Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on IEEE 802.11 WLANs

Amanjot Singh Toor*
PhD Scholar
Department of Instrumentation & Control Engineering
Dr. B.R Ambedkar National Institute of Technology
Jalandhar, Punjab, India

A. K. Jain
Professor
Department of Instrumentation & Control Engineering
Dr. B.R Ambedkar National Institute of Technology
Jalandhar, Punjab, India

Abstract— Over the past few decades, world has witness significant progress in the area of wireless networking. Wireless networking is gradually replacing the wired networks. This paper surveys about IEEE 802.11 WLANs in detail.

Keywords— Wireless Local Area Network (WLAN), IEEE802.11, DCF AND PCF.

I. INTRODUCTION

The motivation behind the development of Wireless technologies is to provide services comparable with the wired networks, easy to install and provides any time ubiquitous access. Wireless Networks can be of various forms like WLAN, WMAN, and WPAN [1]. But, here authors have focused on WLANs Networks. A wireless Network (WLAN) is a type of network that uses wireless data connections for data transmission (short-to-medium distances) as compared to the wired network. Wireless networking is not only less expensive than more traditional wired networking but also much easier to install. With the Origin of wireless networking technology, computer networks are not only using a wireless communication but also using specific amount of bandwidth for communication. Due to this, nowadays user can have ubiquitous access to the network resources anywhere at any place and at any time. Today Wireless networks have become a widespread adoption in every environment or market like laptops, PCs, cell phones, MP3 players, offices and even at incorporative offices. With the development of wireless technology, there is a huge amount of security threats from outside intruders in case of internal connections which is not much provided in wired connections. Also in future, wireless technology will be a great stepping-stone for providing secure connection to any wireless communication.

In the rest of the paper, Section II includes taxonomy of wireless network, Section III defines IEEE 802.11 standards and in Section IV, the WLAN protocol architecture is defined and in Section V, the benefits IEEE 802.11 network is given. Finally the last section gives the conclusion of the whole paper.

II. TAXANOMY OF WIRELESS NETWORKS

perceive quality of wireless network is that the packets are communicated between the different users are through wireless links mostly via radio waves (air), provided that the receiver is within the transmission range of the transmitter. So this feature of wirelessly transmission helps in the connection of laptops to the internet or between your business network and its applications. Also for businesses, Wireless networks give more mobility and flexibility by allowing employees to stay connected to the Internet and to the network as they roam. This provides workability to show how a wireless network is constructed and originated. Examples of wireless network include satellite communication, cellular networks, Wi-Fi LAN, terrestrial microwave networks and many more [2].

III. IEEE 802.11 STANDARDS

The Institute of Electrical and Electronics Engineers (IEEE) has produces a number of standards referred to as 802.X, which involves LANs (Local Area Network), MANs (Metropolitan Area Network) and PANs (Personal Area Network). The committee of IEEE 802.X is divided into Working Groups (GS) numbered 802.1 through 802.17. The most common wireless Working Groups and their descriptions are as follows [3]:

- 802.11- Wireless LAN standards (WLANs)
- 802.15- Wireless PAN standards (WPANs)

The IEEE 802.11 standard was first introduced in 1997 which provide data rate up to 2 Mbps at 2.4 GHz. IEEE 802.11 standards is most researched standard. An Overview of various members of IEEE 802.11 family has been provided in Table I [12].

The IEEE standard initiates two modes for operation of wireless networks [7,11], specifically named as, the infrastructure networks and the ad hoc networks.

A. Infrastructure Networks/Basic Service Set(BSS)

In an Infrastructure mode (Figure 1), wireless networking bridges a wireless network to a wired Ethernet network through wireless access point (AP). The AP and all local wireless clients must be configured to use the same network. The AP is cabled to the wired network to allow wireless clients to access. For example, Internet connections or printers.

