VoIP over Wireless LAN Survey

Răzvan Beuran

Internet Research Center
Japan Advanced Institute of Science and Technology (JAIST)

April 20, 2006
IS-RR-2006-005

Japan Advanced Institute of Science and Technology (JAIST)

Internet Research Center
1-1 Asahidai, Nomi, Ishikawa, 923-1292 Japan

http://www.jaist.ac.jp

ISSN 0918-7553

Table of Contents

Abstract

Wireless LANs (WLANs) are being more and more widely deployed at present. They are a key element in dynamic business environments where permanent access to network resources is vital. They also provide a perfect solution for the creation of *ad-hoc* networks in emergency conditions within areas where dense wireless networks are in place.

Voice over IP (VoIP) is a form of voice communication that uses data networks to transmit voice signals. The signal is appropriately encoded at one end of the communication channel, sent as packets through the data network, then decoded at the receiving end and transformed back into a voice signal.

Since both technologies are sufficiently mature at the moment, VoIP over WLAN communication is being developed. However the intrinsic characteristics of each of these two technologies cause specific issues to appear that must be addressed in order to ensure a successful deployment of VoIP over WLANs. This is particularly important when considering the use of WLAN technology in the context of emergency situations.

This document is a survey of the current state of the art in voice communication over wireless networks. The properties of WLANs and VoIP are presented, then the issues related to the deployment of VoIP over WLAN are analysed. The main findings of this survey are the following. WLAN QoS parameters have a high variability in real-world environments, with a significant effect on application performance. Existing WLAN QoS mechanisms are only of limited use for managing contention for applications with different QoS requirements. VoIP is a multimedia application that requires timely servicing of the voice traffic; this is a challenging task in WLANs, even when using QoS enforcement. Roaming between access points introduces communication gaps that can be unacceptably large for real-time applications.

An experiment testbed is proposed at the end that allows an objective verification of the properties of existing technologies, as well as the development of new techniques. The testbed can make use of WLAN emulation to allow experimentation in a wide range of controllable network conditions.

1 Introduction

Wireless LANs (WLANs) are being more and more widely deployed at present, since the number of mobile users is increasing steadily. WLANs are a key element in any business environment where "anytime, anywhere" access to network resources is vital. They also represent a solution for the creation of *ad-hoc* networks in emergency conditions within areas where dense wireless networks exist.

Given the different environments in which WLANs are used, the types of information that need to be transmitted on these networks vary. Convergence, i.e. the use of the same network for multiple purposes, such as communicating data, telephony, video conferencing, is an important trend in the field of ICT. Although convergence has become increasingly prevalent, satisfactory solutions have not yet been found even for the traditional fixed networks. Due to the inherent properties of wireless networks, the situation becomes even more challenging in this case.

First of all the bandwidth available in WLANs is significantly lower than in the case of fixed LANs. For the most widely-spread wireless networks, the maximum theoretical rate is either 11 Mb/s or 54 Mb/s. These rates are considerably lower that the current extensively-used 100 Mb/s and 1 Gb/s fixed LANs.

Moreover, tests with wireless 802.11b equipment, which can in theory run up to 11 Mb/s, have shown that in practice the sustained rate only climbs up to about 6-7 Mb/s [Net-05]. The significant amount of 802.11 management and control traffic, plus contention for the radio frequency spectrum, constitute the overhead. Additional features, such as encryption, increase even more the overhead and diminish the goodput[1] of the system.

Beside that, since the transmission medium for WLANs is air, performance depends on signal strength, which varies significantly depending on local topology and possible radio interference. This phenomenon was taken into account in wireless LAN technology design. The result is that when adapting to signal conditions WLAN operating rate may diminish, and this decrease can be of one order of magnitude. The adaptation itself, sometimes termed *auto-rate fallback*, has also significant consequences on the link QoS (Quality of Service).

Another difference between the wired and wireless networks is that in wired networks the last part of the connection (from the LAN switch to the PC, for example) is dedicated to one user. However in WLANs the medium is not only shared between the applications of one user, but between all the applications of all the users that happen to be using the same access point at the same moment of time. Hence network quality is more prone to degrade significantly.

In WLANs where more access points are simultaneously active, another issue is roaming. When a node moves or reception conditions change, it will usually select the access point in its range that has the highest signal strength. Roaming is the event of switching from one access point to another. Even though the data rate might improve once the switching is accomplished, roaming itself may take several seconds. This communication gap is usually unacceptable for most real-time applications; in addition the data rate of TCP-based transfers also diminishes. Therefore roaming is sometimes a trade-off between potential performance gain through switching to a better access point, and effective performance loss due to the roaming itself.

1 Goodput is defined as the rate of sending *useful* data, compared to throughput, which is the data transmission rate and includes protocol overheads.

Voice over IP (VoIP), also known as Internet telephony, is a form of voice communication that uses data networks to transmit audio signals. When using VoIP the voice is appropriately encoded at one end of the communication channel, and sent as packets through the data network. After the data arrives at the receiving end, it is decoded and transformed back into a voice signal.

Many enterprises consider replacing traditional PBX[2] phone systems with a VoIP telephony server. PBX costs may be prohibitive for the new companies that need to set up a telephony system from scratch. On the other hand, following deployment, VoIP systems require in principle no significant specific running costs, since they use the same network infrastructure that already exists and is maintained.

Using VoIP on wireless LANs solution enables support of mobile devices within the building or campus. Although this seems desirable and promising, it only brings out the specific issues related to WLANs that have been mentioned in the beginning. This will make people think twice before deploying VoIP on a wireless network, since "a wireless LAN for voice costs about double what a data-only one costs," according to Gartner analyst Ian Keene [Inf-05].

The main reason is related to the use of the same network for applications with different requirements concerning the allowed level of quality degradation. Data transfers are in this sense usually more resilient than real-time applications such as VoIP. This implies that contention must be managed by means of QoS mechanisms in order to ensure user satisfaction.

Although this issue is not specific to VoIP on WLAN, it is even more challenging when the media is wireless due to its inherent instability. Moreover managing contention is the only way to support mission-critical or safety-critical applications over WLANs. IEEE has finally published in November 2005 the first standard for QoS on WLAN, 802.11e, which is expected to improve application performance in WLAN environments, especially for real-time applications.

This document is a survey of the current state of the art in voice communication over wireless networks. Due to the nature of wireless networks and its aforementioned characteristics, specific issues appear that must be addressed in order to ensure a successful deployment of VoIP over WLANs.

The report is structured as follows. First we introduce the most widely spread WLAN standards, with emphasis on 802.11 networks and their recently added QoS features (chapter 2). In chapter 3 we present VoIP telephony and the particular issues related to it. The following chapter (chapter 4) will discuss VoIP over WLAN in the light of the information provided previously and in a critical perspective. Several public-domain reviews and papers will be used to support the performance discussions. Chapter 4 also outlines a suggested research methodology for application performance on WLAN. The report ends with a section of conclusions that summarizes the main findings of this survey, followed by a list of acronyms and references.

2 Private Branch eXchange.

2 Wireless LANs

As computer equipment users chose to become mobile, the technology had to adapt and offer wireless connectivity. Wireless will probably replace fixed connections in the same way in which mobile phones became the method of choice for person-to-person communication. However the transition may not be straightforward because of the inherent characteristics of WLANs.

2.1 Wireless LAN standards

Wireless LAN standards can be grouped into several families. The most important ones will be briefly described next.

The *IEEE 802.11* family is comprised of:

- 802.11a – Up to 54 Mb/s in the 5 GHz band, using OFDM[3] modulation scheme and WEP[4] & WPA[5] security;
- 802.11b – Up to 11 Mb/s in the 2.4 GHz band, using DSSS-CCK[6] modulation, and WEP & WPA security;
- 802.11g – Up to 54 Mb/s in the 2.4 GHz band, using OFDM or DSS with CCK modulation, and WEP & WPA security.

At the moment 802.11b is probably the most widely used WLAN standard, but there are devices that are compatible with all three standards in the same time. As always in the ITC the tendency is to migrate to faster technologies as soon as they become affordable.

Each standard from the 802.11 family has its strengths and weaknesses. For example, there is less potential for Radio Frequency (RF) interference for 802.11a, than for 802.11b or 802.11g. Given the larger bandwidth, this solution is better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated environments. However the range is shorter than for 802.11b and they are not interoperable.

In the case of 802.11b fewer access points are required than for 802.11a for the coverage of large areas (with a range of up to 100 m from the base station). A number of 14 channels is available, with three non-overlapping channels. 802.11b is compatible with 802.11g, which may eventually replace 802.11b since it provides higher data rates and security enhancements.

An important element of the 802.11 family of standards is the concept of *ad-hoc* network. This operation mode is intended to allow wireless communication in locations where an access point is not available, or access to a wired network is not required. In *ad-hoc* mode stations communicate directly with each other, without an access point serving as intermediary. To join an ad-hoc WLAN, a wireless station must be configured for *ad-hoc* mode, but apart from this there is no difference at user level. Certainly there are important technical issues to be solved, such as the routing algorithms for choosing an optimum path in the mesh of the *ad-hoc* network, but they are not the object of this survey.

3 Orthogonal Frequency Division Multiplexing.
4 Wired Equivalent Privacy.
5 Wi-Fi Protected Access.
6 Direct-Sequence Spread Spectrum with Complementary Code Keying.

The *IEEE 802.16* family (WiMAX) is a specification for fixed broadband wireless metropolitan access networks (MANs) with a bandwidth of up to 75 Mb/s. It operates in the 10-66 GHz range (with support for 2-11 GHz for the 802.16a variant). WiMAX uses OFDM modulation and DES3[7] & AES[8] security. Features like Quality of Service (QoS) establishment on a per-connection basis, strong security, and support for multicast and mobility are being added to WiMAX as well. This technology is currently used to interconnect local WLAN clouds over larger distances, hence extending significantly the potential coverage area of a wireless network.

Bluetooth is another wireless technology, which can deliver up to 2 Mb/s in the 2.4 GHz band. It uses FHSS[9] modulation and PPTP[10], SSL[11] or VPN[12] security. Bluetooth offers point-to-point links and has no native support for IP, therefore it doesn't support TCP/IP and wireless LAN applications well. Bluetooth is best suited to connect PDAs[13], cell phones and PCs in short intervals.

