2.1 Introduction

This section provide the necessary background on the structure of VoIP applications on their main system components, and the (IPv4 & IPv6) wi-fi wireless network.

2.2 Voice over IP (VoIP)

voice over internet protocol (VoIP) is one of the most important technologies in the world of communication .it is a simply a way to make phone calls through the internet. VoIP system transmits packet via packet-switched network in which voice packets may take the most efficient path. on the other hand, the traditional public switched telephone network (PSTN) is a circuit-switched network which requires a dedicated line for telecommunications activity [4].furthermore, internet was initially used for transmit data traffic and it is performing this task really well. however, internet is best-effort network and therefore it is not good enough for the transmission of real-time traffic such as VoIP [5]. there are about 1 billion fixed telephone line sand 2 billion cell phones in the world that use PSTN systems .in the near future, they will move to networks that are based on open protocols known as VoIP. this can be seen from the increasing number of VoIP users. for instance there, are more than eighty million subscribers of Skype ; very popular VoIP commercial application [6] . VoIP has gained popularity due to the more advantages it can offer than PSTN systems that voice is transmitted in digital form which enables VoIP to provide more features such as multimedia transfer mobility and cost savings. however, VoIP still suffer few drawbacks which user should consider when deploying VoIP system. VoIP converts standard telephone voice signals into compressed data packets that can be sent over IP. before transmitted over packet switched networks, the speech signal has to be digitized at the sender;

the reverse process is performed at the receiver. the digitalization process is composed of sampling, quantization and encoding [7].

the spread of internet and its underlying communication protocols IP gave rise to the notion of everything over IP. one of the applications that are experiencing high growth and popularity is voice over IP . voice over IP is gaining success because of multiple reasons like lower equipment cost, integration of voice and data and the widespread availability of IP [7].

2.2.1 VoIP protocols

there are two standard protocols used in VoIP network:

1. **H.323**

(ITU-R REC.H.3231999) is international tele- communication union (ITU) standard based on real-time protocol (RTP) and real-time control protocol (RTCP); h.323is a set of protocols for sending voice, video and data over ip network to provide real-time multimedia communications. it is reliable and easy to maintain technology and also there commendation standard by ITU for multimedia communications [8].

2. **SIP**

the session initiation protocol (SIP) is an ASCII-based, peer-to-peer application layer protocol that defines initiation, modification and termination of interactive, multimedia communication sessions between users [9].

sip is developed by the internet engineering task force (IETF) and is derived from hyper-text transfer protocol (HTTP) and simple mail transfer protocol (SMTP). SIP is defined as a client-server protocol, in which requests are issued by the calling client and responded to by the called server, which may in itself be a client for other aspects of the same call. SIP is not dependent on TCP for reliability but

rather handles its own acknowledgment and handshaking. this makes it possible to create an optimal solution that is highly adjusted to the properties of VoIP [9].

sip and h.323 provide similar functionality: call control, call setup and teardown, basic call features such as call waiting, call hold, call transfer, call forwarding, call return, call identification, or call park, and capabilities exchange. each protocol exhibits strengths in different applications. h.323 defines sophisticated multimedia conferencing which can support applications such as white boarding, data collaboration, or video conferencing. sip supports flexible and intuitive feature creation with sip using SIP-CGI (sip common gateway interface) and CPL (call processing language). third party call control is currently only available in sip that why used in this thesis. work is in progress to add this functionality to h.323 [10].

2.2.2 Over transmission layer protocol

generally, there are many protocols available at the transport layer when transmitting information through an IP network. these are TCP (transmission control protocol), UDP (user data-gram protocol) and (real-time transmission protocol). in most situations UDP is used instead of TCP especially for transmitting multimedia applications like voice and video across a wireless network. UDP has less overhead since it does not provide several functions such as sequencing the datagrams. packet send, packet receipt verification, missing packet retransmission and other flow control services [11]. in this thesis we use UDP because passes data along from the application layer to IP to be transmitted. it performs none of the error checks that TCP provide no time waste, no retransmit of lost packet effect on the reordering of received packet. no form of flow control

the UDP is a simple protocol that passes data along from the application layer to IP to be transmitted. it performs none of the error checks that TCP does, and is therefore unreliable. figure (2.1) shows atypical field of UDP protocol header.

