

Transmissão de voz sobre redes IEEE 802.11: um levantamento dos principais problemas e restrições

Arlindo F. da Conceição
Instituto de Matemática e
Estatística
Universidade de São Paulo
arlindo@ime.usp.br

Jin Li
Communication and
Collaboration Systems
Microsoft Research
jinl@microsoft.com

Dinei A. Florêncio
Communication and
Collaboration Systems
Microsoft Research
dinei@microsoft.com

ABSTRACT

This work analyzes the voice communication over IEEE 802.11 networks (VoWiFi). It empirically characterizes the transmission problems of VoWiFi and describes scenarios where it could be used over the existing network technologies. The two major problems found were: the excessively long handoffs and the occurrence of bursts. We conclude that is feasible to use VoWiFi if, during a voice call, mobility is kept low, signal strength is high enough and the network capacity is not exceeded.

RESUMO

Este trabalho faz uma avaliação da comunicação de voz sobre redes IEEE 802.11 (VoWiFi). Para isto, caracteriza empiricamente os problemas de transmissão e aponta cenários em que a implantação de VoWiFi é viável utilizando-se as tecnologias atualmente disponíveis. Os dois principais problemas encontrados foram: a longa duração das migrações (*handoffs*) e a ocorrência de tráfegos em rajada. Concluímos que, com as tecnologias atuais, a utilização de VoWiFi é viável desde que, durante uma chamada, a mobilidade seja baixa, a qualidade do sinal seja suficientemente alta e que a capacidade de transmissão da rede não seja excedida.

Categories and Subject Descriptors

C.2.1 [Computer-communication networks]: Network Architecture and Design—*Wireless communication*; H.4.3 [Information Systems Applications]: Communications Applications

General Terms

Measurement, Performance, Experimentation

Keywords

VoWiFi, VoWLAN, VoIP, IEEE 802.11, Wi-Fi

1. INTRODUÇÃO

Na última década, Voz sobre IP (VoIP) deixou de ser uma tecnologia usada apenas em determinados nichos de mercado para tornar-se uma tecnologia à disposição da grande massa de usuários finais. Empresas como Vonage, AT&T e Skype já oferecem serviços baseados em VoIP para milhões de clientes ao redor do mundo. Durante esse mesmo período, em paralelo à popularização de VoIP, a utilização das redes locais sem fio baseadas no padrão IEEE 802.11 (Wi-Fi) cresceu gradualmente e este tornou-se o padrão *de facto* para redes locais sem fio. A cada dia, seja na cafeteria ou no centro de compras, essas redes estão cada vez mais presentes no nosso cotidiano. Desse modo, apesar das redes IEEE 802.11 ainda não oferecerem suporte adequado às aplicações de tempo real, seu relativo baixo custo e sua ampla utilização fizeram de IEEE 802.11 a alternativa natural para se agregar mobilidade às aplicações de VoIP.

Voz sobre Wi-Fi, também conhecido como VoWiFi ou VoWLAN, atraiu o interesse da comunidade acadêmica e da indústria por fornecer uma alternativa de baixo custo para comunicações móveis. Tanto a academia quanto a indústria propuseram extensões às especificações originais de IEEE 802.11 com o intuito de melhorar o seu desempenho e adequá-lo aos requisitos das aplicações de tempo real; algumas soluções proprietárias de *hardware* já foram inclusive implementadas, como os produtos advindos da parceria entre Linksys e Vonage.

No entanto, apesar do uso de soluções proprietárias permitirem a criação de soluções interessantes, neste trabalho estamos particularmente interessados em investigar a utilização de VoWiFi que se faz possível usando-se apenas a tecnologia atualmente disponível. Em outras palavras, queremos saber, dadas as tecnologias atualmente consolidadas, quais são os problemas que afetam negativamente as transmissões de voz sobre redes IEEE 802.11 e como esses problemas limitam o uso de VoWiFi. Com esse objetivo, este trabalho investiga esses problemas e, além disso, propõe cenários — limitados, mas importantes — nos quais VoWiFi pode ser implementado usando-se as soluções de rede sem fio atualmente disponíveis.

Antes de prosseguir, cabe dizer que este trabalho concentra-se no uso de IEEE 802.11 no último salto de acesso à Internet. Mais especificamente, concentra-se no comportamento da transmissão de pacotes de voz sobre redes IEEE 802.11 infra-estruturadas. Os problemas não diretamente relacio-

nados à entrega de pacotes, tais como as questões de consumo de energia e de interconexão com a rede pública de telefonia, não fazem parte do escopo deste trabalho.

As próximas seções estão organizadas da seguinte maneira: a fim de familiarizar o leitor com as aplicações de voz, a Seção 2 resume os requisitos das aplicações para VoIP. A Seção 3 apresenta a metodologia usada para obtenção dos traços de execução de VoWiFi. Na Seção 4, esses traços são analisados, dando atenção especial a dois problemas que nos pareceram ser os principais: os *handoffs* e os tráfegos em rajada. Apresentados os problemas principais, a Seção 5 expõe alguns problemas adicionais que podem dificultar a ampla implementação de VoWiFi. A Seção 6 discorre sobre aspectos de VoWiFi que devem ser levados em conta por pesquisadores e desenvolvedores. A Seção 7 recapitula os trabalhos relacionados. A Seção 8, baseada nas constatações e observações feitas nas seções anteriores, propõe cenários onde acreditamos que VoWiFi pode ser utilizado com as tecnologias atuais e também oferece sugestões de como os problemas atuais podem ser contornados. Por fim, apresentamos as conclusões sobre o uso de VoWiFi e os trabalhos futuros.

2. REQUISITOS DAS APLICAÇÕES VOIP

Antes de apresentar como as características das redes IEEE 802.11 afetam as aplicações de VoIP, façamos uma revisão das métricas normalmente utilizadas para se definir a qualidade de uma sessão de VoIP; são elas: latência, *jitter*, taxa de perda de pacotes e vazão.

2.1 Latência

A latência, também conhecida como atraso unidirecional (*one-way delay*), é a métrica mais crítica para as aplicações de VoIP; trata-se do tempo necessário para que uma mensagem de voz seja transmitida do emissor para o receptor. Se a latência é longa, a conversação é comprometida e a comunicação pode tornar-se não natural, apresentando cortes e correções audíveis. De acordo com as recomendações da ITU-T [15], a latência pode acumular até 150 milissegundos sem que haja grandes impactos na qualidade da ligação. Porém, a partir de 150ms de latência, as consequências negativas começam a ser gradualmente perceptíveis. Atrasos de até 200ms ainda são definidos na literatura como aceitáveis [16].

Em redes IEEE 802.11, considerando-se apenas um salto de conexão, a latência é normalmente menor do que 10ms [1]. Sendo assim, a latência da conexão IEEE 802.11, que é da ordem de poucos milissegundos, é muito menor do que a latência total de uma comunicação pela Internet, que é da ordem de dezenas de milissegundos [5]. Ou seja, apesar de a latência ser uma métrica crítica, a latência média de IEEE 802.11 não é um problema para o uso de VoWiFi.