Another WLAN standard is *HiperLAN*, with versions 1 and 2, that can operate up to 20 Mb/s and 54 Mb/s, respectively. However this standard is only used in Europe. HiperLAN/2 provides better QoS than HiperLAN/1, and bandwidth guarantees.

2.2 WLAN equipment

The key element of the wireless to wired LAN connectivity are the wireless access points. They aggregate wireless radio signals and then connect the two LANs. Access points contain a radio transceiver, communication and encryption software, and an Ethernet port for a cable connection to a hub or switch on the wired LAN.

The radio transceiver built into the access point negotiates a connection between the end user and the wired LAN, connecting the user to the LAN in the same way a cable would. The greater the distance is from the computer to the access point, the poorer the signal and the slower the connection. Because of this limitation, large offices often deploy several access points with overlapping ranges. In an open-space environment free of obstruction, 802.11b access points can be as much as 100 m apart. In areas with walls and ceilings in the way 15 m is a useful maximum range. Some access points manufacturers are 3Com (8250), Aruba (A61), Cisco (Aironet), etc.

Larger WLANs, that need more than a couple of access points, can benefit if in addition to access points a WLAN switch is used as well. This device is able to centrally manage and control a certain number of managed access points (for example 12 in case of the 3Com Wireless LAN Switch WX1200). WLAN switches provide more functionality than access points, such as security policies and QoS enforcement, and are ideally suited for moderate sized, but complex, wireless environments with strict security requirements. In addition, through signal strength measurements they can adjust the traffic loads, power and channel assignments of the managed access points so as to maximize transfer rates. The wireless switch uses either radio waves or a direct connection (usually with PoE[14] ports) to communicate with the access points. WLAN switch manufacturers are 3Com

7 Triple Data Encryption Standard.
8 Advanced Encryption Standard.
9 Frequency-Hopping Spread Spectrum.
10 Point-to-Point Tunneling Protocol.
11 Secure Sockets Layer.
12 Virtual Private Network.
13 Personal Digital Assistant.
14 Power over Ethernet.

(WX1200), Aruba (A2400, A800), Cisco (WLSM), Chantry Networks (BeaconMaster), Colubris (CN1250), Symbol (WS 2000), etc.

Some features of several WLAN switches follow [Net-05]. Cisco's Wireless LAN Services Module blade for the Catalyst 6500 switch is essentially a WLAN switch within a switch. It offers access control, plus switching, routing, security and content management functions from other Catalyst blades. While Chantry BeaconMaster supports the OSPF (Open Shortest Path First) routing protocol, and Colubris supports Routing Information Protocol, the Cisco offering supports virtually every major routing protocol available.

Many of the higher-end switches don't require direct attachment to their access points. A company can use one WLAN switch to manage dozens, or even hundreds, of access points scattered throughout the corporation, including at different physical locations. Aruba claims support for 50 access points on its A2400 switch (and 256 access points on the larger A5000). Chantry claims support for up to 200 access points, and Cisco claims support for up to 300 access points with a single WLSM blade.

There are some architectural differences in the methods used to shuttle traffic between access points and switches. Aruba and Cisco products set up Generic Routing Encapsulation (GRE) tunnels between the access points and switches, but each system uses different structures within the GRE tunnel. For example, a protocol analyser that decodes Aruba's traffic will not read Cisco's traffic. Chantry's BeaconMaster encapsulates traffic using IP-in-IP encapsulation. The Colubris CN1250 does not encapsulate traffic, being a stand-alone access point.

The varying transport methods raise inter-operability and performance issues. According to Aruba and Chantry, their switches inter-operate with third-party access points, but they may not offer all the same features as their own gear. Encapsulation adds more overhead, which reduces performance and may introduce packet fragmentation. But encapsulation can be very useful to manage client roaming because it lets clients keep the same credentials and IP address as clients move from one access point to another.

2.3 QoS on WLAN

When a conventional Ethernet segment is saturated, the easy fix is to allocate more bandwidth by increasing the port count or port speed. WLAN environments on the other hand are considerably more dynamic, and static solutions are not very effective. In WLANs, node mobility leads to a significant variation in the workload of each access point. In addition, access points interfere with each other if they are in excess, and port speed is limited by technology to considerably lower values. Moreover more bandwidth is not always *the* solution, especially for applications that are delay/jitter sensitive. Therefore specific QoS mechanisms must be employed on WLANs in order to manage the contention.

2.3.1 IEEE 802.11e

The current Quality of Service (QoS) standard for wireless networks from the widely-used 802.11e family is IEEE 802.11e, which has been approved and published in November 2005. The scope of this standard is to enhance the existing 802.11 Media Access Control (MAC) so as to improve and manage QoS, to expand support for LAN applications with QoS requirements and provide classes of service. In addition the

standard provides improvements in the capabilities and efficiency of the protocol. These enhancements, in combination with the improvements in PHY capabilities of 802.11a and 802.11b, are expected to increase overall system performance, and expand the application space for 802.11. Example applications include transport of voice, audio and video over 802.11 wireless networks, video conferencing, and media stream distribution.

Original 802.11 MAC protocol

The original 802.11 MAC protocol was designed with two modes of communication for wireless stations. The first, Distributed Coordination Function (DCF), is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), sometimes referred to as "listen before talk". A station waits for a quiet period on the network, then begins to transmit data and detect collisions. The time lapse used to check the network is “quiet” is given by a back-off counter which has an initial random value within a predetermined range[15]. DCF provides coordination, but it doesn't support any type of priority access to the wireless medium. As a consequence DCF provides only best-effort service, and there is no mechanism to provide better service for real-time multimedia traffic compared to data traffic.

An optional second mode, Point Coordination Function (PCF), supports time-sensitive traffic flows. Wireless access points periodically send beacon frames to communicate network identification and management parameters specific to the wireless network. Between the sending of beacon frames, PCF splits the time into a contention-free period and a contention period. With PCF enabled, a station can transmit delay & jitter sensitive data during contention-free polling periods.

Although designed to support time-bounded multimedia applications, PCF has several limitations:

(i) PCF lacks differentiation, since it only defines a single class round-robin scheduling, and therefore cannot handle the various requirements of different types of traffic;

(ii) Beacon transmission depends on media contention, and the delay in transmitting a beacon frame affects all data frames that follow it ([Man-02] mentions values of up to 4.9 ms beacon delay for 802.11a);

(iii) Controlling the absolute transmission time of a station is difficult, since legal frames sizes range from 0 to 2304 bytes, and channel rate can vary as well depending on RF conditions.

A common QoS problem for both DCF and PCF is that the 802.11 MAC doesn't specify any admission control mechanism. This implies that under high loads performance will deteriorate in an uncontrollable manner.

Enhanced QoS support

Because of all the aforementioned limitations, the IEEE developed enhancements to both original coordination modes of 802.11 MAC protocol to facilitate QoS. These changes would let critical service requirements be fulfilled while maintaining backward-compatibility with current 802.11 standards, and are grouped in the 802.11e standard.

15 This predetermined range becomes larger as more unsuccessful attempts to access the media are made.

In 802.11e a new MAC layer function called the Hybrid Coordination Function (HCF) is proposed. HCF uses a contention-based channel access method, also called Enhanced Distributed Channel Access (EDCA), that operates concurrently with a polling-based HCF-Controlled Channel Access (HCCA) method.

One important new feature of HCF is the concept of transmission opportunity (TXOP), which refers to a time duration during which a station is allowed to transmit a burst of data frames. Thus, one can solve the problem mentioned earlier of unpredictable transmission time of a polled station in PCF. The maximum value of a TXOP is bounded by $TXOP_{Limit}$.

IEEE 802.11e distinguishes two approaches to QoS, prioritized and parameterized QoS. Prioritized QoS refers to requirements expressed in terms of relative delivery priority, without strict and quantitative service support. Parameterized QoS is a strict QoS requirement that is expressed in terms of quantitative values, such as data rate, delay bound, and jitter bound. EDCA and HCCA address these two modalities, respectively.

Enhanced Distributed Channel Access

The proposed enhancement to DCF – the Enhanced Distributed Channel Access (EDCA) – introduces the concept of traffic categories, therefore enables prioritized QoS. Each station has four traffic access categories (or priority levels), each of which uses a different queue.

EDCA differentiates service classes through three mechanisms: Arbitration Inter-Frame Space (AIFS), minimum and maximum Contention Window size values (CW_{min} and CW_{max}), and transmission opportunity limits ($TXOP_{Limit}$).

When using EDCA, stations try to send data after detecting the medium is idle and after waiting a period of time defined by the corresponding traffic category called the Arbitration Inter-Frame Space (AIFS). Each service class can use specific AIFS values to differentiate the QoS received by the corresponding traffic. A higher-priority traffic category will have a shorter AIFS than a lower-priority traffic category. Thus stations with higher-priority traffic must wait for shorter intervals than those with low-priority traffic before trying to access the medium; hence, they receive better QoS in the sense the delay they experience is lower (see Figure 1).

To avoid collisions within a traffic category, the station counts down an additional random number of time slots, known as a contention window (CW), before attempting to transmit data. If another station transmits before the countdown has ended, the station waits for the next idle period, after which it continues the countdown where it left off. Stations that use smaller CW_{min} and CW_{max} receive better service than the other stations as they need to wait for shorter time periods before they can transmit. Therefore in EDCA such values are associated to higher-priority service classes.

EDCA also allows stations to transmit multiple frames without contending again, known as Contention-Free Bursting (CFB). CFB is limited by the $TXOP_{Limit}$ specified for each service class. A longer limit means that the service class can transmit more frames, thus being given a better QoS from the point of view of throughput. Note that in saturation conditions however CFB has little effect on the operation of the system, since the media will not become idle for sufficiently long in this case.

In EDCA, each station implements a queue for each Access Category (AC). Each queue has its own QoS parameters and back-off counter. A collision within a station is handled

virtually, whereby the frame from the highest priority queue involved in the collision is chosen and transmitted to the access medium. This mechanism is known as virtual collision.

An EDCA contention-based admission control mechanism is also suggested in 802.11e. This mechanism which is based on traffic specifications (e.g., mean/peak data rate, mean/maximum frame size), as advertised by the application when establishing a connection.