16	32 bits
source port	destination port
length	checksum
data	

figure (2.1): UDP header [12]

source port: source port is an optional field. when used, it indicates the port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. if not used, a value of zero is inserted.

destination port: destination port has a meaning within the context of a particular internet destination address.

length : the length in octets of this user datagram, including this header and the data. the minimum value of the length is eight.

checksum : the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

data : UDP data field.

a UDP header merely consists of an optional source port, a destination port, the length of the datagram, and a checksum [12] . as previously mentioned, the main reason for using UDP over TCP in VoIP applications is the reduced delay. in general, the sporadic loss of packets in a conversation will not be as disruptive as

excessively long delay times. in fact, a packet loss of about 5% is said to be tolerable depending on how the losses are distributed [13].

2.2.3 Over network layer protocol

- **IP versions:**

as the growing popularity of VoIP will make it a significant component of traffic in the future internet, it is of interest to compare VoIP performance over ipv6 and ipv4. the results would help to determine if there are any differences in VoIP performance over ipv6 compared to ipv4 due to overhead resulting from the larger ipv6 header (and packet size). this thesis focuses on comparing VoIP performance with ipv6 and ipv4 during the exchange of voice data only. the following sections introduce the IP versions used in this research.

A. IPv4

is the fourth version of internet protocol (IP). it is the most widely deployed IP version. ipv4 uses 32-bit address. there are 4,294,967,296 (232) ipv4 addresses in total. currently, ipv4 address exhaustion is a serious problem. although, there are many ways to solve this problem but it will increase the network delay this one issue such as NAT (network address translation), ipv4 addresses is not a long term option. figure (2.2) shows the header field of ipv4.

<table>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td>time to live</td><td colspan="2">protocol</td><td colspan="2">header checksum</td></tr>
<tr><td colspan="5">source address</td></tr>
<tr><td colspan="5">destination address</td></tr>
<tr><td colspan="4">Option</td><td>Padding</td></tr>
</table>

figure (2.2): ipv4 header [14]

■ **Version**:

the version field indicates the version of IP and is set to 4. the size of this field is 4 bits see figure (2.2).

■ **Internet header length**:

the internet header length (IHL) field indicates the number of 4-byte blocks in the ipv4 header. the size of this field is 4 bits. because an ipv4 header is a minimum of 20 bytes in size, the smallest value of the IHL field is 5. ipv4 options can extend the minimum ipv4 header size in increments of 4 bytes. if an ipv4 option is not an integral multiple of 4 bytes in length, the remaining bytes are padded with padding options, making the entire ipv4 header an integral multiple of 4 bytes. with a maximum IHL value of 0xf, the maximum size of the ipv4 header, including options, is 60 •options

■ **Type of service**:

the type of service field indicates the desired service expected by this packet for delivery through routers across the ipv4 internetwork. this is usually done based on the needs of an application. for example, voice over IP and other real-time packets take precedence over e-mail in congested areas of the network. this is commonly referred to as quality of service (QoS). the low-order 2 bits of the type of service field are used for explicit congestion notification (ECN), as defined in RFC 3168.

■ **Total length**:

the total length field indicates the total length of the ipv4 packet (ipv4header + ipv4 payload) and does not include link-layer framing. the size of this field is16 bits, which can indicate an ipv4 packet that is up to 65,535 bytes long.

■ **Identification**:

the identification field identifies this specific ipv4 packet. the size of this field is 16 bits. the identification field is selected by the source node of the

ipv4 packet. if the ipv4 packet is fragmented, all the fragments retain the identification field value so that the destination node can group the fragments for reassembly.

■ **flags**:

the flags field identifies flags for the fragmentation process. the size of this field is 3 bits; however, only 2 bits are defined for current use. there are two flags—one to indicate whether the ipv4 packet can be fragmented and another to indicate whether more fragments follow the current fragment.

■ **Fragment offset:**

the fragment offset field indicates the position of the fragment relative to the beginning of the original ipv4 payload. the size of this field is 13 bits.

■ **Time-to-live the time-to-live (TTL)**

field indicates the maximum number of links on which an ipv4 packet can travel before being discarded. the size of this field is 8 bits. the TTL field was originally defined as a time count for the number of seconds the packet could exist on the network. an ipv4 router determined the length of time required (in seconds) to forward the ipv4 packet and decremented the TTL accordingly. modern routers almost always forward an ipv4 packet in less than a second, and they are required by RFC 791 to decrement the ttl by at least one. therefore, the TTL becomes a maximum link count with the value set by the sending node. when the TTL equals 0, an icmpv4 time exceeded-time to live exceeded in transit message is sent to the source of the packet and the packet is discarded.

