UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

EDUARDO MENDES TAVARES

UM ESTUDO DE VOZ SOBRE IP EM REDES EM MALHA 802.11

NITERÓI
2008

EDUARDO MENDES TAVARES

UM ESTUDO DE VOZ SOBRE IP EM REDES EM MALHA 802.11

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Comunicação de Dados Multimídia

Orientador: Prof^{o} Luiz Cláudio Schara Magalhães, Ph.D

Niterói

2008

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

T231 Tavares, Eduardo Mendes.
Um estudo de voz sobre IP em redes em malha 802.11 / Eduardo Mendes Tavares. – Niterói, RJ : [s.n.], 2008.

89 f.

Orientador: Luiz Cláudio Schara Magalhães.
Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2008.

1. Engenharia de telecomunicação. 2. Redes em malha sem fio. 3. Redes sem fio. I. Título.

CDD 621.382

EDUARDO MENDES TAVARES

Um Estudo de Voz sobre IP em Redes em Malha 802.11

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito para obtenção do Grau de Mestre. Área de Concentração: Sistemas de Telecomunicações.

Aprovada em 15 de Abril de 2008.

BANCA EXAMINADORA

Prof. Dr. Luiz Cláudio Schara Magalhaes - Orientador
Universidade Federal Fluminense

Prof. Dr. Edjair de Souza Mota
Universidade Federal do Amazonas

Prof. Dr. Célio Vinicius Neves de Albuquerque
Universidade Federal Fluminense

Niterói
2008

Aos meus pais, pelo esforço e dedicação dispensada a mim. À minha esposa, pelo apoio e incentivo constante.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por tudo que fez, tem feito e há de fazer em minha vida. O final desta etapa de minha trajetória é parte de um plano maior seu.

Agradeço especialmente à minha esposa, que acompanhou de perto esta jornada e contribuiu de tantas formas para que eu chegasse até o fim.

Agradeço aos meus pais, irmão e toda família por abraçarem esta causa e darem todo o incentivo que precisei.

Aos amigos que participaram direta ou indiretamente desta história também rendo meus agradecimentos.

Aos professores convidados para compor a banca pelas sugestões, contribuições e comentários.

Ao meu orientador pelo apoio, conselhos e por prover sempre os recursos necessários para a realização deste trabalho.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ABREVIATURA	INGLÊS	PORTUGUÊS
ACELP	Algebraic Code Excited Linear Prediction	Predição Linear de Código Algébrico
AF	Assured Forwarding	Transferência Assegurada
AKC	Acknowledgement	Reconhecimento
AP	Access Point	Ponto de Acesso
BA	Behavior Aggregate	Agregado de Comportamento
BSS	Basic Service Set	Conjunto de Serviço Básico
CAC	Call Admission Control	Controle de Admissão de Chamada
CBR	Constant Bit Rate	Taxa Constante de Bit
CRTP	Compressed Real-Time Protocol	Protocolo de Tempo Real Comprimido
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	Acesso Múltiplo de Detecção de Portadora com Prevenção de Colisão
CST	Carrier-Sense Threshold	Limiar de Detecção da Portadora
CTS	Clear to Send	Livre para Enviar
CW	Contention Window	Janela de Contenção
DCF	Distributed Coordination Function	Função de Coordenação de Distribuição
DiffServ	Differentiated Services	Serviços Diferenciados
DIFS	Distributed Inter-Frame Space	Espaço Entre Quadros Distribuído
DSCP	Differentiated Services Code Point	Ponto de Código de Serviços Diferenciados
DSP	Digital Signal Processor	Processador de Sinal Digital
EF	Expedited Forwarding	Transferência Apressada
FCC	Federal Communications Commission	Comissão de Comunicação Federal
FHSS	Frequency Hop Spread Spectrum	Espalhamento Espectral por Salto de Freqüência
FIFO	First In First Out	Primeiro a Entrar Primeiro a Sair
FQ	Fair Queuing	Enfileiramento Justo
HTB	Hierarchical Token Bucket	Balde de Ficha Hierárquico
IBSS	Independent BSS	BSS Independente
IEEE	Institute of Electrical and Electronics Engineers	Instituto de Engenheiros Elétricos e Eletrônicos
IETF	Internet Engineering Task Force	Força Tarefa de Engenharia da Internet
IFS	Inter-Frame Space	Espaço Entre Quadros
IntServ	Integrated Services	Serviços Integrados
IP	Internet Protocol	Protocolo da Internet

ISP	Internet Service Providers	Provedor de Serviço de Internet
LAN	Local Area Network	Rede de Área Local
MAC	Medium Access Control	Controle de Acesso ao Meio
MAN	Metropolitan Area Network	Rede de Área Metropolitana
MOS	Mean Opinion Score	Escala de Opinião Média
MSDU	MAC Service Data Unit	Unidade de Dados de Serviço MAC
NAM	Network Animator	Animador de Rede
NS-2	Network Simulator	Simulador de Rede
OLSR	Optimized Link State Routing	Roteamento de Estado de Enlace Otimizado
PCF	Point Coordination Function	Função de Coordenação de Ponto
PDU	Protocol Data Unit	Unidade de Dados de Protocolo
PHB	Per-Hop Behavior	Comportamento por Salto
PHY	Physical Layer	Camada Física
PLCP	Physical Layer Convergence Protocol	Protocolo de Convergência de Camada Física
PMD	Physical Medium Dependent	Dependente do Meio Físico
PQ	Priority Queuing	Enfileiramento Prioritário
QDISC	Queuing Disciplines	Disciplinas de enfileiramento
QoS	Quality of Service	Qualidade de Serviço
RTCP	Real Time Control Protocol	Protocolo de Controle de Tempo Real
RTP	Real Time Protocol	Protocolo de Tempo Real
RTS	Request do Send	Requisição para Transmitir
RXT	Receiver Threshold	Limiar de Recepção
SDU	Service Data Unit	Unidade de Dados de Serviço
SIFS	Short Interframe Space	Espaço entre quadros curto
SIP	Session Initiation Protocol	Protocolo de Iniciação de Sessão
TC	Traffic Control	Controle de Tráfego
TCP	Transmission Control Protocol	Protocolo de Controle de Transmissão
UDP	User Datagram Protocol	Protocolo de Datagramas de Usuário
VAD	Voice Activity Detection	Detecção de Atividade de Voz
VoIP	Voice over Internet Protocol	Protocolo de Voz sobre Protocolo de Internet
WFQ	Weighted fair queuing	Enfileiramento Justo Ponderado
WAN	Wide Area Network	Rede de Área Grande
WLAN	Wireless Local Area Network	Rede de Área Local sem Fio

RESUMO

Este trabalho apresenta um estudo do desempenho de aplicações de tempo real, particularmente de voz sobre IP (VoIP), diante das características peculiares de uma rede em malha 802.11. Este tipo de aplicação exige que a rede forneça determinadas garantias com relação aos parâmetros de vazão, atraso, *jitter* e perda. A abordagem apresentada lança mão de experimentos realizados em uma rede em malha sem fio real, com o intuito de analisar os principais fatores de degradação de qualidade das aplicações de tempo real. Paralelamente, os experimentos trazem à luz o impacto destes fatores na capacidade de tráfego da rede de um modo geral. De posse destes resultados, é possível apontar algumas alternativas para amenizar os efeitos dos fatores que degradam a capacidade da rede e os efeitos da utilização destas alternativas sobre as principais métricas de medição de qualidade das aplicações de voz.

Palavras chave: Redes em malha sem fio; Voz sobre IP; Interferência; Qualidade de serviço; Capacidade de redes em malha sem fio; Capacidade de chamadas de voz.

ABSTRACT

This work presents a study of the performance of real time applications, particularly of voice over IP (VoIP), in an 802.11 Mesh network. This type of application requires that the network can supply guarantees in terms of throughput, delay, jitter and loss parameters. This work combines analytical, simulation and experiments carried out in a real network to analyze the main factors that degrade the quality of real time applications in Mesh networks. In addition, the experimental results reveal the impact of these factors over the network traffic capacity. With these results, it is possible to point out some alternative ways to reduce the effect of the degradation on network capacity and the effect of these alternatives on the quality metrics in voice applications.

Keywords: Mesh networks; Voice over IP; Interference; Quality of service; Mesh networks capacity; Voice call capacity.

1 INTRODUÇÃO

As redes 802.11 [1] e suas extensões 802.11b [2] e 802.11g [3] são atualmente as redes locais sem fio (*wireless local area network* – WLAN) mais populares em todo o mundo. Ao longo do tempo, esta tecnologia amadureceu e os preços dos dispositivos diminuíram a ponto de tornarem-se acessíveis ao usuário final. Suas aplicações são inúmeras, seja para uso educacional, doméstico, empresarial ou governamental. Existe uma tendência mundial em utilizar redes 802.11 para oferecer, em ambientes públicos, acesso à Internet de forma gratuita.

