Is IEEE 802.11 ready for VoIP?

Arlindo F. da Conceição*, Jin Li†, Dinei A. Florêncio† and Fabio Kon*
*Department of Computer Science, Institute of Mathematics and Statistics, University of São Paulo
†Communication and Collaboration Systems, Microsoft Research

***Abstract*— In this paper, we empirically explore voice communication over IEEE 802.11 networks (VoWiFi). The objective is to understand the limitations of the current WiFi network for VoWiFi deployment. Our experiment finds two major problems of VoWiFi: unstable and excessively long handoffs and unpredictable occurrence of bursts. We also discuss several other minor factors that could hinder VoWiFi deployment, such as network capacity, fairness, and interference susceptibility. Finally, we describe the scenarios where VoWiFi could be used. We conclude that VoWiFi is feasible if used moderately, with low mobility and good signal strength.**

I. Introduction

In the last decade, Voice over IP (VoIP) has moved from a niche market to mainstream. Companies such as Vonage and AT&T offer paid phone services based on VoIP. At the same time, wireless Local Area Networks based on IEEE 802.11 standard (also called Wi-Fi) are becoming widespread. While these wireless networks have not been designed with real-time communication in mind, their widespread availability and low cost makes them an inviting solution to add mobility to VoIP. The combination of VoIP and Wi-Fi (often referred to as VoWiFi), has attracted a lot of interest. Several extensions to IEEE 802.11 have been proposed to improve its real-time capability. Also, Linksys/Vonage have proprietary solutions that use dedicated equipment based on the IEEE 802.11. While extending the 802.11 standard and/or employing dedicated equipment solutions may be interesting, we are particularly interested in investigating to what extent the *existing* Wi-Fi networks could support VoWiFi. Since most of the existing Wi-Fi network operates in the infrastructure mode, we limit ourselves to this mode. VoIP in adhoc wireless network — where routing of packets and QoS is still an unsolved academic problem — is beyond the scope of this paper. The focus of this paper is thus to analyze the problems faced when running VoIP over Wi-Fi networks using existing equipment and solutions in infrastructure mode. We present a summary of the problems we observed and propose limited solutions, which we believe allow the deployment of VoWiFi today.

The remainder of this paper is organized as follows. Section II summarizes the typical requirements for VoIP applications. Section III presents the method that we use to obtain the VoWiFi traces. We analyze a number of problems in VoWiFi in Section IV. Section V recapitulates 802.11 extensions and amendments. Section VI, based on previous observations, proposes specific scenarios where we believe VoWiFi can be deployed today, and a few suggestions on how to circumvent remaining problems. Finally, we present our future work in Section VII.

II. VoIP requirements

Before discussing how the characteristics of an Wi-Fi link affect real-time voice communication, let us review the metrics typically used to define the quality of a VoIP session: one-way delay, jitter, packet loss rate, and throughput.

Average one-way delay is probably the most critical parameter for VoIP. If it is too long, conversation flow is compromised and communication may become unnatural. ITU-T guidelines [11] recommend a one-way delay of up to 150 milliseconds. Beyond that, negative consequences gradually accrue. In IEEE 802.11 networks, the one-way delay between client and access point is usually less than 10 milliseconds [1], and therefore should not be a problem in VoWiFi.

Jitter is the packet-to-packet variation in the one-way delay. Most modern systems will use some type of adaptive playback to smooth out the jitter [13], but this increases the one-way delay, and can introduce artifacts into the speech. In Wi-Fi networks, jitter is generally small, partially because one-way delay and packet sizes are small, too [1]. However, Section IV-B will show that there are times when extreme delay variations can occur with significant impact on voice quality.

Packet loss rate also affects speech quality, as the decoded speech will present artifacts associated with the lost packets. For VoIP, packet loss rates of up to 1% are generally acceptable [11], [12]. In IEEE 802.11 networks, collisions and other losses are hidden by an automatic re-transmission strategy [7], [4]. Since these retransmissions are transparent to the application layer, the final packet loss rate is typically less than 1% [1] and, therefore, acceptable for typical VoIP applications. Note, however, that as a mobile terminal gets out of the range, the loss rates increase abruptly; quickly making speech communication impossible.