■ **Protocol:**

the protocol field identifies the upper-layer protocol. the size of this field is 8 bits. for example, a value of 6 in this field identifies TCP as the upper-layer protocol, a decimal value of 17 identifies UDP, and a value of 1identifies icmpv4 .the protocol field is used to identify the upper-layer protocol that is to receive the ipv4 packet

payload

■ **Header checksum**:

the header checksum field provides a checksum on the ipv4 header only. the size of this field is 16 bits. the ipv4 payload is not included in the checksum calculation, as the ipv4 payload usually contains its own checksum. Each ipv4 node that receives ipv4 packets verifies the ipv4 header checksum and silently discards the ipv4 packet if checksum verification fails. when a router forwards an ipv4packet, it must decrement the TTL. Therefore , the header checksum value is recomputed at each hop between source and destination.

■ **Source address**:

the source address field stores the ipv4 address of the originating host. the size of this field is 32 bits.

■ **Destination address:**

the destination address field stores the ipv4 address of an intermediate destination (in the case of source routing) or the destination host. the size of this field is 32 bits.

■ **Options:**

the options field stores one or more ipv4 options. the size of this field is a multiple of 32 bits (4 bytes). if an ipv4 option does not use all 32 bits, padding options must be added so that the ipv4 header is an integral number of 4-byte blocks that can be indicated by the IHL field [14].

B. IPv6

ipv6 is the version of internet protocol that is going to replace ipv4 in the future. ipv6 was developed by internet engineering task force (IETF). it was described in RFC 2460 on 1998. ipv6 is considered as the long term solution for ipv4 address exhaustion. ipv6 uses 128-bit address. the number of ipv6 addresses is about 3.4*1038 (2128). it is the best solution for IP address exhaustion [14].

Version	traffic class	flow label	
payload length	next header	hop limit	
source address			
destination address			

figure (2.3): ipv6 header [14]

■ **Version:**

the version field indicates the version of IP and is set to 6. the size of this field is 4 bits see figure (2.3)

■ **Traffic class:**

the traffic class field indicates the ipv6 packet's class or priority. the size of this field is 8 bits. this field provides functionality similar to the ipv4 type of service field.

■ **Flow label:**

the flow label field indicates that this packet belongs to a specific sequence of packets between a source and destination, the flow label is used for prioritized delivery, such as delivery needed by real-time data (voice and video). for default router handling, the flow label field is set to 0. to distinguish a given flow, an intermediate router can use the packet's source address, destination address, and flow label.

■ **Payload length:**

the payload length field indicates the length of the ipv6 payload. the size of this field is 16 bits. the payload length field includes the extension headers and the upper-layer PDU. with 16 bits, an ipv6 payload of up to 65,535 bytes can be indicated. for payload lengths greater than 65,535 bytes, the payload length field is set to0 and the jumbo payload option is used in the hop-by-hop options

extension header .

■ **Next header:**

the next header field indicates either the type of the first extension header (if present) or the protocol in the upper-layer pdu (such as TCP, UDP, or ICMPV6) . the size of this field is 8 bits . when indicating an upper-layer protocol,

■ **Hop limit:**

the hop limit field indicates the maximum number of links over which the ipv6 packet can travel before being discarded. the size of this field is 8 bits. the hop limit field is similar to the ipv4 TTL field, except that there is no historical relation to the amount of time (in seconds) that the packet is queued at the router.

■ **Source address:**

the source address field indicates the ipv6 address of the originating host. the size of this field is 128 bits.

■ **Destination address:**

the destination address field indicates the ipv6 address of the current destination node. the size of this field is 128 bits. [14]

figure (2.4) show the VoIP protocols that work on each layer at TCP/IP model

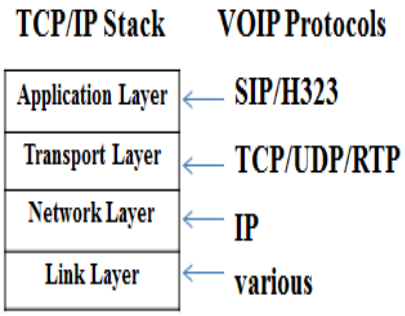

figure (2.4): VoIP protocols over TCP/IP stack [15]

2.2.4 VoIP network components

focusing on the packet-level and VoIP system performance , there are three indispensable VoIP components at the end-systems: codecs, packetizer and play out buffer, as shown in figure (2.5).the analogue voice signals are digitized, compressed and then encoded into digital voice streams.