We have seen so far that EDCA establishes a probabilistic priority mechanism to allocate bandwidth based on traffic categories. Although the standard itself doesn't require guarantee provisioning, one can model the behaviour of the mechanisms included in 802.11e and calculate the worst-case behaviour. It is thus possible to statistically determine the throughput and delay that application traffic will experience, if the values of the EDCA parameters are known. See for example [Tao-04] for such an analysis.

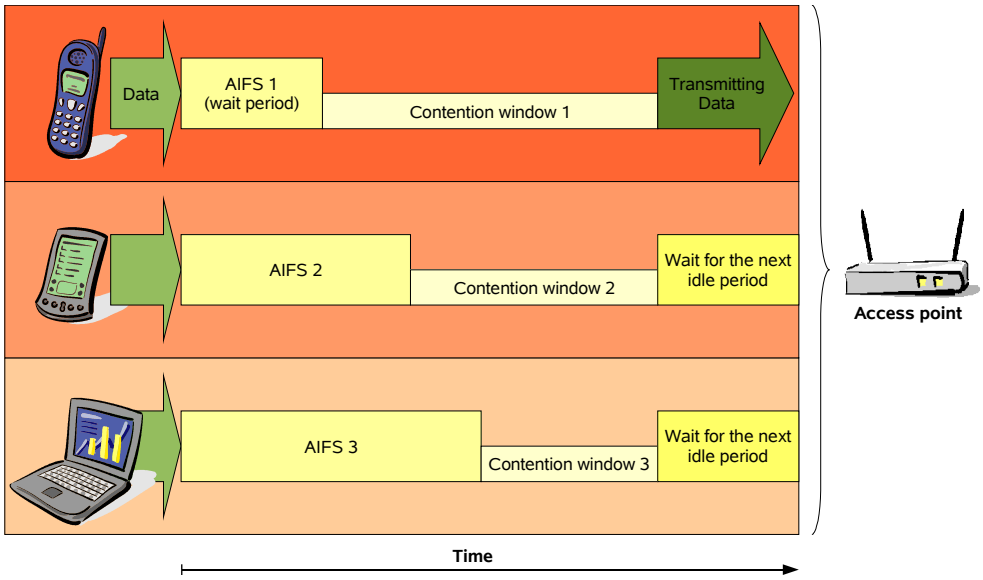

Figure 1: 802.11e operation for different priority categories (source: [Net-05]).

Another performance analysis of EDCA, done through simulation, can be found in [Ni-05]. This paper verified and quantified the properties of the Enhanced Distributed Channel Access. The results confirm that differentiation mechanisms of EDCA can protect higher-priority class from a lower-priority class, but cannot reduce the contention between different traffic flows within the same priority class. The same paper concludes that the default CW values provided in 802.11e may be too small for applications with important bandwidth requirements (such as video streams) when the load approaches 80%. Adaptation of back-off parameters is also deemed useful under variable channel conditions.

HCF-Controlled Channel Access

A different approach to QoS is that of parameterized QoS, and IEEE addresses it through an extension of the polling mechanism of PCF: the HCF-Controlled Channel Access (HCCA). A hybrid controller polls stations during an initial period called contention-free period (CFP). The polling grants a station a specific start time and a maximum transmit

duration. Hence the QoS standard can accommodate time-scheduled and polled communications during such periods. Improved channel access during CFP results in a more efficient polling. The ability to schedule transmissions and chain a sequence of polls in a single command is also included.

HCCA solves the limitations of PCF as follows:

(i) HCCA defines different traffic classes, so that manufacturers can design multi-class scheduling algorithms to support various types of applications;

(ii) A station is not allowed anymore to transmit if the process cannot finish before the next beacon, thus eliminating the potential delay variation;

(iii) The absolute transmission time of a station is bounded through the use of $TXOP_{Limit}$.

An HCCA admission control algorithm is suggested in 802.11e as well. The method checks whether the TXOP of the request summed with the current TXOP allocations exceed or not the maximum fraction of time that can be used by HCCA.

A simulation analysis in [Ni-05] shows that HCCA behaves appropriately when used with Constant Bit Rate traffic streams, but fails to deliver consistent performance for streams with Variable Bit Rate, such as video applications. As a consequence several adaptive schemes are proposed. The paper also emphasizes the fact that admission control mechanisms are a mandatory complement for performance assurance both for EDCA and HCCA.

Other features

The mechanisms that are part of HCF and were described so far provide for maximum efficiency for high-bandwidth streams, power-management friendly implementations, and polled-style access for variable bit rate and bursty streams. The centralized scheduler used in 802.11e guarantees collision avoidance and, therefore, improved ability to deliver time-critical payloads. The ability to honour critical QoS contracts such as delay, jitter and bandwidth is much improved. Channel access is tied to the allocations made by subnet bandwidth manager-like higher-layer protocols and mechanisms so that system reliability is achieved.

In addition to these mechanisms 802.11e proposes improvements in channel robustness, which are achieved through forward error correction (FEC) and selective retransmission. Channel robustness in wireless systems is an important consideration because noise, interference and multi-path effects lead to degraded channel throughput in the 2.4 and 5 GHz bands, adversely affecting the ability to reliably transmit latency-sensitive or high-bandwidth traffic such as voice and video. The proposed schemes include the ability to specify the correction, acknowledgement and retransmission policy on a per-stream basis, thereby accommodating a range of traffic types with policies designed specifically for each. Channel throughput is further improved through the possibility of dynamic channel change.

While 802.11e was being discussed, a group of vendors have proposed the Wireless Multimedia Enhancements (WME) to provide an interim QoS solution for 802.11 networks. Without a standard, the risk of non-interoperable mechanisms proliferating in the marketplace would have inhibited the overall goals of 802.11e. The intention of WME was to provide a well-defined and accepted 802.11 QoS mechanism that will prevent the spread of non-interoperable methods while waiting for the ratification of the 802.11e

standard. How well this worked in practice is debatable, since several companies do have proprietary techniques, sometimes for specific purposes (such as the Air Traffic Control technology from Meru Networks, advertised mainly in connection with VoIP over WLAN). Still, many vendors already implemented preliminary versions of 802.11e, which means in the near future this standard will be supported by most manufacturers.

2.3.2 Related QoS standards

As discussed so far, IEEE 802.11e is mainly a standard for packet prioritization and scheduled access, or call admission control. But even after 802.11e is fully implemented in purchasable products, it probably still won't be enough to ensure quality and reliability for real-time applications in a large enterprise environment, depending on how large an installation is, and on the particular Wi-Fi system vendor's architecture.

In order to improve performance, one is likely to rely on a few other 802.11 extensions. These other extensions relate to speeding up roaming times among wireless Basic Service Sets[16] (BSS) so that sessions aren't interrupted, packets aren't dropped, and quality doesn't degrade. Here are the extensions that should potentially play an important role in QoS enforcement over WLANs:

- 802.11r – This is the fast-roaming protocol (in development) that speeds session hand-off times as a client device moves from one access point (AP) to another, while keeping the user's authentication credentials and real-time session intact. The current working goal is to keep this hand-off time under 50 milliseconds, a value acceptable for real-time applications such as VoIP. *Standard status:* Expected to be stable by September 2006 and ratified in April 2007.
- 802.11k – This is the Radio Resource Management protocol (on which 802.11r relies), which aims to hasten a client's roaming decisions by pre-discovering all neighbouring APs, the distances to them and their available call capacity. *Standard status:* Expected to be stable by June 2006 and ratified in January 2007.
- 802.11i – The pre-authentication component of the security standard reduces roaming time by enabling the client to authenticate with neighbouring APs before roaming effectively. *Standard status:* Complete.

2.4 WLAN performance

There are several factors that impede WLAN performance. This section will review them, as well the issues related to the objective evaluation of the performance of a WLAN system. Some additional issues will be discussed at the end.

2.4.1 Performance factors

Signal strength is probably one of the most important issues that affects WLAN performance. In order to improve signal strength it is essential to place the access points in appropriate places, so that the area they cover is as large as possible. This can be done either by experts with sufficient know-how, or by using automated tools provided by some of the AP manufacturers; when provided the topology of the building these programs can make recommendations concerning AP placement. However the wireless environment is dynamic by definition, and planning cannot do much when the

16 A Basic Service Set is a network of one access point and the stations associated with it.

environment changes. Node mobility and interference with other RF sources (e.g., other APs, or even microwave ovens) diminish static placement effectiveness.

Related to signal strength is the fact that wireless networks employ bit-rate selection algorithms which choose lower or higher transmission rates (and the associated encoding) depending on the presence or absence of packet loss over a certain interval. A typical example is the Auto-Rate Fallback (ARF) mechanism of 802.11 networks. Note that the goal of these algorithms can be to minimize loss or to maximize throughput, which are not necessarily equivalent. Extensive research is carried out in order to dynamically maintain an optimum bit-rate that maximizes throughput (see, for example, [Bic-05]). On the other hand loss has a significant effect on the performance of applications such as VoIP, which are particularly loss sensitive. It is certain that no matter what mechanism is used under poor signal conditions the WLAN will operate at a lower rate than the maximum nominal rate.

Another issue that most users overlook is the significant overhead that the wireless communication protocol involves. The WLAN MAC protocols have the following effects [IEC-05]:

- Ethernet type CSMA/CA protocols, such as DCF and EDCA, limit capacity at approximately 37% of the peak data rate;
- Scheduled TDMA (Time Division Multiple Access) protocols such as PCF and HCCA can theoretically reach around 90% capacity of the network, but under full load they will typically carry only approximately 75% of capacity;
- DCF/EDCA protocols do not effectively manage network latencies as the capacity limit is approached;
- PCF/HCCA protocols control latencies by providing fair weighted queuing so that in principle all users will receive service even under full load conditions.

The following table shows the throughput rates for PCF/HCCA and DCF/EDCA for various modulations. These values should be further reduced when applied in connection with larger cells that operate with lower capacity modulations.

	Throughput (Mb/s)	
Modulation	**PCF/HCCA (75%)**	**DCF/EDCA (37%)**
54 Mb/s OFDM	40.5	19.98
22 Mb/s PBCC[17]	16.5	8.14
11 Mb/s CCK	8.25	4.07
5.5 Mb/s CCK	4.125	2.035

Table 1: WLAN throughput rates for CSMA/CA and TDMA type protocols (source: [IEC-05]).

