Implementation of Ad Hoc and Relay Mode in WLAN

Harshitha T N
Department of Electronics and Communication
RRCE, Bangalore-74, Karnataka,
India.

Kumudha B S
Department of Electronics and Communication
RRCE, Bangalore-74, Karnataka,
India.

***Abstract*— The ad hoc mode is used in an emerging field which places lot of contribution in networking. Now a day's people frequently communicate with smart phones in the majority cases, making calls or sending messages through internet. However, cellular based communication may not be possible after a disaster due to damages in the telecommunication or access point is destroyed by the enemy in military scenario, etc. In these situations we use the ad hoc network for communication purpose. The wireless ad hoc network consists of a collection of wireless nodes that communicate over a common wireless medium. The nodes communicate without an infrastructure, such as base station, wired access point, etc. The establishment of the network must be in distributed and decentralized manner.**

A relay network is used where the source and destination are interconnected by means of some nodes. In such a network the source and destination cannot communicate to each other directly because the distance between the source and the destination is greater than the transmission range of both of them, hence the need for intermediate node(s) to relay.

Keywords—Ad hoc, Relay, WLAN, Acess point (AP), FPGA, ARM processor, Tee* adopter, *ADP5050, Filters, Physical layer(PHY), EPCS, multi-hop, infrastructure less.

I. INTRODUCTION

A. AD HOC MODE

Ad hoc network is an autonomous system node connected with wireless link. The node in the ad hoc network communicates with other node without any physical representation. The nodes in the ad hoc organization instantly form the network whenever the communication is established. Each node in the network communicates with other node using radio waves. The entire network is distributed and nodes are collaborated with each other without fixed station access point (AP) or base station. An ad hoc network is local area network that builds an automatic connection to the nodes in the network. The wireless network architecture is be classified in two ways, first one is infrastructure where the node are connected with the fixed physical representation. Thus, the nodes are communicated through AP (Fig.1). Examples for these kinds of wireless networks are GSM, UMTS and WLAN etc. Second is infrastructure less where the node is communicated without any fixed physical representation. The ad hoc networks are formed by connecting the terminals in the multi-hop distributed architecture. Due to the absence of centralized structure, the nodes in the ad hoc network acts as router to send and receive the data (Fig. 2). Due to the non-static nature, ad hoc network avoid the single point of failure and make the network more robustness. In ad hoc network, the transmission occurs between the source and destination via intermediate nodes e.g. conference applications, intelligent devices or sensor.

Fig.1. Infrastructure based wireless networks.

Fig.2. Ad hoc wireless network.

B. *RELAY MODE*

Relay transmission can enhance coverage and throughput, while it can be vulnerable to eavesdropping attacks due to the additional transmission of the source message at the relay. Thus, whether or not one should use relay transmission for secure communication is an interesting and important problem. In this paper, we consider the transmission of a confidential message from a source to a destination in a decentralized wireless network in the presence of randomly distributed eavesdroppers. The source-destination pair can be potentially assisted by randomly distributed relays. For an arbitrary relay, we derive exact expressions of secure connection probability for both colluding and non-colluding eavesdroppers. We further obtain lower bound expressions on the secure connection probability, which are accurate when the eavesdropper density is small. By utilizing these lower bound expressions, we propose a relay selection strategy to improve the secure connection probability. By analytically comparing the secure connection probability for direct transmission and relay transmission, we address the important problem of whether or not to relay and discuss the condition for relay transmission in terms of the relay density and source-

destination distance. These analytical results are accurate in the small eavesdropper density regime.

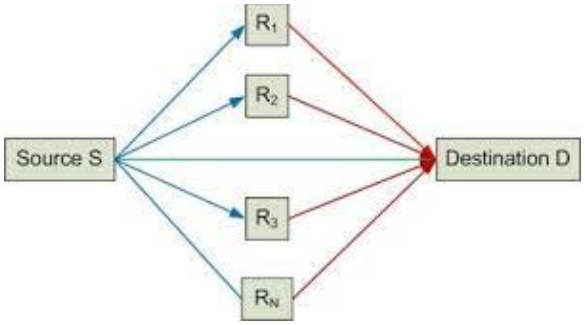

Fig.3. Relay mode

II. SYSTEM ANALYSIS

A. *Limitation of existing system*

In the existing systems, the limitations of ad hoc mode are

i. *Security*: Wi-Fi devices in ad hoc mode offer minimal security against unwanted incoming connections.

ii. *Signal strength monitoring*: The normal operating system software indications seen when connected in infrastructure mode are unavailable in ad hoc mode without ability to monitor the strength of signals, maintaining a stable connection can be difficult especially when the ad hoc devices change their position.

iii. *Speed*: Ad hoc mode often runs slower than infrastructure mode. Specifically, Wi-Fi networking standard like 802.11g require only that ad hoc mode communication supports 11Mbps connection speed.

B. *Problem definition*

Now a day's people frequently communicate with each other by using smart phones in the majority of cases, making calls or sending text messages through internet and via applications such as whatsapp, facebook and line among others. However, cellular based communications may not be possible after a disaster due to the damages in the telecommunication system. Routing protocols are use to find route for transmission of packets. Routing is the most fundamental research issue in ad hoc networking.