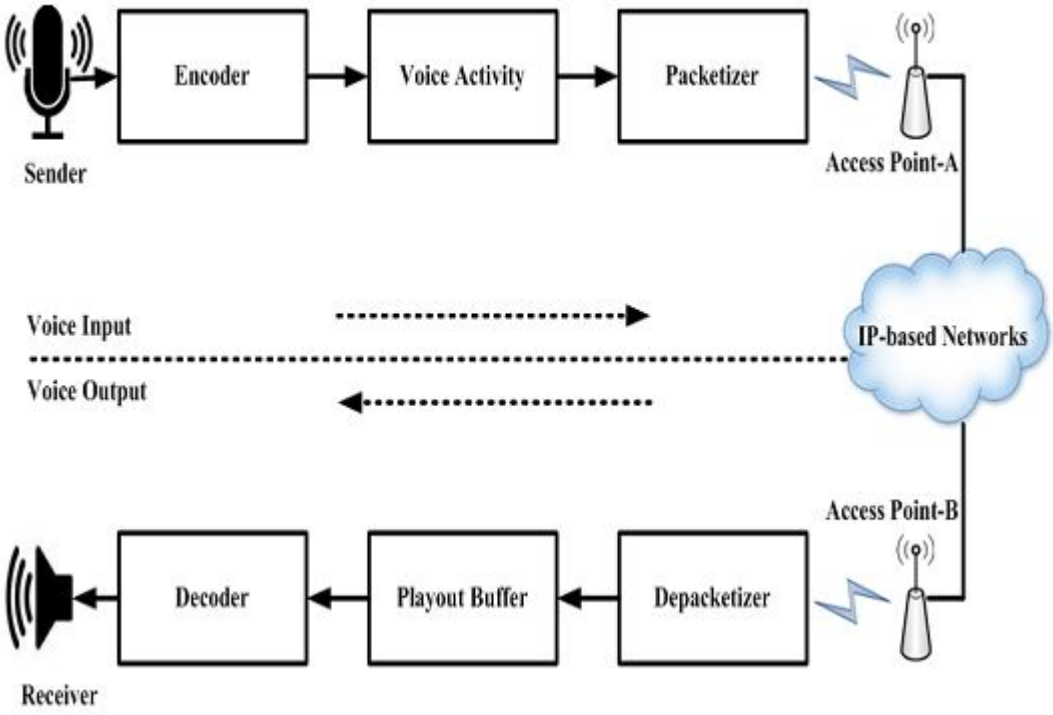

figure (2.5) vowifi component [16]

from figure (2.5) the packets are then sent out over ip network to its destination where the reverse process of decoding and depacketizing of the received packets is carried out. during the transmission process, time variations of packets delivery (jitter) may occur. hence, a play out buffer is used at the receiver end to smoothen the play out by mitigating the incurred jitter. packets are queued at the play out buffer for a play out time before being played. however, packets arriving later than the play out time are discarded. the principle components of a VoIP system, which covers the end-to-end transmission of voice, are illustrated in figure (2.5)[16].

2.2.5 VoIP codecs.

a codec is the term used for the word coder-decoder, converts of analog audio signals into compressed digital form for transmission and then back into an uncompressed audio signal for the reception. there are different codec types based on the selected sampling rate, data rate, and implemented compression. the most common codecs used for VoIP applications are g.711, g722, g723, g726, g728, g729a, etc. each of which varies in the sound quality, the bandwidth required, the computational requirements, encoding algorithm and coding delay [17]. the most popular codecs are explained below .

G.711

G. 711 is a public domain codec widely used in VoIP applications. it was introduced in 1972 by the itu. it employs a logarithmic compression that compresses each 16-bit sample to 8-bits. as a result, its bit-rate is 64 kbps, which is considered the highest bit-rate among the codecs. g. 711 offers very good audio quality and the MOS value of 4.3 [18].

G.723

G. 723 is a licensed codec. it is designed for calls over modem links with data-rates of 28.8 and 33 kbps. [18].

G.729

G729 is also a licensed codec designed to deliver good call quality without consuming high bandwidth. it is built based on the conjugate-structure algebraic-code-excited linear prediction (CS-ACELP) algorithm with bit-rate of 8 kbps and MOS value of 4.0 [18].

table (2.1) bandwidth requirements of some common codec's [18]