2.2 Jitter

O *jitter* é a variação da latência. A maioria dos sistemas multimídia modernos utilizam mecanismos adaptativos baseados em *buffers* para suavizar os efeitos dessa variação [17]. Porém, o uso de *buffers* aumenta a latência média e pode

introduzir artefatos¹ na voz. Em redes IEEE 802.11, o *jitter* é normalmente pequeno [1]. Apesar disso, a Seção 4.2 mostrará que podem ocorrer variações extremamente altas na latência, as quais possuem impacto relevante na qualidade da voz transmitida.

2.3 Taxa de perda de pacotes

A taxa de perda de pacotes expressa a quantidade de pacotes não entregues. Em aplicações de VoIP, a taxa de perda de pacotes é considerada aceitável até a razão de 1% [15, 16]. No entanto, acima de 1%, os impactos na qualidade da voz normalmente tornam-se perceptíveis, surgem artefatos audíveis que dificultam a comunicação. Em redes IEEE 802.11, apesar de as taxas reais de perda de pacotes serem mascaradas pelo mecanismo de retransmissão automática [11, 6], a taxa de perdas de pacotes observada é normalmente menor do que 1% [1], sendo assim aceitável para as aplicações de VoIP. Porém, se uma unidade móvel se afasta da área de cobertura de um ponto de acesso, a taxa de perdas de pacotes pode crescer abruptamente, impossibilitando a conectividade e a comunicação.

2.4 Vazão

A vazão necessária para uma conexão de VoIP é muito menor do que a capacidade nominal das redes IEEE 802.11. Uma sessão típica de voz requer cerca de 64 Kbps, enquanto 802.11g oferece 54 Mbps. Entretanto, se um ponto de acesso é utilizado para transmitir múltiplas chamadas de voz, pode haver um problema de capacidade. A Seção 5.1 discutirá a questão de capacidade em mais detalhes.

Desse modo, as redes IEEE 802.11 parecem ser — com certa margem de folga — apropriadas para VoIP, pois os valores médios de latência, *jitter*, vazão e a taxa de perda de pacotes dessas redes indicam que VoWiFi deveria poder ser usado sem maiores problemas. Entretanto, as próximas seções enumeram características das redes IEEE 802.11 atuais que, apesar de não afetarem o comportamento “médio”, consistem em barreiras significativas para a ampla utilização de VoWiFi.

3. METODOLOGIA E AMBIENTE EXPERIMENTAL

Para a análise dos tráfegos de VoWiFi, implementamos programas geradores de tráfego sintético nas linguagens C e Java que simulam o tráfego de uma sessão de VoIP. Os programas transmitem fluxos bidirecionais de pacotes à taxa de 50 pacotes por segundo; ou seja, um pacote a cada 20ms. A carga útil dos pacotes é de 60 octetos. Dessa forma, simulamos uma sessão de VoIP de 24 Kbps sem supressão de silêncio. Cabe dizer que o uso de tráfegos sintéticos não reduz a validade dos experimentos, pois as análises apresentadas concentram-se nos atrasos e perdas de pacotes (fatores

¹Artefato é o termo utilizado para denotar as falhas perceptíveis que podem ocorrer quando uma transmissão de voz e de vídeo é reproduzida. Os artefatos mais comumente percebidos nas aplicações de voz são os cortes na fala — aquelas pequenas interrupções. Nas aplicações de vídeo, o artefato mais comum é a exibição de pequenos quadrados que nitidamente destoam da imagem.

estes que não são afetados pelo uso, ou não, de tráfegos reais). Os experimentos foram exaustivamente repetidos, tomamos o cuidado de apresentar apenas os eventos que foram consistentemente observados durante a execução dos experimentos.

Além disso, para evitar que as especificidades de um ou outro dispositivo Wi-Fi atrapalhassem as medições, executamos os geradores de tráfego em diferentes cenários e ambientes de rede. Também utilizamos diferentes interfaces IEEE 802.11 (*Network Interface Cards* ou NICs) — modelos WMP55AG, AIR-PCM340, WUSB54GP Ver. 4, WUSB54G Ver. 4, WUSB54AG, WPC54G Ver. 1.2, e PC24E-H-FC — e cinco redes IEEE 802.11 diferentes, sendo três dedicadas (usando os pontos de acesso: Netgear FWAG114, Dlink DI624+ e Linksys WRT54GS) e duas não dedicadas (uma da Microsoft Research e outra da Universidade de São Paulo).

Os programas geradores de tráfego, a cada pacote recebido, registram: o instante de recebimento do pacote, a força do sinal, a perda de pacotes e o atraso. Do instante de recebimento, derivamos um atraso relativo, o Intervalo Entre Pacotes (IEP), que consiste na diferença de tempo entre a chegada de dois pacotes consecutivos. Se a diferença entre o número de seqüência de dois pacotes recebidos é k , o intervalo esperado entre esses dois pacotes é $k \times 20ms$. A força do sinal foi obtida através da API de NDIS [7]. A perda de pacotes foi detectada comparando-se o número de seqüência de dois pacotes consecutivos (o número de seqüência está registrado no cabeçalho RTP de cada pacote). A medição do atraso, porém, foi não trivial e será explicada a seguir.

3.1 Método para estimar o atraso

Para obter o valor absoluto do atraso de cada pacote são necessários os instantes de tempo em que cada pacote foi enviado e recebido. Marcar o instante (*timestamping*) de envio e de chegada de um pacote é simples; o problema é que essas marcas de tempo pertencem a computadores diferentes e, para serem corretamente interpretadas, precisam ser sincronizadas.

Além disso, nos computadores atuais, a contagem de tempo é feita por cristais de quartzo nos quais as frequências de contagem de tempo podem ser diferentes. A frequência pode variar em função dos cristais usados, ou mesmo da temperatura de trabalho a que esses cristais estão submetidos. Desse modo, as marcações de tempo feitas em computadores diferentes podem divergir ao longo do tempo; a esse comportamento é dado o nome de *clock drifting*. É comum que relógios baseados em cristais de quartzo variem aproximadamente 1ppm (parte por milhão) para cada grau centígrado de temperatura; sendo que 1ppm implica 1ms de diferença a cada 16,7 minutos de contagem.

Sendo assim, para obter a latência de entrega de um pacote enviado do computador A para o computador B, nosso programa converte as marcas de tempo feitas em um computador A para o referencial de tempo de um computador B. Para fazer essa conversão, sincroniza os relógios de maneira similar ao protocolo NTP [19] e atualiza o *clock drifting*. Para implementar esse mecanismo, foi necessário estender o protocolo RTP adicionando dois campos: *last received timestamp* e *last received sequence number*. A Figura 1 mostra

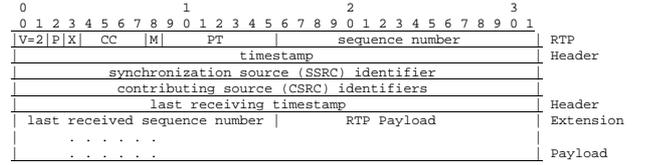


Figura 1: Cabeçalho estendido do protocolo RTP.

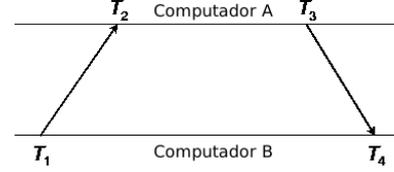


Figura 2: Marcas de tempo usadas para obtenção do atraso.

como ficou o cabeçalho estendido.