As a rule of thumb, in WLAN planning one should de-rate the theoretical performance figures to approximately 70% to 80% of the peak capacity. It has been shown that with packet aggregation and proper use of 802.11 protection mechanisms, DCF/EDCA can achieve higher levels of throughput (approximately 50% to 55% higher) with a limited number of users and limited number of connections requiring QoS capabilities. However this does not address however the concerns related to the stability of DCF/EDCA under a high user load [IEC-05].

17 Packet Binary Convolution Coding.

Note that in addition to the widely recognized throughput problems documented above there are other performance issues as well with WLAN MAC protocols, namely regarding delay and packet loss. Unfortunately these issues are not yet thoroughly explored, although it is has been proven that for real-time streaming applications such as VoIP it is the delay and packet loss that have the most important influence on user satisfaction and not the global throughput (see [Beu-04] for a related analysis on wired networks). The next section will explore in more detail the issues that exist in connection with WLAN performance and its measurement.

2.4.2 Performance measurement

The wireless Ethernet, IEEE 802.11, evolved to be more elaborate than its wired counterpart, 802.3. The inherent mobility and erratic transmission environment require new MAC protocols, therefore lead to an increased complexity. This adds significantly to the number of test metrics that are needed to quantify WLAN system performance and behaviour. A rough count shows that WLAN metrics outnumber traditional Ethernet metrics by a factor of 5:1 [Mli-04] (see also Table 2).

In order to assess performance, troubleshoot problems and do research on WLANs, a methodology for measuring performance is required. Testing of 802.11 devices is still a challenge for industry. Protocol complexity determines a test complexity that is further cumulated with the prevalence of RF interference and the mobility of wireless devices.

RF interference makes it difficult to obtain reproducible results that can be correlated with those obtained in other locations. Interference from phones, microwave ovens and adjacent wireless networks may force devices to retransmit or continuously vary data rate, thereby producing random results. [Mli-04] reports that in a particular experiment open-air frame forwarding rate varied, in an non-reproducible way, between about 2260 frames/s and 1750 frames/s (compared to the stable 2270 frames/s in a controlled RF environment).

The IEEE committee that standardizes the procedure for testing wireless systems is 802.11T. The corresponding standard is expected to be finalized in January 2008. The goal of the 802.11T project is to provide a set of performance metrics, measurement methodologies, and test conditions to enable manufacturers, test labs, service providers, and users to measure the performance of 802.11 WLAN devices and networks at the component and application level. The standard that is being developed by this group should supply IT managers with a set of standard benchmarks similar to that existing for wired Ethernet. Therefore the 802.11T committee plans to model its work after the IETF[18] RFCs[19] 2285, 2544, and 2889 ([Man-98], [Bra-99], [Man-00], respectively) that specify metrics and methods for evaluating the performance of Ethernet switches. Measurements such as throughput, packet loss, delay, and jitter can be based on these RFCs, but in addition 802.11T will have to define new wireless-specific metrics.

Table 2 is a comparison between wired and wireless metrics, as proposed in the 802.11T draft, showing the relative complexity of wireless protocols [Mli-03]. The metrics are divided in five categories: packet forwarding, security, QoS, behavioural (i.e. handling of abnormal conditions), rate adaptation, and roaming. Note the high impact an unstable physical layer would have on practically every measurement.

18 Internet Engineering Task Force.
19 Requests for Comment.

Metric category	Wired-network metrics	Wireless-network metrics	Impact of an unstable wireless environment
Packet forwarding	Loss	Loss	**High**
	Forwarding rate	Impact of rate adaptation on loss	**High**
		Impact of roaming on loss	**High**
		Impact of overlapping BSSs on loss	**High**
		Impact of RTS/CTS[20] on loss	**High**
		Impact of power management on loss	**High**
		Impact of MAC layer fragmentation on loss	**High**
		Impact of encryption on loss	**High**
Security		Association performance	**High**
		Authentication performance	**High**
		Association and authentication capacity	Low
QoS	Delay	Delay	**High**
	Jitter	Jitter	**High**
		Impact of rate adaptation on delay & jitter	**High**
		Impact of roaming on delay & jitter	**High**
		Impact of overlapping BSSs on delay & jitter	**High**
		Impact of RTS/CTS impact on delay & jitter	**High**
		Impact of power management on delay & jitter	**High**
		Impact of MAC layer fragmentation on delay & jitter	**High**
		Impact of encryption on delay & jitter	**High**
		WME relative priority forwarding rate	**High**
		WSM stream bandwidth allocation	**High**
Behavioral	Head-of-line blocking	Forwarding in presence of congestion	Medium
	Error analysis (runts, jabber, etc.)	Security counter measures	Low
		Power save	Medium
Rate adaptation		Rate adaptation time	**High**
		Rate adaptation hysteresis	**High**
		Rate vs. range	**High**
Roaming		Roaming time	Medium
		Roaming session continuity	Medium
		Roaming hysteresis	**High**

Table 2: A comparison of wired and wireless metrics (source: [Mli-03]).

20 Request To Send/Clear To Send optional function of 802.11, intended to minimize collisions among hidden stations.

From the point of view of QoS, real-time services require bounds on roaming speed, network delay and jitter. The Wi-Fi Alliance [WiFi] is developing specific test metrics for its two MAC layer QoS protocols, Wireless Multimedia Extension (WME) and Wireless Scheduled Multimedia (WSM), that are subsets of the 802.11e specification. WME is a contention based protocol that manages relative priorities and is similar to DiffServ [Bla-98]. WSM is a polling based protocol that supports bandwidth reservation for data streams, and is similar to RSVP [Bra-97].

The 802.11T committee is also considering several solutions to deal with mobility and interference when testing wireless systems. One is based on a cabled environment that uses programmable RF attenuators to emulate variable distances between devices. In such an environment, each device in a test setup is placed in a shielded chamber for isolation. RF cables connect the antenna ports of each device under test to other devices through programmable attenuators that emulate physical distances between devices by controlling the signal levels at the antenna ports. Shielding and filtering protect the test setup from outside interference and achieve device-to-device isolation. Devices can connect through a network of attenuators and combiners to emulate complicated multi-BSS topologies.

At the moment there are several manufacturers who provide equipment for testing WLANs. VeriWave, for example, provides WaveTest, a multi-client traffic generator and performance analyser. WaveTest offers a set of purpose-built test suites for various aspects related to roaming, scalability, load, security. The same company provides a specifically-tailored test system that can be used to test the performance of VoIP on WLAN, the VoIP over WLAN Test Analysis Suite. AiroPeek series of products from WildPackets is another example of WLAN analysis systems.

When the wireless devices have rich capabilities (e.g., PDAs such as Sharp Zaurus), it is possible to perform some tests using traditional bandwidth-measurement tools for wired networks such as Iperf [NLA-05]. However these solution are not very accurate for delay measurements. Moreover access to low-level control and information for the wireless cards is required in order to perform the all the meaningful tests and acquire the full data needed to interpret the results.

2.4.3 Other issues

Another problem, which is not essential for application performance, but that may nevertheless affect user satisfaction is that of security. Most WLANs today, for reasons of simplicity and performance, use WEP (Wired Equivalent Privacy) for data encryption over wireless networks. Unfortunately WEP can be cracked relatively easy, and this can pose problems to business users [Vau-03].

Alternative solutions exist, such as WPA (Wi-Fi Protected Access), but WPA has other vulnerabilities. By design WPA will shut itself down if unauthorized access from the same user is attempted twice within one second. The sensitivity of detecting that the system is under attack makes it simultaneously prone to very simple Denial of Service (DoS) attacks [Vau-02].

Other solutions are available, such as that of building VPNs, or SSL encryption, but as mechanisms become more secure, the overhead they imply gets larger, thus lowering even more the communication performance of WLANs. Obviously in the end this is a matter of trading-off speed for security.

3 Voice over IP

Voice over IP (VoIP) is the real-time application that is probably the most widely-spread on today's networks. I'll provide here some basic facts related to VoIP. For a more detailed description and a performance analysis of VoIP over fixed LANs see for example [Beu-04].

3.1 Overview

Figure 2 shows the end-to-end path as needed for VoIP communication (a similar path exists in the opposite sense for a bi-directional connection). An audio input device, such as a microphone, is required at the sending end. The audio signal is transformed into digital form by an analog-to-digital converter. Due to the packet-switched nature of computer networks, voice data has to be packetized and encoded prior to being transmitted. Encoding (as well as decoding) is done by codecs that transform sampled voice data into a specific network-level representation and back. Most of the codecs are defined by standards of the International Telecommunication Union, the Telecommunication division (ITU-T). Each of them has different properties regarding the amount of bandwidth it requires but also the perceived quality of the encoded speech signal.

After binary information is encoded and packetized at the sender end, packets encapsulating voice data can be transmitted on the network. Voice packets interact in the network with other application packets and are routed through shared connections to their destination. At the receiver end they are decapsulated and decoded. Decoding may include other steps as well, the most typical being dejittering. Other examples are error correction and packet loss concealment. The flow of digital data is then converted to analogue form again and played at an output device, usually a speaker.

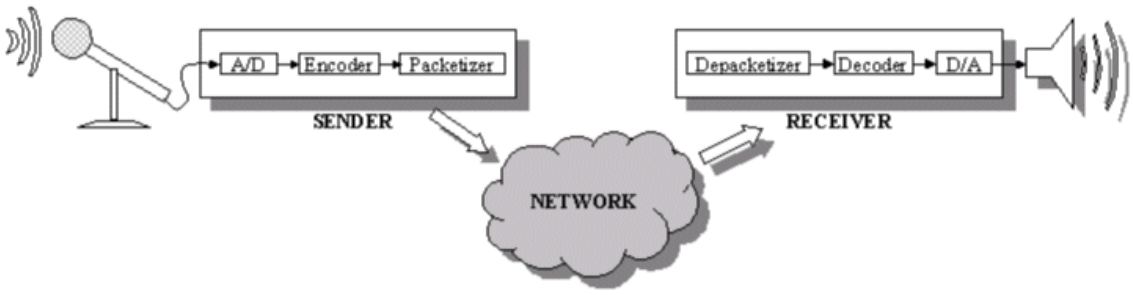

Figure 2: End-to-end data path for VoIP communication.