IUT-T Codec	Algorithm	Codec Delay (ms)	Bit Rate (Kbps)	Packets Per Second	IP Packet Size (bytes)
G.711	pulse-code modulation (PCM)	0 .375	64	100	120
G.723.1	Multipulse maximum likelihood quantization/algebraic-code excited linear prediction	97.5	5.3	33	60
G.729A	Conjugate Structure – Algebraic Code Excited Linear Prediction (ACELP)	35	8	100	50

moreover, recently voice codecs are so developed to detect additional parameters talk-spurt and silence lengths within a conversation. during a voice communication the time duration during which the user speaks is called a talk-spurt and the time duration during which the user is silent is called the silence length or gap. silence within a-communication period leads to the packetization of the background noise and sending it over the network. this causes bandwidth wastage. usually, during a conversation talk 35% of the time and remain quiet rest of the time. silence suppression is done by the voice activity detection (VAD) algorithm. with silence suppression during the silence period, the codec does not send any voice data. instead of voice data the VAD algorithm generates comfort noise which has packet size much less than the voice traffic this decreases channel utilization and thereby saves bandwidth [19].

2.2.6 VoIP challenges

communication over wi-fi medium is noise sensitive. noise causes the signal to reach the destination with a lead or lag in time. wi-fi bandwidth is limited network which may limit the number of VoIP calls. Vowi-fi security challenges in comparing to PSTN, VoIP faces many security issues and PSTN provide high level of security due to their loosely characters but some of the issues are similar for both like eaves dropping type of attacks and toll fraud. “man in the middle" is a type of eaves dropping which listening and changing conversation is possible for attacker. attacker is able to interrupt the conversations then play back previous conversation instead to change the conversation like "yes" to "no" or take advantage by asking username and password. making free calls especially for high cost long .available solutions: some recommendations in end-user level and infrastructure level for secure VoIP in configuration mode make it as wep(wired equivalent privacy) is the weakest attempt, WPA (wi-fi protected access)is stronger and wpa2 (enhanced wpa)is advance encryption algorithm suggested to have secure ieee 802.11 wlans. moreover, the isolation of the corporate VoIP network from the public internet will enhance network security and performance.. implementing security mechanism such as encryption will lead to more delay due to encryption and decryption also building new header to packets thus it has effect on QoS and capacity therefore it should be consider before tuning and developing security policies [20].

2.3 Background of wireless lan

wireless lan is one of the mainly organized wireless technologies all over the world and is likely to play a major function in the next-generation wireless voice call networks. the architecture of this type of network is the same as local area network

(lan)'s except that the transmission happens via radio frequency (RF) or infrared (IR) and not through physical wires/cables, and at the mac sub-layer, it uses different standard protocol. connects two or more devices using orthogonal frequency division multiplexing (OFDM) or direct sequence spread spectrum (DSSS) modulation techniques to establish communication between devices within a limited range . the main characteristics of the wlans are mobility, simplicity, scalability, edibility and cost effectiveness. simply, wireless network allows nodes to communicate with each other wirelessly and it can be configured in two ways defines in the 802.11 specification [20] [21].

2.3.1 Ad hoc mode

in ad hoc mode, also known as independent basic service set (IBSS) or peer-to-peer mode, all of the computers and workstations connected with a wireless nic card can communicate with each other via radio waves without an access point.

ad hoc mode is convenient for quickly setting up a wireless network in a meeting room, hotel conference center, or anywhere else sufficient wired infrastructure does not exist. [21]

2.3.2 Infrastructure mode

in infrastructure mode, all mobile and wireless client devices and computers communicate with the access point, which provides the connection from the wireless radio frequency world to the hard-wired lan world. the access point performs the conversion of 802.11 packets to 802.3 ethernet lan packets. data packets traveling from the lan to a wireless client are converted by the access point into radio signals and transmitted out into the environment. all wireless clients and devices within range can receive the packets, but only those clients with the appropriate destination address will receive and process the packets. a basic wireless infrastructure with a single access point is called a basic service set (BSS).

when more than one access point is connected to a network to form a single sub-network, it is called an extended service set (ESS). [21]

2.4 benefits of wireless lan

wireless lan has a lot of benefits such as:

2.4.1 Mobility:

with the development of public wireless network, a user can access the internet even if he is not within his normal working area. for example, almost all the coffee shops and big malls are offering free of charge internet [20] [21].

2.4.2 Cost stability:

as compared to the wire lan, every time you add a new device, you have to run cable, while with wireless lan, include an ap/wireless router and you can connect a sufficient number of devices to it without any further cost [20] [21].

2.4.3 Easy to install:

it is really easy to install the wireless ap/router, even for a home user. to install the wireless equipment at home or SOHO (small office home office), there is no need for a technician. on the other hand, you need a technician every time for installing an rj45 jack, or running a ceiling cable [20] [21].