Throughput. The bandwidth required by a single VoIP connection is significantly less than the nominal capacity of IEEE 802.11 networks. Typical speech codecs require no more than 64 Kbps, while 802.11g offers 54 Mbps. However, if the same access point is used to support multiple calls, we may have a capacity problem, as discussed in Section IV-C.

Thus, at first glance, IEEE 802.11 seems to be appropriate for VoIP. One-way delay, jitter, packet loss rate and throughput of a typical connection all seem to indicate VoWiFi should not run into major problems. However, that is not necessarily the case. The following sections enumerate characteristics of Wi-Fi networks that – while not common enough to appear in the "average" behavior – induce significant barriers for VoWiFi in existing networks.

III. VoWiFi traces

To characterize VoIP traffic in Wi-Fi and landlines, we collected traffic from real networks and measured packet delays and loss events in a meticulous way. To avoid device-related Wi-Fi implementation problems, we used a variety of Wi-Fi network interface cards (NICs), including WMP55AG, AIR-PCM340, WUSB54GP Ver. 4, WUSB54AG, WUSB54G Ver. 4, WPC54G Ver. 1.2, and PC24E-H-FC. We also gathered the traces using different Wi-Fi networks, including three private Wi-Fi networks (powered by access points from Netgear FWAG114, Dlink DI624+, and Linksys WRT54GS) and two corporate networks (from Microsoft Research, in Redmond-WA, and University of São Paulo, Brazil).

A probing program has been written to simulate the traffic of a VoIP session. The program sends a continuous sequence of packets to its partner every $20ms$. The payload size of each packet is 60B. This simulates a VoIP session of 24 Kbps with no silence suppression. We recorded all packet loss events and the transmission delay of each packet. We also recorded the Wi-Fi signal strength at the time each packet was received. The signal strength information was obtained using the API for NDIS (Network Driver Interface Specification).

The probing program uses an enhanced RTP protocol to record the precise time a packet is sent and received. The timestamp in the RTP header records the time that the packet is sent, and the sequence number allows the detection of the lost packets. Both the timestamp and the sequence number are part of the standard RTP protocol. Using these, we may obtain a relative delay measure called *inter-packet arrival time* by measuring the receiving time difference of two consecutive packets. Assuming that the sequence number gap between the two arriving packets is k, if the network is normal, the expected inter-packet arrival time between the two packets is $k \times 20ms$. To obtain the absolute network transmission delay of each packet, we need the time that the packet is sent and received. Timestamping the packet at its departure and arrival is simple; the tricky part is that the timestamp belongs to two different computers, whose clocks are not necessarily in sync.

Our solution is to use an NTP-like protocol [14] and add two RTP extension fields: the last received timestamp and the last received sequence number in the header of the packet. We develop a meticulous clock algorithm to synchronize the clocks of the two peers. The algorithm is then used to convert the departure timestamp into a timestamp that can be used by the receiver, and calculate the absolute network transmission delay of the packet.

IV. Major obstacles to VoWiFi

We identify two major obstacles for VoWiFi: the handoff and the burst behavior. We also look at a few additional obstacles to VoWiFi, such as capacity, equilibria, and interferences.

A. Handoff

Since the distance covered by an access point is only 300 feet and multiple Wi-Fi access points may compete for the connection of the Wi-Fi device, handoff is expected during a voice conversation in which the speaker moves. Practical traces of the VoWiFi show that the handoff in Wi-Fi networks is not as smooth as it should be.

Figure 1 shows a typical VoWiFi trace involving a handoff. We recorded the trace when the Wi-Fi device is moved around a building that is covered by a corporate IEEE 802.11b network. Figures 1(a) and 1(b) show, respectively, the delay and the packet loss behavior in the presence of handoffs. We also show the signal strength during the movement. The horizontal axis shows the time of the experiment.