TABLE I: An Overview of IEEE 802.11 Family

Release Year	Protocol	Purpose
1997	802.11	2 Mbps, 2,4 GHz standard (original standard)
1999	802.11a	54 Mbps, 5 GHz physical layer standard
1999	802.11b	11 Mbps, 2,4 GHz physical layer standard
2001	802.11d	International roaming extensions for 5 GHz Band
2005	802.11e	QoS enhancements
2003	802.11g	54 Mbps, 2,4 GHz PHY layer standard (current standard)
2004	802.11h	Spectrum managed 802.11a for satellite and radar compatibility
2004	802.11i	Security enhancements
2004	802.11j	Extensions for Japan
2007	802.11k	Radio resource measurement extensions (for areas with multiple APs)
2007	802.11n	Up to 540 Mbps, 2,4 GHz higher throughput
2008	802.11p	Wireless access for the vehicular environment (WAVE)
2007	802.11r	Fast roaming between WLANs
2008	802.11s	Mesh topology support
Preliminary	802.11u	Internetworking between different WLANs
Preliminary	802.11v	Wireless network management
2008	802.11w	Protected management frames
Preliminary	802.11y	3.65–3.7 GHz PHY layer standard
2010	802.11z	Extensions to Direct Link Setup (DLS)

Additional APs can be joined to this network to increase reach of the infrastructure and support more wireless clients. Along with that, an infra-structured network is also established with quasi-static or a dynamic topology. A satellite network belongs to this which includes space segment and ground segment. The space segment includes satellites whereas ground segment includes base stations through which all transmission takes place. This base station is a critical element for communication to take place. Cellular networks and most of WLANs (Wireless local area networks) utilize this infrastructure mode network.

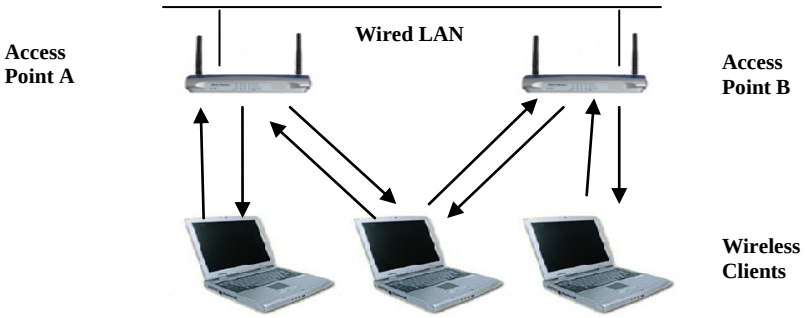

Fig.1 Infrastructure Wireless Network

All the mobile users within the transmission range of the base station are connected to this network and use it to communicate with the backbone network. A Handoff terminal is used whenever a mobile user moves away from the coverage area of its own base station which provides proxy for communication from one base station to another base station so that communication cannot be interrupted.

B. Ad hoc Networks/ Independent Basic Service Set (IBSS)

In ad-hoc mode, wireless devices are in direct communication range with each other. Ad-hoc networks are those networks that do not have any fixed topology. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points (routers). An ad hoc network mode is as shown below (Figure 2):

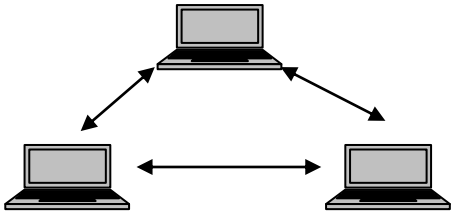

Fig.2 Ad hoc Wireless Network

And if a wireless host wants to send a packet message to another wireless host that is not in the coverage range then it will first relay the message to a host in its transmission range. This host acts as a relay to deliver the packet message to the destination user. The main advantage of this mode is that it is flexible and more robust as compared with infrastructure mode. However there are some disadvantages also like it is very difficult to perform routing due to often change in the topology (Host Mobility). In addition to that, it is very difficult to control the operation of the network because each host may have different algorithm to perform various operations like packet organizing, time synchronization and power distribution.