A conversão das marcas de tempo do computador A para o computador B é modelada da seguinte maneira:

$$T_B(r_a) = \theta_0 + \beta \cdot (r_a - r_b) + \chi \cdot (r_a - r_b)^2, \quad (1)$$

onde, dada uma marca de tempo r_a registrada no computador A e uma marca de tempo r_b registrada no computador B (usada como referência de tempo no passado), a primeira é convertida para a escala de tempo do computador B. Além disso, θ_0 , β e χ são os coeficientes de primeira, segunda e terceira ordem da variação de tempo e denotam, respectivamente: a diferença inicial entre as marcas de tempo, a diferença entre as frequências de atualização do relógio e o fator de *drifting*.

Sendo as marcas de tempo T_1 , T_2 , T_3 e T_4 tomadas como ilustra a Figura 2, ou seja, T_1 e T_4 obtidas em B e T_2 e T_3 obtidas em A, queremos determinar o tempo de transmissão — o atraso — do computador A para o computador B. Lembrando que os pacotes de VoIP são continuamente enviados de A para B, podemos assumir que o i -ésimo pacote sai de A no instante $T_{i,3}$ e chega em B em $T_{i,4}$. Além disso, podemos assumir que o computador A reporta para o computador B, através do cabeçalho estendido de RTP, a marca de tempo $T_{i,2}$ e o último pacote recebido de B. Observe que, em função do número de seqüência do último pacote recebido de B no computador A, o computador B pode determinar $T_{i,1}$.

Para o i -ésimo pacote recebido em B, calculamos o deslocamento de tempo θ_i entre os relógios dos computadores A e B da seguinte maneira:

$$\theta_i = \frac{1}{2} [(T_{i,2} + T_{i,3}) - (T_{i,1} + T_{i,4})], \quad (2)$$

Além disso, para o i -ésimo pacote recebido em B, calculamos também o tempo total de ida e volta de uma mensagem (*round trip delay*) δ_i entre os computadores A e B:

$$\delta_i = (T_{i,4} - T_{i,1}) - (T_{i,3} - T_{i,2}). \quad (3)$$

Pesquisas sobre o protocolo NTP [20] mostram que o valor de θ_i é tão preciso quanto menores forem os valores do atraso δ_i . Sendo assim, armazenamos os 32 pares θ_i e δ_i mais significativos, ou seja, os 32 pares dentre os últimos 100 que possuem o menor valor de δ_i . Então, os 32 pares mais significativos e as respectivas marcas de tempo T_3 e T_4 são usados para encontrar, através do método de erros quadráticos mínimos [21] (*Least Square Error* ou LSE), os coeficientes θ_0 , β e χ da Equação 1, os quais são utilizados para converter a marca de envio $T_{i,3}$ em uma marca de tempo no computador B , calculando assim o atraso absoluto referente à transmissão de um pacote. Mais detalhes sobre essa abordagem de conversão podem ser consultados em [9].

4. OBSTÁCULOS PARA A IMPLANTAÇÃO DE VOWIFI

A partir da análise dos traços de execução, identificamos os principais obstáculos para a implantação de VoWiFi: a migração de ponto de acesso (*handoff*) e o comportamento bloqueio/rajada das redes IEEE 802.11.

4.1 Handoff

Espera-se que os usuários de dispositivos IEEE 802.11 possam mover-se durante uma chamada de voz. Sendo assim, dado que o raio de cobertura de um ponto de acesso em espaços abertos é de aproximadamente 100m, espera-se também a ocorrência de *handoffs* durante as chamadas. Entretanto, os traços de execução mostraram que a migração em redes IEEE 802.11 não é suficientemente suave a ponto de não ser percebida durante a execução de uma chamada de voz.

A Figura 3 demonstra o comportamento típico de um *handoff*. Nessa execução, o traço foi registrado enquanto a unidade móvel era movida através de uma rede sem fio corporativa composta por vários pontos de acesso IEEE 802.11. As Figuras 3(a) e 3(b) mostram, respectivamente, o comportamento dos atrasos e das perdas de pacotes. Na Figura 3(a), o eixo vertical esquerdo demonstra a variação nos atrasos, o eixo horizontal mostra o tempo do experimento e o eixo vertical direito, com o objetivo de ilustrar o movimento da unidade móvel, mostra a força do sinal. Por sua vez, na Figura 3(b), o eixo vertical esquerdo dimensiona as perdas de pacotes.

Nas figuras, podem ser observadas quatro operações de *handoff*: aos 251s, 310s, 336s e 382s, aproximadamente. O momento em que os *handoffs* são executados caracteriza-se por um salto na força do sinal, pois o NIC desconecta-se do ponto de acesso de sinal mais fraco e conecta-se a outro de sinal mais forte — e provavelmente mais próximo. Também se podem observar duas conseqüências principais dos *handoffs*: a incidência de perda de pacotes e o aumento no atraso. Por sua vez, a conseqüência da perda de pacotes e do aumento nos atrasos é a ocorrência de artefatos audíveis nesses períodos de conversação.

Se estabelecermos que o início de um *handoff* acontece quando

a perda de pacotes atinge 1% e a latência atinge 200ms, e que o fim desse *handoff* acontece quando a latência volta aos níveis normais, a duração dos períodos de *handoff* mostrados na Figura 3 é de 1.18, 3.75, 1.25 e 1.82s, respectivamente. Esses valores estão consistentes com os reportados na literatura [22].

A Tabela 1 resume o comportamento observado em dois traços de execução registrados enquanto as unidades móveis eram movidas e estavam, portanto, sujeitas a *handoffs*. Para cada traço, a tabela apresenta: 1) o ambiente onde o traço foi coletado; 2) o número de *handoffs* executados durante a coleta do traço; 3) o tempo médio de duração dos *handoffs* (segundo os critérios de início e fim definidos no parágrafo anterior); 4) desvio padrão da duração média dos *handoffs*; 5 e 6) o tempo mínimo e máximo de duração dos *handoffs*; 7) número médio de pacotes perdidos por *handoff*; 8 e 9) o número mínimo e máximo de pacotes perdidos por *handoff*.

Da análise dos traços podemos extrair três considerações importantes. A primeira era esperada: a duração dos *handoffs* varia em função dos ambientes onde foram executados. A segunda: todos os *handoffs* em nossos experimentos gastaram pelo menos um segundo para serem completados; esse tempo é uma forte restrição para aplicações de VoIP, pois durante esse período não há comunicação entre os pares de uma chamada de voz. Por fim, a terceira: a duração dos *handoffs* é muito variável, podendo variar significativamente de uma execução para outra. Por exemplo, no traço colhido na rede IEEE 802.11 da Universidade de São Paulo, os tempos para execução dos *handoffs* variaram de 4.25 a 16.19s.

Esse comportamento — indesejável — dos *handoffs* deve-se às recomendações feitas no padrão IEEE 802.11f, ou *Inter Access-Point Protocol* (IAPP), como é mais conhecido. O protocolo IAPP define que a unidade móvel deve conduzir o processo de migração sem o auxílio dos pontos de acesso. Além disso, com o objetivo de alcançar maior simplicidade e segurança, IAPP define que uma unidade móvel deve estar associada apenas a um — e apenas um — ponto de acesso. Em função dessas restrições, a migração consiste em um processo seqüencial composto de quatro fases: busca (*scanning*), autenticação, associação e reassociação. Dentre esses passos, a busca é a fase mais demorada, podendo consumir cerca de 90% do tempo total de migração; ou seja, alguns segundos [26].