2.5 Deficiency in wireless lan

there are also some weaknesses in wireless lan, but can overcome these weaknesses by using the correct design model and strategy.

2.5.1 Security:

in wire lan, the hacker or malicious person must have to be inside the building, and have the access to the rj-45 jack, to attack the network or sniff the packets.

however, for wireless lan, the situation is totally different because of the nature of radio transmission the intruder does not have to be inside the building. radio signals leak outside the building and anyone within the range can use them to access the internal network of the company, due to which must have to implement proper security, so that no unauthorized person can access our wireless lan. [22]

types of security

- WEP (wired equivalent privacy):
  WEP is the original wireless security standard, release in 1997, to secure the wireless networks, but it is the weakest form of wireless security. [22]
- WPA (wi-fi protected access):
  it was released by the wi-fi alliance to overcome the weakness of WEP in 2003. it uses the same hardware as WEP but it gives the far better security than WEP. it gave the three solutions: temporal key integrity protocol (TKIP), message integrity code (mic), and 802.1x [22]
- WPA2 (IEEE 802.11i):
  this was released by the wi-fi alliance in 2004. it needs hardware upgrade, and uses the aes (advance encryption standard) as encryption. it is backward compatible with TKIP-hardware also, which means that if client connect to AP that only support TKIP encryption, it provides that, and if the client supports the AES, then it will provide this. [22]

2.5.2 Interference

because the wireless lan uses the unlicensed band, so the other devices in the wireless network that are using the same channel, such as microwave ovens and cordless phones, can interfere the wireless signal, and this can create significant impacts on the performance of wireless lan. properly designed networks can mitigate the impact of interference[22] .

2.6 Architecture of wireless lan

2.6.1 Station:

all devices that have the ability to connect to the wireless medium are called “stations”. all stations have wireless nics. wireless station can be access point (AP) or clients. access points are devices that are capable of sending and receiving rf to the backbone network for wireless clients that associate with it. wireless clients are any devices that have wireless NIC, e.g. laptops, IP phones, PDA etc.

2.6.2 Basic service set:

basic service set (BSS) is a collection of all the access point and clients that can communicate with each other. there are two kinds of BSS, independent BSS and infrastructure BSS. each BSS has its id, which is known as SSID.

2.7 IEEE 802.11 standards:

the IEEE 802.11 is a collection of standards that are used to carry the data in wireless lan using the RF waves in the range of 2.4 ghz and 5.0 ghz. a lot of amendments have been made in original 802.11 standards to make it more efficient and feasible for home users and industry. some of them are here:

2.7.1 IEEE 802.11a

ratification of 802.11a took place in 1999. the 802.11astandard uses the 5 ghz spectrum and has a maximum theoretical 54 mbps data rate. similar to 802.11g, as signal strength weakens due to increased distance, attenuation (signal loss) through obstacles or high noise in the frequency band ,the data rate automatically adjusts to lower rates(54/48/36/24/12/9/6 mbps) to maintain the connection. the 5ghz spectrum has higher attenuation (more signal loss) than lower frequencies, such as 2.4 ghz used in 802.11b/g standards. penetrating walls provides poorer performance than with 2.4 ghz. products with 802.11a are typically found in larger corporate networks or with wireless internet service providers in outdoor backbone networks see table (2.2) [22].

2.7.2 IEEE 802.11b

in 1995, the federal communications commission had allocated several bands of wireless spectrum for use without a license. the FCC stipulated that the use of spread spectrum technology would be required in any devices. in 1990, the IEEE began exploring a standard. in 1997 the 802.11 standard was ratified and is now obsolete. then in july 1999 the802.11b standard was ratified. the 802.11 standard provides a maximum theoretical 11 megabits per second (mbps) data rate in the 2.4 ghz industrial, scientific and medical (ISM) band in 2003, the ieee ratified the 802.11g standard see table (2.2)[22].