À medida que ganha espaço o conceito de convergência tecnológica, é desejável e esperado que as redes sem fio, especialmente as redes 802.11, também sejam cada vez mais utilizadas para trafegar os mais diversos tipos de aplicação. Dentre estas aplicações, uma que merece grande destaque é a disponibilização de serviços de voz sobre IP (VoIP). Há uma recente proliferação de serviços VoIP, tanto no âmbito residencial quanto no corporativo e o surgimento de diversos serviços gratuitos na Internet de fácil acesso e uso. Diante deste cenário, VoIP sobre WLAN tem o potencial de tornar-se uma importante aplicação.

1.1 REDE EM MALHA 802.11

O padrão IEEE 802.11 define dois modos de operação, o modo infra-estrutura e o modo ad hoc. As redes em malha surgiram a partir das redes ad hoc e se caracterizam por possuírem seu núcleo (*backbone*) formado por elementos que se interconectam por uma rede sem fio. O acesso a estes elementos por parte dos usuários pode ser realizado também através de dispositivos sem fio ou por meio cabeado. O *backbone* pode cobrir uma extensa área com um custo menor de infra-estrutura em comparação a outras alternativas como ADSL e

modems que utilizam a infra-estrutura de TV a cabo (*cable modems*). A partir deste *backbone* os usuários podem ter acesso à Internet através de *gateways*.

Algumas redes em malha que utilizam a tecnologia 802.11 mantêm os roteadores do *backbone* fixos, o que facilita o provimento de energia em comparação a uma rede em que todos os elementos são móveis. A limitação de energia é um problema que atinge as redes ad hoc, uma vez que os elementos são potencialmente móveis e utilizam em sua maioria baterias.

As redes em malha têm sido amplamente utilizadas ao redor do mundo. Diversas implantações têm sido feitas em universidades, empresas, comunidades e escolas. Na proporção em que a tecnologia destas redes amadurece, cresce o interesse na sua utilização para os mais diversos fins, abrindo um vasto horizonte para o uso de aplicações de dados e multimídia.

1.2 VOZ EM REDES EM MALHA

Dentre os vários serviços suportados pelas redes em malha, há um interesse crescente na utilização de VoIP. O uso de VoIP em redes em malha representa uma solução de baixo custo que oferece inúmeros benefícios como a possibilidade de interligar seus usuários à Internet para comunicações VoIP e até mesmo à Rede de Telefonia Pública Comutada através do uso de *gateways* de voz.

Todavia, o padrão 802.11 não foi originalmente desenvolvido para suportar aplicações de tempo real. Há uma necessidade de utilização de mecanismos que viabilizem seu uso. Particularmente, para a utilização de aplicações de voz em redes em malha, vários requisitos básicos devem ser atendidos. A diminuição da vazão em função do aumento do número de saltos [4], a grande quantidade de bytes de cabeçalho da pilha de protocolos, as perdas de pacotes devido às colisões e à interferência por conta da utilização de banda de freqüência não licenciada são alguns dos desafios enfrentados quando se deseja oferecer este tipo de serviço neste tipo de rede. Assim, algumas exigências se fazem necessárias para a obtenção de qualidade de serviço (QoS) satisfatória nas transações de voz em redes em malha.

A provisão de QoS para os serviços multimídia, incluindo voz, vídeo e dados é crucial. Particularmente, a garantia de um padrão aceitável de qualidade nas aplicações VoIP vai depender da utilização apropriada de mecanismos de QoS que viabilizem seu uso.

1.3 OBJETIVOS

À medida que as redes 802.11 tornam-se cada vez mais populares e seu uso gradativamente mais difundido, discutir como os serviços de voz podem ser disponibilizados nestas redes ganha uma profunda importância. Este é o objetivo desta dissertação. Especificamente, este trabalho apresenta um estudo da viabilidade de utilização de redes em malha 802.11 para prover serviços de voz com níveis aceitáveis de qualidade.

O conhecimento da capacidade de tráfego suportada por uma rede é um primeiro passo para o estudo da utilização das aplicações de voz. Porém, estimar a capacidade de tráfego em redes em malha não é uma tarefa fácil, uma vez que esta capacidade depende de diversos fatores tais como o perfil do tráfego que cursa na rede, o tamanho dos pacotes, o número de saltos, além de fatores externos, sob os quais na maioria das vezes não há controle, como a interferência gerada por outros sistemas. Por conta disto, este trabalho começa com um estudo baseado em modelos analíticos propostos para a estimativa da capacidade de tráfego em redes 802.11 e redes em malha, considerando-se diversas idealizações e simplificações. A partir desta análise, a capacidade nominal de chamadas de voz pode ser então estimada.

Diversos fatores são responsáveis pela redução da capacidade de tráfego e degradação da qualidade dos serviços em uma rede em malha. Esta é outra questão abordada neste trabalho. Estes fatores são analisados separadamente e alguns foram investigados através de experimentos, realizados por meio de simulações e medições em dispositivos 802.11.

Também foram investigados alguns mecanismos de QoS aplicáveis a redes em malha e outros recursos, que podem contribuir para a melhoria da qualidade das chamadas de voz, assim como o aumento da capacidade da rede.

Com o objetivo de estender a investigação para um ambiente real, foram conduzidos diversos experimentos em uma rede em malha implementada na Universidade Federal Fluminense, na cidade de Niterói, Rio de Janeiro, pelo projeto GTMesh, financiado pela Rede Nacional de Ensino e Pesquisa (RNP). Os experimentos validam os resultados da abordagem teórica apresentada para a estimativa de capacidade em uma rede em malha e revelam os efeitos dos fatores responsáveis pela degradação da qualidade das chamadas de voz através da disparidade dos resultados encontrados na abordagem analítica e nos experimentos.

1.4 TRABALHOS RELACIONADOS

Algumas abordagens para a estimativa de capacidade de redes 802.11 têm sido propostas ao longo dos últimos anos. Grande parte possui um enfoque voltado apenas para redes em configuração infra-estrutura ou ad-hoc. Jangeun Jun, Pushkin Peddabachagari e Mihail Sichitiu [5], por exemplo, apresentam uma fórmula para o cálculo da vazão máxima teórica obtida em uma rede 802.11b em modo infra-estrutura. O trabalho assume algumas condições ideais como ausência de erro, de colisão e de perda por descarte devido a *overflow* no receptor.

O trabalho de Kamesh Medepalli, Praveen Gopalakrishnan, David Famolari e Toshikazu Kodama [6], também voltado para redes infra-estrutura, apresenta um modelo analítico probabilístico mais completo, considerando, por exemplo, os efeitos de colisões entre os pacotes transmitidos.

Garg e Kappes [7] propõem um modelo analítico que considera algumas simplificações na camada MAC. O modelo é validado por meio de medições em uma rede 802.11.

David P. Hole e Fouad A. Tobagi [8] sugerem um modelo para redes infra-estrutura que considera o canal em condições não ideais, incluindo uma simplificação que representam tais condições através de uma taxa de erro constante (Bit Error Rate – BER). A validação do modelo é realizada através de simulações.

Alguns trabalhos abordam a capacidade de redes ad hoc, como o de Gupta e Kumar [9] onde o valor da capacidade dos nós de uma rede ad hoc são estimados. Encontramos na obra de Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee e Robert Morris [4] um estudo de capacidade para redes ad-hoc que pode ser aplicado em alguns cenários de uma rede em malha.

Já a abordagem de Jangeun Jun e Mihail L. Sichitiu em [10] é voltada especificamente para redes em malha. Porém, os resultados são obtidos levando-se em conta algumas simplificações tais como, todos os nós da rede geram a mesma taxa de tráfego e o tráfego considerado é unidirecional.

O trabalho de Bin Hong Lee, Guan Yan Cai, Yu Ge e Winston K. G. Seah [11] apresenta resultados de capacidade de voz em redes em malha baseados apenas em medições em uma rede real.

Estes estudos têm o foco voltado para a análise de capacidade de redes em malha. Este trabalho também tem este objetivo, porém traz um enfoque que avalia seqüencialmente

as seguintes questões: o estudo da capacidade de aplicações de voz em redes em malha de uma forma analítica, seguido de uma descrição e avaliação de alguns dos fatores de degradação e algumas alternativas para o aumento de capacidade da rede, terminando com uma análise experimental destas abordagens.

1.5 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em cinco capítulos. O Capítulo 1 contém alguns conceitos básicos sobre redes em malha e de voz sobre IP, bem como os desafios enfrentados na utilização deste tipo de serviço nestas redes.