Existem vários esforços com o objetivo de otimizar o processo de migração em redes IEEE 802.11 [26], principalmente na fase de busca [22]. O processo de *handoff* é reconhecida-mente um dos pontos fracos de IEEE 802.11 e por isso está sendo revisto na especificação IEEE 802.11r. Porém, os primeiros dispositivos compatíveis com o padrão IEEE 802.11r devem levar alguns anos para serem lançados e chegarem aos usuários.

4.2 Tráfego em rajadas

Além dos problemas relacionados à execução de *handoffs*, os traços de execução revelaram outro problema de VoWiFi: a alta incidência de tráfegos em rajada. A ocorrência de uma rajada caracteriza-se pelo fato de vários pacotes de voz ficarem bloqueados na rede por algumas centenas de milissegundos e então serem entregues praticamente ao mesmo tempo.

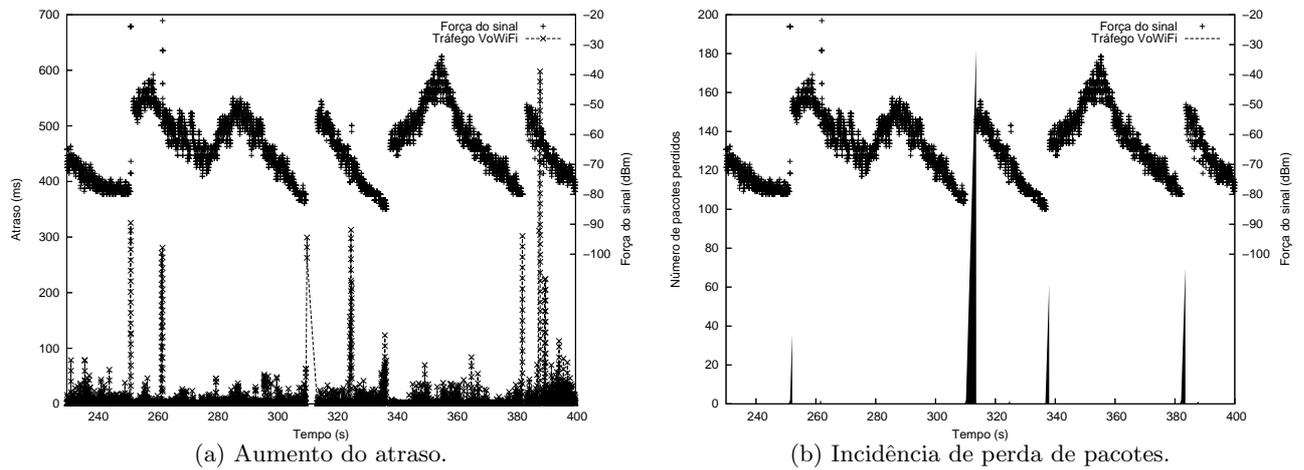


Figura 3: Implicações da operação de *handoffs* nos tráfegos de VoWiFi.

Table 1: Comportamento dos *handoffs*.

Ambiente	Número de <i>Handoffs</i>	Duração Média (s)	Desvio Padrão	Mín. (s)	Máx. (s)	Perda Média Pacotes	Mín.	Máx.
MSR Lab.	12	2,55	1,41	1,13	4,28	118,67	36	208
USP	10	8,4	4,12	4,25	16,19	386,1	187	799

A entrega de pacotes em rajada também pode ser acompanhada da perdas de pacotes, mas não necessariamente.

As rajadas não são exclusividade das redes sem fio, pois também podem ocorrer em redes Ethernet cabeadas; observamos a ocorrência de rajadas tanto em conexões Internet tradicionais, quanto em conexões Wi-Fi. No entanto, elas são mais comuns nas redes IEEE 802.11. A Figura 4 mostra um experimento no qual se pôde observar a incidência de rajadas durante uma sessão de VoWiFi: o transmissor está conectado ao ponto de acesso e o receptor é a unidade móvel; as rajadas podem ser observadas aos 608, 629, 639, 644, 646 e 658s. Durante as rajadas, um certo número de pacotes fica bloqueado na rede e então são todos entregues praticamente ao mesmo tempo; mas, é claro, com atraso. No traço apresentado na Figura 4, os atrasos vão de 200ms a 380ms (de 10 a 19 pacotes ficam bloqueados na rede). Pode-se observar também que o atraso decresce em aproximadamente 20ms para cada pacote recebido, isso ocorre porque os pacotes são transmitidos a cada 20ms e os pacotes atrasados são entregues praticamente ao mesmo tempo.

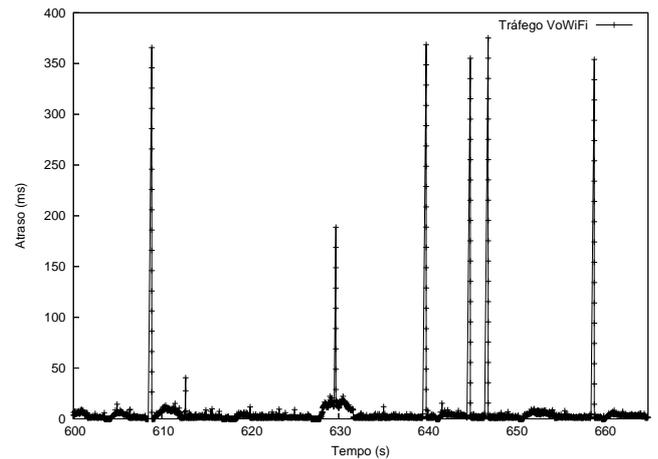


Figura 4: Exemplo do comportamento dos tráfegos em rajada.

A ocorrência de rajadas foi consistentemente observada nas redes IEEE 802.11, mesmo usando-se diferentes ambientes e configurações; o que inclui o uso de diferentes NICs, pontos de acesso e ferramentas geradoras de tráfego. Pode-se, portanto, afirmar que as rajadas não ocorrem em função das peculiaridades de um ou de outro dispositivo, mas são uma característica dessas redes. As rajadas podem ser originadas por diferentes fatores, tais como: *scannings*, interferências externas, interrupções de processamento etc. Além disso, pode-se afirmar que as rajadas não ocorrem devido a uma razão única, mas sim devido a um conjunto de fatores. Por exemplo, as rajadas não podem ocorrer apenas devido à colisão de pacotes, pois, se um pacote colide e os esforços de re-

transmissão também falham, em atrasos da ordem de 100ms, ou mais, o pacote seria dado como perdido; e não seria simplesmente atrasado, como acontece nas rajadas. Em outras palavras, uma perda não seria confundida com uma rajada. As rajadas também não ocorrem apenas em função da carga excessiva das redes, pois foram observadas rajadas mesmo em redes ociosas. E também não podem ser atribuídas apenas aos *scannings*, pois foram observadas em locais onde a força do sinal era máxima e, portanto, os *scannings* não deveriam acontecer.

