

Specification Performance of WLAN Parameters with MatLab Simulink of IEEE 802.11

Noora H. Sherif¹, Ghufran Saady Abd-almuhsen²
¹Al-Turath University College
²Madenat Alelem University College
 (noora.hani.na@gmail.com, ²ghufransaady@yahoo.com)

Abstract-Wireless networks have gained popularity, providing users flexibility and mobility in accessing information. The IEEE 802.11 Wireless Local Area Network (WLAN) standard has become the dominant architecture in practice. In this paper IEEE 802.11 standard implemented in Mat lab Simulink, where Allowing to modify beacon frame parameters such as beacon interval, SSID, supported rates, etc. also include or exclude the CF parameter set element from the generated beacon frame, DBPSK and DQPSK modulation techniques BER performance included in this paper to illustrate the performance of the model in AWGN and Rayleigh channels.

Keywords- IEEE Standard, IEEE 802.11, MAC layer, DBPSK, DQPSK

I. INTRODUCTION

Wireless networks are emerging as a significant aspect of networking; wireless local area networks WLANs, Bluetooth, and cellular systems have become increasingly popular in the business and computer industry, with consequent security issues. WLANs, especially the Institute of Electrical and Electronics Engineers (IEEE) 802.11 networks, are becoming common access networks in private and public environments. The freedoms of movement and simplicity in its implementation have made WLANs popular in the home and businesses sectors, as well as hotspots 1 such as airports and cafes. The increasing availability of and therefore increasing reliance on, wireless networks makes it extremely important to maintain reliable and secure communications in the wake of network component failures or security breaches. However, recent news reports on a number of attacks against wireless networks, especially WLANs, have alarmed wireless adopters, developers, and intended users. The broadcast nature of wireless communication links makes them unique in their vulnerability to security attacks and their susceptibility to intentional threats. Organizations that want to deploy a secured WLAN infrastructure are challenged by the flaws in the existing wireless mechanism design, such as the wired equivalent privacy (WEP) protocol. WLANs provide greater flexibility and scalability than traditional LANs. Unlike a wired LAN, which requires a wire to access the network, a WLAN facilitates network transmissions of data from computers and other components through an access point (AP). An AP typically provides a range (cell or area coverage) of 100

metres. IEEE 802.11 is an international standard providing transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The 802.11b is the dominant WLAN technology at present [WECA, 2001b], and provides an expected data throughput of 5.5 Mbps. High performance radio LAN is a European Telecommunications Standards Institute (ETSI) standard operating in the 5 GHz frequency band; Hiper LAN/1 has a transmission speed of 19 Mbps, while Hiper LAN/2 operates at 54 Mbps. Hiper LAN/2 supports quality of service (QoS) and is based on an infrastructure topology, whereas Hiper LAN/1 is more suitable for forming ad-hoc networks.

II. IEEE 802.11 STANDARD

The standard provides three *physical* (PHY) layers and one *medium access control* (MAC) layer for deploying wireless communication in local networks (Fig. 1). As for the *logical link control* (LLC) layer, there is no difference between wireless (802.11) and wired (802) LANs, such as the IEEE 802.3 Ethernet network. The MAC protocol provides two service types: asynchronous using the *distributed coordination function* (DCF), and synchronous using the *point coordination function* (PCF) that is contention-free. [1].

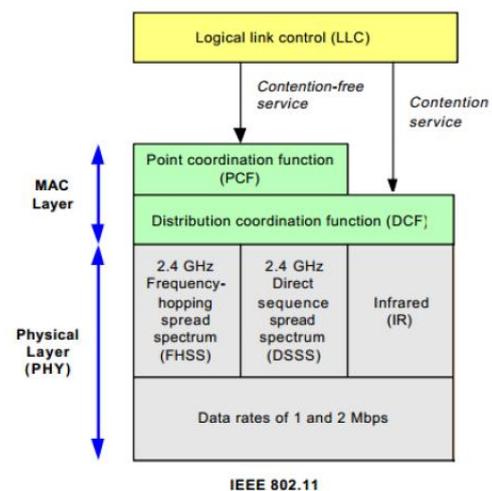


Figure 1. The 802.11 Protocol Stack

The 802.11 standard is a family of specifications originally providing a 1 to 2 Mbps data transmission rate using either the frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). After revisions, the standard includes 802.11a, operating in a 5 GHz frequency band at 54 Mbps, and 802.11b and IEEE 802.11g, operating in a 2.4 GHz frequency band at speeds of 11 Mbps and 54 Mbps, respectively. [2,4]