O Capítulo 2 apresenta uma avaliação da capacidade de tráfego e da capacidade de chamadas de voz suportadas em redes em malha. A elaboração de modelos que descrevam de forma precisa o comportamento das redes em malha é uma tarefa extremamente difícil, pois estão envolvidos diversos fenômenos aleatórios. Assim, em sua grande maioria, os modelos sempre restringem sua aplicação a condições específicas.

O Capítulo 3 apresenta os principais fatores responsáveis pela degradação da qualidade das aplicações de voz em uma rede em malha.

O Capítulo 4 aborda algumas técnicas utilizadas para a obtenção de melhorias na qualidade e aumento de capacidade de chamadas de voz. Estas questões possuem grande aplicabilidade, mas a quantidade de pesquisa a elas dedicada tem sido reduzida.

O Capítulo 5 descreve uma série de experimentos realizados através de simulações e medições em uma rede em malha real. Nas simulações realizadas, foi utilizado o *Network Simulator* (NS-2) [12]. As medições foram efetuadas em uma rede em malha implantada na Universidade Federal Fluminense na cidade de Niterói, no Rio de Janeiro. Em seguida, é apresentado um estudo comparativo entre os resultados obtidos nos experimentos e os valores obtidos a partir dos modelos descritos no capítulo anterior. Devido às restrições dos modelos propostos, existem algumas diferenças nos valores encontrados e para uma melhor compreensão destas diferenças é realizada uma avaliação dos fatores de maior impacto na redução da capacidade de redes em malha. Finalmente, o Capítulo 6 apresenta as conclusões e sugestões para trabalhos futuros.

2 CAPACIDADE DE REDES MESH 802.11

Entende-se por capacidade de chamadas a quantidade máxima de chamadas simultâneas de voz com qualidade aceitável que pode ser estabelecida na rede. No contexto deste trabalho, a capacidade nominal de chamadas refere-se ao número máximo de chamadas que uma rede em malha pode suportar ao mesmo tempo. Existem quatro requisitos que estão relacionados com a qualidade e capacidade de chamadas em uma rede em malha: a vazão, o *jitter*, o atraso e a perda de pacotes. Cada um deles afeta de uma forma particular a qualidade das chamadas e, de certa forma, em uma rede em malha todos estão inter-relacionados.

Um dos primeiros requisitos a ser avaliado no processo de estimativa da capacidade de chamadas de voz em uma rede é a capacidade de tráfego que esta rede pode oferecer. No caso das redes em malha, por exemplo, um grande fator limitante é a redução da capacidade de tráfego na medida em que aumenta o número de saltos que o fluxo de dados deve cursar na rede. Este capítulo apresenta um estudo de como a vazão está relacionada à capacidade de chamadas em uma rede em malha. Diversos modelos analíticos têm sido propostos para a avaliação da capacidade nominal de tráfego em redes sem fio. São abordados aqui os que melhor se aplicam às redes em malha e a partir daí, a capacidade nominal de chamadas de voz é então estimada.

A seguir, são apresentados de uma forma breve alguns conceitos importantes referentes às redes 802.11 e redes em malha, necessários para a compreensão das metodologias propostas para a estimativa de capacidade da rede que serão abordadas.

2.1 O PADRÃO 802.11

O padrão 802.11 trata das camadas Física e MAC do modelo OSI . A camada física é dividida nas subcamadas *Physical Layer Convergence Protocol* (PLCP) e *Physical Medium Dependent* (PMD). A Ilustração 1 mostra a composição das camadas e os cabeçalhos que são acrescentados por cada uma delas.

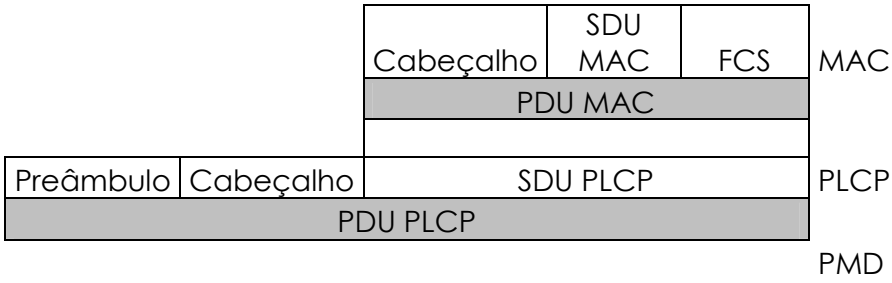

Ilustração 1: Cabeçalhos das diferentes camadas do 802.11

O *payload* de cada camada é denominado *Service Data Unit* (SDU) e consiste na carga útil de dados da camada, ou seja, desconsiderando os bytes de cabeçalho. Assim, o payload da camada MAC recebe o nome de MAC SDU (MSDU). A quantidade total de bytes transmitidos por camada, incluindo o cabeçalho é denominada *Protocol Data Unit* (PDU).

O padrão 802.11 oferece duas funções na subcamada de acesso ao meio (*medium access control* - MAC): a *Distributed Coordination Function* (DCF) e a *Point Coordination Function* (PCF). A PCF requer um ponto de acesso realizando a função de Coordenador de Acesso, não sendo, portanto, adequada para uma rede com múltiplos saltos. Assim, apenas o mecanismo DCF é abordado aqui.

O método de acesso fundamental do padrão é o DCF, que realiza o compartilhamento do meio entre as estações utilizando o método de acesso *Multiple Access with Collision Avoidance* (CSMA/CA). Segundo este método, cada estação antes de transmitir deve observar o meio e determinar se existe outra estação transmitindo. Se o meio estiver ocupado, a estação deve aguardar até o final da transmissão corrente. Isto é feito para reduzir a probabilidade de colisão de quadros transmitidos pelas estações.

O intervalo de tempo entre os quadros é denominado *Interframe Space* (IFS). A estação deve se assegurar de que o meio está livre por um intervalo de tempo específico, utilizando o mecanismo de detecção da portadora (*carrier sense*). Quatro IFS diferentes são definidos no padrão. No DCF são utilizados o *Distributed Interframe Space* (DIFS) antes da

transmissão de quadros de dados e quadros de gerenciamento e o *Short Interframe Space* (SIFS) antes de um quadro ACK.

Antes de transmitir um quadro de dados ou de gerenciamento, a estação aguarda um intervalo de tempo igual ao DIFS mais um intervalo de tempo de *backoff* aleatório dado por:

$$tempo\ de\ backoff = aleatório() \times aSlotTime \qquad (1)$$

Onde:

Aleatório() - inteiro selecionado aleatoriamente dentro de um intervalo [0, CW] e CW (*contention window* – janela de contenção) é um inteiro dentro de um intervalo de valores que vai de CWmin a CWmax.

aSlotTime – intervalo de tempo definido pelo padrão.

Após a escolha do tempo de *backoff*, a estação deve decrementar o contador de *backoff* enquanto o meio estiver livre. Se o meio se tornar ocupado novamente, o contador é interrompido e só volta a ser decrementado após o meio tornar-se livre novamente por um intervalo de tempo igual a DIFS. Quando o contador é zerado, a estação então realiza a transmissão de um quadro. Na primeira transmissão realizada pela estação, o valor da janela de contenção é (w = CWmin), que é o denominado janela de contenção mínima. A cada transmissão sem sucesso, o valor da janela de contenção é dobrado até CWmax. Após receber com sucesso um quadro, a estação receptora deve aguardar um tempo SIFS e então enviar à estação transmissora um quadro de reconhecimento (ACK). Se a estação transmissora não receber o ACK dentro de um intervalo de tempo pré-definido, ou detecta a transmissão de um pacote diferente no canal, a transmissão é considerada mal sucedida e o pacote é retransmitido de acordo com as regras de *backoff* descritas anteriormente. A Ilustração 2 mostra o ciclo de transmissão dos dados de um quadro 802.11 no CSMA/CA.

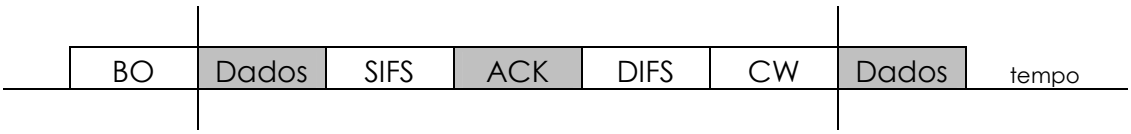

Ilustração 2: Ciclo de transmissão do CSMA/CA

Para amenizar o conhecido problema do terminal escondido, um mecanismo de solicitação do canal foi desenvolvido. Assim, sempre que um nó deseja transmitir, ele transmite um pacote *Request to Send* (RTS) para seu destinatário. O destinatário então responde com um pacote *Clear to Send* (CTS) comunicando a todos os outros nós ao seu redor que uma transmissão será efetuada. Estes nós aguardam então o fim da transmissão do nó que solicitou o meio. O problema do terminal escondido é descrito na seção 3.5.