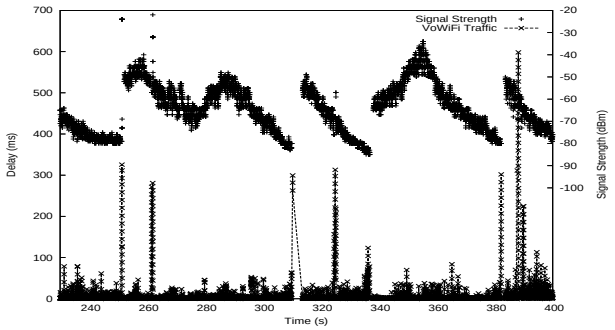
In this VoIP session, we observe four handoffs; around 251s, 310s, 336s and 382s, respectively. The handoffs are characterized by a leap in the signal strength, indicating that the Wi-Fi device is moving away from the current access point onto a new access point, with a stronger signal.

We observe that during the handoffs, the packet loss rate is high and delay increases. Let us consider a handoff to begin when packet loss rate is greater than 1% or delay reaches 200 ms. Applying this criterion, the duration of the handoffs showed in Figure 1 are 1.18, 3.75, 1.25, and 1.82s, respectively. Table I shows the handoff behavior of two traces collected in two of our experiments. For each trace we present: 1) the environment where the trace was gathered, 2) number of handoffs during the trace, 3) average duration of handoffs (as defined in last paragraph), 4) standard deviation of average handoff duration, 5 and 6) minimum and maximum handoff duration in the trace, 7) average number of packets lost during each handoff, 8 and 9) minimum and maximum number of packets lost during handoffs.

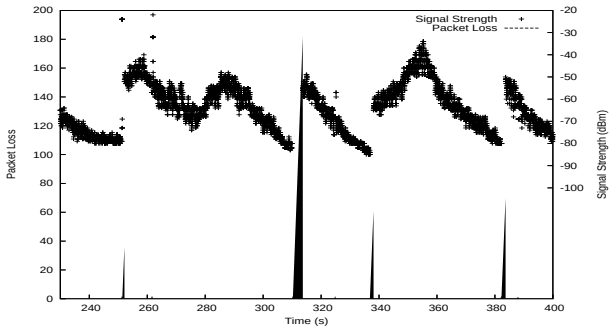
From the experiment, we have three important findings. First, as expected, the handoff duration depends on the environment. Second, every single handoff in our experiments lasts more than one second, which is beyond the acceptable range for VoIP application. Finally, the handoff duration varies greatly from instance to instance; at University of São Paulo, the handoff duration varied from 4.25 to 16.19s.

This undesired behavior of the handoffs is due to the design of the Inter Access-Point Protocol (IAPP), defined in the IEEE 802.11f standard. The protocol dictates that the mobile unit should conduct the handoff without help from the access points. In addition, for the sake of simplicity and security, the IAPP forces a unique association from a mobile unit throughout access points (Extended Service Set, or ESS). By using this design, the handoff consists of a sequential process composed of four steps: scanning, authentication, association, and re-association. Among these steps, the scanning is the most time-consuming phase; it can amount to 90% of the entire handoff time and can take several seconds [18].

To study the effect of scanning in voice traffic, we forced a scanning during a VoWiFi session. The result of this experiment is shown in Figure 2. The scanning request was implemented using the NDIS API (OID_802_11_BSSID_LIST_SCAN request). We made sure that the NIC could latch only to one and only one Wi-Fi access point. We observe two delay peaks in the forced scanning experiment of Figure 2. We believe that one delay peak is



(a) One-way delay behavior.



(b) Packet loss incidence.

Fig. 1. Handoff behavior in a Wi-Fi network.