III. METHODOLOGY

In general Ad hoc network can be implemented anywhere with N number of nodes. Here the Block diagram consisting of three units i.e. U1, U3 and U5. Each unit consists of WLAN and laptops. The WLAN (nodes) and laptops are connected through Ethernet cables. Unit U1 and U5 are connected to U3 through tee-adopter.30dB attenuator is used to reduce the level of the signal. The data transmission can takes place between any nodes. In order to cover longer distance relay mode is implemented. If the data is corrupted or lost while transmitting then again the destination will send the request to the source. Then the retransmission takes place and the maximum attempt for retransmission is restricted .After every transmission acknowledgement as to be sent between the source and destination.

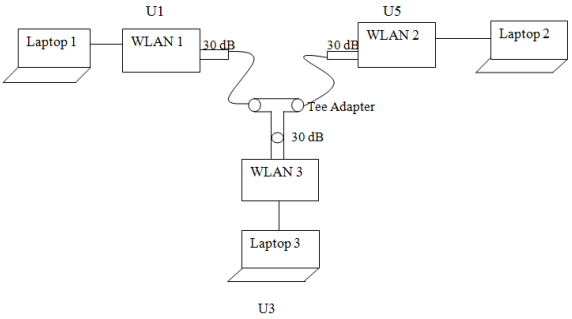

Fig.4. Block diagram of ad hoc and relay mode

IV. HRADWARE DESCRIPTION

A. *Transmission of WLAN signals*

The baseband architecture consists of a MAC layer processing module followed by an encryption module and PHY layer module (encoder/decoder). During transmission the user data from laptop/computer is forwarded to baseband card via Ethernet port.

The application either (text/video/voice) first digitized and converted to 802.3 Ethernet packets by following the Ethernet IP protocol functions. The Ethernet packets are forwarded to baseband PHY layer processor module after encryption. The baseband PHY processor module does the BPSK/QPSK/QAM16/QAM64 with OFDM (Orthogonal Frequency Division Multiplexing) modulation as per IEEE 802.11g standard. The processed PHY signals (I&Q) are sent to the RF transceiver AD9361 for digital to analog conversion of this baseband signal to specified frequency and bandwidth. The signal also gets boosted in power by power amplifier for achieving higher ranges.

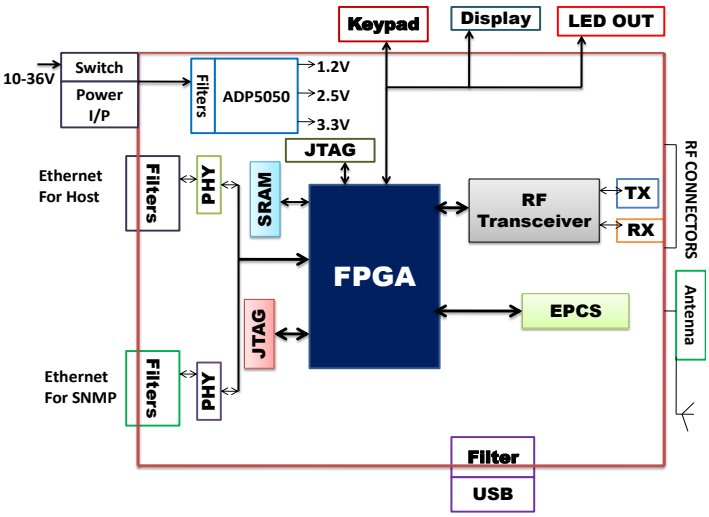

Fig.5. Transmission of WLAN signals

i. *Switch*: Switch connect segment of LAN. It contains multiple port so when a packet arrives at one port, it is copied to other port so that all segments of the LAN can see all packet.

ii. *Power input*: In our project we are using 10-36v power input.

iii. *Filters*: Basically filters are used to improve security by limiting the devices that can join the network.

iv. ADP5050: ADP5050 evaluation board can connect to high input voltage up to 15V directly without any preregulators. Here we choose the 3 voltages ranges from 1.2V, 2.5V and 3.3V.

v. PHY: PHY connects a link layer device (often called MAC) to a physical medium such as an optical fiber or copper cable.

vi. SRAM: SRAM is a type of semiconductor memory that uses bistable latching circuitry (Flip-flop) to store each bit.

vii. *JTAG*: JTAG can take control the pins of all the IC's. JTAG Is going make all CPU pins output and all FPGA make sure that the board connections are fins.

viii. *FPGA and ARM processor*: A final point is that when a VHDL model is translated into the "gates and wires" that are mapped on to a programmable logic device such as FPGA. Basically ARM processor is used for encryption purpose.

ix. *EPCS*: EPCS device is a flash memory device that can store reconfiguration data that you use for FPGA configuration purpose after power on.

x. *RF transceiver:* Main application of RF module is embedded system to communicate with another device wirelessly.

xi. USB: Universal serial port is an industry standard that was developed cables, connectors and protocols for connection, communication purpose and power supply between personal computers and their peripheral devices.

xii. RF Connectors: Coaxial RF connector (radio frequency connector) is an electrical device designed to work at radio frequencies in multi-megahertz range.