IV. WLAN PROTOCOL ARCHITECTURE

IEEE 802.11/WLAN follows standardized process and procedures and takes place in bottom two layers of OSI (Open System Interconnection) Reference model basically in MAC (Media Access Control) or Link layer and the Physical layer. The WLAN Architecture is as shown below (Figure 3):

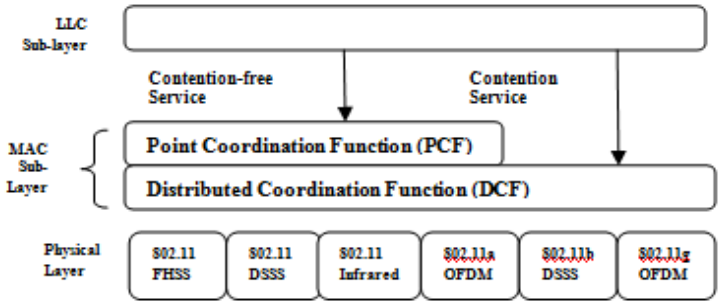

Fig.3 WLAN Architecture

A. Physical Layer

WLAN physical layer deals with the transmission and reception of radio signals. IEEE 802.11 standard provides wireless local area connectivity and it supports various types of transmission technologies:

1) Infrared (IR)

Infrared technology (IR) uses the infrared signal for transmission of data from one place to another. Line of sight propagation is must in this technology. The most common application of this is Inter-Building usage. The prime benefit of WLAN technology is that it carries high bandwidth signals. The frequency range of IR is of $3x10^{14}$ Hz with maximum coverage of up to 30 to 80 feet. The rated speed in % of 10 Mbps wire is from 50% to 100%. Along with that, this technology does not require any license for transmission.

2) Spread Spectrum including FHSS, DSSS and HR-DSSS

Spread spectrum technology is widely used these days for transmission. Here, the message/signal is spread over a wide range of frequencies in electromagnetic spectrum. The most common techniques used are Frequency Hoping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), High Rate Direct Sequence Spread Spectrum (HR-DSSS). It ranges from 902 MHz to 928 MHz; 2.4 GHz to 2.4385 GHz; 5.725 GHz to 5.825 GHz with 105 to 800 feet of maximum coverage. These techniques requires a small amount of transmit power that is of about less than 1 W. In this case, the rated speed in % of 10 Mbps wire is from 20% to 50%. For Example, for Inter-Building usage an antenna has to be used. Also, no license is required here.

3) Orthogonal Frequency Division Multiplexing (OFDM)

OFDM increases the general throughput of Access Points. Various OFDM techniques are used for multiplexing and some are used with Multi Input Multi Output (MIMO) mechanism. Mostly all the IEEE standards operate at a frequency band of 2.4 GHz, Bandwidth of 20 MHz, outdoor range of 5000 meter and with 13 different channels as specified above. The obtain ability of these channels differ from one country to another. OFDM and HR-DSS were introduced in 1999 in WLAN Family.

B. Medium Access Control (MAC)Sub-Layer

The data link layer is divided into two parts that is MAC (Medium Access Control) sub-layer and LLC (Logical Link Control) sub-layer [15]. The LLC layer is responsible for providing interface with higher layers especially with the network layer and performs flow and error control. The MAC layer of WLAN deals with the rules of how suitable exchange of formatted packets can be done between medium and data link components. It assembles the packets into frames with error detection fields. This layer provides following sessions:

1) Distributed Coordination Function (DCF)

DCF is based on the mechanism of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). DCF is a contention based method and a mandatory mode for all the stations [13]. It uses both the infrastructure and ad hoc model configuration. DCF uses to access methods for transmission; Basic Access Mechanism and RTS/CTS access mechanism.

a) Basic Access Mechanism

The Basic Access mechanism is as shown in Figure 4 below:

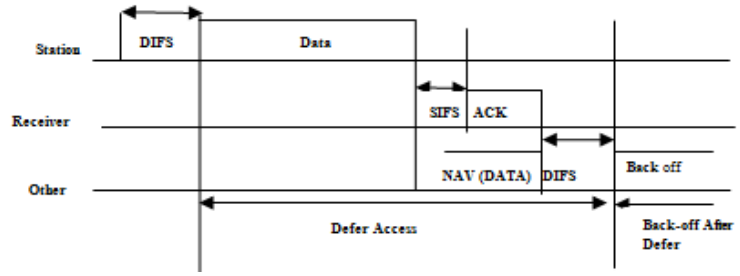

Fig.4 Basic Access Mechanism

Here, in this mechanism, any station that wants to transmit a data frame, first senses the channel to check whether the channel is free or not for some duration of time called DIFS (Distributed Inter Frame Space). If the channel is free, then the station starts transmitting the data frame to the receiver station. All the receiving stations that can hear the transmission of data frame, they can set their NAV (Network Allocation Vector) equal to the length of the transmission data frame. This is known as virtual carrier sensing mechanism. However, if the channel is sensed to be as busy by either physical carrier sensing or by virtual carrier sensing then in that case, the station needs to wait for a specific period of time. After the successful reception of data frame, the receiver station needs to wait for SIFS (Short Inter Frame Space) interval followed by the data frame, and sends an acknowledgement (ACK) signal back to the transmitting station which indicates the successful reception of data frame.

b) RTS/CTS access mechanism

The RTS/CTS Access mechanism is as shown in Figure 5 below [20]:

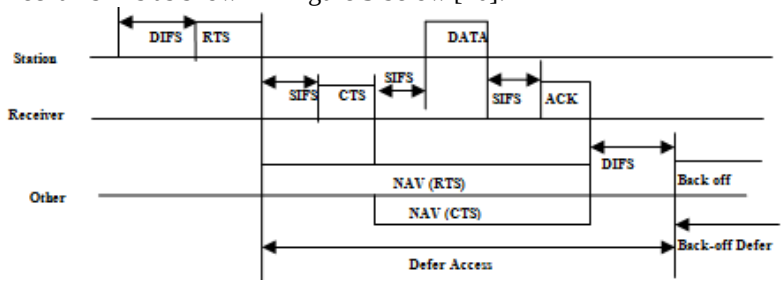

Fig.5 RTS/CTS Access Mechanism

The RTS/CTS access mechanism uses the four way handshake mechanism to reduce the bandwidth loss which occurs due to data-data collision that might occur due to hidden terminals. Here in this mechanism, a station that wants to transmit a data frame, first sense the transmission channel for DIFS (Distributed Inter Frame Space) duration. If the channel is free then a RTS (Request to Send) frame is sent to the receiver station. After the successful reception of RTS frame, the receiver station waits for a SIFS (Short Inter Frame Space) interval and then sends a CTS (Cleat to Send) frame back to the source station. After the reception of CTS, the source station starts transmitting the data frame along with SIF interval. Then, after the successful reception of data frame, the receiver waits for a SIFS interval and sends back the acknowledgement (ACK) frame back to the source station. So, a station that gets either the RTS, CTS or data frame can updates its NAV based on the duration of the corresponding data frame. Since the size of RTS/CTS frame is very small in size, the RTS/CTS access mechanism successfully helps in reducing the bandwidth of loss which occurs due to data-data collision.

2) Point Coordination Function (PCF)

PCF is an optional method which in implemented only on infrastructure network model and not in Ad-hoc networks. It is implemented on the top of DCF. PCF is a centralized polling access method. In PCF time is divided into contention free periods (CFP), where Access Points (AP) gives a station an opportunity to transmit by sending a poll message, where DCF is executed [17]. Since PCF is an optional function and it is not implemented in all the devices. To have an access to DCF stations, DCF periods are necessary. The interleaving of Contention free periods (CFP) and Contention Periods (CPs) is shown in Figure 5.