TABLE I
HANDOFF BEHAVIOR

Environment	Number of handoffs	Average Duration (s)	Standard Deviation	Min (s)	Max (s)	Average Packet Loss	Min	Max
MSR Lab.	12	2.55	1.41	**1.13**	4.28	118.67	36	208
Univ. of São Paulo	10	8.4	4.12	4.25	16.19	386.1	187	799

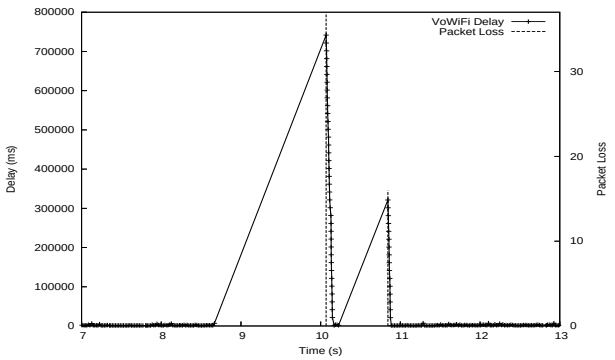


Fig. 2. Impact of scanning activity in voice traffic.

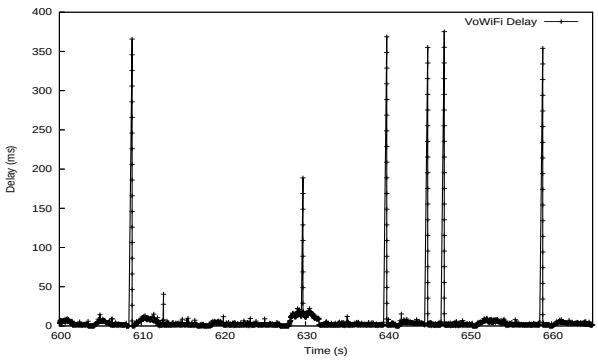


Fig. 3. Example of Bursts behavior.

due to the scanning, and the other delay peak is due to the remaining phase of the handoff (authentication, association, and re-association.)

There are a number of efforts to optimize the IEEE 802.11 handoff process [18] and, mainly, the scanning phase [15]. It is worth noting that the handoff is a well known weakness of IEEE 802.11 and it is currently under redevelopment in the IEEE 802.11r standard. However, IEEE 802.11r compliant Wi-Fi devices will not be commercially ready for a few years, and wide deployment is likely to take even longer.

B. Burst traffic

We observe that VoWiFi traces show more *burst* events compared with similar landline VoIP traffic. In a burst event, multiple voice packets are blocked in the network for up to several hundred milliseconds and are then delivered to the receiver at almost the same time, frequently, but not always, without packet loss. Although we also notice that certain bad landline connections exhibit burst, and certain good Wi-Fi connections do not experience bursts, overall, bursts are more common in Wi-Fi than in the Internet.

Figure 3 shows a VoIP trace with bursts, observed at 608s, 629s, 639s, 644s, 646s, and 658s. During each of the bursts, 10-19 packets are blocked in the network and delayed from $200ms$ to $380ms$. They then arrive at the receiver almost all at the same time — as indicated by the decrease of the one-way delay by almost $20ms$ for each successively arriving packet.

The bursts in Wi-Fi networks were observed with different NICs, access points, and traffic generators and were persistent in Wi-Fi environments. There are several possible causes of Wi-Fi bursts: scannings, external interferences, processing interruptions, etc. We could not pin-point a single reason for the bursts. However, we deduce that the bursts are not due to a collision of Wi-Fi packets and the subsequent retransmissions, since the delay of even a small burst exceeds $100ms$ — which is beyond the time required by the maximum number of retransmissions. That is, if a packet collides with another Wi-

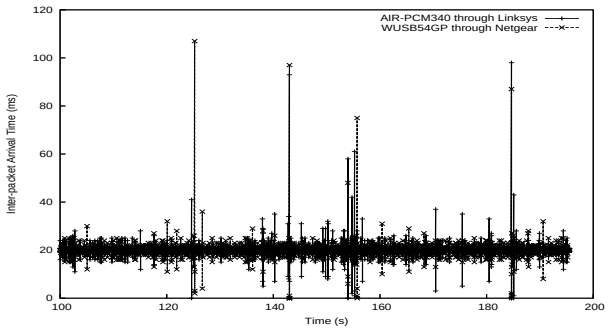


Fig. 4. Correlated bursts in distinct voice traffics.