The 802.11 standard takes advantage of radio spectrum technologies, allowing multiple users to share the radio frequencies without end-user licenses. Specifically, it makes use of the 2.4 GHz Industrial, Scientific, and Medical band (ISM) band for 802.11 and 802.11b networks, and the 5 GHz Unlicensed National Information Infrastructure (UNII) band for 802.11a-based networks. The International Telecommunication Union (ITU) defines both bands. However, interference issues remain, especially in the 2.4 GHz band; if the technology interferes with an authorized operation such as an airline radio frequency, it will cease to operate. In addition, there is no protection from other technologies, such as Bluetooth, accessing 802.11 frequencies. A portal is a logical point, which is required to integrate the 802.11 architecture with existing wired LANs facilitating the transmission. An AP with software implementation can offer the portal service. [5,6].

III. MAC LAYER

The 802.11 specifications provide asynchronous (DCF) and contention-free (PCF) services. The asynchronous service is always available whereas the contention-free service is optional. DCF implements the basic access method of the 802.11 MAC protocol, or path sharing. The PCF provides contention-free service, which implements a polling access method. It uses a point coordinator (PC), usually the AP, which cyclically polls stations, giving them the opportunity to transmit. Thus the access priority provided by a PCF may be utilized to create a contention-free access method. The PC controls the frame transmissions of the stations in order to eliminate contention for a limited period of time. Unlike the DCF, the implementation of the PCF is not mandatory. Furthermore, the PCF itself relies on the asynchronous service provided by the DCF (Fig.1). All physical layers support one common MAC layer. Task Group 802.11e focuses on enhancing the MAC layer for QoS. [7, 8]

IV. PHYSICAL LAYERS

The physical layer processes data to and from radio signals over the airwave. In other words, it handles the transmission of the frame via the air interface. The standards define three alternative physical layers (Figure 2):

1. Frequency-hopping spread spectrum (FHSS)
2. Direct sequence spread spectrum (DSSS)
3. Infrared (IR)

The first three physical layers belong to radio spread spectrum technology that operates in the 2.4 GHz band, while OFDM operates in the 5 GHz band. IR operates in the 300-428 GHz band and operates at a slow speed with line-of-sight connection. IR has become a legacy protocol thus will not be addressed in this discussion [8]

A. FHSS

FHSS modulates data signals with a carrier signal that hops from one frequency to another, using time as its measurement, over a wide range of frequencies. The carrier frequency (between 2.4 and 2.483 GHz) is changed periodically to avoid collisions. A collision occurs only when both a narrowband system and the spread spectrum signals are transmitting at the same frequency simultaneously. A hopping code is used to decide the order of data transmission and which frequency to hop to. FHSS provides a maximum data transmission speed of 2 Mbps [9].

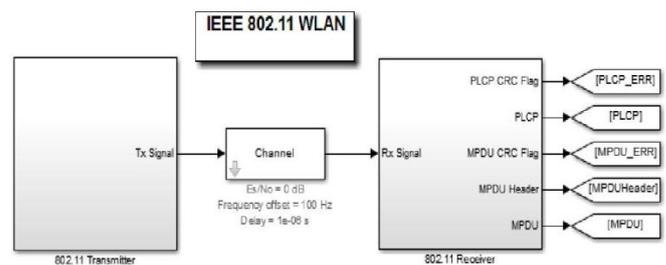


Figure 2. IEEE 802.11 Simulink model

B. DSSS

DSSS combines a data signal at the sending station with a higher data rate bit sequence, known as the chipping code or processing gain. This chipping code reduces interferences by dividing the user data according to a spreading ratio, enabling a faster data transmission rate of 11 Mbps. It sets a specific string of bits to be sent for each data bit. A redundant bit pattern is included in the chipping code to increase resistance to interference.

V. WLAN IEEE 802.11 SIMULINK MODEL

IEEE 802.11 have been implemented with Matlab Simulink as shown in fig.2, where the model has three main parts: Model Parameters, where the information can be selected and sent within the beacon frame and the channel parameters, 802.11 System, which is formed of the transmitter, channel, and the receiver, Results, where there is a viewing to the most important received information, such as CRC flags, packet type, and received SSID.

The transmitter implements a lightweight MAC sub layer and physical layer that construct the PHY layer frame as shown in fig. 3. It transmits each PHY frame using several consecutive channel frames.