2.7.3 IEEE 802.11g

with a maximum theoretical data rate of 54 megabits per second (mbps) in the 2.4 ghz(ism) band . as signal strength weakens due to increased distance, attenuation (signal loss) through obstacles or high noise in the frequency band, the data rate automatically adjusts to lower rates (54/48/36/24/12/9/6mbps) to maintain the connection. when both 802.11b and802.11g clients are connected to an 802.11g

router, the802.11g clients will have a lower data rate. many routers provide the option of allowing mixed 802.11b/g clients or they may be set to either 802.11b or 802.11g clients only. to illustrate 54 mbps, if you have dsl or cable modem service, the data rate offered typically falls from 768 kbps (less than 1mbps) to 6 mbps. thus 802.11g offers an attractive data rate for the majority of users. the 802.11g standard is backwards compatible with the 802.11b standard. today 802.11g is still the most commonly deployed standard; see table (2.2). [22]

2.7.4 IEEE 802.11n

in january, 2004 the ieee 802.11 task group initiated work .there have been numerous draft specifications, delays and lack of agreement among committee members. yes, even in the process of standards development, politics are involved .the proposed amendment has now been pushed back to early 2010. it should be noted it has been delayed many times already. thus 802.11n is only in draft status. therefore, it is possible that changes could be made to the specifications prior to final ratification. the goal of 802.11n is to significantly increase the data throughput rate. while there are a number of technical changes, one important change is the addition of multiple input multiple output (MIMO) and spatial multiplexing. multiple antennas are used in MIMO, which use multiple radios and thus more electrical power. 802.11n will operate on both 2.4 ghz (802.11b/b) and 5 ghz (802.11a) bands. this will require significant site planning when installing 802.11n devices. the 802.11n specifications provide both 20 mhz and 40 mhz channel options versus 20 mhz channels in 802.11a and 802.11b/g standards. by bonding two adjacent 20 mhz channels, 802.11n can provide double the data rate in utilization of 40 mhz channels. however, 40 mhz in the 2.4 gb and will result in interference and is not recommended nor likely which inhibits data throughput in the2.4 ghz band. it is recommended to use 20 mhz channels in the 2.4 ghz

spectrum like 802.11b/g utilizes. for best results of 802.11n, the 5 ghz spectrum will be the best option .deployment of 802.11n will take some planning effort infrequency and channel selection. some 5 ghz channels must have dynamic frequency selection (DFS) technology implemented in order to utilize those particular channels see table (2.2) [22].

the table below which is explains the main feature of each IEEE802.11 release:

table (2.2) explain the main feature of each IEEE802.11 release [22]

Standard	Maximum Data Rate (Mbps)	Typical Throughput (Mbps)	Operating Frequency Band	Maximum Non-Overlapping Channels (Americas)
802.11b	11	6.5	2.4 GHz	3 *1
802.11g	54	8 (Mixed b/g) 25 (Only 802.11g)	2.4 GHz	3 *1
802.11a	54	25	5 GHz	24 (20 MHz channels) 12 (40 MHz channels)
802.11n	248	74 *2	2.4 GHz & 5 GHz	*3

2.8 Quality of Service (QoS)

quality of service (QoS) can be defined as the network ability to provide good services that satisfy its customers. in other words, QoS measures the degree of user satisfactions ;the higher the QoS, the higher degree of user satisfaction . QoS is a big concern ,when wlan is mainly used to transmit data packets, as opposite with the increasing demand on applying VoIP over wlan and transmitting voice packets ,QoS has become a critical issue, because real-time applications, unlike data (non

real-time) applications, are very sensitive to delay .therefore, QoS of VoIP is an import concern to ensure that voice packets are not delayed, lost or dropped during the transmission over the network. on the other hand, as VoIP is considered a viable alternative of pstn and it is expected to replace it in the future. VoIP has to provide customers with high quality of services, the same as the quality of pstn services or better. therefore, VoIP applications require stringent QoS in order to satisfy their users. however, ip networks still cannot meet the required QoS of VoIP .VoIP quality of service is measured based on different parameters like delay, jitter, packet loss, throughput and echo. VoIP QoS is improved by controlling the values of these parameters to be within the acceptable range [23] .

2.9 V0IP QoS factors

The main factors affecting QoS are briefly described in the following sections.

2.9.1 Throughput

this parameter concerns about the maximum number of bits received out of the total number of bits sent during an interval of time. in IEEE 802.11 networks, the bit rate of each standard is specified such as IEEE 802.11b transmits at1mbps, 2mbps, 5.5mbps and 11mbps. furthermore, the standard has the capability of performing dynamic rate switching with the objective of improving performance of wireless link however ,transmission throughput is still less than that specified in the standard due to the overhead introduced by wlan network protocols. the throughput achieved is between the range 50% to 70% of the transmission rate which is low comparing to Ethernet throughput which achieves 80%to 90% of the transmission rate .there are methods have been introduced to improve the throughput of wlan such as aggregation technique and adaptive techniques. [23]

throughput can be calculated using the following equation:

$$Throughput = \frac{Amount\ of\ transferred\ data}{Duration} \qquad E(2.1)$$

2.9.2 End to End Delay

delay can be defined as the total time it takes since a person, communicating another person, speaks words and hearing them at the other end. unlike data applications, VoIP applications are very sensitive to delay although they can tolerate packet loss to some extent. end-to-end or mouth to ear delay is one of the main factors affecting QoS and should be less than 150ms for good network connection as defined by itu g.114 while delay of less than 100ms is defined by the european telecommunications standard institute (ETSI).delay is mainly caused by network congestion which leads to a slow delivery of packets furthermore, delay is affected by several parameters or algorithms which can be categorized into: delay at the source, delay at the receiver, and network delay. some of the delay parameters are known while some others are inconsistent.