2.2 REDES EM MALHA 802.11

A unidade básica do padrão 802.11 é o Basic Service Set (BSS). Um BSS pode ser configurado como um *independent BSS* (IBSS) ou *infrastructure BSS*. No modo *infrastructure BSS*, ou modo infra-estrutura, as estações comunicam-se através de uma estação denominada ponto de acesso (*Access Point* – AP). Já no modo IBSS, também conhecido como modo ad hoc, as estações são capazes de comunicar-se diretamente. As redes em malha, ou simplesmente redes *Mesh*, são formadas por um *backbone* sem fio com a finalidade de transmitir dados em localidades onde não existe infra-estrutura física ou onde o custo de comunicação por outras redes seria elevado. As redes em malha são formadas por um conjunto de nós fixos auto configuráveis e auto organizáveis que podem ser utilizados para prover serviços em uma área extensa que não poderia ser coberta por um único AP. Um ou mais nós da rede podem atuar como um *gateway* fornecendo acesso a outras redes como a Internet, conforme pode ser observado na Ilustração 3.

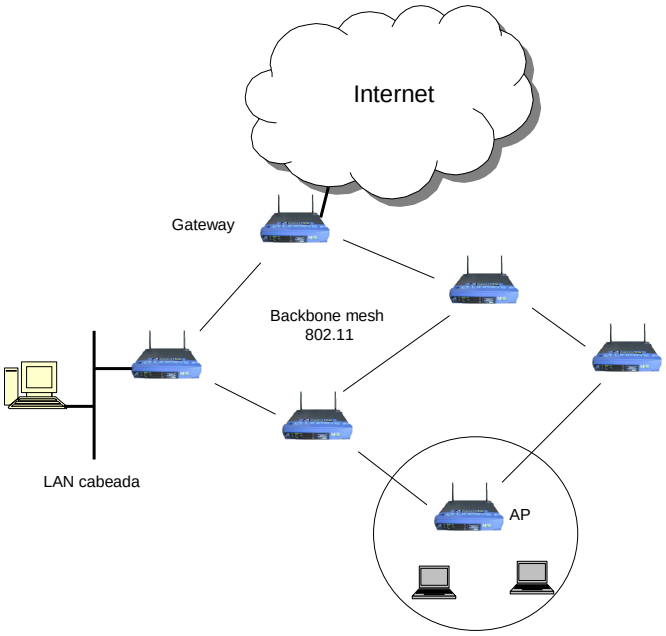

Ilustração 3: Diagrama de uma rede em malha

As redes em malha têm amadurecido de tal forma que seu uso em larga escala tem se tornado proeminente. Elas possuem um extenso leque de aplicações tais como o uso em ambiente doméstico, empresarial, militar e em redes de acesso de banda larga utilizadas por *Internet Service Providers* (ISPs). Devido à capacidade de autoconfiguração, o processo de crescimento da rede torna-se mais simplificado, podendo-se acrescentar um nó de cada vez, conforme o necessário.

2.3 REQUISITOS DE VOZ SOBRE IP

Quatro requisitos estão diretamente ligados à capacidade de uma rede em suportar VoIP: a vazão, o atraso, o *jitter* e a perda de pacotes [13] [17]. Cada um deles afeta de uma maneira particular a qualidade das chamadas de voz, podendo servir de fator limitante para a quantidade de chamadas que pode ser estabelecida com qualidade aceitável. O objetivo desta seção é descrever como cada um destes elementos se comporta em uma rede em malha. Porém, inicialmente alguns conceitos importantes de voz sobre IP precisam ser apresentados.

2.3.1 Conceitos básicos de VoIP

Toda chamada de voz é iniciada pelo protocolo de sinalização. Os mais conhecidos são o *Session Initiation Protocol* (SIP) [14] da IETF e o H.323 [15] da ITU-T. As aplicações de voz utilizam o protocolo *Real-Time Transport Protocol* (RTP), descrito na RFC 3550 [16] para transmissão do fluxo de mídia, como voz e videoconferência. O RTP é independente do protocolo de camada de transporte, porém o UDP normalmente é utilizado, uma vez que o mecanismo de controle de congestionamento do TCP traz prejuízos para o tráfego de voz.

O RTP opera em conjunto com o protocolo *Real-Time Transport Control Protocol* (RTCP). O RTCP é utilizado para fins monitoração da qualidade do serviço e transporte de informações úteis aos envolvidos na comunicação. Pacotes de controle são periodicamente enviados entre os participantes para este objetivo.

A transmissão de voz inicia-se através do processo de codificação e compressão onde o sinal analógico de voz é convertido em sinal digital. Para isto são utilizados dispositivos denominados codecs. No processo de codificação, um fluxo de dados contendo a voz digitalizada é produzido a uma taxa constante. Estes dados são gerados em forma de quadros, que serão agrupados e formarão o *payload* do pacote RTP, sendo em seguida processados nas camadas subseqüentes da rede. Na recepção, o processo inverso é realizado até a recuperação do sinal analógico de voz.

Duas técnicas de compressão são normalmente utilizadas: codificação baseada em forma de onda e codificação baseada na fonte ou codificação paramétrica. A codificação baseada em forma de onda realiza um processo de amostragem sobre o sinal analógico convertendo-o assim em sinal digital. Exemplos deste tipo de codificação são utilizados nos padrões G.711 e G.726. Na codificação paramétrica, é utilizado um dispositivo denominado Vocoder, que analisa a fala e realiza um processo de modelagem resultando em uma série de parâmetros. No receptor, um oscilador gera sinais que passam por um estágio de filtragem linear. Os filtros utilizam os parâmetros transmitidos e a voz é então reconstituída. Este esquema de compressão é utilizado pelos padrões G.728 e G.729. Uma técnica utilizada para redução do consumo de banda na rede é denominada *Voice Activity Detection* (VAD) ou supressão de silêncio.

2.3.2 Vazão

A vazão refere-se à quantidade de dados transmitidos de um nó a outro em um determinado intervalo de tempo. Normalmente é expressa em kilobits por segundo (Kbit/s) ou megabit por segundo (Mbit/s). A vazão distingue-se da taxa de dados física de um canal de comunicação, também chamada de velocidade de conexão, largura de banda digital ou capacidade do canal, que é a capacidade nominal de um enlace. A utilização do canal em termos percentuais é a vazão obtida em um canal relacionado com a taxa de dados física do canal em bits por segundo. Para exemplificar, na Ethernet, o intervalo interframes é de 12 bytes e o tamanho máximo dos frames é de 1538 bytes (1500 bytes de payload + 12 bytes de intervalo interframe + 8 bytes de preâmbulo + 14 bytes de cabeçalho + 4 bytes de trailer). Isto corresponde a uma utilização máxima do canal de [(1538-12)/1538] × 100% = 92,2% ou uma vazão máxima de 99,2 Mbps em um enlace de 100 Mbps.

Em uma rede de computadores, a vazão alcançada é menor que a vazão máxima e conseqüentemente menor que a capacidade do canal, por várias razões, tais como:

- Atrasos nodais: Em uma transmissão de dados fim a fim, cada pacote passa por uma série de nós intermediários onde sofre atrasos de processamento, de enfileiramento e de transmissão, no caso de elementos que utilizam a técnica *store and forward*, ou seja, armazenam o pacote antes de retransmiti-lo;
- Perda de pacotes devido a congestionamento: Os pacotes podem ser descartados em *switches* e roteadores quando a fila de pacotes torna-se cheia devido a congestionamento;
- Compartilhamento do canal: Se um canal com taxa R é compartilhado por N usuários, cada usuário deve experimentar uma vazão de aproximadamente R/N;
- Controle de fluxo: No protocolo TCP, por exemplo, a vazão é afetada se o produto largura de banda × atraso é maior que a janela TCP (tamanho do buffer). Neste caso o remetente deve esperar pelo reconhecimento dos pacotes antes de enviar outros;
- Controle de congestionamento do TCP: O mecanismo *slow start* do TCP é utilizado no início da transmissão de dados e cada vez que há perda de pacotes por congestionamento ou erro;
- Algoritmos de escalonamento em roteadores e *switches*: Se um mecanismo apropriado de enfileiramento de pacotes nos buffers dos roteadores não for utilizado, usuários que enviam pacotes maiores experimentam largura de banda maior. O tráfego de alguns usuários pode ser priorizado se algum mecanismo de QoS for utilizado;

- Tempo de espera de *backoff* do protocolo CSMA/CA após colisões, entre outros.

A vazão está diretamente relacionada com a capacidade de chamadas VoIP em uma rede em malha. Portanto, para descrever a capacidade de chamadas de voz é necessário descrever inicialmente qual a capacidade de tráfego da rede. A análise começa com a estimativa da vazão máxima de uma rede 802.11 em modo infra-estrutura, ou seja, com apenas um salto. Esta vazão será denotada a partir daqui pela variável B. Para o cálculo de B, algumas considerações são feitas. Assume-se inicialmente que:

- Não ocorrem colisões durante o processo de transmissão dos pacotes;
- As estações têm sempre pacotes para transmitir;
- Não há perda por erro de transmissão.