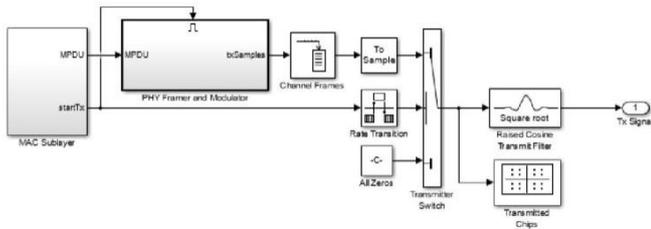


Figure 3. The transmitter block in the IEEE 802.11 Simulink Model

The MAC sub layer constructs the beacon frame, which is a type of a management frame. Fig.4 shows the management frame format. This frame is also called a MAC protocol data unit (MPDU).

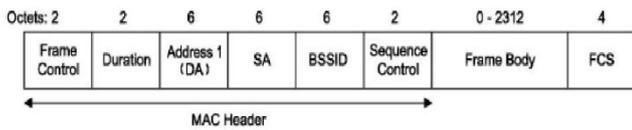


Figure 4. MAC sublayer beacon frame

The implements a beacon frame with a frame body that contains the following fields: Timestamp, Beacon interval, Capability, SSID elements, supported rates element, Direct sequence (DS) parameter set element, Contention Free (CF) parameter set element (optional) The transmitter turns on periodically to transmit a beacon frame. The beacon interval parameter determines the transmission period.

The PHY Framing and Modulator creates as shown in figure 5 and 6, the PLCP protocol data unit (PPDU) by adding the physical layer convergence procedure (PLCP) preamble and header to the MPDU. The PLCP preamble contains 128 bits of ones (SYNC), which are later scrambled. The receiver determines the presence of a PPDU frame using this SYNC signal. The LENGTH field of the PLCP header determines the MPDU frame length. PLCP header also contains a 16-bit CRC.

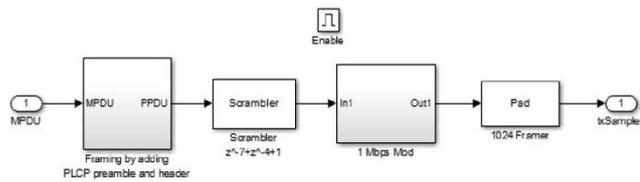


Figure 5. PHY Framing and Modulator block



Figure 6. 1Mbps Mod block

The transmitter scrambles the PPDU frame, modulates using differential binary phase shift keying (DBPSK or DQPSK) at a rate of 1 Mbps, and applies spreading using a length 11 Barker code. This subsystem also pads extra chips to the spread symbols to reach a 1024-bit maximum PPDU length. This way, the system forces the MAC layer to work at a period of 1024 microseconds, which is a time unit (TU).

The transmitter emits 128 modulated symbols (1408 chips), which is a channel frame, at a time. Modulated symbols pass through a square root raised cosine pulse shaping filter. Pulse shaped symbols are sent through an AWGN channel that also applies a frequency offset and delay.

A **Barker code** or **Barker sequence** is a finite sequence of N values of $+1$ and -1 , with the ideal autocorrelation property, such that the off-peak (non-cyclic) autocorrelation coefficients.

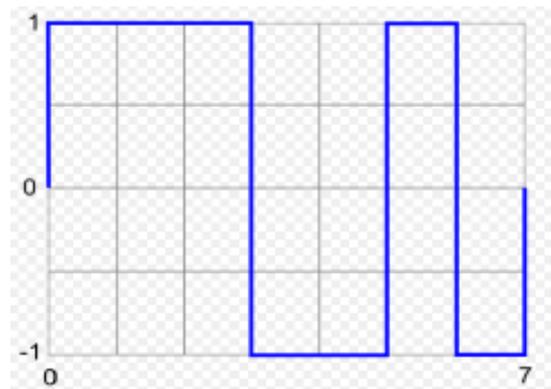


Figure 7. Graphical representation of a Barker-7 code

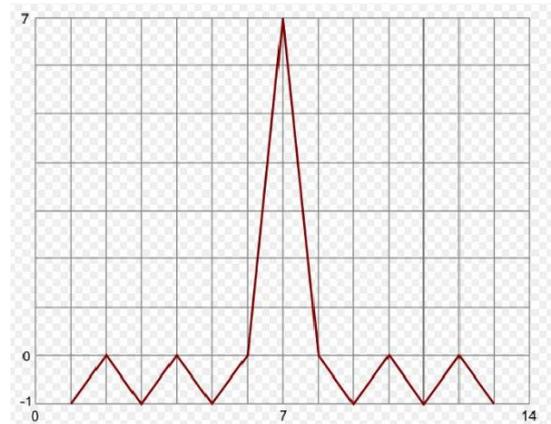


Figure 8. Autocorrelation function of a Barker-7 code

A Barker code has a maximum autocorrelation sequence which has side lobes no larger than 1. It is generally accepted that no other perfect binary phase codes exist [3]. (It has been proven that there are no further odd-length codes [3], nor even-length codes of $N < 10^{22}$.) [3,4].