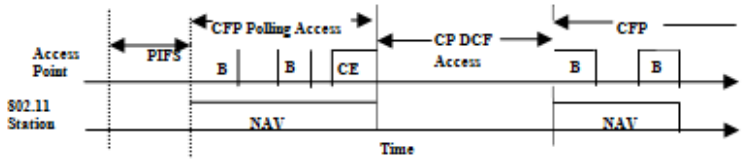

Fig.5. PCF interleaves CFPs with CPs

Here, the Access Point initiates the process by periodically sending a beacon to the Contention Free Period (CFP). The first beacon followed by a Contention Period (DCF access) is transmitted after a Point Coordination Function Inter Frame Space (PIFS). Here, the duration of PCF Inter frame Space (PIFS) is shorter than Distributed Inter Frame Space (DIFS) but longer than Short Inter Frame Space (SIFS). So it means that the initialization of CFP provides less priority than the transmission of control packets, but provides higher priority than transmission of data packets. The CFP ends when access point send a CE (CFP end) Control packets. In CFP process, only that station is allowed to transmit data that is polled by the Access points (AP) or by the destination station which receives the data and provides acknowledgement (ACK) to that received data (If applicable, combine the ACK with data in the same packet). Also in some PCF, some packets can combine together to increase the efficiency of the communication by reducing the number of MAC and PHY headers. An example [19] below illustrates the operation of PCF;

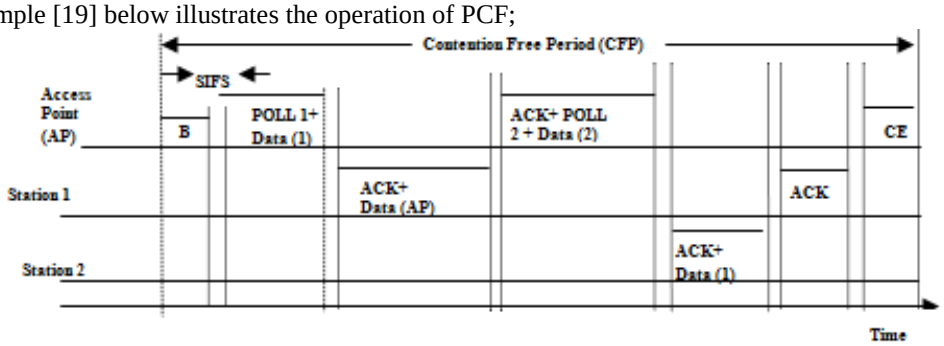

Fig.6 PCF operation

Here in this Figure 6, the Access Point (AP) transmits a beacon (B) and initiates a contention free periods (CFP). After a period of time says SIFS, it combines a poll packet along with Data and sends it to station 1. After the reception of this combined packet, station 1 sends an acknowledgement that the packet has been received. And station 1 reply to poll by sending a packet data to the Access Point (AP). Remember that this is also a combined packet. After that, the Access Point (AP) acknowledges the received data packet from station 1 and combines a poll packet with data and sends it to station 2. After the reception of this packet, station 2 acknowledges the packet back to the Access Points (AP) and transmits the data to station 1. Then after the reception of this packet, station 1 acknowledges that the packet is received. So in this way CFP is finished with the transmission of a CE packet.

V. MERITS OF WLAN NETWORKS

A. Mobility

Wireless LAN systems allows the users to an Ubiquitous Access along with mobility. Also no licence is required for Wireless LAN. WLAN is used in various applications like at home or at workplace, tthousands of universities, hotels, Coffee shops and public places use public wireless connection [5,8].

B. Installation Speed and Simplicity

The installation of wireless LAN system is very easy and fast and it eliminate the need of using wires or cables run through walls and ceilings [5,8].

C. Reduced Cost-of-Ownership

As wireless networks eliminate or lessen the use of wiring connection, which helps in reducing the cost of overall wireless network [5, 8].