3.2 VoIP issues

There are at the moment IP phones which are similar in shape with the regular telephones but instead of being connected to a phone socket they are plugged into a network connection. There exist as well IP phones with built-in wireless support. Hence the act of making a phone call using VoIP can be identical to that of using regular phones. The quality of the communication itself can be different however, and it is the most important aspect of the transition from standard telephone networks to Internet telephony.

One reason for such a transition is that VoIP communication is more flexible than standard telephony. By making the appropriate choice for the codec one can control the amount of bandwidth required and one determines the intrinsic associated quality.

Moreover, by managing properly the network one can use the codec which provides the desired quality level, since resources in computer networks can be allocated in different manners for various uses. Nevertheless the main advantage is probably that with VoIP one can use the computer network infrastructure for voice communication, thus eliminating the need for the parallel phone infrastructure.

However, since the communication channel is not reserved but shared with other applications, voice packets can arrive at the receiver with a different inter-packet gap than they had at the sender, out of order, and some of them can even be lost. Assessing the relationship between precisely these factors, as quantified by means of network QoS parameters, and the User-Perceived Quality (UPQ) of VoIP communication is a prerequisite for any performance and dependability analysis of VoIP over WLAN.

The main QoS parameters that quantify the quality degradation over a certain connection are the following: throughput, delay & jitter and packet loss. Note that this discussion refers to both cases of wired and wireless networks. Even though wireless networks are characterized by significantly more parameters (due to multiple causes that induce delay and jitter, for example; see section 2.4.2), the factors that influence application performance are still the same.

Let's analyse the influence of each of the main QoS parameters now. Given the low requirements of VoIP in terms of bandwidth (64 kb/s maximum), bandwidth in usually not a problem, at least for individual voice calls. Simultaneous voice calls however can have a cumulated throughput requirement that approaches the limits of the network equipment used.

Delay & jitter are probably the most important for VoIP as a real-time streaming application. Packets containing voice data must be delivered in a timely manner in order to ensure user satisfaction. One-way delay influences interactivity: the larger the delay the lower the perceived interactivity for the persons who communicate. Jitter on the other hand (i.e. one-way delay variation) influences quality if it exceeds a maximum value. This maximum value is system dependent, and is related to the size of the dejittering buffer used. A large buffer means that jitter has a smaller effect on perceived quality, but it decreases interactivity through the effect of delay. If the induced jitter value exceeds the size of the dejittering buffer, then VoIP packets don't arrive in time for playback, and playback signal quality drops. Hence this distortion is the main effect that jitter has on user satisfaction. Packets that don't arrive in time for playback can be considered lost; therefore this effect is sometimes termed *jitter-loss*.

VoIP data streams are usually of UDP type, and in this case packet loss has only momentary effects. When packets are missing for playback, the system either introduces gaps in playback, or tries to recover from this error by replacing the gap with something more appropriate (previous voice samples, a reconstructed signal, etc.). No matter what the system's robustness is, packet loss will surely cause a certain quality degradation to occur. This degradation is larger when loss happens in bursts (a number of consecutive packets being lost) since such an event has a higher influence on VoIP perceived quality than spaced losses. Unfortunately bursts are precisely how losses occur in real networks, since congestion will hardly ever affect only one packet at a time.

3.3 VoIP quality measurement

In order to evaluate system performance when using various applications it is necessary to use specific metrics for each application; this makes it possible to measure the User-

Perceived Quality (UPQ) for the corresponding application in an objective manner.

Modern telecommunication networks provide a large set of voice services using many transmission systems. The rapid deployment of digital technologies in particular has lead to an increased need for evaluation of the transmission characteristics of new communication equipment in terms of user-perceived quality.

The methods for UPQ assessment can be divided in two main classes: intrusive and non-intrusive. Intrusive methods use special test signals, generally produced artificially by a stimulus generator so as to have similar characteristics with human speech. These test signals are sent through the network between two end points. Based on the reference input signal and the received degraded signal a quality metric is computed that corresponds to the connection between those two end points.

Non-intrusive UPQ measurement requires the use of traffic monitors. One category of such methods uses general traffic measurements of QoS parameters to predict the quality of a voice communication that would take place over that channel. Another category of methods analyses the content of the real voice traffic transiting the network. Comparing it's properties with that of human speech such methods can estimate the associated quality metric.

ITU-T has defined several standards that allow an evaluation of the quality of voice communication. The first of them was a subjective metric (the MOS), but successive attempts have been made to define objective metrics as well. The two main methods to measure the VoIP UPQ that are currently used are the E-model, and the PESQ score. These three ITU-T recommendations are detailed next.

3.3.1 Mean Opinion Score (MOS)

In 1996 ITU-T has defined the methodology of determining how satisfactorily given telephone connections may be expected to perform [P.800]. The methods described by this recommendation are intended to be generally applicable for any possible form of degradation: loss, circuit noise, transmission errors, environmental noise, talker echo, distortion due to encoding, etc.

The evaluation procedure is based on subjective tests in which quality is graded by human experimenters. The following values are assigned depending on the quality of the connection:

$$Excellent = 5;\quad Good = 4;\quad Fair = 3;\quad Poor = 2;\quad Bad = 1$$

The distinction between mean conversation-opinion score (MOS_C) and mean listening-opinion score (MOS_L) is made. In the second case only the intrinsic audio quality is taken into account, whereas the first case includes the experimenter's opinion about the level of interactivity.

3.3.2 E-model

The E-model first appeared in 2000, and was updated several times, the last revision being from 2005 [G.107]. This recommendation proposes a non-intrusive UPQ assessment method. The E-model is a computational model for use in transmission planning, hence a transmission rating model that can be used to help ensure that users will be satisfied with end-to-end transmission performance.

The model integrates in the rating value R, called *transmission rating factor* (R-value), the impairment factors that affect communication equipment, including delay and low bit-rate codecs. These impairments are computed based on a series of input parameters for which default values and permitted ranges are specified. These should be used if the corresponding impairment situation occurs. The general formula is:

$$R = R_0 - I_s - I_d - I_{e-eff} + A$$

where:

R_0	=	basic signal-to-noise ratio
I_s	=	factor for impairments that are simultaneous with voice transmission
I_d	=	delay impairment factor
$I_{e\text{-}eff}$	=	packet-loss-dependent effective impairment factor
A	=	advantage factor (system specific)

Since the computation of the rating factor R involves a large number of parameters, complementary recommendations and appendices have been proposed by ITU-T, such as [G.108] and [G.113] that give the values for these parameters for pre-determined conditions for which the model has been calibrated.

The MOS score (equivalent to the mean conversation-opinion score MOS_C from [P.800]) can be obtained from R using the following formulae:

$$For\ R < 0: \quad MOS = 1$$

$$For\ 0 \le R \le 100: \quad MOS = 1 + 0.035 \cdot R + R(R-60)(100-R) \cdot 7 \cdot 10^{-6}$$

$$For\ R > 100: \quad MOS = 4.5$$

The graph of the dependency of MOS on R is shown below. Note that the maximum obtainable MOS is 4.5, the average score that usually results from subjective tests for excellent quality, since experimenters' grades are known to vary between 4 and 5 in such conditions.

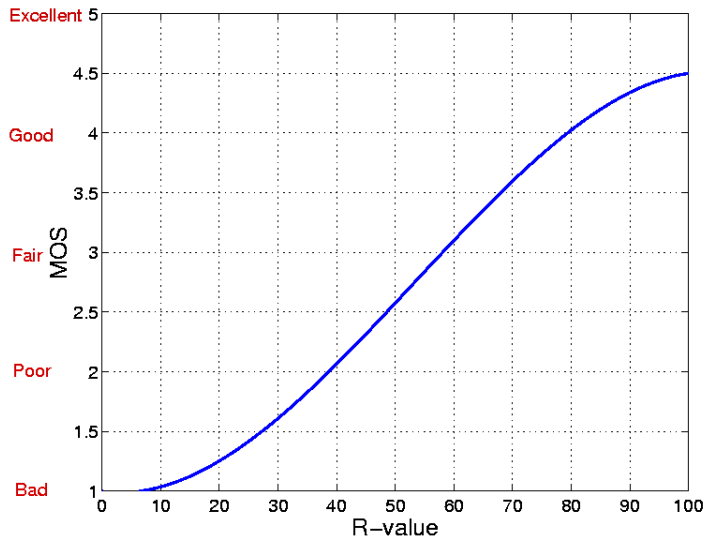

Figure 3: MOS versus rating factor R.

A guide of the relationship between the rating factor R (R-value), MOS value and user satisfaction is given in the table below:

R-value (lower limit)	MOS (lower limit)	User satisfaction
90	4.34	Very satisfied
80	4.03	Satisfied
70	3.60	Some users dissatisfied
60	3.10	Many users dissatisfied
50	2.58	Nearly all users dissatisfied

Table 3: The relation between the rating factor R, MOS value and user satisfaction.

3.3.3 PESQ

In February 2001 ITU-T has defined the PESQ score [P.862], which is an objective method for predicting the subjective quality of narrow-band telephony and speech codecs. PESQ combines the best features of two previous standards: PSQM (Perceptual Speech Quality Measure) and PAMS (Perceptual Analysis/Measurement System), as a result of being produced jointly by their respective developers KPN[21] and British Telecom). In addition to PSQM, PESQ takes into account filtering, variable delay, coding distortions and channel errors. PESQ has been thoroughly tested and has demonstrated acceptable accuracy for the following applications: codec evaluation and selection, live network testing using digital or analogue connection to the network, testing of emulated and prototype networks.

PESQ score computation requires both the original and the degraded voice signal, therefore it is an intrusive method. The key process in PESQ is the transformation of both the original and degraded signal into representations analogous to the psychophysical representation of audio signals in the human auditory system.

The PESQ score is mapped by design to a MOS-like scale, a number in the range of -0.5 to 4.5, although for most cases the output range will be between 1.0 and 4.5, the normal range of MOS values found in subjective listening quality experiments.

According to [Ser-01] the relationship between PESQ scores and audio quality is the following:

- PESQ scores between 3 and 4.5 mean acceptable perceived quality, with 3.8 being the PSTN[22] threshold – this will be termed as *good quality*;
- Values between 2 and 3 indicate that effort is required for understanding the meaning of the voice signal – this will be named *low quality*;
- Scores less than 2 signify that the degradation rendered the communication impossible, therefore the quality is *unacceptable*.