Barker codes of length N equal to 11 and 13 are used in direct-sequence spread spectrum and pulse compression radar systems because of their low autocorrelation properties (The side lobe level of amplitude of the Barker codes is $1/N$ that of the peak signal). [3, 4] A Barker code resembles a discrete version of a continuous chirp, another low-autocorrelation signal used in other pulse compression radars.

The positive and negative amplitudes of the pulses forming the Barker codes imply the use of bi-phase modulation or binary phase-shift keying; that is, the change of phase in the carrier wave is 180 degrees.

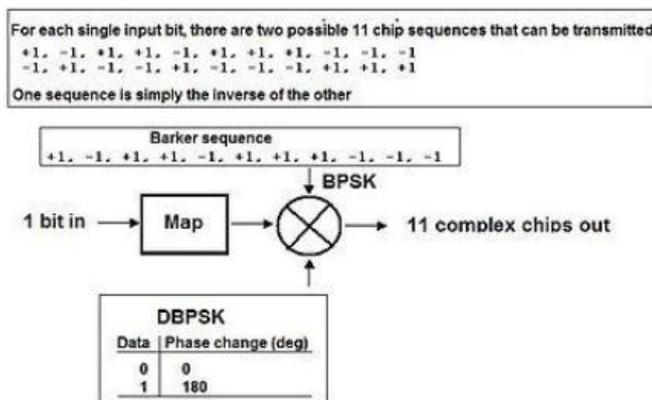


Figure 9. Barker code used in BPSK modulation

Similar to the Barker codes are the complementary sequences, which cancel side lobes exactly when summed; the even-length Barker code pairs are also complementary pairs. There is a simple constructive method to create arbitrarily long complementary sequences.

For the case of cyclic autocorrelation, other sequences have the same property of having perfect (and uniform) side lobes, such as prime length Legendre sequences and maximum length sequences (MLS). Arbitrarily long cyclic sequences can be constructed.

In wireless communications, sequences are usually chosen for their spectral properties and for low cross correlation with other sequences likely to interfere. In the 802.11b standard, an 11-chip Barker sequence is used for the 1 and 2 Mbit/sec rates. The value of the autocorrelation function for the Barker sequence is 0 or -1 at all offsets except zero, where it is $+11$. This makes for a more uniform spectrum, and better performance in the receivers [3, 4].

VI. THE RESULTS

Simulink model that implemented in this paper allowing to modify beacon frame parameters such as beacon interval,

SSID, supported rates, etc. also include or exclude the CF parameter set element from the generated beacon frame as shown in figure 10 setting the noise level (E_s/N_0), delay, and frequency offset introduced by the channel.

Received MPDU	
Time stamp (usec):	1052672
Beacon interval (TU):	2
SSID:	MathWorks SDR team
Supported Rates (Mbps):	[1 2]
DS Parameters:	Received
Channel number:	11
CF Parameters:	Received
CFP Count:	2
CFP Period:	20
CFP MaxDuration (TU):	10
CFP DurRemaining (TU):	5

Figure 10. Received MPDU

The simulation also displays the scatter plots of transmitted and received chips, and the despread symbols as shown in figure 11-13 respectively. You can see the rotating scatter plot due to the frequency offset. The differential demodulator is able to track the phase change and correctly demodulate the symbols.