Inicialmente, acreditávamos que as rajadas ocorressem devido à ação de interferências externas. Essa suposição nos

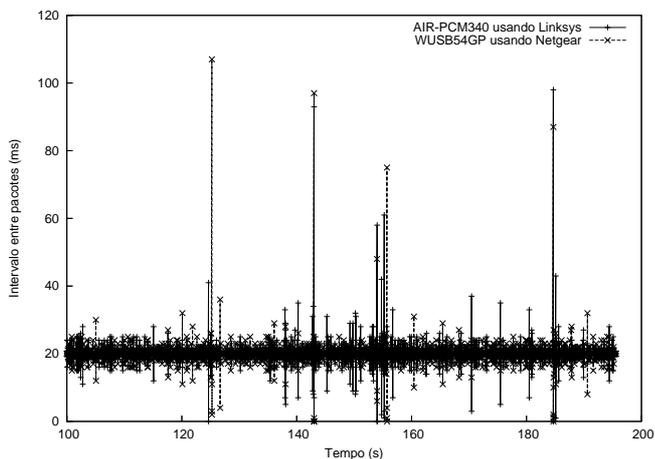


Figura 5: Correlação da ocorrência de rajadas em tráfegos distintos.

levou a pesquisar e explorar o uso de duas ou mais conexões IEEE 802.11 [4, 2]. A idéia era reduzir o impacto das rajadas e dos *handoffs*, mantendo-se sempre duas conexões ativas em redes distintas [25]. Por redes distintas, entenda-se o uso de dois NICs diferentes (AIR-PCM340 e WUSB54GP) conectados a dois pontos de acesso diferentes (linksys WRT54GS e Netgear FWAG114), operando nos canais 1 e 11, respectivamente, ou seja, em canais diferentes e que não interferem entre si.

Ao usar duas conexões distintas, observamos, mesmo assim, a ocorrência de *rajadas correlacionadas*, isto é, rajadas que ocorrem exatamente ao mesmo tempo em ambas as conexões. A Figura 5 mostra a ocorrência de rajadas correlacionadas aproximadamente aos 143s e 185s. A ocorrência dessas rajadas não elucida a razão de sua existência, mas deixa claro que as razões não estão restritas às questões de rede: podem também estar associadas, por exemplo, à capacidade dos computadores atuais de lidar com aplicações de tempo real. Outra alternativa — porém menos provável — é a existência de interferências externas capazes de bloquear todo o espectro de transmissão de IEEE 802.11.

A Tabela 2 apresenta um estudo mais extenso sobre as rajadas. Ali comparamos a execução de VoIP sobre a Internet tradicional e sobre IEEE 802.11. Os traços possuem de 2 a 30 horas de tráfego e os resultados são apresentados em nove colunas, sendo que cada coluna informa: 1) locais de coleta dos traços; 2) duração da coleta do traço, em segundos; 3) atraso médio, em milissegundos; 4) desvio padrão; 5) taxa de perda de pacotes (TPP), em porcentagem; 6) número de ocorrências de perdas de pacotes em rajada por segundo (PPR/s), sendo considerada perda em rajada a perda de 3 ou mais pacotes consecutivamente; 7) número de ocorrências de atrasos em rajada por segundo (AR/s), sendo considerado atraso em rajada atrasos de mais de 100ms e mais de 5 pacotes entregues quase ao mesmo tempo; e 8) tamanho da rajada (aumento médio do atraso em caso de rajada), em milissegundos.

Note que os traços IEEE 802.11 apresentados na Tabela 2 são formados por um trecho IEEE 802.11g (último salto)

e pelo trecho restante, que é composto pela Internet tradicional; ou seja, o trecho Internet também pode afetar as características da conexão sem fio. Apesar disso, podemos fazer algumas observações interessantes: em geral, a qualidade das conexões IEEE 802.11 é pior do que da Internet sobre Ethernet; em média, a taxa de perda de pacotes das conexões IEEE 802.11 é 0.97% versus 0.28% da Internet, a frequência de perdas em rajada é 0.26 versus 0.12 por segundo e a frequência de atrasos em rajada é 0.022 versus 0.005 por segundo.

Além disso, mesmo quando as estatísticas da conexão Internet parecem similares às da conexão IEEE 802.11, os traços revelam diferentes características de comportamento entre as conexões. Por exemplo, a Figura 6 mostra duas partes de traços de VoIP (um usando apenas Internet e outro usando também Wi-Fi) referentes à conexão entre Philadelphia e Seattle; observe que a diferença de comportamento entre os tráfegos é bem maior do que revelam as estatísticas.

5. PROBLEMAS ADICIONAIS

Além dos dois problemas principais, os *handoffs* e as rajadas de tráfego, também identificamos outros problemas que poderiam dificultar a implantação de VoWiFi.

5.1 Capacidade

Apesar de a capacidade nominal de vazão das redes IEEE 802.11 ser maior do que a vazão usada pelas aplicações de VoIP, na prática, um ponto de acesso mal pode acomodar uma dezena de chamadas de voz [18]. Na verdade, uma rede sem fio IEEE 802.11b consegue acomodar bem apenas 6 sessões de VoIP [10].

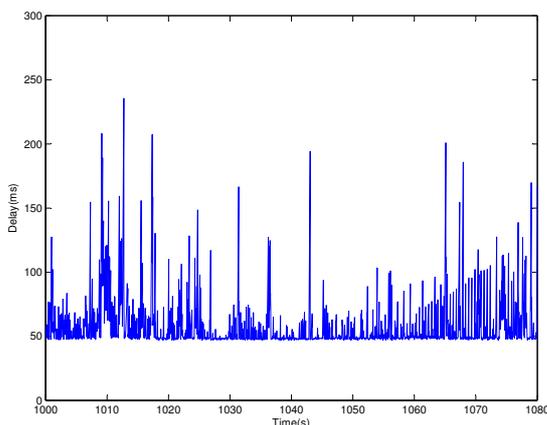
Essa diferença entre a capacidade nominal e a capacidade real deve-se principalmente às sobrecargas relacionadas ao uso de cabeçalhos e troca de mensagens de controle. Por exemplo, ao se usar RTP para transmitir 60 octetos de voz, transmitem-se também 40 octetos de cabeçalhos (sendo 12 octetos de RTP, 8 de UDP e 20 de IP). Considerando-se apenas essa sobrecarga, a utilização efetiva da rede pelos tráfegos de VoIP já se reduz para apenas 60%. Quando são considerados outros fatores, tais como os cabeçalhos usados pela camada MAC e PHY de IEEE 802.11 e os tempos gastos com sincronização e trocas de mensagens, essa eficiência se reduz ainda mais, podendo chegar a menos de 3% [27]. Na prática, uma sessão de VoIP a 64 Kbps toma cerca de 900 Kbps da vazão total efetiva do sistema [10], que é de 6 a 7 Mbps em redes IEEE 802.11b [6].