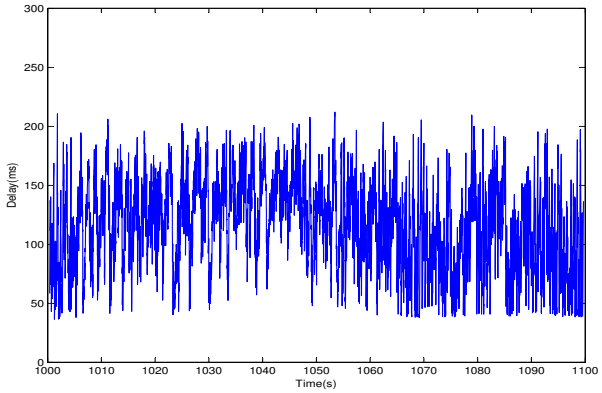


Fig. 5. A segment of Internet VoIP trace (Philadelphia to Seattle).

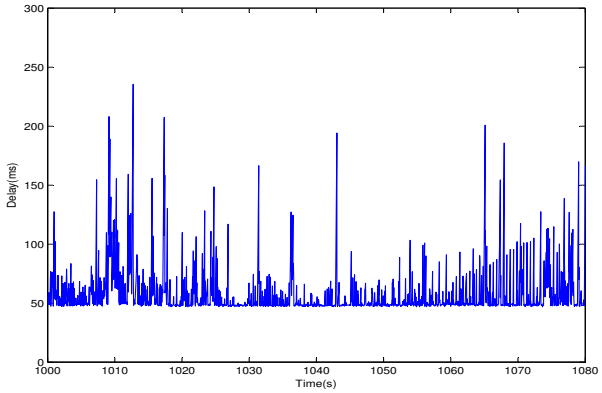


Fig. 6. A segment of Wi-Fi VoIP trace (Philadelphia to Seattle).

Fi packet and fails in the retransmission effort, the packet will be dropped and not delayed, as observed in the burst events. Moreover, bursts cannot be due to the existence of concurrent traffic, since bursts were observed even in quiet and idle Wi-Fi environments. And, bursts cannot be due only to scannings, because we observed them even with very good signal quality, when scannings are not supposed to happen.

Initially, we believed that the bursts were due to external interferences. This assumption led us to conduct an experiment using two wireless interfaces [3], [2]. The idea was to reduce the impact of the bursts and the handoffs by keeping connections to two distinct IEEE 802.11 networks [17]. By distinct networks we mean two different NICs (AIR-PCM340 and WUSB54GP) connected through two different access points (linksys WRT54GS and Netgear FWAG114) operating at different channels.

Figure 4 illustrates the results of the experiment. We observe a number of *correlated bursts*, i.e., the bursts that occur at exactly the same time in both connections, e.g., at approximately 143s and 185s. Since the traffics were sent over distinct networks, the occurrence of correlated bursts means that some bursts may happen due to strong noises that block the entire Wi-Fi spectrum. In addition, correlated bursts may be caused by the computer system and its support for real-time traffic.

A more extensive study of bursts can be found in Table II. In the table, we compare the VoIP traces over a landline (the Internet) and over Wi-Fi plus a landline (Wi-Fi). Each trace is an aggregate of 2-30 hours of data. The trace data are summarized in 9 columns as follows: 1) locations of the trace, 2) duration of the trace experiment (in seconds), 3) average delay (in milliseconds), 4) standard deviation of the delay (in milliseconds), 5) packet loss ratio (PLR, in percent), 6) burst loss frequency (in occurrences per second, with the burst loss defined as more than 3 packets lost consecutively), 7) burst delay frequency (in occurrences per second, with the burst delay defined as increase of delay for more than 100ms *and* more than 5 packets arrive almost at the same time), and 8) magnitude of burst (average increase in delay in the event of a burst delay).

Notice that the Wi-Fi traces in Table II consist of a segment of Wi-Fi connection followed by a landline connection; the Wi-Fi connection characteristics may thus be affected by the quality of the corresponding landline connection. Nevertheless, we have a number of interesting observations. We observe that in general, the quality of Wi-Fi connections is poorer. On average, the packet loss ratio of Wi-Fi connections is 0.97% versus 0.28% of that of landlines, the frequency of burst loss is 0.26 per second versus 0.12 of landlines, and the frequency of burst delay is 0.022 per second versus 0.005 of landlines.

