International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 8955-8962

http://www.ripublication.com

"Wi-Chat" Application Using Wifi For Closed Group Communication

P. Karthikeyan[1*], S. Shilpa[2], P. A. Theofilla Paul[3]
[1]School of Information Technology and Engineering,
VIT University, Vellore
E-mail : shilpamse94@gmail.com [2], theosbeloved@gmail.com[3]

Abstract

Wi-Fi is the predominantly employed technology for wireless communication. But the Wi-Fi is inadvertently used, particularly for its internet sharing feature. Most organizations provides Wi-Fi in their premises and the employees are interconnected in that. Even though employees are interconnected they prefer communicating via mobile networks, Bluetooth for chatting and sharing of files and this is due to the unaccounted features of Wi-Fi which they are interconnected. The capabilities of Wi-Fi are feasibly stretched out for P2P communications, video and voice callings and Wi-Fi PANs are used for home automations and many such features[3]. But all these features are not fully explored and the availability of basic features like file sharing and chatting are also not well utilized as they lack in ease of use. Here propose an idea on how Wi-Fi can be used to make our daily life easier.

Keywords: Peer to Peer , Service Set Identifier, Local Area Network, Wireless Fidelity, Near Field Communication, Wireless-Fidelity Personal Area Network

Introduction

Now-a-days there is a great impact on using Wi-Fi networks as a home network. Most of the corporations have already installed Wi-Fi in their premises to offer a collaborative environment for the employees. The scenario in which an employee connects to the corporate network from a home network is of particular interest. But the prospects of using higher bandwidth capacity of Wi-Fi networks remain unexplored in great detail. Many people are unaware of the diverse functionalities of Wi-Fi and those who are aware of Wi-Fi networks are not ready to use it for sharing sensitive information due to the fact that Wi-Fi is prone to more security attacks. So users prefer communicating via SMS and mobile chat applications that access internet as these provide secured means to communicate. But all of these SMS and mobile

chat applications are payable for its network usage and requires dedicated server's responsibility and has latency issues for loading, downloading high volume data. Whereas Wi-Fi provides us with server-less fast communication and act as alternate for internet in LAN communications if its security measures are enhanced[1]. The usage of Wi-Fi can also be extended in terms of Personal Area network that can be used for connecting with various Wi-Fi enabled devices

Proposed Architecture

A. Network Design Methods

Wireless networks follow any of the following network design i) Point-To-Point- direct communication between single computers. ii) Point-To-MultiPoint- single computers connect to a centralized point which comprises many such single computers. iii)Multipoint-To-MultiPoint called Adhoc Mode –any computer can communicate with any other computers in the network. Here Wi-Fi cards operates in four modes among which Adhoc is one of the mode frequently used. The Wi-Fi modes are i) Master Mode – creates a service with specified name and provides the services for others use. ii) Managed Mode often called clients – uses the services created by master mode cards. iii) Adhoc Mode –uses MultiPoint-To-MultiPoint, master and managed mode will not be available, each Wi-Fi card can communicate with any other Wi-Fi Cards. iv)Monitor Mode – Analyzes traffic in wireless link , it cannot support communication.

B. Proposed Architecture Description

The proposed architecture uses a Adhoc based communication and describes a connection model that can be used by Wi-Fi devices say a laptop to connect and carry out functionalities like file transfer, chatting and remote access without having to connect to any global network. It provides a close range personal area network similar to that of Bluetooth networks, but works with a higher bandwidth and speed.

The connection takes place with the help of default Wi-Fi security mechanism WPA-2 that serves as the current authentication mechanism for Wi-Fi connections.[2].The users can set their own keys which can be shared among user groups and this key will be used as **the SSID** key for the connecting to the hotspot.

A recent technology called ‘Wi-Fi Direct’ enables a more straightforward connection where peers can connect with each other and share information via a P2P connection established using Wi-Fi. But at present Wi-Fi Direct is available only in few smartphones and the scope in Windows 8 machines is limited only to document printing. The hardware for enabling Wi-Fi direct and software applications that make use of it are very few and do not cover the wide spectrum of a Wi-Fi PAN.