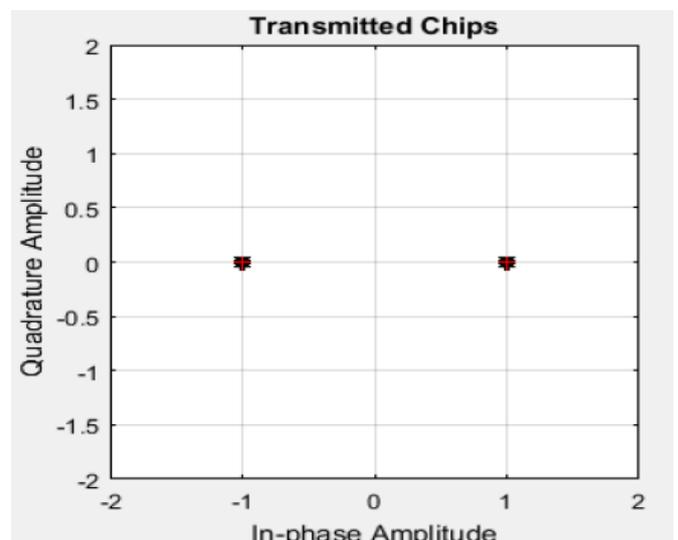


Figure 11. Scatter plot of transmitted chip

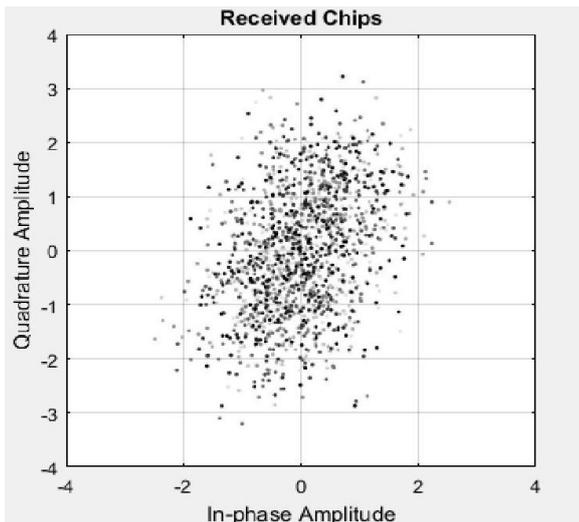


Figure 12. Scatter plot of received chip

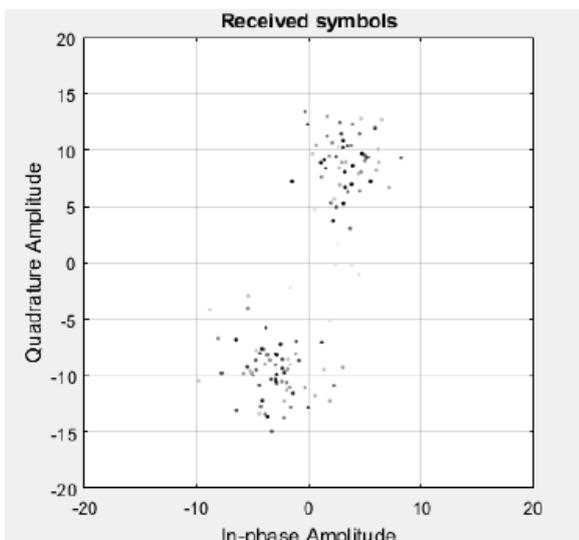


Figure 13. The despread symbols

Modulation techniques that used in the Simulink model which are DBPSK and DQPSK are tested under AWGN channel, figure 14 shown BER parameter of both modulation techniques where DBPSK shows better BER with 2dB gain in E_b/N_0 . while in Rayleigh channel both techniques shows same BER as shown in figure 15.

VII. CONCLUSION

In this paper IEEE 802.11 standard implemented in Matlab Simulink where transmitter, channel and receiver designed. Allowing to modify beacon frame parameters such as beacon interval, SSID, supported rates, etc. also include or exclude the CF parameter set element from the generated beacon frame and displaying the scatter plots of transmitted and received chips,

and the despread symbols. Modulation techniques that used in the Simulink model which are DBPSK and DQPSK are tested under AWGN channel and Rayleigh channel. DBPSK shows better BER with 2dB gain in E_b/N_0 . while in Rayleigh channel both techniques, Wireless networks have gained popularity, providing users flexibility and mobility in accessing information. IEEE 802.11 networks, are becoming common access networks in private and public environments.