Even when the summary statistics of the Internet connection seem to be close to those of the Wi-Fi connection, the detailed trace reveals that the two connections have different characteristics. We show a segment of a trace from Philadelphia to Seattle for landline and Wi-Fi in Figures 5 and 6, respectively. We observe that the Wi-Fi connection experiences more short term burst events than the corresponding landline connection, even though both connections show similar statistics.

C. Capacity

The nominal capacity of IEEE 802.11 is many times greater than the bandwidth required for VoIP applications. Nevertheless, in practice, an IEEE 802.11b wireless network can hardly accommodate 6 VoIP sessions [6]. This is due to operations such as header transmission, backoffs, acknowledgements, etc. To transmit, for instance, 60 bytes of voice data in RTP, a VoIP application has to transmit an additional 46 bytes (18 of RTP, 8 of UDP, and 20 of IP). On top of that, we have to add all the synchronization, acknowledgement, and back-off periods for Wi-Fi protocol, which are quite significant regardless of

TABLE II
VOIP TRAFFIC TRACES

Location	Duration (s)	Average Delay (ms)	Std. Deviation (ms)	PLR	Burst Loss Freq. (s^{-1})	Burst Delay Freq. (s^{-1})	Magnitude of Burst (ms)
Internet							
Beijing ↔ Seattle (1)	21,998	108	114	0.02%	0.000	0.000	260
Beijing ↔ Seattle (2)	11,455	148	148	0.07%	0.032	0.001	237
Philadelphia ↔ Seattle	107,761	63	75	0.76%	0.313	0.013	170
Wi-Fi							
Amsterdam ↔ Seattle	10,426	93	93	1.10%	0.506	0.002	154
New York City ↔ Seattle	49,567	110	203	0.53%	0.025	0.064	308
Philadelphia ↔ Seattle	6,529	54	70	0.71%	0.095	0.016	184
Beijing ↔ Seattle	28,592	216	220	1.54%	0.426	0.005	249

the payload size. Wi-Fi protocol is thus very inefficient for the transmission of small packets. Analysis demonstrates [19] that the overall efficiency of Wi-Fi can be as low as 3% for small packets. For example, a VoIP connection of 64 Kbps actually reduces the throughput of an IEEE 802.11b wireless network by approximately 900 Kbps [6].

D. Equilibria

Equilibria, or fairness, is hard to achieve in IEEE 802.11 networks due to several reasons. First, the capacity of an access point is limited and must be shared among mobile units; consequently, a greedy mobile unit can negatively affect other stations. Second, the IEEE 802.11 MAC layer was designed to give approximately equal probability of channel access to all mobile units, disregarding their packet size, signal quality, or transmission rate. Hence, a mobile unit that transmits at 1 Mbps can negatively affect other mobile units that are, for example, transmitting at 11 Mbps [10]. Finally, mobile units employ local strategies to maximize their throughput irrespective of the impact in the overall system performance [16].

In the heart of the equilibria problem are the Automatic Rate Control (ARC) mechanisms [9]. In the IEEE 802.11 devices, these mechanisms elect different coding schemes to exploit the tradeoff between data rate and error rate. In other words, if signal quality is low, the ARC mechanism chooses a more resilient modulation that reduces the transmission rate in order to reduce the frame loss rate and expand the transmission range. However, using different transmission rates leads to an unfair equilibria of the bandwidth sharing among the mobile units [16]. Moreover, the criteria used by the ARC mechanisms to decide when and how to adapt are not defined in the standard, each supplier implements its own strategy and defines its own thresholds in an undisclosed manner. Hence, in an IEEE 802.11 network, the ARC mechanisms may lead to unpredictable and unfair sharing of bandwidth among the mobile units.