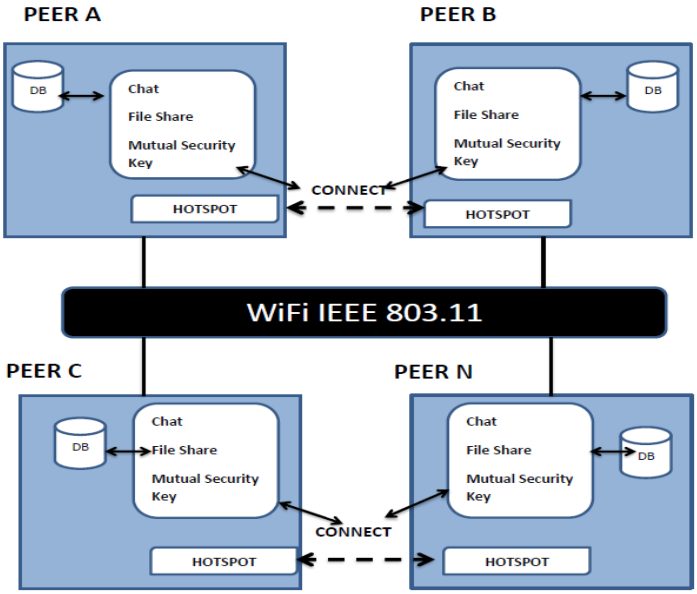


Figure 1: Proposed Architecture

C. Applications of Wi-Fi

Some of the possible applications of a WiFi network are listed down below

- Work collaboration without having to access to the Internet in an office environment
- Easier and faster transfer of huge amount of data and files.
- Remote access within a closed range
- Sharing of printers and other resources.
- Home automation
- Internet Sharing
- Synchronize between PCs and smart devices (PDAs, Smart Phones)
- Event organization
- Video calls and conferencing within closed range
- Wi-Fi calls.

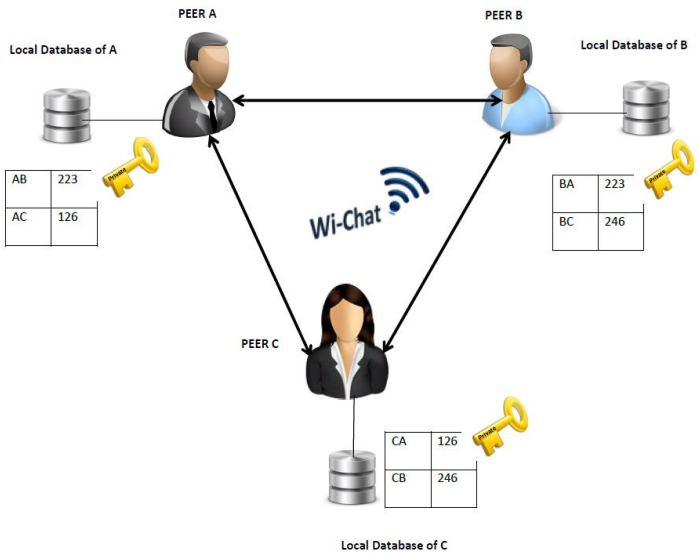
All the mentioned applications can be implemented with the help of Wifi enabled devices and supporting software without having to spend extra money for data connections via internet.

D. Wi-Chat Security

One major pitfall that is associated with WiFi is its vulnerability to security threats. Several mechanisms are in development and the most common used are VPNs, captive portals and the default WiFi authentication protocols like WEP, WPA and WPA2. In addition to these mechanisms the following suggestions can be made use of to enhance secured communication in P2P communication.

- During the connection phase, which usually takes the WPA-2 encrypted password for verification, once the peers are verified with their WPA-2 password and got connected between them , an additional private key for pair of peer is generated and stored at their database.The pair of peers connected now have this common private key stored in their local database and used for encrypting the messages during a communication. The algorithm ensures no two different pairs of peers can have the same key and there is no requirement for the transfer of the keys between the peers and keys in the local database is encrypted . The key to encrypt the database stays private with respective user and it is not shared among the peers , this key here called as DbPrivateKey. For instance, if peer A connects to B and then to C, the private key for the connection between A and B is different from that of B and C. The A, B and C have their own DbPrivateKey to encrypt and protect their local database. This ensures that the messages can be read only by authenticated users even if they somehow manage to reach an illegal receiver.
- The above mentioned idea is well suited in cases where there is a need to transfer the sensitive files or messages. In case of group chat to ensure the chat stays private among group members the same concept as mentioned above is used, the user who needs to join a group must get authenticated to the group adminWPA-2 Password, once verified the private key for the group is stored in the user local database and the user gets added as a member of the group .The member of the group is eligible to access to the messages and files shared among group members, but a member cannot individually connect to the other member in group unless they are formerly connected as peers.