2.3.2.1 Vazão em uma topologia em modo infra-estrutura

No contexto aqui considerado, a vazão de um enlace refere-se à vazão da carga útil obtida pela camada MAC da rede, ou seja, a vazão do *payload* da camada MAC, ou vazão do MSDU. O valor de B pode ser então obtido dividindo-se o tamanho do MSDU pelo tempo consumido para transmiti-lo [5], conforme a equação abaixo:

$$B = \frac{payloadMSDU}{tempoMSDU} \qquad (2)$$

Para obter o tempo necessário para transmitir o MSDU, basta somar o tempo consumido na transmissão dos dados do MSDU ao tempo dos demais componentes de atraso envolvidos na transmissão, conforme a equação:

$$tempoMSTU = Tdados + Tsifs + Tack + Tdifs + Tbo \qquad (3)$$

Onde Tdados é o tempo necessário para transmitir o *payload* MSDU e depende do tamanho do *payload* e da taxa de transmissão, Tsifs e Tdifs são os tempos do SIFS e DIFS respectivamente, Tack é o tempo de transmissão do ACK e Tbo o tempo consumido no procedimento de *backoff*. Todos estes valores estão definidos no padrão. A Tabela 1 mostra

os valores dos parâmetros considerados e a capacidade máxima teórica, para um payload de 200 bytes, calculada a partir das equações (2) e (3), para os valores mandatórios de taxa de transmissão definidos no padrão 802.11g. Os valores de tempo estão em micro segundos, o valor de B em Mbit/s e as taxas de transmissão em Mbit/s.

Taxa de transmissão	Tdifs	Tsifs	Tbo	Tack	Tdata	Bmac
1	128	28	375	240	2058,50	0,565
2	128	28	375	240	1093,25	0,858
1	50	10	310	304	2064,00	0,584
2	50	10	310	304	1128,00	0,888
5,5	50	10	310	304	532,36	1,326
11	50	10	310	304	362,18	1,544
6	34	10	67,5	44	335,67	3,258
12	34	9	67,5	32	219,37	4,421
24	34	9	67,5	28	98,92	6,739
54	34	9	67,5	24	55,07	8,440

Tabela 1: Capacidade máxima teórica

Estes resultados mostram que para pacotes pequenos a vazão máxima da camada MAC de uma rede 802.11 possui valores bem menores do que os valores efetivos de taxa de transmissão da camada física definidos no padrão. Isto se deve por conta do grande número de bytes de cabeçalho de toda a pilha de protocolos em relação ao tamanho do quadro 802.11, além do tempo dedicado aos mecanismos de disputa do meio, definidos pelo protocolo CSMA/CA. Os valores de vazão são ainda menores quando o RTS/CTS é utilizado devido ao acréscimo no número de pacotes de controle.

2.3.2.2 Vazão em uma topologia linear

A partir da capacidade máxima teórica de uma rede em modo infra-estrutura, é possível expandir a análise de estimativa de capacidade para uma rede em malha. Nesta seção serão obtidos resultados de vazão máxima para uma rede em malha com topologia linear, como mostrado na Ilustração 4, onde o nó de número 6 representa um gateway e os nós de 1 a 5 são roteadores comuns da rede em malha.

Em redes sem fio, há uma distinção entre os limiares de nível de potência usados como referência na recepção dos dados. O *Carrier-Sense Threshold* (CST) refere-se ao nível de potência do sinal que chega ao nó receptor, a partir do qual é considerado que há interferência. O *Receiver Threshold* (RXT), por sua vez, indica o nível de potência do sinal no receptor para que haja uma recepção bem sucedida do quadro MAC. Normalmente, o valor de CST é menor do que o valor de RXT. Na rede com topologia linear considerada na análise, os nós estão dispostos de tal forma que cada nó recebe o sinal de seu nó adjacente com um nível de potência P tal que P > RXT, recebe também o sinal dos nós com 2 saltos de distância com potência RXT > P > CST e finalmente, recebe o sinal dos demais nós com nível de potência CST > P. Desta forma, um nó pode receber com sucesso apenas os pacotes enviados por seu nó adjacente (e por isto é interferido por ele), sofre interferência nó seguinte à direita e à esquerda (2 saltos), mas não é interferido pelos demais nós.

Considere inicialmente a transmissão de um fluxo de dados do nó 1 para o nó 6. A capacidade de transmissão do nó 1 pode ser deduzida da seguinte forma. Se o nó 1 sofre interferência das transmissões realizadas pelos nós 2 e 3, a capacidade do canal é compartilhada entre os 3 nós. O nó 1 terá, portanto, 1/3 da banda disponível para transmitir seus dados. Se o nó 2, por sua vez, sofrer interferência dos nós 1, 3 e 4, sua capacidade de transmissão será 1/4 da capacidade do canal. O nó 3, neste caso, disputa o meio com os nós 1, 2, 4 e 5, tendo 1/5 da banda do canal ao seu dispor. A situação é a mesma para o nó 4, que também contará apenas com 1/5 da banda disponível. Seguindo este raciocínio, o nó 5 terá disponível 1/4 da capacidade do canal. Pode-se concluir, portanto, que apesar de poder ocupar 1/3 do canal, o nó 1 tem sua capacidade de transmissão limitada pelo gargalo gerado pelos nós 3 e 4, que só podem transmitir a uma taxa de 1/5 da capacidade do canal.

Considere agora uma transmissão originada no nó 2 tendo como destino o nó 6. Repetindo-se a análise anterior, conclui-se que a capacidade do nó 2 é limitada pelo gargalo gerado pelo nó 4, novamente no valor de 1/5 do canal.

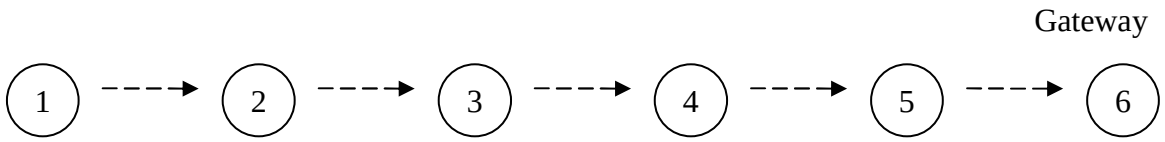

Ilustração 4: Rede em malha com topologia linear

Assim, a capacidade máxima de transmissão em uma rede com uma configuração linear pode ser estimada, conforme mostra a Tabela 2.

Número de saltos	Capacidade estimada
1	B
2	B/2
3	B/3
4	B/4
5	B/5
6	B/5

Tabela 2: Capacidade de transmissão de uma rede em configuração linear

2.3.3 Atraso

O atraso fim a fim constitui-se no atraso experimentado pelo sinal de voz do instante em que é produzido pelo locutor até o instante em que é recebido pelo ouvinte. Uma conversação telefônica é muito sensível ao atraso. Valores altos de atraso tornam-se perceptíveis pelo usuário. Segundo a Recomendação ITU-T G.114 [17], o valor máximo de atraso para uma boa qualidade de conversação é de 150 ms em um sentido. Quando o atraso ultrapassa este limite, a conversação torna-se confusa e com freqüência os locutores tendem a falar simultaneamente ou esperam um outro falar.

São várias as fontes de atraso em uma comunicação telefônica que devem ser levadas em conta. Os atrasos podem ser classificados em atrasos de rede, atraso de codificação, atraso de decodificação e atraso variável do *dejitter buffer*.