Being the most recently developed metric, PESQ outperforms the previous ones, such as PSQM or PAMS. Unlike the E-model, it doesn't require any knowledge regarding the network and uses only the original and degraded signal to compute the PESQ score.

21 Koninklijke PTT Nederland, the Dutch telecommunication company.
22 Public Switched Telephone Network.

3.3.4 Metric comparison

Since MOS is not suited for automated testing, we'll focus in this section on a comparison between the two objective metrics presented above: the E-model and the PESQ score.

Being given only by mathematical formulas, the E-model's R-value is very easy to compute once the values for its parameters are decided. Note however that the values of these parameters are provided only for a pre-determined range of conditions (i.e. specific codecs etc.). Therefore this model cannot be used, for example, to test the deployment of a newly developed codec since the associated parameters for this codec are not provided by ITU-T. On the other hand the PESQ score is computed based on the original and the degraded waveforms, hence the codec or other experimental conditions are irrelevant for its computation. However effectively obtaining both these waveforms may be challenging, depending on the particular experimental conditions.

The E-model takes into account one-way delay by design, unlike the PESQ score which is only a listening score. For PESQ predetermined thresholds are used to determine the level of interactivity: good, if the one-way delay doesn't exceed 150 ms, acceptable if the delay is between 150 and 400 ms, and unacceptable otherwise. As specified in section 3.2, jitter influences voice quality through the packet loss it induces during its interaction with the dejittering buffer. Therefore the R-value doesn't take jitter into account directly, and the packet loss due to jitter under certain conditions must be evaluated separately and integrated in the formula. This is not an issue for PESQ, where the effects of jitter are present in the degraded waveform.

To conclude, for PESQ score computation voice recording capabilities are essential in order to have an accurate estimate, whereas for the E-model's R-value it is mandatory to make traffic measurements and appropriately choose the values of the model parameters. The comparison above is summarized in the table below:

R-value	PESQ score
Requires traffic measurements	Requires voice recording
Test pre-determined conditions	Independent on conditions
Easy to compute	Uses complex models
Accounts for one-way delay	Listening-only score
Jitter needs separate treatment	Jitter is taken into account

Table 4: R-value versus PESQ score.

3.4 VoIP codecs

The voice signal must be encoded (and compressed) in order to be sent over the packet network. For this task systems called codecs are used. Each codec has different characteristics concerning the data rate it uses (and implicitly the compression level) and also the associated user-perceived quality. For example, the G.711 codec [G.711] sends data at 8 kHz with 8 bits per sample, resulting in a data rate of 64 kb/s. The sound is in PCM[23] format, encoded using the μ-law. Another codec, G.726 codec [G.726], converts a 64 kb/s μ-law or A-law PCM channel to and from a 40, 32, 24 or 16 kb/s channel. The GSM (Global System for Mobile telecommunications) codec [Rah-93] uses linear predictive coding (LPC) to compress speech data at 13 kb/s. The G.729 codec [G.729] is

23 Pulse Code Modulation.

frequently used for VoIP communication. It sends data at 8 kb/s using conjugate-structure algebraic-code-excited linear-prediction (CSACELP).

The table below summarizes the main characteristics of these codecs, including the MOS score for User-Perceived Quality (these values are based on the results in [Beu-04]):

Codec	Data rate [kb/s]	Network rate [kb/s]	Audio data [ms]	MOS value
G.711	64	76	40	4.3
G.726	32	38	80	3.8
GSM	13	19	80	3.4
G.729	8	17	80	3.5

Table 5: Codec characteristics for several commonly-used codecs (source: [Beu-04]).

3.5 VoIP call equipment

The most encountered way of making VoIP calls used to be by using headphones and a microphone while sitting in front of a computer. However nowadays there are manufacturers who provide VoIP phones. All the firmware required to make phone calls is built into these devices, and they are identical in shape to regular phones. Although more convenient, these systems have the disadvantage of being less configurable than pure software solutions.

Recently mobile phone manufacturers have also introduced a new type of device: the mobile phone that has both GSM and WLAN capabilities, and even more. An example of such a phone is HP's 6300 series Smartphone that has GSM, GPRS, Wi-Fi, and Bluetooth networking. Motorola also manufactures the CN620 handset, which has similar functionality, except for Bluetooth. Ideally this introduces the possibility of moving seamlessly between GPRS and Wi-Fi networks, with the phone automatically selecting the type of network that provides the best performance at one particular location.

When making VoIP calls, it is usually necessary to have a call server, that manages the multiple simultaneous calls and establishes the connections. The function of the call server is similar to that of the PSTN switch. For example a device like the SpectraLink H.323 call server can be used for this purpose.

4 VoIP over wireless LANs

Users of wireless networks are involved in several domains: enterprise (managers, IT personnel and other campus mobile workers), education (principals, professors, maintenance staff), health (doctors, nurses, technicians), manufacturing (supervisors, quality control people, experts), retail (managers, inventory clerks, shipping/receiving personnel). Several reasons make WLANs essential for their activity. These users are highly mobile, either because they don't have a desk or because they are away from their desk a significant amount of time. They need to be instantly reachable (currently the primary communication strategy is voice, plus messaging). They also require instant access to key data.

In this context VoIP over WLAN (VoWLAN) appears as the most obvious solution for the voice communication of mobile type that these users need. IP telephony has low-bandwidth requirements (below 64 kb/s), therefore one may assume that VoIP is easy to use on wireless LANs. However combining the two technologies today is difficult. Experiments show that even a small amount of data traffic on the same network can lead to seriously degraded audio quality and dropped calls, even with QoS features enabled [Net-05].

The main reason is that, when handling voice and data traffic on the same network, contention must be managed in terms of delay & jitter rather than forwarding rates. Most vendors only begin to adjust their products for voice/data convergence, therefore performance of VoIP (and real-time applications in general) over wireless media can be an issue. Note that the difficulty in finding appropriate QoS solutions derives from some of the inherent properties of WLANs. In wireless networks packet error rates can be in the range 10-20%. Moreover bit rates vary according to channel conditions; hence bandwidth reservation at connection setup time might not hold throughout the entire duration of the communication.

4.1 No QoS-enforcement scenario

We'll analyse first the everyday situation when no contention management techniques is used. Under these circumstances systems usually encounter no problem in delivering near-toll-quality audio, even without QoS enforcement, when only a small number of calls are active. Depending on system features, a number of simultaneous calls of six and above may lead to decreased audio quality, and some of the calls may even be dropped [Net-05].

If background data is added to the scenario then VoIP performance deteriorates seriously. This is the case even when the total amount of traffic doesn't exceed half of the sustainable rate of a network (3 Mb/s compared to 6 Mb/s as reported in [Net-05][24]).

This situation is not unexpected given that the lack of QoS implies that there is no control over the interaction between different application traffic flows. Not managing contention leads to unpredictable results, which can have adverse effects on real-time applications such as VoIP.

24 Note that in these tests UDP traffic was used. The characteristics of the traffic in real networks are still an object of research. UDP-type traffic is the simplest model, but bursty traffic, as generated by TCP/IP transfers is probably a more realistic model. Such bursty traffic usually increases the observed performance degradation.

Under such circumstances the "miracle solution" in fixed networks is to throw bandwidth at the problem and over-provision the network capacity by a couple of orders of magnitude. It is a known fact that on many existing 1 Gb/s and higher-rate networks the average utilization is below 1%. Unfortunately this is not feasible for wireless networks, where rates of only 54 Mb/s are still a luxury.

The industry realized that to deploy successfully VoIP on WLANs the networks need to be optimised for voice traffic. QoS enforcement is nowadays recommended by WLAN equipment manufacturers when deploying multiple applications with different requirements on the same WLAN.

4.2 QoS-enforcement scenario

As discussed in Chapter 2, several complementary solutions exist for managing contention in WLANs, and the existing standard was only published in November 2005. As a consequence it is not surprising that VoIP over WLAN tests in [Net-05] demonstrate that various issues appear even when enforcing QoS.

This is not to say that enabling QoS has no effect. The same report shows that, generally, the QoS mechanisms currently implemented in WLAN devices can cope with handling the quoted maximum number of simultaneous VoIP calls for the corresponding system without a significant decreased in perceived quality.

However, as soon as background data traffic is added[25], VoIP performance worsens significantly, going to levels at which some or even many users will be dissatisfied (according to the ITU-T view on perceived voice quality in [G.107]). When using both voice and data some products could not even handle the recommended maximum number of calls.

Measurements of delay & jitter in the same scenario using voice and data simultaneously, are reported in [Net-05] as well. The results show that, even though their average values were acceptable (below 50 ms generally), there were packets which had significantly higher delays and jitter values (up to 5 times higher).

Since no QoS over WLAN standard existed until recently, most manufacturers, both for WLAN equipment and WLAN phones, implemented either proprietary QoS mechanisms or preliminary versions of 802.11e (such as a subset of 802.11e, the Wireless Media Enhancements protocol). Hence there is no unified way to manage quality in current day WLANs, and one can only hope that such an unified way will emerge once all manufacturers integrate 802.11e in their products.

The QoS mechanism most often supplied is related to bandwidth management. Existing QoS implementations in WLAN devices allow the allocation of bandwidth to a given workgroup. Allocating bandwidth to a given workgroup is useful in distinguishing between employees and guests associated with the enterprise network. Some devices, such as Aruba and Cisco products, can also allocate bandwidth on a per-user basis. However in the case of VoIP and other real-time applications it is the timely servicing of high-priority traffic that matters, not the average data rates.

Aruba, Chantry and Cisco manufacture wireless LAN switches that are intended to improve QoS enforcement in networks with more that a few access points. In this case user authentication and spectrum management decisions are made by the wired Ethernet switch (handling user authentication and radio frequency management), not by the access

25 Again of UDP type, according to the cited report.

points. The switch not only controls access to the wired network, but also dynamically adjusts wireless radio signal strength in response to changes in the RF environment.