1) Delay at the source

the delay of the whole process performed at the sender side before transmitting the voice packet over the network is caused by several components: codec, packetization and process codec functions introduce some delays when processing the analogue-to-digital conversion. the more bits compressed, the less the bandwidth required, and the longer the delay added. for packetization delay, it's the time taken to place the chunks of frames in packets which would be transmitted across the network. the third component of source delay is when the computer passes the packets into then network for transmission to other side [23].

2) Delay at the receiver

that process carried out at the sender is performed at the receiver adding more delay: process delay and decoding delay including decompressing delay .additionally, playback delay is incurred when playing out the voice stream which includes the jitter buffer delay as well [25].

3) Network delay

network delay in wlan environment is the total delay of both wlan and backbone networks queuing, transmission and propagation are other components of network delays. the propagation delay is the delay in the physical media of the network, while transmission delay includes router's delay and mac retransmission delay

$$Delay\ total = D_1 + D_2 + D_3 \quad E(2\text{-}2)$$

Delay total =D1+D2+D3

Where :

D1=codec delay

D2=play out delay

D3=network delay

2.9.3 Jitter

ip network does not guarantee packets delivery time which introduces variation in transmission delay. this variation is known as jitter and it has more negative effects on voice quality since voice packets of the same flow are not received at the same time. therefore, jitter buffer are introduced to diminish the jitter effect and make the conversation smoothly as it holds a number of packets in a queue before play

out. the buffer queue size can be fixed or adaptive which varies based on network condition, voice character for better performance. buffer jitter adaptive techniques perform better as it reduces the possibility of buffer overflow and underflow. overflow issue is where number of packets received is getting larger than the buffer size as a result buffer discards packets that cannot hold. on the other hand, underflow buffer occurs when some packets are needed for play out but buffer is empty. hence, several adaptive buffer algorithms, such as interference are introduced to adjust buffer size in order to improve quality of VoIP [23].

total jitter (*t*) is the combination of random jitter (*r*) and deterministic jitter (*d*):

$$\boldsymbol{T = \left(D_{peak-to-peak} + (2 \times n \times R_{rms})\right)} \quad \boldsymbol{E(2.3)}$$

$$T = D_{peak\text{-}to\text{-}peak} + 2\times\ n\times R_{rms},$$

in which the value of *n* is based on the bit error rate (BER) required of the link.
a common bit error rate used in communication standards such as ethernet is 10^{-12}

2.10 Related work

in [24] simulation of VoIP (voice over internet protocol) traffic through umts (universal mobile telecommunication system) and wi-fi (IEEE 802.11x) alone and together are analyzed for quality of service (QoS) performance. the average jitter of VoIP transiting the wi-fi-umts network has been found to be lower than that of either solely through the wi-fi and the umts networks. it is normally expected to be higher than traversing through the wi-fi network only. both the mos (mean opinion score) and the packet end-to-end delay were also found to be much lower than expected through the heterogeneous wi-fi-umts network.

in [25] VoIP over wireless lan (wlan) faces many challenges, due to the loose nature of wireless network. issues like providing QoS at a good level, dedicating capacity for calls and having secure calls is more difficult rather than wired lan.
VoIP can tolerate packet loss to some extent, it is very sensitive to delay factor. jitter also plays a main role on voice quality. echo and throughput. wlan is a bandwidth limited network which leads to a limited number of VoIP calls.

in [18] foundation of technical education , iraq. in this paper, there is an analysis and evaluation of the performance of VoIP based integrated wireless lan/wan with taking into account various voice encoding schemes. these schemes are: g.711, g722, g723, g726, g728, g729a.the network model was simulated using opnet modeler software. different parameters that indicate the QoS like mos, jitter, end to end delay, traffic send and traffic received are calculated and analyzed in wireless lan/wan scenarios. depending on this evaluation, selection codecs g.729a consider the best choice for VoIP.