Here a desktop application “Wi-Chat” developed incorporating the basic features that can be carried out via Wi-Fi connection with an established Wi-Fi hotspots between PCs. The functionalities include scanning and connecting to Wi-Fi devices, personal and group chat, local backend connectivity to store user profile, chat and file histories, option to block other users and set our status.



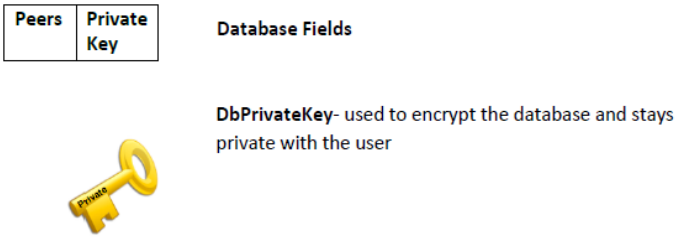


Figure 2: Wi chat Security

Processes involved in Wi-chat application:

1. Wi-Fi status = on / enable
2. Establish hotspot and set the WPA-2 password.
3. Scan the other peers (devices) in the Wi-Fi network.
4. Select the desired peer.
5. Enter the network security key and get authenticated with peer.
   //Private key for connecting peers gets generated automatically and stored.
6. Encrypt Share files or messages by using the private key in the local database.
7. Decryption used in the same private key which is common for pair of peers in their local database.
8. Encrypt the local database by providing DbPrivateKey, which is stored on local machine in encrypted form and stays private.
9. Enter into group-chat for closed group communication.
   9.1 Create a group (Admin).
   9.2 Private Key for the group created automatically and stored in admin local database.
   9.3 Set WPA-2 password for group network.
   9.4 A user who needs to join the group will get authenticated by WPA-2 password of the group network.
   9.5 The authenticated user will be added as a member and the copy of DbPrivateKey is stored in the member local database.