5.2 Justiça

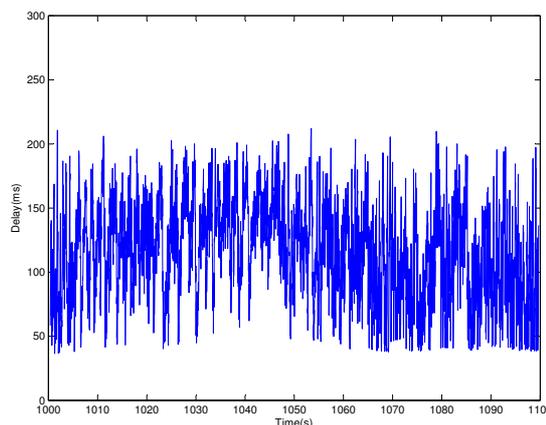
Equilíbrio, justiça, ou ainda *fairness*, é um conceito difícil de ser obtido em redes IEEE 802.11. Isso porque, primeiro, os pontos de acesso têm capacidade limitada e essa capacidade é compartilhada entre as estações móveis; conseqüentemente, unidades móveis “gulosas” podem afetar negativamente o tráfego de outras unidades. Segundo, a camada MAC de IEEE 802.11 foi projetada com o objetivo de prover a mesma probabilidade de acesso ao meio a todas as unidades móveis, independentemente do tamanho dos pacotes, da qualidade do sinal ou da taxa de transmissão. Desse modo, uma unidade móvel transmitindo a 1 Mbps pode afetar negativamente outras unidades que transmitem a 11 Mbps [14].

Table 2: Tráfego de VoIP.

Local	Duração (s)	Atraso (ms)	Desvio Padrão	TPP (%)	PPR/s	AR/s	Tamanho da Rajada (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
IEEE 802.11							
Beijing ↔ Seattle	28.592	216	220	1,54	0,426	0,005	249
Philadelphia ↔ Seattle	6.529	54	70	0,71	0,095	0,016	184
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



(a) Tráfego Internet.



(b) Tráfego Wi-Fi.

Figura 6: Comportamento de tráfegos de VoIP (Philadelphia ↔ Seattle).

Por fim, os dispositivos IEEE 802.11 aplicam estratégias locais para otimização de seus fluxos, sem considerar o impacto que essas estratégias possam ter no desempenho do sistema como um todo [24].

No centro do problema de justiça, está um mecanismo interno de IEEE 802.11: o Controle Automático da Taxa de Transmissão (*Automatic Rate Control* ou ARC). Ele é responsável por escolher a modulação adequada às condições do canal, com o objetivo de explorar o compromisso entre a taxa de erros e a capacidade de transmissão [13]. Seu princípio de atuação é: quanto pior a situação do canal, mais robusta deve ser a modulação utilizada (e menor a taxa de transmissão); quanto melhor o canal, menos robusta pode ser a modulação utilizada (e maior a taxa de transmissão). O padrão IEEE 802.11g define o uso de até 14 diferentes modulações, que resultam nas seguintes taxas de transmissão: 54, 48, 36, 33, 24, 22, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps. Porém, o padrão deixa em aberto o algoritmo e os critérios usados pelo mecanismo de ARC para escolher dentre essas possíveis modulações [13]. Como consequência dessa não-definição, os mecanismos de ARC são implementados pelos fabricantes de interfaces de rede IEEE 802.11 de maneira proprietária e “fechada”; isso não seria um problema não fosse o impacto direto do mecanismo de ARC na capacidade da rede e na distribuição justa dessa capacidade [24, 12]. Em poucas palavras, o mecanismo de ARC faz com que as redes IEEE 802.11 sejam menos previsíveis e o comparti-

lhamento da capacidade de vazão menos justa.

5.3 Interferências

As redes IEEE 802.11 são susceptíveis a interferências externas. As redes IEEE 802.11b e 802.11g são particularmente susceptíveis porque utilizam a mesma frequência (2.4 GHz) de alguns outros dispositivos, tais como fornos de microondas, telefones sem fio (*cordless phones*) e dispositivos Bluetooth. Além disso, a propagação do sinal é afetada por fatores como a disposição física de objetos, a orientação das antenas e, inclusive, as condições climáticas. A força do sinal pode variar significativamente, mesmo em períodos curtos de tempo (veja a Figura 3), devido à mobilidade e ao efeito *multi-path* [23]. Em suma, são tantos os fatores capazes de afetar e interferir negativamente em uma conexão IEEE 802.11, que é muito difícil prever e dimensionar essas interferências [3].

5.4 Diversidade de implementação

Definimos como diversidade de implementação a diferença de comportamento que pode ser observada nas transmissões quando são utilizados diferentes dispositivos IEEE 802.11. Chamamos a atenção para essas diferenças em trabalhos anteriores [6, 7, 8] e para o fato de que os trabalhos baseados em simulações não consideravam esses problemas. Nossos últimos experimentos com VoWiFi ajudaram a reforçar essas questões, pois em tráfegos de tempo real, como os de

VoIP, a questão de diversidade de implementação deixa de ser um problema sutil, como o é em determinados tráfegos TCP. De maneira geral, o uso de diferentes NICs, computadores e configurações implicam características diferentes de transmissão, ou seja, implicam transmissões sujeitas a diferentes taxas de perdas de pacotes e valores médios de atraso e *jitter*. Além disso, outro aspecto da diversidade de implementação pode-se notar na Figura 3(a).

Ali, dentre os valores de força de sinal, existem valores que nunca são apresentados, como se nunca ocorressem, por exemplo -61 dBm. Essa pequena “anomalia” acontece porque o valor da potência do sinal é mapeado em uma escala de -10 a -200 dBm, como define NDIS, mesmo que para o NIC esses valores sejam, por exemplo, de 1 a 50. Além disso, os sistemas Windows e Linux usam diferentes formas de mapeamento para a força do sinal [7]. Mais informações sobre como — e quão diferentemente — a força do sinal é relatada pelos NICs para a camada de aplicação podem ser encontradas em [28].

Uma vez que IEEE 802.11 não define detalhadamente como alguns de seus mecanismos devem atuar, estes são implementados de maneira proprietária e fechada. Sendo assim, fica restrita nossa capacidade de determinar com precisão seus comportamentos. Conseqüentemente, é impossível prever ou calcular o comportamento e as sobrecargas das redes IEEE 802.11 [10, 13]. A diversidade de implementação, em outras palavras, dificulta a interpretação das métricas de adaptação e da real qualidade da conexão.

5.5 Métricas de qualidade de conexão

Existem várias métricas a partir das quais podemos inferir a qualidade de uma conexão, como por exemplo a taxa de perda de pacotes, a força do sinal, o *jitter* etc. Entretanto, nas redes IEEE 802.11, as métricas usuais não são suficientes para definir a qualidade de uma conexão; ou, no mínimo, são métricas menos confiáveis.

A taxa de perda de pacotes, por exemplo, é afetada pelo mecanismo de retransmissão automática de IEEE 802.11. Recapitulando, o mecanismo de retransmissão automática, antes de notificar a perda de um pacote, tenta retransmitir o pacote até sete vezes [11]. Dessa forma, a camada de aplicação percebe a perda de pacotes de maneira imprecisa e, mais do que isso, pode percebê-la apenas quando a taxa dessas perdas for excessivamente alta, de forma tal que pouco pode ser feito para recuperar-se dos erros ocorridos.

A taxa de perda de quadros de transmissão (*Frame Error Rate* ou FER), ou seja, o número de quadros cuja transmissão não foi confirmada através de uma mensagem ACK, é uma métrica melhor do que a taxa de perda de pacotes. Entretanto, nem todo NIC fornece essa informação. A implementação da requisição `OID_802_11_STATISTICS`, a requisição de NDIS que retorna FER, é apenas recomendada. Ou seja, os NICs não são obrigados a implementá-la. Em nossos experimentos, testamos a requisição em quatro NICs diferentes, mas ela funcionou em apenas um deles, no NIC modelo WUSB54GP, da Linksys.