2.3.3.1 Atrasos de rede

São os atrasos gerados pela rede e compreendem o atraso de propagação, atraso de transmissão, atraso de enfileiramento, atraso devido a colisões e atraso devido ao desvanecimento.

a) Atraso de propagação

É o atraso relacionado ao tempo de propagação do sinal no meio de transmissão, sendo função da velocidade da luz no meio. O valor descrito na Recomendação G.114 da ITU-T para transmissão via rádio é de 4µs/Km, sendo portanto desprezível no cômputo atraso total fim a fim.

b) Atraso de transmissão

É o tempo gasto para se realizar a transmissão de um quadro de dados e é função da taxa de transmissão do enlace e do tamanho do quadro. Sendo *L* bits o tamanho do quadro e *R* bit/s a taxa de transmissão o atraso de transmissão é dado por *L/R*. Este tipo de atraso normalmente possui valores na ordem de microsegundos ou menos para redes de alta velocidade, porém passa a ter valores significativos em enlaces com baixa taxa de transmissão.

c) Atraso de enfileiramento

Após ser empacotado o pacote de voz é enfileirado para aguardar sua transmissão na rede. Devido à disputa dos pacotes de voz pela banda do enlace surge um atraso aleatório chamado de atraso de enfileiramento. O atraso médio de enfileiramento causado pela competição entre pacotes de voz compartilhando a mesma fila de prioridade pode ser modelado usando-se a teoria de enfileiramento para tráfego de taxa constante compartilhando uma mesma fila. Por cada nó por onde o pacote passa antes de chegar ao seu destino ocorre o mesmo tipo de atraso.

d) Atraso devido a colisões

O método de acesso CSMA/CA utilizado no padrão 802.11 provê mecanismos para a obtenção dos recursos da rede por parte dos nós, conforme descrito no Capítulo 2. Porém, durante o período de contenção, dois ou mais nós podem transmitir simultaneamente ocasionando colisões dos quadros 802.11. Cada colisão é seguida de uma retransmissão, realizada após o tempo escolhido para a janela de contenção e a cada colisão o valor da janela

de contensão aumenta. Com a rede em estado de saturação, o atraso médio sofrido por um nó devido à contenção cresce com o aumento do número de nós disputando o meio [18].

e) Atraso devido ao desvanecimento

Conforme descrito no item 2.3.2.2, o sinal que chega ao receptor deve possuir um valor de potência maior que o *Receiver Threshold* (RXT). Quando o nível da potência do sinal de um quadro 802.11 recebido está abaixo deste valor, o receptor descarta o pacote. Ao perceber a ausência do reconhecimento de recepção do quadro (ACK) o transmissor efetua a retransmissão após o novo intervalo escolhido para a janela de contenção. Consequentemente o valor do atraso fim a fim aumenta com o excesso de quadros perdidos por desvanecimento.

2.3.3.2 Atraso de codificação

O detalhamento deste tipo de atraso está disponível na Recomendação ITU-T G.114 [17] e na sessão 5.2.1 da PN-4689 [19]. Consiste em atrasos fixos, atraso de *look ahead* e atrasos referentes ao tempo de processamento do algoritmo como o tempo empregado no processo de codificação e empacotamento. Estes atrasos são descritos a seguir.

a) Atraso de processamento do vocoder

Grande parte dos codificadores de voz trabalha com o processamento de quadros. Em vez de comprimir amostra por amostra, as amostras são acumuladas em blocos e então comprimidas. O atraso de codificação, também chamado de tempo de processamento do codificador, é o tempo que o *Digital Signal Processor* (DSP) leva para comprimir um bloco de amostras. Ele varia com o tipo de codificação utilizada e com a velocidade do processador. O algoritmo *Algebraic Code Excited Linear Prediction* (ACELP), por exemplo, analisa um bloco de 10 ms com amostragens PCM e então realiza a compressão.

b) Atraso de *look ahead*

Também conhecido como atraso algorítmico, é o tempo que algumas codificações levam para conhecer mais amostras do que aquelas contidas em um quadro a fim de realizar o processo de codificação. O algoritmo de compressão precisa conhecer as características do sinal de voz para processar corretamente um bloco N de amostras bem como o conteúdo do

bloco N + 1 para realizar a reprodução correta das amostras do bloco N. Este procedimento denominado *look ahead* acrescenta um atraso ao processo de codificação. Exemplos deste tipo de atraso para alguns codecs são mostrados na Tabela 3.

Codec	**Atraso**
G.726	0 ms
G.729	5 ms
G.723.1	7,5 ms

Tabela 3: Atraso de *look ahead* de alguns codecs, conforme Recomendação G.114 [17]

c) Atraso de empacotamento

Atraso de empacotamento é o tempo necessário para preencher o pacote IP com quadros de voz codificadas/comprimidas. É uma função do tamanho dos quadros contendo as amostragens do vocoder e do número de quadros inseridos no pacote IP. Quanto menor a quantidade de quadros inseridos no pacote IP, menor é o tempo de atraso, porém mais quadros serão transmitidos por segundo e com isto, maior é a taxa de geração de quadros. Sendo maior a taxa de geração de quadros, maior é a quantidade de bytes de cabeçalho transmitida e conseqüentemente, maior é a banda ocupada pelo fluxo de voz.

2.3.3.4 Atraso de decodificação

O atraso de descompressão é normalmente 10% do tempo de compressão para cada bloco. Entretanto, o tempo de descompressão é proporcional ao numero de amostras por quadro devido à presença de múltiplas amostragens. Conseqüentemente, no pior caso, o tempo de descompressão para um quadro com três amostras é 3 × 1 ms ou 3 ms. Normalmente, dois ou três blocos de saídas G.729 comprimidas são colocados em um quadro enquanto uma amostra de uma saída G.723.1 é enviada em um único quadro. O atraso do *decoder* é detalhado na Recomendação G.114 da ITU-T [17].

2.3.3.5 Atraso do *dejitter buffer*

O receptor tipicamente utiliza um mecanismo de compensação do *jitter* gerado na rede, denominado *dejitter buffer*, que reage à perda de pacotes ou ao aumento do *jitter* na rede. Quando há perda de pacotes por descarte o tamanho do *dejjiter buffer* aumenta e quando não há descartes seu tamanho diminui [20]. O *dejjiter buffer* será explicado mais detalhadamente na seção 2.3.4.

Juntando-se todos estes elementos, o valor do atraso total fim a fim em uma rede em malha pode ser obtido pela equação abaixo:

$$Atraso = Rede + Codificação + Decodificação + Dejjiter\ Buffer \quad (4)$$

2.3.4 Jitter

O *jitter* é a variação do atraso fim a fim sofrida pelos pacotes que transitam na rede. Dois grandes responsáveis pela introdução do *jitter* em uma rede em malha são o atraso aleatório gerado no processo de enfileiramento dos pacotes nos roteadores e devido à janela de contenção da camada MAC. A solução normalmente utilizada para remover esta variação é a introdução de *buffers* (*dejitter buffers*) no último elemento do percurso, com o objetivo de armazenar os pacotes que chegam com atraso variável e entregá-los ao receptor em uma taxa constante, gerando com isto um atraso fixo. As amostras do primeiro pacote recebido são armazenadas por um período de tempo antes de serem encaminhadas para o processo seguinte. Este período inicial de armazenamento é denominado *play out delay* inicial. Um valor máximo tolerável de *jitter* é assumido e qualquer pacote recebido que ultrapassar este valor é descartado.

Alguns fatores devem ser levados em conta no cálculo do *jitter*. Quando a supressão de silêncio (VAD) é utilizada, o período de supressão deve ser desconsiderado no cálculo. No caso de perda de pacotes, o tempo de chegada dos pacotes pode parecer excessivo. Para um cálculo de *jitter* mais preciso, o número de seqüência dos pacotes deve então ser considerado e a ausência de pacotes devido a perdas deve ser compensada. Pacotes que chegam fora de ordem também podem comprometer o cálculo. Novamente o problema pode ser evitado considerando-se no cálculo o número de seqüência dos pacotes.

O valor do *dejitter buffer* pode ser ajustado na maioria dos sistemas. Quanto maior seu valor, maior o tempo de atraso final na reconstituição da voz, ocasionando efeitos

perceptíveis ao ouvinte. Porém, se seu tamanho for pequeno demais, o processo de recuperação dos pacotes no receptor ficará mais vulnerável ao *jitter* ocasionando perda de pacotes por descarte. O ajuste no tamanho do *dejitter buffer* é então uma relação de compromisso entre atraso e perda.

2.3.5 Perda

A perda de pacotes é um fator que impacta diretamente na qualidade da comunicação. Uma conversação é muito sensível ao atraso e ao *jitter*, porém pode tolerar algum grau de perda de pacotes, dependendo da resiliência ao erro do codec utilizado. Nas redes em malha, as perdas podem ser classificadas em duas categorias: perdas de pacotes na rede, perda por atraso excessivo. A seguir é descrito de forma mais detalhada cada um destes tipos de perda.

2.3.5.1 Perda de pacotes na rede

Duas causas de perda de pacotes que ocorrem na rede podem ser destacadas, a perda por falha nos enlaces e a perda devido a congestionamento.

a) Perda por falha nos enlaces e mudança de rota

Quando há falha em um enlace, seja por obstrução, desvanecimento ou qualquer outro motivo, o algoritmo de roteamento tem que recalcular uma nova rota para o tráfego. Em redes muito grandes nas quais o tempo levado para a realização do cálculo é mais significativo, pode ocorrer perda de pacotes, ocasionando a degradação na qualidade da chamada.

b) Perda por congestionamento

Os pacotes transmitidos são enfileirados nos *buffers* dos roteadores ao longo da rede. Quando a taxa de pacotes recebidos por um roteador é maior que a capacidade de transmissão em sua interface de saída, a quantidade de pacotes armazenados nos *buffers* aumenta e o que excede sua capacidade é então descartado. Para o suporte adequado das aplicações de voz na presença de aplicações de dados é necessário um gerenciamento adequado do esquema de enfileiramento dos pacotes em todos os elementos da rede.