Screenshots

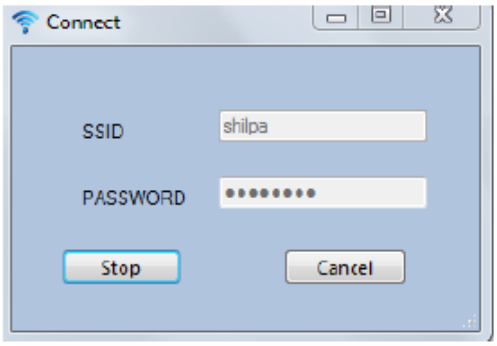


Figure 3: Creating hotspot

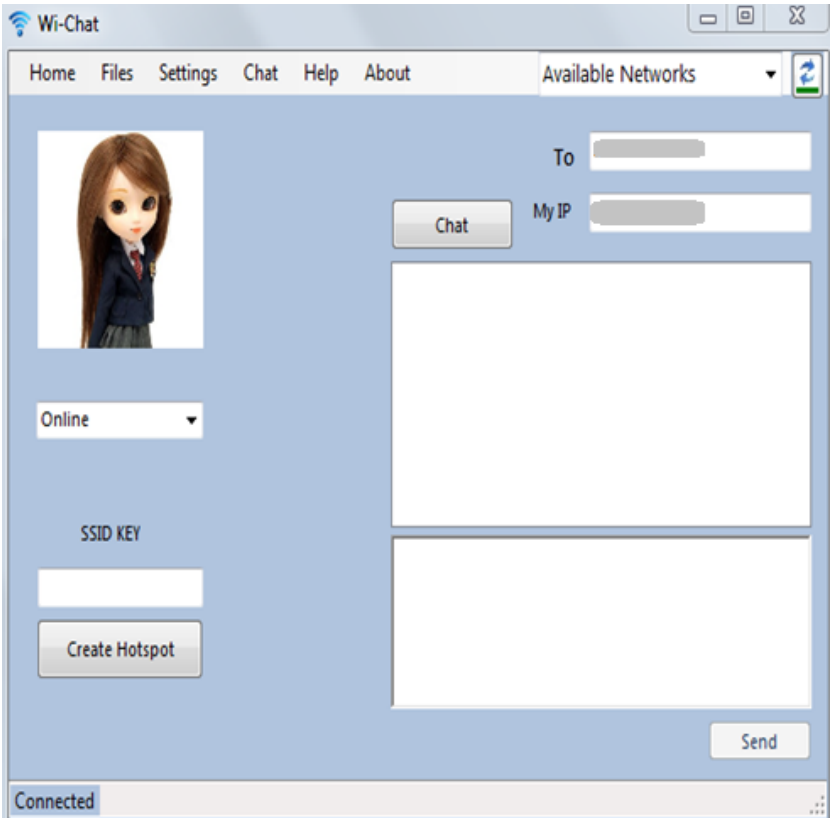


Figure 4: Homepage

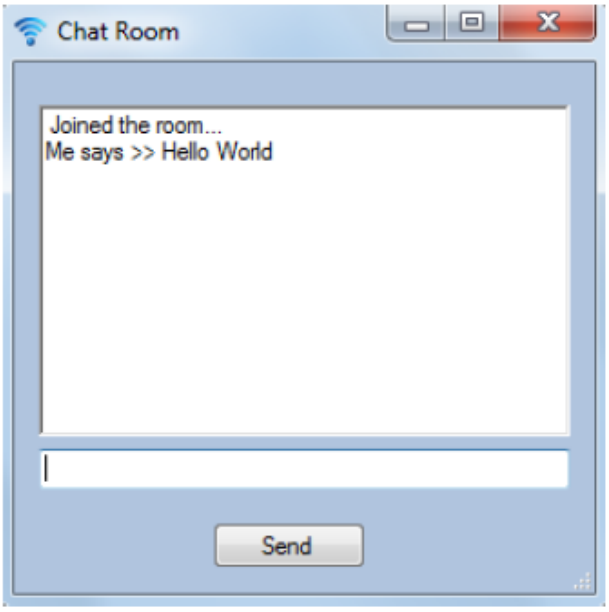


Figure 5: Chat Room

Limitations For The Proposed Systems

- Only Closed group communication is possible within the wifi range.
- WiFi signals get disrupted due to interferences from micro waves and other electromagnetic waves. Signal strength also varies from open space and buildings.
- The system is most suitable for communications within the same room or building and can be used in conferences, classrooms but requires internet connection for long distance communication.
- It uses existing encryption algorithms only and has made no improvisation on data encryption algorithms.
- Users must know each other's IP address and passcode to be connected. Though this adds security as passcodes ca n be obtained only directly from the other person, it may hinder the interactive usage of the application.

Conclusion and Futurework

LAN communication has become an indispensable means in today's organizations for meetings/conferences and other informal discussions among the employers and employees. Effective communication is required among the students community where LAN communication plays important role to share their academic materials and ideas. Hence WiFi based applications would serve all the mentioned needs expected for a LAN communication with an enhanced security.

NFCs can be used to transfer the pass codes and other profile information eliminating the need for a manual connection setup[4]. The scope and benefits of WiFi Direct technology can also be employed as an enhancement towards the usage of wifi technology. The hardware for these technologies are not readily available in all personal computers but are increasingly included in the latest smart phones and other mobile devices like Laptops, Notepads etc. Hence an improved WiFi communication along with Wifi calling can be implemented in mobile devices.

References

[1] Paul S. Henry and Hui Luo, "WiFi : What's Next?", AT & T Labs, 2002

[2] IEEE Security and privacy, "Wireless Security's Future", IEEE Computer Society, 2003

[3] Emily H. Qi, Marc Meylemans, Myro hatting, "Augmenting Wireless LAN Technology for Wi-Fi PAN", Mobile Wireless group – Intel Corporation, 2009

[4] Alfred Matos, Daniel Romao, Paulo Trezentos, "Secure HotSpot Authentication through a near Field Communication Side –Channel", Caixa Magica Software, 2012

[5] ABI Research, Wi-Fi IC Market Share Analysis and ForeCast, 2007

[6] Stuart Cheshire, Marc Krochmal, ―DNS- based service discovery‖, Expired Internet Draft, dresf-cheshire-dnsext-dns-sd-05.txt.
[7] Wi-Fi Alliance, Wi-Fi Protected Setup Specification- version 1.0, December 2006.
[8] IEEE P802.11v/7.0 Draft Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks-Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Wireless Network Management
[9] Wi-Fi Alliance, P2P Technical Group, Wi-Fi Peer-to Peer (P2P) Technical Specification v1.0, December 2009
[10] Wi-Fi Alliance, ―The State of Wi-Fi Security: Wi-Fi Certified WPA2 Delivers Advanced Security to Homes, Enterprises and Mobile Devices,‖ Wi-Fi Alliance, Tech. Rep., January 2012.