As métricas baseadas na qualidade de sinal, tais como força do sinal e SNR, são afetadas negativamente pela alta vari-

abilidade das conexões IEEE 802.11. Além disso, o ruído, uma das informações necessárias para o cálculo de SNR, não está disponível na API de NDIS.

Em suma, não existem métricas apropriadas para determinar a qualidade da conexão. As métricas existentes são instáveis e podem não refletir a real qualidade da conexão. Além disso, as métricas existentes são locais, isto é, não há uma métrica de adaptação capaz de prover o nível de utilização da rede como um todo; ou quanto está sendo utilizado da capacidade de um ponto de acesso, ou quanto ainda poderia ser utilizado. Se fossem oferecidas às unidades móveis métricas de adaptação capazes de indicar o desempenho global da rede, essas unidades poderiam ser mais proativas com relação à adaptação e à solução dos problemas de conexão.

6. MAIS ALGUMAS CONSIDERAÇÕES SOBRE VOWIFI

É importante notar que os problemas apresentados nas seções anteriores não podem ser considerados separadamente, pois eles podem acontecer simultaneamente, por vezes tornando-se ainda piores. Por exemplo, as rajadas podem ficar mais intensas com o aumento do tráfego e da mobilidade e os *scannings* são mais freqüentes em ambientes com maior incidência de interferências.

Sob a ótica do desenvolvimento de sistemas, os problemas de VoWiFi representam, grosso modo, as razões porque é tão complexo desenvolver aplicações adaptativas para redes IEEE 802.11 [7]. A imprevisibilidade e vulnerabilidade a interferências das redes IEEE 802.11 fazem com que o projeto de estratégias adaptativas para essas redes seja uma tarefa “artesanal”, única para cada circunstância. Além disso, é muito difícil, se não impossível, determinar a causa dos problemas e, conseqüentemente, prover as reações adaptativas apropriadas que acabem não afetando negativamente outros usuários do sistema.

Do ponto de vista da pesquisa, a diversidade de comportamento entre implementações e a imprevisibilidade de IEEE 802.11 dificultam a proposta e a validação de algoritmos e modelos. Existem tantas variáveis — e variância(s) — que se torna excessivamente trabalhoso produzir experimentos representativos, especialmente experimentos relacionados à mobilidade.

7. TRABALHOS RELACIONADOS

Os principais trabalhos relacionados à VoWiFi são especificações em andamento². Por exemplo, a especificação IEEE 802.11r otimiza o processo de *handoff*, 802.11n aumenta a capacidade de vazão, 802.11k especifica melhores métricas para se definir a qualidade da conexão e 802.11w reduz as interferências.

A melhoria do problema de tráfego em rajadas, porém, não deve ser tratada por uma, mas sim por várias especificações conjuntamente: IEEE 802.11r deve reduzir os efeitos dos *scannings*, 802.11e deve permitir o controle de QoS e permitir a gerência de filas. As especificações IEEE 802.11n

²Veja <http://grouper.ieee.org/groups/802/11/802.11-Timelines.htm>

e 802.11w também devem contribuir indiretamente para a redução das rajadas.

Outra iniciativa importante foi a recente inclusão na API de NDIS do comando `OID_802_11_MEDIA_STREAM_MODE`. Incluído em abril de 2005, o comando deve permitir que as aplicações entrem em modo protegido de operação durante as transmissões de tráfego de tempo real, evitando assim que operações e mecanismos da rede sem fio, como *scannings* e PSM [11], interfiram nas transmissões. A inclusão desse comando na API de NDIS, antes de tudo, demonstra a sensibilização da comunidade para a importância do tráfego multimídia sobre redes IEEE 802.11.

No decorrer deste trabalho, foram citadas propostas para a melhora do desempenho de VoWiFi, tais como estratégias mais inteligentes de migração [22, 26], algoritmos adaptativos [17], melhorias na camada MAC de IEEE 802.11 [24, 12], o uso de multi-conexões [2, 4] e de multi-caminhos [25]. Essas propostas, porém, ainda estão em desenvolvimento e provavelmente levarão anos para chegarem aos usuários. Mas, afinal, o que pode ser feito agora?

8. CENÁRIOS ATUALMENTE VIÁVEIS

Nas seções anteriores, apresentamos as razões porque a implementação de VoWiFi é um desafio. Além disso, também apresentamos as extensões que podem ser aplicadas para viabilizar VoWiFi — mesmo que algumas dessas extensões só venham a estar disponíveis daqui a alguns anos. Nesta seção, contudo, nosso objetivo é discutir em que cenários VoWiFi é viável atualmente.

Nossos experimentos mostraram que VoWiFi provê qualidade satisfatória quando as seguintes restrições são observadas:

- o usuário fica conectado a um único ponto de acesso durante a chamada. Isso requer que o usuário tenha pouca mobilidade; movimentar-se em regiões cobertas por vários pontos de acesso levará à realização de migrações, que afetam fortemente a qualidade da ligação;
- a força do sinal a qual o usuário está conectado é alta. Apesar de reduzir a necessidade de *scannings* e de retransmissões, isso limita a área de utilização de VoWiFi para as proximidades do ponto de acesso. Em nossos experimentos, as taxas de erros em tráfegos VoWiFi foram consistentemente baixas para qualidades de sinal superiores a -70 dBm, mas esse limite³ pode variar em função, entre outros fatores, dos NICs utilizados e da carga da rede;
- um número reduzido de chamadas é feito em cada ponto de acesso. Para redes IEEE 802.11b, por exemplo, o limite é de aproximadamente 6 conexões, aproximar-se desse limite pode reduzir a qualidade das chamadas;

³Um método para monitoração e utilização efetiva da qualidade do sinal como uma métrica de adaptação pode ser encontrada em [7].

- se possível, não se deve fazer *scannings* durante a realização das chamadas de voz, o que futuramente poderá ser feito em alguns NICs chamando-se o comando `OID_802_11_MEDIA_STREAM_MODE`.

Acreditamos que existem basicamente dois cenários para o uso de VoIP. No primeiro cenário, a chamada é roteada através do sistema de telefonia padrão e VoWiFi é usado apenas para agregar mobilidade; isto seria equivalente a telefones sem fio (*cordless phones*). Este cenário poderá ser comum em ambientes corporativos e é menos complexo, pois o atraso inserido pelo uso de IEEE 802.11 deve ser insignificante.

No segundo cenário, a chamada é toda roteada através da Internet. Apesar de desafiador, esse cenário é mais próximo das necessidades dos usuários finais e, por isso, é nossa principal preocupação. Nesse caso, o usuário tem um “número” de telefone VoIP e pode migrar entre redes durante a realização de uma chamada. Os atrasos e perdas de pacotes, nesse cenário, somar-se-ão aos da Internet. Esta é uma aplicação muito interessante e acreditamos que, colocadas as restrições acima, VoWiFi é uma alternativa de boa qualidade, barata e flexível para os sistemas de comunicação de voz em tempo real.