2.3.5.2 Perda por atraso excessivo

Os pacotes que chegam ao receptor com um tempo de atraso acima do valor limite determinado pelo *dejitter buffer* são descartados. Para o tratamento adequado deste tipo de atraso é necessária uma implementação eficiente de algoritmos de *dejjiter buffer*. Além disto, conforme descrito anteriormente, o valor limite de atraso tolerado pelo *dejjiter buffer* deve ser uma relação de compromisso entre atraso e perda.

2.4 CAPACIDADE DE CHAMADAS DE VOZ EM REDES EM MALHA

A capacidade máxima nominal de chamadas de voz em uma rede em malha é limitada inicialmente pela vazão máxima da rede. Quanto maior a vazão suportada, maior a quantidade de chamadas que poderão ser estabelecidas. Esta seção apresenta uma descrição da relação entre vazão e capacidade de chamadas. Posteriormente, será verificada a influência dos fatores *jitter*, atraso e perda na capacidade de chamadas.

2.4.1 Dimensionamento de canais de voz

O perfil do tráfego gerado por uma chamada de voz é bem definido, pois o codec gera os quadros de voz a uma taxa constante. Com isto, é possível realizar o dimensionamento de tráfego consumido por uma chamada de voz.

Um pacote de voz é composto pelo *payload* de voz gerado no processo de codificação mais os cabeçalhos da pilha de protocolos utilizada. A Tabela 4 apresenta o tamanho dos cabeçalhos dos protocolos normalmente utilizados.

Cabeçalhos	**Tamanho (bytes)**
IP	20
UDP	8
RTP	12

Tabela 4: Tamanho dos cabeçalhos

O tamanho de um pacote de voz pode ser então obtido a partir da seguinte equação:

$$tamanho\ do\ pacote = cabeçalhos\ IP/UDP/RTP + payload\ de\ voz \quad (5)$$

A quantidade de pacotes transmitida por segundo (pps) depende da taxa do codec e do tamanho do *payload* de voz utilizado, e pode ser calculado pela equação:

$$pps = \text{taxa de bit do codec (bit/s)} / \text{payload de voz (bit)} \quad (6)$$

A taxa de bit gerada pelo codec está relacionada ao tamanho do *payload* de voz segundo a equação seguinte:

$$\text{taxa de bit do codec} = \text{payload de voz (bits)} / \text{tempo do payload de voz (s)} \quad (7)$$

Desta forma, a banda ocupada por uma chamada VoIP, apenas em um sentido, é obtido pela equação a seguir:

$$\text{banda consumida} = \text{tamanho do pacote} \times pps \quad (8)$$

Ou ainda pela equação:

$$\text{banda consumida} = (\text{cabeçalhos IP,UDP, RTP} + \text{payload de voz}) \times 8 \times pps \quad (9)$$

Como exemplo, para o codec G.711 utilizando 2 quadros de 80 bytes por pacote, temos:

$$\text{banda consumida} = [(40 \text{ bytes} + 160 \text{ bytes}) \times 8] \times 50 \text{ pps}$$
$$\text{banda consumida} = 80 \text{ Kbit/s}$$

Este valor representa a banda ocupada por uma chamada de voz em apenas um sentido. Para obter a banda total consumida pelos fluxos nos dois sentidos, basta multiplicar este valor por 2. Este cálculo desconsidera o silêncio dos interlocutores.

2.4.2 Estimativa de capacidade de chamadas

De posse dos valores da banda ocupada pelo codec utilizado, a capacidade nominal de chamadas de voz de um determinado nó de uma rede em malha é encontrada dividindo-se a capacidade máxima de tráfego que pode ser obtida por este nó pela banda ocupada por cada chamada, conforme mostra a equação a seguir.

capacidade de chamadas = vazão máxima do nó / banda de cada chamada (10)

Prosseguindo com o exemplo do codec G.711 apresentado no item anterior, considerando que o limite que pode ser atingido pela rede 802.11b com o tamanho do pacote IP igual a 200 bytes (MSDU = 160 + 40) é de 1,544 Mbit/s, conforme a Tabela 1, e que uma chamada utiliza fluxos nos dois sentidos, temos:

capacidade de chamadas = 1544 Kbit/s / (80 Kbit/s × 2) = 9 chamadas (11)

Portanto, o número máximo teórico de chamadas em uma rede 802.11b utilizando o codec G.711 e considerando apenas 1 salto é de 9 chamadas.

Como mostrado anteriormente, a vazão máxima de um nó em uma rede 802.11 é inversamente proporcional ao tamanho do pacote transmitido. Com isto, não apenas a taxa dos codecs deve ser levada em consideração no dimensionamento de uma rede em malha, mas também o tamanho dos pacotes. Desta forma, quanto maior a quantidade de amostras do codec inseridas em um pacote, maior será seu tamanho e conseqüentemente, maior a vazão máxima obtida. Evidentemente, conforme visto, quanto maior o pacote, maior o atraso de empacotamento. Isto sugere que deve haver uma relação de compromisso entre atraso de empacotamento e vazão.

Outro fator que deve ser considerado é que, na medida em que o número de saltos em uma rede em malha aumenta, a vazão máxima diminui e do mesmo modo a capacidade máxima teórica de chamadas também é reduzida.

Os valores de capacidade obtidos aqui são aproximados, uma vez que são derivados de valores estimados de capacidade de banda da rede, obtidos através de abordagens em sua maioria amarradas a várias considerações e restritas a cenários específicos, conforme descrito anteriormente. Além disto, embora uma chamada VoIP possa ser suportada havendo banda disponível na rede, existem diversos fatores que afetam sua qualidade, o que pode conduzir a conversação a níveis inaceitáveis de degradação. Com isto, apesar dos resultados encontrados através dos métodos descritos neste capítulo serem extremamente úteis na elaboração de projetos de dimensionamento de tráfego em redes em malha, os valores efetivos de capacidade de chamadas encontrados no mundo real serão consideravelmente menores se não houver uma aplicação eficiente de mecanismos que busquem garantir valores aceitáveis de Qualidade de Serviço.

Por tudo isto, para uma aferição mais precisa da capacidade de chamadas VoIP em uma rede em malha, a análise apresentada até aqui não é suficiente. É necessário incluir na avaliação de capacidade os fatores que afetam diretamente a percepção do usuário quanto à qualidade da fala recebida, tais como pouca tolerância a atraso e perda de pacotes.

3 FATORES QUE DEGRADAM A CAPACIDADE

A capacidade de chamadas de voz que uma rede em malha pode suportar está intrinsecamente ligada ao comportamento dos valores de capacidade de tráfego da rede e dos parâmetros de atraso, *jitter* e perda. Conforme descrito anteriormente, tais requisitos podem ter seus valores afetados diretamente por diversas causas, presentes tanto em redes cabeadas quanto em redes sem fio. Entretanto, alguns dos fatores que contribuem para a diminuição da vazão máxima obtida na rede, bem como o aumento dos valores de atraso, *jitter* e perda de pacotes são inerentes às redes em malha 802.11. Alguns deles, como a interferência ocasionada por outros nós, o desvanecimento e a saturação advém da própria rede. Outros, tais como interferências oriundas de outros sistemas, provêm de fatores externos.

Neste capítulo são descritos diversos elementos que limitam a capacidade das redes em malha, dentre os quais interferência, desvanecimento e até mesmo produção de dispositivos que não atendem às recomendações estabelecidas no padrão 802.11.

3.1 INTERFERÊNCIA

Para uma melhor utilização do espectro eletromagnético, é necessária uma utilização eficiente dos recursos de rádio, de modo a amenizar os efeitos da interferência, um fenômeno presente em redes 802.11 e que ocasiona uma significativa perda de desempenho. Descrever de forma precisa a interferência é um processo desafiador, pois deve-se levar em conta fatores muito específicos como condições do ambiente, hardware, etc. Os tipos básicos de interferência podem ser classificados conforme apresentado na Tabela 5.

Interferências	do próprio sistema
	de outros sistemas (ex. outra rede em malha)
	externas (ex. forno microondas, telefones sem fio, etc.)

Tabela 5: Tipos de interferência em uma rede em malha

3.1.1 Interferência do próprio sistema

A interferência do próprio sistema refere-se à interferência gerada entre os nós de uma mesma rede em malha. A transmissão de um nó está interferindo na transmissão de outro quando, no receptor, o nível da razão portadora/ruído está abaixo de certo valor limite.