D. Scalability

Wireless Networks can be configured in a variety of topologies to meet the needs of specific applications and installations. So it is highly scalable network [5,8].

E. Convenience

The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (a home or office). With the increasing use of laptops now-a-days, this is particularly relevant [5,8].

F. Expandability

Wireless networks can increase the number of clients with the existing equipment (Router). Whereas in case of a wired network, additional clients means it would require additional wiring [5,8].

VI. LIMITATIONS OF WLAN NETWORKS

A. Power and Energy

A mobile device is mostly handy and small size devices which normally operate on its power source [5,6,7,8]. And this power source supplies power until it is installed in a fixed manner. In that case a mobile device needs to operate in an efficient and intelligent manner so that certain operations for communication can take place.

B. Data Rate

Data Rate may be defined as the number of bits transmitted per second. It may depend upon various factors like data compression algorithm, power control and the data transfer protocol [5,6,7,8]. So, it is essential that a manufacturer must thought well on these factors before designing so as to achieve higher data rates. Data compression algorithms play an important factor in various multimedia applications like video conferences. In that case, MPEG-4 is used to compress the video of the order of 75 to 100. So the challenge now is to improve these data compression algorithms to produce high quality audio and video signal at these compression rates. Due to this, the compressed data is more sensitive to network errors and interference. Now the use of algorithm for protection of data is must. One more way to advance the data rate is to engage intelligent data transfer protocols which maintain the traffic characteristics and adapt the time-varying network.

C. Handoff

In wireless networking, all devices are free to move anywhere but with the condition of maintaining the ongoing connection [5,6,7,8]. So for that purpose, a handoff occurs when a mobile user moves from one coverage area of a base station to another one in case of infrastructure network. A protocol is therefore required to ensure smooth transition of calls during a handoff. These protocols decide when a handoff should take place and how data is routed during his process of handoff. Also some packets are lost occasionally in this case. Whereas in case of ad-hoc network, a topology is changed when mobile user moves from one coverage area to another. Since this type of network consists of a large number of mobile users, so this forces a significant challenge for designing an efficient routing protocol that work well in any environment with frequent topological changes.

D. Signal Fading

As we know that in wireless networking, a signal must propagate through a wireless medium basically through the air or radio waves [5,6,7,8]. So the signal may get distorted or weakened due to propagation through the open, unprotected and changing medium with irregular boundary. This distortion occurs due to many factors like reflection, diffraction and scattering caused by obstacles before the signal reaches the destination and this signal is notably distorted and attenuated as compared to the signal that is transmitted from the receiver side. As a result of this receiver is unable to recognize the signal. So this causes a large number of packets to be lost.

E. Quality of Service(QoS)

Quality of Service is a most significant challenge in wireless networking. It may be defined as the performance of the network, particularly seen by the users of the network [5,6,7,8]. It reflects the available network transmission quality and services. Quality of service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, grade of service, etc. An important characteristic of wireless network includes handoff, dynamic connections and actuating transport QoS (throughput, delay, and loss rate). In a wireless environment, connections may be temporarily broken during a process called handoff. Loss rate should only reflect losses due to buffer overflow or transmission errors. Also, connection interruption is another important performance parameter in wireless network. For example, a voice connection will not be broken more than once per minute. So a low interruption in frequency means that a handoff do not occur too often.

F. Security

Security is one of the major demerits of management issues in wireless networking especially in e-commerce and m-commerce. The main objective of security is to provide confidentiality, authentication, ensuring integrity and access control [5,6,7,8]. As we know that network configuration and reconfiguration is easier, less expensive and faster in case of wireless network. However, it also generates new threats and attacks to the existing information security. For example, as communications takes place "through the air" that is by using radio frequencies; the risk of interception is greater here. If the message is not encrypted properly, or it is encrypted with an inadequate algorithm, the intruders can easily read it, thereby compromising confidentiality. Also IEEE 802.11 standard provides wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the workstation and wireless LAN access points. Also virtual private network (VPN) is another way to access the network in a reliable way. So that's why a wireless security features needs to be updated constantly.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network

[2] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/what_is_a_wireless_network/index.html

[3] www.nettwerked.net/GHU/Docs/IEEE.htm

[4] IEEE 802.11-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 12, 1999.