Observamos que, respeitadas as restrições definidas acima, a qualidade de VoWiFi é ligeiramente inferior à de VoIP. Mesmo assim, achamos que a flexibilidade de uma conexão sem fios é atrativa para muitos usuários, fazendo com que VoWiFi seja uma evolução natural de VoIP, assim como o foram outras tecnologias de telefonia sem fio. Além disso, uma das razões do sucesso da telefonia celular foram os serviços agregados que se tornaram possíveis pela digitalização. De maneira análoga, novas aplicações poderiam se tornar viáveis e VoWiFi, desse modo, poderia oferecer serviços com maior valor agregado ao usuário.

9. CONCLUSÕES

Este trabalho apresentou os dois principais problemas para a ampla utilização de comunicação de voz sobre redes sem fio IEEE 802.11, que são: os *handoffs* excessivamente longos e instáveis e a alta incidência de rajadas. Além disso, fizemos uma revisão dos requisitos das aplicações de VoIP e apontamos outros problemas, além dos dois principais, que podem dificultar a utilização de VoWiFi. Apesar desses problemas, a partir dos experimentos realizados, podemos concluir que VoWiFi oferece boa qualidade quando: a capacidade de vazão da rede não é excedida, a qualidade do sinal mantém-se alta durante a realização da chamada e a mobilidade é moderada. Trabalhamos também em algoritmos para reduzir o problema de diversidade de implementação; esses algoritmos assemelham-se a processos de calibração das métricas de adaptação [7, 8].

No horizonte de trabalhos futuros, gostaríamos de utilizar os mecanismos de sincronização presentes em IEEE 802.11, *Time Synchronization Function* (TSF), para aproximadamente sincronizar o tempo de transmissão entre as unidades móveis. A idéia é distribuir estatisticamente essas transmissões de VoIP, a fim de reduzir as colisões. Isso é possível

porque em tráfegos de VoIP as transmissões se dão em intervalos regulares de tempo, por exemplo, a cada 20ms. Também estamos investigando mecanismos capazes de fazer a transição entre o modelo tradicional de comunicação bidirecional para modelos *push-to-talk* (P2T), mais resilientes a perdas de pacotes e atrasos. A transição automática poderia ser acionada quando a qualidade da conexão viesse a ficar inaceitável para a comunicação bidirecional, pois no modo P2T as restrições de latência podem ser relaxadas.

Por fim, resta observar que as tecnologias em que se baseia VoWiFi estão amadurecendo; os seus problemas estão sendo resolvidos à medida que evoluem os produtos baseados em IEEE 802.11. Se hoje ainda há algo de artesanal em VoWiFi, em alguns anos VoWiFi deve estar plenamente disponível para os usuários.

10. AUTORES ADICIONAIS

Prof. Dr. Fabio Kon, Instituto de Matemática e Estatística, Universidade de São Paulo.

11. REFERÊNCIAS

- [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 F72–F77, 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] J. Bezerra, F. Roberto, J. C. e Silva, M. Fernandez, and J. C. Jr. Previsibilidade do comportamento do canal em redes IEEE 802.11. In *24th Brazilian Symposium on Computer Networks (SBRC)*, Curitiba-PR, Brazil, May 2006. Short paper.
- [4] R. Chandra, V. Bahl, and P. Bahl. MultiNet: connecting to multiple IEEE 802.11 networks using a single wireless card. In *23rd Conference on Computer Communications (INFOCOM)*, volume 2, pages 882–893, Hong Kong, China, March 2004.
- [5] Cisco Systems. Understanding delay in packet voice networks. White Paper, September 2002. Available in <http://www.cisco.com/warp/public/788/voip/delay-details.pdf>, last visit in October 2006.
- [6] A. F. da Conceição and F. Kon. Adaptação de fluxos contínuos UDP sobre redes IEEE 802.11b. In *5th Workshop de comunicação sem fio e computação móvel (WCSF)*, pages 91–101, São Lourenço-MG, Brazil, October 2003.
- [7] A. F. da Conceição and F. Kon. Desenvolvimento de aplicações adaptativas para redes IEEE 802.11. In *24th Brazilian Symposium on Computer Networks (SBRC)*, Curitiba-PR, Brazil, May 2006.
- [8] A. F. da Conceição and F. Kon. O uso de pares de pacotes para monitoração da taxa de transmissão e da capacidade de vazão em redes IEEE 802.11. In *24th Brazilian Symposium on Computer Networks (SBRC)*, Curitiba-PR, Brazil, May 2006.
- [9] A. F. da Conceição, J. Li, D. A. Florêncio, and F. Kon. Is IEEE 802.11 ready for VoIP? In *8th International Workshop on Multimedia Signal Processing (IEEE MMSP)*, Victoria, Canada, October 2006.
- [10] S. Garg and M. Kappes. An experimental study of throughput for UDP and VoIP traffic in IEEE 802.11b networks. In *IEEE Wireless Communications and Network Conference (WCNC)*, pages 1748–1753, New Orleans, USA, March 2003.
- [11] M. S. Gast. *802.11 Wireless Networks. The definitive guide*. O’Reilly Media, 2002.
- [12] R. Gupta. *Quality of Service in Ad-Hoc Networks*. PhD thesis, Department of Electrical Engineering and Computer Science, University of California, Berkeley, USA, May 2005.
- [13] 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.
- [14] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *22nd Conference on Computer Communications (INFOCOM)*, volume 2, pages 836–843, San Francisco, USA, March 2003.
- [15] ITU-T Recommendation G.114. One-way transmission time, May 2003.
- [16] J. H. James, B. Chen, and L. Garrison. Implementing VoIP: a voice transmission performance progress report. *IEEE Communication Magazine*, 42(7):36–41, July 2004.
- [17] 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.
- [18] K. Medepalli, P. Gopalakrishnan, D. Famolari, and T. Kodama. Voice capacity of IEEE 802.11b, 802.11a and 802.11g wireless LANs. In *IEEE Global Telecommunications Conference (GLOBECOM)*, Dallas, USA, 2004.
- [19] D. L. Mills. RFC 1305 - network time protocol (version 3): Specification, implementation and analysis, March 1992.
- [20] D. L. Mills. Improved algorithms for synchronizing computer network clocks. *IEEE/ACM Transactions on Networking (TON)*, 3(3):245–254, June 1995.
- [21] W. H. Press (Ed.), S. A. Teukolsky (Ed.), W. T. Vetterling, and B. P. Flannery. *Numerical Recipes in C++: the Art of Scientific Computing*. Cambridge University Press, 2 edition, February 2002.
- [22] I. Ramani and S. Savage. SyncScan: Practical fast handoff for 802.11 infrastructure networks. In *24th Conference on Computer Communications (INFOCOM)*, Miami, USA, March 2005.
- [23] J. Schiller. *Mobile Communications*. Addison Wesley, 2000.
- [24] G. Tan and J. Guttag. The 802.11 MAC protocol leads to inefficient equilibria. In *24th Conference on Computer Communications (INFOCOM)*, Miami, USA, March 2005.
- [25] 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 *24th Conference on Computer Communications (INFOCOM)*, Miami, USA, March 2005.
- [26] H. Velayos and G. Karlsson. Techniques to reduce IEEE 802.11b handoff time. In *IEEE International Conference on Communications (ICC)*, Paris, France, June 2004.
- [27] 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):366–384, January 2005.
- [28] WildPackets. Converting signal strength percentage to dBm values. White Paper, November 2002. Available in http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf, last visit in October 2006.