Another important fact to consider is that the 802.11e QoS over WLAN standard doesn't provide by design any guarantees concerning the level of quality degradation, and implicitly the associated application performance. However extensive research on 802.11e has shown that it's behaviour can be modelled with a sufficient degree of accuracy [Che-04], [Kim-04], [Oe-05], [Tao-04]. This means that one can configure the parameters of 802.11e so that in worst-case conditions it always enforces the required boundaries on quality degradation. Note that there is a reverse side for this: over provisioning will inevitably occur when designing a system for worst-case conditions; therefore a significant amount of WLAN valuable resources will probably be wasted under normal operation conditions.

One should also bear in mind that the ordinary “thin” access points have limited capabilities, and sometimes cannot ensure timely traffic delivery even if they implement 802.11e mechanisms. Using switches as indicated before and their more advanced QoS mechanisms, such as scheduling, should improve performance. Other suggestions for further improving quality are reducing the number of concurrent calls through access control, and using the other standards related to IEEE 802.11e (see section 2.3.2).

4.3 Multiple access points

Mobility for voice communication is a major driver for WLAN deployment. Just as cellular phone users move from one coverage area to another, so will WLAN handset users on any site which has more than one access point. The time needed for a call to migrate from one access point to another (i.e. to roam) is an essential parameter in this case.

The report in [Net-05] presents measurements related to roaming in various configurations involving one, six and seven calls, with and without background data. According to this paper Cisco performed best in the single-call case, with a roaming time of 0.433 seconds, and all systems roamed one call in about 0.5 seconds. Compare these values with the working goal of the roaming-related standard IEEE 802.11r, which is to keep the hand-off time under 50 ms. A half-second gap is clearly noticeable to the human ear – as is any gap of around 70 ms or more – but except for this audio quality was generally deemed high.

To illustrate the differences between various systems, here is a summary of the full results in [Net-05]. Aruba excelled in the roaming tests. Its average hand-off times ranged from about a half-second for one call, to just more than 1 second for the seven-calls-with-data scenario. While that kind of delay will be noticeable to callers, it was still by far the fastest roaming performance of any product. In Cisco's case average roaming time went from 0.433 seconds with one call to 1.053 seconds with seven calls – and then it leapt to 4.324 seconds with seven calls and background data. Colubris results were counter-intuitive: roaming took an average of more than 5 seconds without data, compared to about 2 seconds with data. Chantry's BeaconMaster couldn't perform the roaming test with six or seven calls, even without background data present. Calls were dropped rather than roamed in those configurations. The highest number of calls that could roam through the BeaconMaster was two.

[Net-05] also underlines the contrast between roaming at the 802.11 link layer and at application layer, which showed startling results. In many cases, delays of even a few

dozen milliseconds in link-layer 802.11 roaming led to delays of 10 seconds or longer at the application layer. The fact that even minor issues at the link layer had a major effect at the application layer emphasises the need for well-behaved 802.11 implementations, as well as the need to model the relationship between application perceived quality and the network delivered quality.

WLAN switches can manage access points at remote locations, hence it is useful to know whether roaming times and call quality would be affected if the access points are at different locations than the switch. [Net-05] presents such tests with a 100 ms round-trip delay between the switch and the APs. The tests were completed with Aruba and Cisco. Without data, local and remote roaming times were essentially identical for both vendors, around 1 s. With data present, Aruba's roaming times rose from the 1 s value in the local case, to about 3.5 s in the remote scenario. Cisco's remote roaming time (around 2 s) was actually lower than the local test (4.3 s, see above), which is counter-intuitive. This result seems to validate in a way Cisco's claim that access points can "pre-authenticate" clients, resulting in no performance penalty for remote access points.

4.4 Critical-condition issues

We have shown so far that in order to ensure a successful VoIP deployment on WLAN it is necessary to take special measures. If the system fails to provide the appropriate conditions, the direct result is user dissatisfaction due to poor audio quality and calls being dropped. Although unpleasant, under normal circumstances this is only important for those who provide VoIP services on WLANs, since it may lead them to lose customers.

However if we consider those environments where VoIP services are used to communicate essential messages, such as in mission-critical or safety-critical environments, the impossibility to communicate in satisfactory conditions can have severe consequences. For example the inability to communicate in a disaster situation can even lead to life losses.

In order to handle calls a VoIP system requires both power and an operational network. For VoIP systems on wired networks this means that backup power and/or a backup communication system are required in the event of network or power outages. However mobile systems already have their own independent power sources, and the fact that WLAN networks can be created *ad-hoc*, hence they are decentralized, makes them more stable and robust than oth er communication networks. For this reason they appear as an optimum solution for life-line or safety-critical services.

Disaster/critical conditions require deptendable communication systems, both in the preceding phase of the events, to issue warnings and evacuation instructions, as well as during and after catastrophes happen, to coordinate the activity of the rescue teams. Unfortunately recent events such as such as the Indian Ocean tsunami in 2004, or the 2005 hurricanes Katrina and Rita in U.S.A. have shown that the current communication systems fail too easily under emergency conditions.

The U.S.A. federal government report on the response to hurricane Katrina [Tow-06] outlines the failure of the communication infrastructure as one of the major problem in the federal response, and identifies correcting this issue as a critical challenge. The report proposes the creation of a National Emergency Communication Strategy, and provides 125 specific recommendations for policy makers and emergency managers. One of the important points of the recommendations related to emergency communication systems

included in this report is that “there is a strong need for rapidly deployable, interoperable, commercial, off-the-shelf equipment”.

An independent study of the same event [Com-05] highlights several incidents that prevented emergency workers to provide a better response: police officers were unable to communicate because their radio channels were overwhelmed, vehicle access could not be coordinated due to improper communication, rescuers lacked basic information about the areas in which they intervened.

While showing the vulnerability of traditional telephone and cellular networks, hurricane Katrina also demonstrated how Internet-based technologies could be used to establish links with the outside world. In Bay St. Louis, for example, students from the Naval Postgraduate School used Wi-Fi equipment to set up wireless access points and mesh them together in a cloud covering 10 miles [For-05]. The Internet connection was then further extended dozens of miles by using WiMax technology. *Ad-hoc* wireless communication has helped rescuers, officials and civilians exchange vital information on many occasions after hurricane Katrina hit the U.S.A. Moreover, the only communication means between the mayor of New Orleans and the outside world was a wireless Internet connection and an Internet phone account [Rho-05].

The discussion above shows that while using WLANs is a viable solution in emergency conditions, the requirements that must be imposed under these circumstances are considerably more stringent than those under normal conditions. For example, when designing VoIP systems companies use a mathematical model to predict the maximum number of simultaneous calls given the maximum number of users of that system. Based on a statistical measure of phone usage capacity, the Erlang function, and an acceptable percentage of blocked calls one can compute the bandwidth required by the probabilistic number of simultaneous calls. This provides usually a 2:1 or even 3:1 over-subscription factor, depending on the total number of users.

However, firstly, in emergency conditions the number of simultaneous calls will exceed that predicted for normal circumstances. Secondly, dropping calls of emergency workers is unacceptable, while dropping calls of ordinary users becomes acceptable under critical conditions. As a consequence a differentiation must be introduced in emergency conditions, and some users must be considered prioritary (e.g., police or fire departments, hospitals, etc.). For this to function, it becomes necessary to provide additional mechanisms in WLANs that will ensure the fact that prioritary calls will still succeed, at the expense of some non-prioritary calls (i.e. those of ordinary users) being either dropped or no longer allowed through admission control.

4.5 Research methodology

To understand VoIP performance on WLAN and facilitate VoIP deployment the properties of existing WLAN QoS standards must be thoroughly checked. We expect that specific techniques must be developed to provide quality assurance in emergency conditions. In order to evaluate the performance of currently existing and new mechanisms a test methodology must be set in place. This methodology is to ensure that the tested techniques do provide the enforcement of bounds on quality degradation in networks even during situations of congestion and overload, such as those occurring during emergency situations.

For this purpose we consider that emulation will be one of the most important tools, along with tests using real equipment, to analyse a wide range of controllable scenarios and test

the hypotheses related to this topic. The testbed at JAIST, StarBED, has been already used successfully to emulate various environments, including wireless networks, through the use of the `dummynet` [Dummy] software network emulator.

In [Beu-04] a test methodology for VoIP over wired networks has already been proposed. According to this approach to measuring quality degradation for the applications of interest it is necessary to take into account the following two inter-related points:

- Measuring the quality degradation at the network level by means of QoS parameters (delay & jitter, packet loss, throughput);
- Quantifying the User-Perceived Quality (UPQ) at application level; for example, assessing the quality of Voice over IP (VoIP) communication by means of objective metrics (see Section 3.3).

The two aforementioned aspects must subsequently be correlated, and the relationship between them used to demand specific network service levels through requirements defined in terms of UPQ.

For the study of VoIP over WLAN we propose to use a test setup similar to the one in [Beu-04], but adapted to the wireless environment. The setup is depicted in Figure 4.

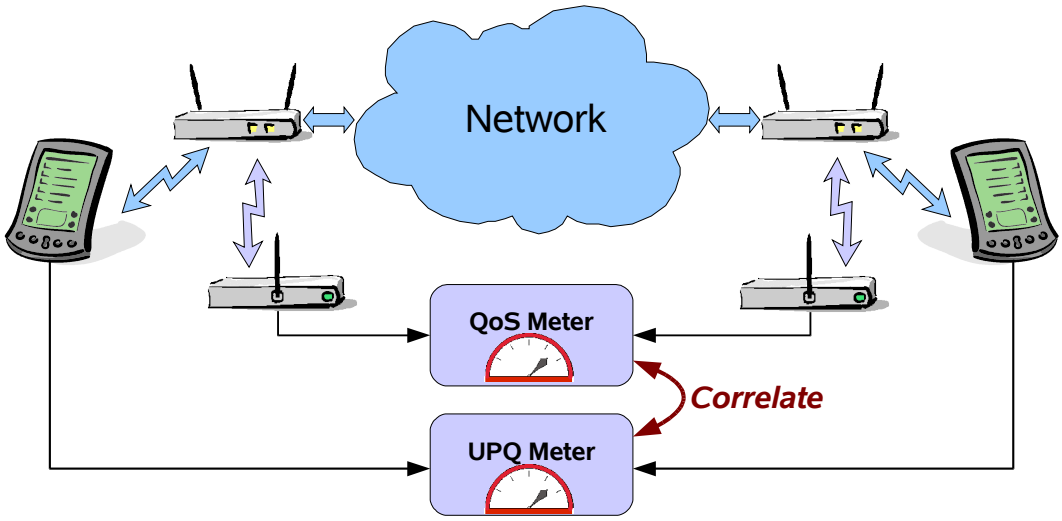

Figure 4: Application performance evaluation in wireless environments.