[5] Shreya Jain, Sukhwinder Singh, "Basic Review Of Wireless Networks", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering Vol. 2, Issue 3, pp-1278-1280, March 2014.

[6] Sandra Kay Miller ―Facing the Challenge of Wireless Security‖ July 2001.
[7] Aniruddha Singh, Abhishek Vaish, Pankaj Kumar Keserwani, "Research Issues and Challenges of Wireless Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, pp-572-575, February 2014.
[8] Raj Kumar Singh, Dr.A.K.Jain, "Research Issues in Wireless Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4,pp-115-119, April 2012.
[9] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering ,Vol. 3, No. 3, pp-77-86, July, 2008.
[10] M A Khan, Tazeem Ahmad Khan, M T Beg, "RTS/CTS Mechanism of MAC Layer IEEE 802.11 WLAN in Presence of Hidden Nodes", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012.
[11] Sourangsu Banerji, Rahul Singha Chowdhury, "On IEEE 802.11: Wireless LAN Technology", International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, Issue. 4, 2013.
[12] Mehmet S. Kuran, Tuna Tugcu, "A survey on emerging broadband wireless access technologies", in Elsevier B.V, Computer Networks 51, pp-3013–3046, 2007.
[13] Sarah Shaaban, Dr. Hesham M. El Badawy, Prof.Dr. Attallah Hashad, "Performance Evaluation of the IEEE 802.11 Wireless LAN Standards", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, London, U.K, July 2 - 4, 2008.
[14] Uthman Baroudi, Mohammed Aijaz Mohiuddin, "Performance analysis of Internet applications over an adaptive IEEE 802.11 MAC architecture", The Franklin Institute. Published by Elsevier Ltd, 343, pp-352–360, 2006.
[15] Shiao-Li Tsao, Chung-Huei Huang, "A survey of energy efficient MAC protocols for IEEE 802.11 WLAN", 2010 Elsevier B.V., Computer Communications 34,pp- 54–67, 2011.
[16] Daji Qiao, Sunghyun Choi, Amjad Soomro, Kang G. Shin, "Energy-efficient PCF operation of IEEE 802.11a WLANs via transmit power control", 2002 Elsevier Science B.V., Computer Networks 42, pp-39–54, 2003.
[17] Moustafa A. Y oussef , Arunchandar V asan , Raymond E. Miller, "Specification and Analysis of the DCF and PCF Protocols in the 802.11 Standard Using Systems of Communicating Machines" Department of Computer Science University of Maryland College Park, MD 20742.
[18] Raul Palacios, Fabrizio Granelli, Danica Gajic, Christian Liß, Dzmitry Kliazovich, "An Energy-efficient Point Coordination Function Using Bidirectional Transmissions of Fixed Duration for Infrastructure IEEE 802.11 WLANs", IEEE ICC 2013 - Communication QoS, Reliability and Modeling Symposium.
[19] Leena Chandran-Wadia,Shruti Mahajan and Sridhar Iyer, "Throughput Performance of the Distributed and Point Coordination Functions of an IEEE 802.11 Wireless LAN" Department of Electrical Engineering Indian Institute of Technology Bombay, Powai, Mumbai – 400 076.
[20] Giuseppe Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", IEEE journal on selected areas in communications, vol. 18, no. 3, pp-535-547, march 2000.
[21] Yu Zheng, Kejie Lu, Dapeng Wu, and Yuguang Fang, \Performance Analysis of IEEE 802.11 DCF in Imperfect Channels," Sep 2006.
[22] https.kbserver.netgear.com/kb_web_files/N100688.asp.

