varying file size

By analyzing above graph we can conclude that transmission speed of WCS with increasing files size is significantly good than Bluetooth .With actual reading it is calculated that WCS outperforms Bluetooth by 92% in transmission speed with varying file size.

Conclusions

The primary aim of this dissertation work is to provide security to the messages that are passed in communication network. A peer-to-peer model is used for sharing files that permits file sharing between mobile smartphones over the Wi-Fi. Currently, this application works only for Android devices including both smartphones and tablets. This application guarantees secure message passing between peers with very little increase in transmission time. Users can also share all types of contents (audio, video, text). The low-cost central server is used for the purpose of authentication and file tracking. Since it works purely on Wi-Fi without the need of internet, it has low cost as compared to other internet based application and it outperforms Bluetooth in speed and range.

REFERENCES

[1] Piotr K. Tysowski, Pengxiang Zhao, Kshirasagar Naik, "Silent broadcast: Experience of connectionless messaging Using Wi-Fi P2P," in Proc.of the (ICIDT), 2012 8th International Conference on Information Science and Digital Content Technology , June 2012, pp. 239–242.

[2] MinSeok Jeon, Sun-Kyum Kim, Ji-Hyeun Yoon, Jinhee Jo, Sung-Bong Yang, "Short Paper: Seamless File Sharing for Android Devices," IEEE World Forum on Internet of Things (WF-IoT) , March 2014, pp. 189–190.

[3] "Specification of the Bluetooth system, part B: baseband specification," The Bluetooth SIG, I Dec 1999.

[4] Theodoros Salonidis, Pravin Bhagwat, and Leandros Tassiulas, "Proximity awareness and fast connection establishment in Bluetooth," Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '00). II Aug. 2000

[5] Woodings, R.W.; Joos, D.O.; Clifton, T.; Knutson, C.D.; , "Rapid heterogeneous ad hoc connection establishment: accelerating Bluetooth inquiry using IRDA," Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE , vol. , no., pp. 342- 349

[6] I. Kelnyi, G. Cscs, B. Forstner, and H. Charaf, Peer-to-Peer File Sharing for Mobile Devices. Dordrecht: Springer, 2007, ch. 15, pp. 311–324.

[7] mbit.tv, "Mobile file sharing," available online at http://mbit.tv/index.jsp.Last accessed on June 8, 2010.

[8] Wi-Fi Alliance Technical Committee P2P Task Group, "Wi-Fi peer-to-peer (P2P) technical specification version I.I,"

[9] G. Ding and B. Bhargava, "Peer-to-peer file-sharing over mobile ad-hoc networks," in Proc.of the 2nd IEEE annual conf. on pervasive computing and communications workshops, march 2004, pp. 104–108.

[10] H. Pucha, S. Das, and Y. Hu, "Ekta: An efficient dht substrate for distributed applications in mobile ad hoc networks," in Proc. of the 6th IEEE workshop on mobile computing systems and applications, 2004.

[11] B. Tang, Z. Zhou, A. Kashyap, and T. Chiueh, "An integrated approach for p2p file sharing on multi-hop wireless networks," in Proc. of the IEEE International Conference on wireless and mobile computing, networking and communication, 2005, pp. 268–274.

[12] M. Conti, E. Gregori, and G. Turi, "A cross-layer optimization of gnutella for mobile ad hoc networks," in Proc.of the 6th ACM intl. symp. on mobile ad hoc networking and computing, 2005, pp. 343–354.