In this setup the application to be evaluated runs on a wireless device, such as a PDA. Access points (and potentially a wired LAN) provide the connection between the two end points. Two wireless monitors ensure the collection of the traffic, so that the QoS parameters at network level can be quantified by the block called "QoS Meter" based on the traffic traces. In parallel, at application level, the "UPQ Meter" assesses the user-perceived quality for the application under study (using for example the PESQ [P.862] score for VoIP). The two measurements are then correlated, and the relationship that exists between quality degradation in the network and UPQ can then be analyzed.

It is important to note that the wireless network used in this testbed can be a real network, but can also be an emulated network. Emulation has the great advantage of allowing researchers to perform controlled and reproducible experiments in a wide range of network conditions. In this context real networks are used for calibration and to provide a reality check of experiment results obtained in emulated environments. The project of developing a WLAN emulator is now in progress at JAIST.

5 Conclusions

In this survey we have analysed the main properties of wireless networks, with emphasis on the WLAN QoS enforcement techniques, including the recent IEEE 802.11e standard. Following that, VoIP communication technology was presented, including aspects related to the objective assessment of the user-perceived quality for voice communication.

The issues related to the effective deployment of VoIP on WLAN were discussed in chapter 4, with reference to the two previous chapters. These issues derive from the inherent properties of the two technologies and can be summarized as follows:

(a) WLAN QoS parameters (bandwidth, packet loss, delay & jitter) have a high variability in real-world environments, and this has a significant effect on application performance;

(b) Existing WLAN QoS mechanisms are only of limited use for managing contention when applications with different QoS requirements, such as VoIP calls and TCP-based data traffic, share the same communication channel;

(c) VoIP is a multimedia application that requires timely servicing of the voice traffic; this is a challenging task in WLANs, even when using QoS enforcement, since most currently-implemented QoS mechanisms focus on bandwidth provisioning;

(d) Roaming between access points, a typical WLAN event, introduces communication gaps that may even be of the order of seconds, an unacceptable situation for real-time applications.

The present survey made it obvious that various QoS enforcement techniques must be used in order to counter these problems and assure a successful deployment of VoIP on WLAN. However the mechanisms to control quality degradation in computer networks are in a primitive form even in wired networks. The increased complexity of the wireless environments renders this problem even more difficult. Nevertheless, the existing IEEE 802.11e WLAN QoS standard seems a promising starting point for contention management in wireless networks, but its performance must be thoroughly studied.

If in everyday environments quality assurance is only related to user satisfaction, when trying to employ the same applications under emergency conditions, or in mission-critical applications and safety-critical communication systems, quality assurance becomes mandatory. Research as well as recent events have demonstrated that the use of wireless networks is a viable solution in emergency conditions, and perhaps the most robust one. Yet emergency communication systems for disaster situations cannot use anymore the current *best-effort* approach in computer networks, and a detailed dependability study is necessary. Specific mechanisms must be employed in order to limit the quality degradation for those traffic flows for which guaranteed levels of service are required. The need to provide (statistical) guarantees becomes evident, even though it is still a challenge in any computer network. In this context, based on our previous research, we proposed a testbed for application performance assessment in wireless environments.

List of acronyms

3DES	Triple Data Encryption Standard
AC	Access Category
AP	Access Point
AES	Advanced Encryption Standard
AIFS	Arbitration Inter-Frame Space
ARF	Auto-Rate Fallback
BSS	Basic Service Set
CFB	Contention-Free Bursting
CSMA/CA	Collision Sense Multiple Access with Collision Avoidance
DCF	Distributed Coordination Function
DiffServ	Differentiated Services
DoS	Denial of Service
DSSS-CCK	Direct-Sequence Spread Spectrum with Complementary Code Keying
EDCA	Enhanced Distributed Channel Access
FEC	Forward Error Correction
FHSS	Frequency-Hopping Spread Spectrum
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile telecommunications
HCF	Hybrid Coordination Function
HCCA	HCF-Controlled Channel Access
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunication Union, the Telecommunication division
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
MOS	Mean Opinion Score
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolution Coding
PBX	Private Branch eXchange
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PESQ	Perceptual Evaluation of Speech Quality
PPTP	Point-to-Point Tunnelling Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RF	Radio Frequency

RFC	Request For Comments
RSVP	Resource reSerVation Protocol
SSL	Secure Sockets Layer
TDMA	Time-Division Multiple Access
TXOP	Transmission Opportunity
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extension
WPA	Wi-Fi Protected Access
WSM	Wireless Scheduled Multimedia

References

[Beu-04] R. Beuran, M. Ivanovici, "User-Perceived Quality Assessment for VoIP Applications", technical report (delivered to U4EA Technologies), *CERN-OPEN-2004-007*, CERN, Geneva, Switzerland, January 2004.

[Bic-05] J. C. Bicket, "Bit-rate Selection in Wireless Networks", *master thesis, Massachusetts Institute of Technology*, February 2005.

[Bla-98] S. Blake, *et al.*, "An Architecture for Differentiated Services", *IETF RFC 2475*, December 1998.

[Bra-97] R. Braden, *et al.*, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", IETF RFC 2205, September 1997.

[Bra-99] S. Bradner, J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", *IETF RFC 2544*, March 1999.

[Che-04] Y. Chen, *et al.*, "Performance evaluation for IEEE 802.11e enhanced distributed coordination function", *Wireless Communications and Mobile Computing*, vol. 4, 2004, pp. 639-653.

[Com-05] Common Cause Association, "A Failure to Communicate: Katrina Pinpoints Dangerous Lapses in Our Telecommunications Policy", report, 2005.

[Dummy] Dummynet FreeBSD network emulator, http://info.iet.unipi.it/~luigi/ip_dummynet.

[For-05] M. Fordahl, "Geek Cavalries Turn Post-Katrina Landscape into Wireless Lab", *Associated Press*, 4 October 2005.

[G.107] ITU-T Recommendation G.107, "The E-model, a computational model for use in transmission planning", *ITU-T*, March 2005.

[G.108] ITU-T Recommendation G.108, "Application of the E-model: A planning guide", Amendment 2 , *ITU-T*, March 2004.

[G.113] ITU-T Recommendation G.113, "Transmission impairments due to speech processing", Appendix 1, *ITU-T*, May 2002.

[G.711] ITU-T Recommendation G.711, "Pulse Code Modulation (PCM) of voice frequencies", *ITU-T*, 1993.

[G.726] ITU-T Recommendation G.726, "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)", *ITU-T*, 1990.

[G.729] ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CSACELP", *ITU-T*, March 1996.

[IEC-05] The International Engineering Consortium, "Including VoIP over WLAN in a Seamless Next-Generation Wireless Environment", *white paper*, 2005.

[Inf-05] Infoworld, "VoIP without Wires", white paper, February 2005.

[Kim-04] J.-D. Kim, C.-K. Kim, "Performance analysis and evaluation of IEEE 802.11e EDCF", *Wireless Communications and Mobile Computing*, vol. 4, 2004, pp. 55-74.

[Man-98] R. Mandeville, “Benchmarking Terminology for LAN Switching Devices”, *IETF RFC 2285*, February 1998.

[Man-00] R. Mandeville, J. Perser, “Benchmarking Methodology for LAN Switching Devices”, *IETF RFC 2889*, August 2000.

[Man-02] S. Mangold *et al.*, “IEEE 802.11e Wireless LAN for Quality of Service”, *Proc. Euro. Wireless*, Florence, Italy, Feb. 2002.

[Mli-03] F. Mlinarsky, B. Mandeville, “Lift Off! Launching Wireless LAN Metrics”, *white paper*, November 2003.

[Mli-04] F. Mlinarsky, “Wi-Fi Metrics”, *Test & Measurement World*, October 2004.

[Net-05] Network World, “Review: Voice over Wireless LAN”, *white paper*, January 2005.

[Ni-05] Qiang Ni, “Performance Analysis and Enhancements for IEEE 802.11e Wireless Networks”, *IEEE Network*, July-August 2005, pp. 21-27.

[NLA-05] National Laboratory for Applied Network Research/Distributed Applications Support Team, “Iperf – The TCP/UDP Bandwidth Measurement Tool”, 2005.

[Oe-05] M. Oe, *et al.*, “An Implementation and Verification of IEEE 802.11e Wireless Network management System”, *Electronics and Communications in Japan*, part 1, vol. 88, no. 12, 2005, pp. 20-28.

[P.800] ITU-T Recommendation P.800, “Methods for subjective determination of transmission quality”, *ITU-T*, August 1996.

[P.862] ITU-T Recommendation P.862, “Perceptual evaluation of speech quality (PESQ), an objective method for end to end speech quality assessment of narrow-band telephone networks and codecs”, *ITU-T*, February 2001.

[Rah-93] M. Rahnema, “Overview of the GSM system and protocol architecture”, *IEEE Communications Magazine*, April 1993.

[Rho-05] C. Rhoads, “After Katrina, city officials struggled to keep order”, *The Wall Street Journal*, 9 September 2005.

[Ser-01] V. Servis, “Measuring speech quality over VoIP networks”, *The TOLLY Group*, December 2001.

[Tao-04] Z. Tao, S. Panwar, “An Analytical Model for the IEEE 802.11e Enhanced Distributed Coordination Function”, *ICC 2004 – IEEE International Conference on Communications*, vol. 27, no. 1, June 2004, pp. 4111-4117.

[Tow-06] F. F. Townsend (editor), “The Federal Response to Hurricane Katrina – Lessons Learned”, *U.S.A. Federal Government Report*, February 2006.

[Vau-02] S. Vaughan-Nichols, “The 'Michael' Vulnerability”, *Wi-Fi Planet*, December 2002.

[Vau-03] S. Vaughan-Nichols, “Making the Most from WEP”, *Wi-Fi Planet*, March2003.

[WiFi] The Wi-Fi Alliance, *http://www.wi-fi.org*.