E. Interferences

IEEE 802.11 networks are susceptible to external interferences. IEEE 802.11b and 802.11g networks are particularly susceptible to interferences because they work at the same frequency (2.4 GHz) as several other radio devices, such as microwave ovens, cordless phones, and Bluetooth devices. The 802.11a, which works at 5 GHz, is less susceptible to interferences. In addition, signal propagation is affected by unmanageable factors such as office layout, antenna orientation, and even weather conditions. Signal strength can also vary significantly in short periods of time (see Figure 1(b)) because of mobility and multi-path effects.

F. Metrics for connection quality

There are several available metrics to measure the quality of a connection, such as packet loss rate, signal strength, and Signal Noise Ratio (SNR). However, these metrics are not reliable indicators of the connection quality. The behavior of the packet loss rate, for example, is affected by the automatic re-transmission mechanism of the IEEE 802.11 MAC layer. The MAC layer, before notifying a packet loss to the application layer, can re-transmit a frame up to seven times if its ACK message is not received [7]. Therefore, the application layer perceives the packet loss rate in an inaccurate manner; the losses are happening, but the application layer may not realize it until the loss is so great that almost nothing can be done to recover from the errors.

The frame error rate (FER), i.e., the number of frames not acknowledged at the MAC layer, should be a better metric than packet loss rate. However, FER information is not available in all NICs. The OID_802_11_STATISTICS request, the request that provides FER information, is defined by the NDIS standard just as a recommended feature; it is not mandatory. In practice, this NDIS request worked fine only for one of the four NICs that we tested.

Metrics based on signal quality, such as Signal Strength and SNR, suffer from expressive variation due to their inherent susceptibility to interferences, mobility, and multi-path effects. Additionally, the noise information, necessary for SNR composition, is not available in the NDIS API.

In summary, there is not a definitive metric for connection quality. The current metrics are unstable and may not reflect the real connection quality. In addition, they do not offer any clue to the state of the access point network. For the application developers, the challenging Wi-Fi environment and the lack of good connection quality measure adds some degree of black art in the programming for these networks.

V. 802.11 Amendments and Extensions

It is worth noting a number of 802.11 amendments that address the real-time performance of Wi-Fi[1]. The burst problem will be mitigated, not by one, but by several 802.11 specifications together: IEEE 802.11r should reduce the scanning effects, and 802.11e will enable QoS control and queue management. Additionally, IEEE 802.11n and 802.11w may indirectly contribute to reduce bursts.

Throughout this paper, we have pointed out important features that can effectively contribute to VoWiFi performance, such as smart scanning strategies [15], [18], adaptive algorithms to playout [13], amendments to improve fairness of Wi-Fi MAC layer [16], [8], multi-connection capability [2], [3], and multi-path techniques [17].

These works, however, are still under development and will likely take several years before wide deployment.

VI. Conclusion and Solutions

We now go back to our original question: *can existing 802.11b/g and 802.11a networks be used for VoWiFi, even before deployment of new 802.11 extensions?* Fortunately, the answer is yes. More specifically, our experiments show that, as long as the following requirements are met, VoWiFi can provide enough quality to be useful:

- The user is connected to a single access point for the duration of the call. This requires that the user stay within the coverage of an access point, and in case of the corporate network, remains reasonably still to avoid crossing access point coverage boundaries. Walking around a building with several access points will likely lead to starting a handoff process, which will greatly impair the call quality;
- Signal strength is good. This may limit the areas in the building where the Wi-Fi call can take place;
- A limited number of calls is handled per access point. Multiple VoWiFi calls approach the system capacity may significantly reduce call quality;
- If possible, scanning should be disabled for the duration of the call.

We point out that even with all the above restrictions, call quality is likely to be below that of a standard telephone call. Nevertheless, if a user is aware of the limitations, the added flexibility of a non-tethered VoIP connection should be appealing enough to many users.

VII. Future Work

We are developing calibration algorithms to mitigate the SNR and ARC implementation diversity problems [5]. In the future, we plan to use timing information, e.g., the Time Synchronization Function (TSF), to reduce the collisions of constant bit rate traffics, including voice traffic. The idea is to statistically distribute the transmissions into the available transmission window.