B. Reception of WLAN signals

The received signal is first processed/amplified through low noise amplifier and then the signal is down converted. Then the gain of the send to e signal is controlled automatically to give the signal to ADC. The digitized I&Q signals are send to PHY Rx processing chain. The processed 802.11g packets are reconverted to Ethernet packets by following 802.3 Ethernet protocols. These packets are sent to host application.

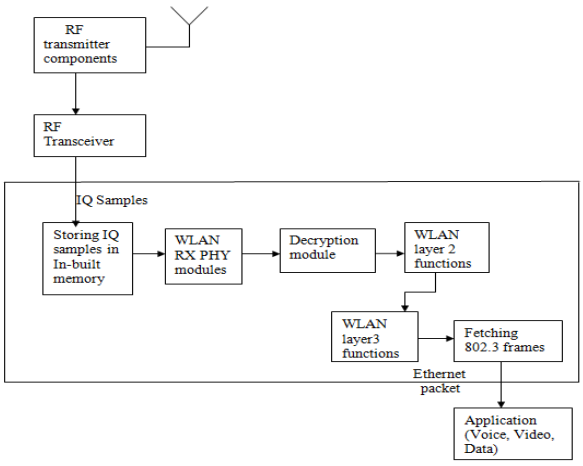

Fig.6. Reception of WLAN signals

V. APPLICATION

A. *Military arena*: An ad hoc networking will allow the military battleground to maintain an information network among the soldiers, vehicles and headquarters.

B. *Provincial level*: Ad hoc networks can build instant link between multimedia network using notebook computers or palmtop computers to spread and share information among participants (e.g. Conferences).

C. *Personal area network:* A personal area network is a short range, localized network where nodes are usually associated with a given range.

D. *Industry sector:* Ad hoc network is widely used for commercial applications. Ad hoc network can also be used in emergency situation such as disaster relief. The rapid development of non-existing infrastructure makes the ad hoc network easily to be used in emergency situation.

VI. ADVANTAGES

A. Separation from central network administration.
B. Self-configuring nodes are also router.
C. Self-healing through continuous re-configuration.
D. Scalability in-corporate the addition of more nodes.
E. Mobility allows ad-hoc networks created on the fly in any situation where there are multiple wireless devices.
F. Flexible ad-hoc can be temporarily setup at anytime, in any place.
G. Lower getting started costs due to decentralized administration.
H. The nodes in ad-hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

After studying the Ad-hoc networks in depth, we believe that they will be the future of wireless networking. It is true that performance suffers as the number of devices grows and large ad-hoc networks become difficult to route and manage. However, much time is being devoted to achieving routing stability, and a few technical issues need to be solved before they become common place. The area of ad hoc networks is a very fast growing area, and due to the vast research in them, we are seeing these problems disappear and they are coming into a world of their own.

Future Work

Mobile ad hoc networks are the future of wireless networks. Why? Because they're practical, versatile, simple, easy to use and inexpensive! We will be living in a world where our network instantly updates and reconfigures itself to keep us connected anywhere we go.

These networks provide a new approach for wireless communication and by operating in a license free frequency band prove to be relatively inexpensive.

Likewise, in education ad hoc networks may be deployed for student laptops interacting with the lecturer during classes.

Similarly, ad hoc networks for cars, sending instant traffic reports and other information. Sensors and robots forming multimedia network that allows remote visualization and control, multiple airborne routers (from tiny robots to blimps) automatically providing connectivity and capacity where needed (e.g., at a football game); an ad hoc network of spacecrafts around and in transit between the Earth and Mars.

ACKNOWLEDGMENT

I would like to thank principal Dr. R Balakrishna and Dr. L Rangaiah HOD department of electronic and communication and management of RajaRajeswari Group of Institutes for extending encouragement and support to represent the paper in National conference.

REFERENCES

[1] Siva Ram Murthy & B.S. Manoj, "Ad Hoc Wireless Networks Architectures and Protocols", Pearson Education, 2nd Edition, 2005.
[2] Amresh Kumar "A Survey on Current & Traditional Routing Protocols for Ad Hoc Wireless Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.10, October 2013.
[3] Chakrabarti, "Quality of Service in Mobile Ad Hoc Networks", Handbook of Ad Hoc Wireless Networks, CRC press, 2003.
[4] Sunita Prasad and Zaheeruddin, "A REVIEW AND COMPARISON OF QUALITY OF SERVICE ROUTING IN WIRELESS AD HOC NETWORKS", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011.
[5] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April 1999.
[6] http://en.wikipedia.org/wiki/Wireless_ad_hoc_network.
[7] http://www.ijarcsse.com/docs/papers/Volume_3/6_June2013/V3I-0379.pdf
[8] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=138596.
[9] http://www.cs.jhu.edu/~cs647/intro_adhoc.pdf.