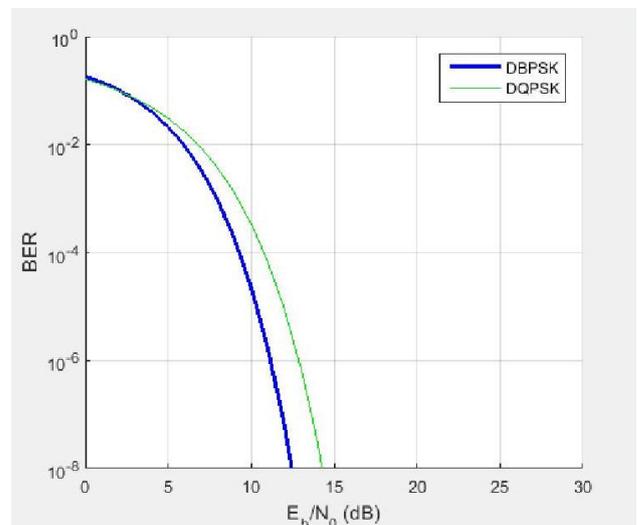


Figure 14. DBPSK and DQPSK in AWGN channel

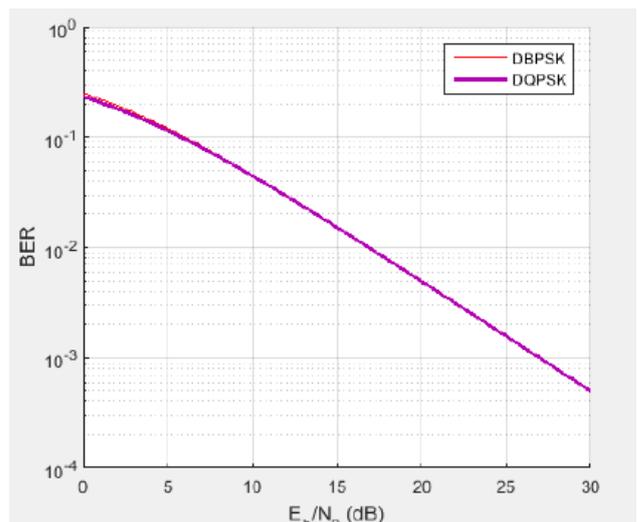


Figure 15. DBPSK and DQPSK in Rayleigh channel

REFERENCE

- [1] Fitchard, Kevin. "Wi-Fi Alliance gobbles up WiGig; plans to certify devices this year". Archived from the original on 5 March 2016. Retrieved 8 January 2016.
- [2] Fleishman, Glenn (December 7, 2009). "The future of WiFi: gigabit speeds and beyond". *Ars Technica*. Archived from the original on December 13, 2009.

- [3] Retrieved 2009. Borwein, Peter; Mossinghoff, Michael J. "Barker sequences and flat polynomials". In James McKee; Chris Smyth. *Number Theory and Polynomials*. LMS Lecture Notes. **352**. Cambridge University Press. 2008.
- [4] Merrill I. Skolnik, McGraw-Hill "Introduction to Radar Systems", 3rd Edition, 2001.
- [5] Sun, Weiping; Choi, Munhwan; Choi, Sunghyun. "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz" (*PDF*). *Journal of ICT Standardization*. July 2013.
- [6] Chen, J. C. Measured Performance of 5-GHz 802.11a Wireless LAN Systems. Atheros Communications, Inc. 27 August. 2001.
- [7] Enterasys Network. Wireless Demilitarised Zone (WDMZ)-Enterasys Network's Best Practices Approach to an Interoperable WLAN Security Solution. Enterasys Network. 2002.
- [8] Goth, G. (2002). Wireless Security Still Ad Hoc and Add-On. DS Online Exclusive. *IEEE Distributed Systems Online*, 3(7). 7 July 2002.
- [9] Tittelbach-Helmrich, K., Miletić, E., Wcislek, P. and Stamenković, Z. MAC
- [10] Hardware Platform for RF-MIMO WLAN, Proceedings of 53rd IEEE International Midwest Symposium on Circuits and Systems, Seattle, 339-342. 2010.

Noora H. Sherif, working at Al-Turath University College as a teacher has a master degree for Engineering of telecommunication, was born in 14/3/1987. Noora got a Bachelor degree of electrical engineering from Al -Mustansiriya University in Baghdad from 2009 also got Master degree in electronic and communication engineering from Al- Mustansiriya University in Baghdad in 2012.

She worked assistant lecturer in Madinat Al- Alelem University College in Baghdad from 2012 until 2017, she is currently working assistant lecturer in Al- Turath University College in Baghdad in 1/9/2018.

Ghufran Saady Abd-almuhsen working at Madinat Alelem University College as a teacher, have master degree in engineering of computer, was born in Baghdad 1989. Ghufran got a Bachelor degree of computer engineering from Al-Nahrain University in Baghdad 2011 also got Master degree in computer engineering from Al-Nahrain University in 2015.

She worked assistant lecturer in Madinat Al-Alelem University College in Baghdad from 2015.