We are also investigating solutions with a graceful transition between bidirectional communication and "walk-talkie" modes, since the latter is more delay-resistant, and may provide a useful fall-back solution when the connection quality becomes poor.

Finally, it is worth noting that IEEE 802.11 and VoWiFi are becoming mature, with increased usage and decreased problems. Thus, even if VoWiFi still has severe limitations – and some kind of black magic in it – we expect that VoWiFi will be, in a few years, just another black box off the shelf.

[1] `http://grouper.ieee.org/groups/802/11/802.11_Timelines.htm`

References

[1] M. Arranz, R. Agüero, L. Muñoz, and P. Mähönen. Behavior of UDP-based applications over IEEE 802.11 wireless networks. In *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, volume 2, pages F–72–F–77, San Diego, USA, september 2001.

[2] P. Bahl, A. Adya, J. Padhye, and A. Walman. Reconsidering wireless systems with multiple radios. *ACM SIGCOMM Computer Communication Review*, 34(5):39–46, October 2004.

[3] R. Chandra, V. Bahl, and P. Bahl. MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card. In *IEEE INFOCOM*, March 2004.

[4] A. F. da Conceição and F. Kon. Adaptação de fluxos contínuos UDP sobre redes IEEE 802.11b. In *Workshop de comunicação sem fio e computação móvel (WCSF)*, pages 91–101, São Lourenço-MG, Brasil, October 2003. In Portuguese.

[5] A. F. da Conceição and F. Kon. Adaptive streaming based on IEEE 802.11 signal quality. In *23rd Brazilian Symposium on Computer Networks (SBRC)*, pages 1147–1150, Fortaleza, Brazil, May 2005. Short paper.

[6] S. Garg and M. Kappes. An experimental study of troughput for UDP and VoIP traffic in IEEE 802.11b networks. In *IEEE Wireless Communications and Network Conference (WCNC)*, pages 1748–1753, march 2003.

[7] M. S. Gast. *802.11 Wireless Networks. The definitive Guide.* O'Reilly, 2002.

[8] R. Gupta. *Quality of Service in Ad-Hoc Networks*. PhD thesis, UC Berkeley, May 2005.

[9] I. Haratcherev, J. Taal, K. Langendoen, R. Lagendijk, and H. Sips. Automatic IEEE 802.11 rate control for streaming applications. *Wireless Communications and Mobile Computing*, 5:421–427, june 2005. special issue on Radio Link and Transport Protocol Engineering for Future-Generation Wireless Mobile Data Networks.

[10] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *IEEE INFOCOM*, San Francisco, CA, 2003.

[11] ITU-T Recommendation G.114. One-way transmission time, may 2003.

[12] J. H. James, B. Chen, and L. Garrison. Implementing VoIP: a voice transmission performance progress report. *IEEE Communication Magazine*, pages 36–41, july 2004.

[13] Y. J. Liang, N. Färber, and B. Girod. Adaptive playout scheduling and loss concealment for voice communication over IP networks. *IEEE Transactions on Multimedia*, 5(4):532–543, December 2003.

[14] D. L. Mills. RFC 1305 - network time protocol (version 3): Specification, implementation and analysis, March 1992.

[15] I. Ramani and S. Savage. SyncScan: Practical fast handoff for 802.11 infrastructure networks. In *IEEE INFOCOM*, Miami, FL, March 2005.

[16] G. Tan and J. Guttag. The 802.11 MAC protocol leads to inefficient equilibria. In *IEEE INFOCOM*, Miami, FL, March 2005.

[17] S. Tao, K. Xu, A. Estepa, T. Fei, L. Gao, R. Guerin, J. Kurose, D. Towsley, and Z.-L. Zhang. Improving VoIP quality through path switching. In *IEEE INFOCOM*, Miami, FL, March 2005.

[18] H. Velayos and G. Karlsson. Techniques to reduce IEEE 802.11b handoff time. In *IEEE International Conference on Communications (ICC)*, june 2004.

[19] W. Wang, S. C. Liew, and V. O. K. Li. Solutions to performance problems in VoIP over a 802.11 wireless LAN. *Transaction on Vehicular Technology*, 54(1), 2005.