3.1.2 Interferência de outro sistema

É a interferência gerada por outras redes 802.11, utilizando o mesmo canal ou um canal adjacente em uma área próxima. Uma maneira de se evitar este problema seria a proibição do reuso do canal em uma mesma região, como é realizado em sistemas de comunicação móvel celular. Porém, esta alternativa seria viável somente em um ambiente altamente controlado. Na maioria das vezes isto é inviável, uma vez que as redes 802.11 têm se tornado cada vez mais populares, sendo utilizadas livremente pelos mais diversos tipos de usuários.

Dos 11 canais definidos pelo padrão 802.11, apenas os canais 1, 6 e 11 podem ser utilizados simultaneamente sem interferência. Isto significa que até 3 redes podem operar simultaneamente sem interferirem entre si, desde que cada uma esteja utilizando um destes 3 canais. Quando redes distintas utilizam o mesmo canal ou canais adjacentes ocorre interferência, pois o meio é compartilhado pelas redes.

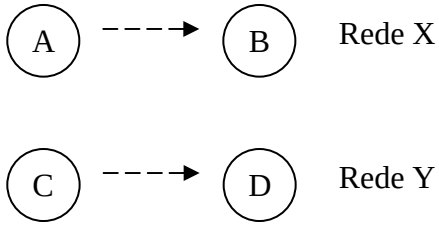

Ilustração 5: Topologia utilizada no experimento para avaliar interferência de outras redes 802.11

Este fenômeno pode ser compreendido melhor através do seguinte experimento. Uma rede X, constituída de dois elementos A e B, foi configurada para utilizar o canal 11. Uma segunda rede Y, formada pelos elementos C e D, foi configurada para operar no mesmo canal. Enquanto o nó A transmitia um fluxo UDP em sua capacidade máxima para um nó B, um nó C transmitia também em sua capacidade máxima para um dó D, conforme apresentado na Ilustração 5. Para a geração do tráfego foi utilizada a ferramenta Iperf. Os nós A e B eram roteadores Linksys WRT56G enquanto os nós C e D eram Laptops com adaptador de rede sem fio. A vazão média obtida pelos fluxos A-B e C-D isoladamente foi de 6,3 Mbit/s e 5,3 Mbit/s, respectivamente. A diferença na vazão média pode ser explicada pelos fatores citados no item 3.3. O fluxo A-B foi iniciado isoladamente e aos 30 segundos deu-se início à transmissão do fluxo C-D. Após 60 segundos do experimento, o fluxo C-D passou a ser transmitido isoladamente. Como observado na Ilustração 6, quando a transmissão foi realizada simultaneamente, o fluxo A-B passou a ter um valor médio de 4,4 Mbit/s, enquanto o fluxo C-D obteve 2,2 Mbit/s de taxa média de transmissão. Estes dois valores médios somados resultam na taxa de 6,6 Mbit/s, que é o valor encontrado para a vazão máxima teórica, conforme a Tabela 1, o que sugere que os recursos do meio foram divididos entre as duas redes. Novamente, a diferença nos valores dos fluxos transmitidos simultaneamente podem ser explicados pelos fatores descritos no item 3.3.

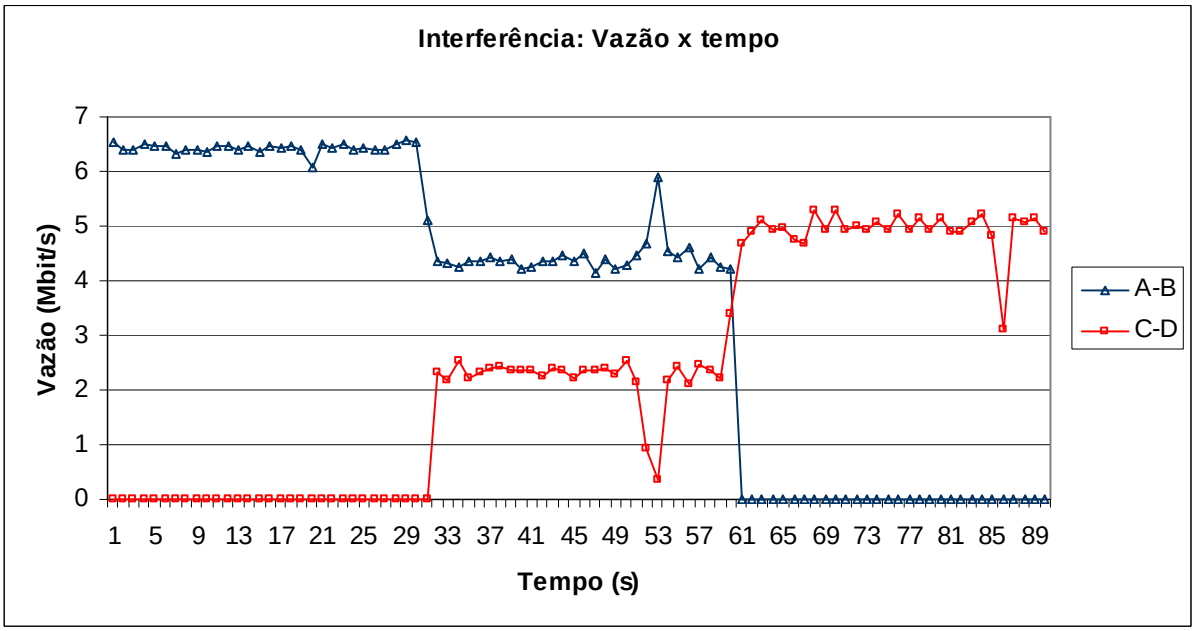

Ilustração 6: Exemplo de interferência de outro sistema

Prosseguindo com o experimento, com a alteração do canal utilizado pela rede Y observa-se o comportamento dos dois fluxos, conforme apresentado na Tabela 6. A ilustração gráfica do comportamento dos fluxos encontra-se no Apêndice A.

Canal do fluxo C - D	Vazão A – B (isolado)	Vazão A – B (com interf.)	Vazão C – D (isolado)	Vazão C – D (com interf.)
11	6,43	4,42	4,93	2,25
10	7,27	5,03	5,02	0,75
9	7,04	4,76	5,14	1,97
8	7,12	2,84	5,05	4,00
7	7,25	7,25	5,19	4,38
6	7,24	7,24	5,10	5,10

Tabela 6: Vazão de dois fluxos gerados em canais diferentes

O que pode ser observado com estes experimentos é que o protocolo CSMA/CA atua distribuindo os recursos do canal segundo seus critérios de acesso ao meio. Com isto, a capacidade tende a ser dividida localmente no domínio de colisão considerado entre os nós de cada rede e entre as redes que estiverem operando simultaneamente.

3.1.3 Interferência externa

As redes 802.11 utilizam uma banda de freqüências que não exige nenhum tipo de licenciamento. Porém, o FCC (*Federal Communications Commission*) e as agências reguladoras, como a Anatel no Brasil, exigem a certificação dos equipamentos e a utilização de baixos valores de potência. Com isto, o alcance destes dispositivos é reduzido. Porém, justamente por não utilizar uma faixa de freqüências exclusiva, o padrão 802.11 foi desenvolvido de forma que a resistência a interferências fosse alta.

Mesmo assim, diversos tipos de dispositivos e tecnologias de transmissão de dados que compartilham a mesma faixa de freqüência das redes 802.11 geram interferência que podem degradar consideravelmente seu desempenho. Alguns dos principais elementos são descritos a seguir.

3.1.3.1 Interferência por forno microondas

Os fornos microondas são uma grande fonte de interferência, pois compartilham a faixa de freqüência das redes 802.11, podendo assim degradar consideravelmente seu desempenho. O tubo de magnetron utilizada por estes aparelhos gera radiação eletromagnética que afeta a comunicação em redes 802.11. Dispositivos alimentados por corrente alternada de 60 Hz geram interferência de aproximadamente 8 ms durante ciclos de 16 ms [21].

A Ilustração 7 apresenta os resultados de um experimento realizado para a averiguação deste tipo de interferência. Durante a transmissão de um fluxo UDP entre um Laptop e um PC, utilizando o padrão 802.11b, um forno microondas foi ligado nas proximidades dos dois nós. O fluxo foi gerado através da ferramenta Iperf, de forma a obter-se a vazão máxima entre os dois nós. Inicialmente, a taxa de transmissão, sem interferência, obteve uma média de 5,27 Mbit/s. Aos 30 segundos, o forno microondas foi ligado e a vazão foi então reduzida a um valor médio de 3,07 Mbit/s, como pode ser observado no gráfico. O formo microondas permaneceu ligado durante 1 minuto, sendo desligado aos 90 segundos do experimento. A partir daí, a transmissão entre os dois nós, novamente sem interferência, continuou a ser realizada por mais 30 segundos. Percebe-se, no gráfico, o retorno da vazão entre os dois nós para valores próximos a 5,2 Mbit/s quando o forno microondas é desligado.

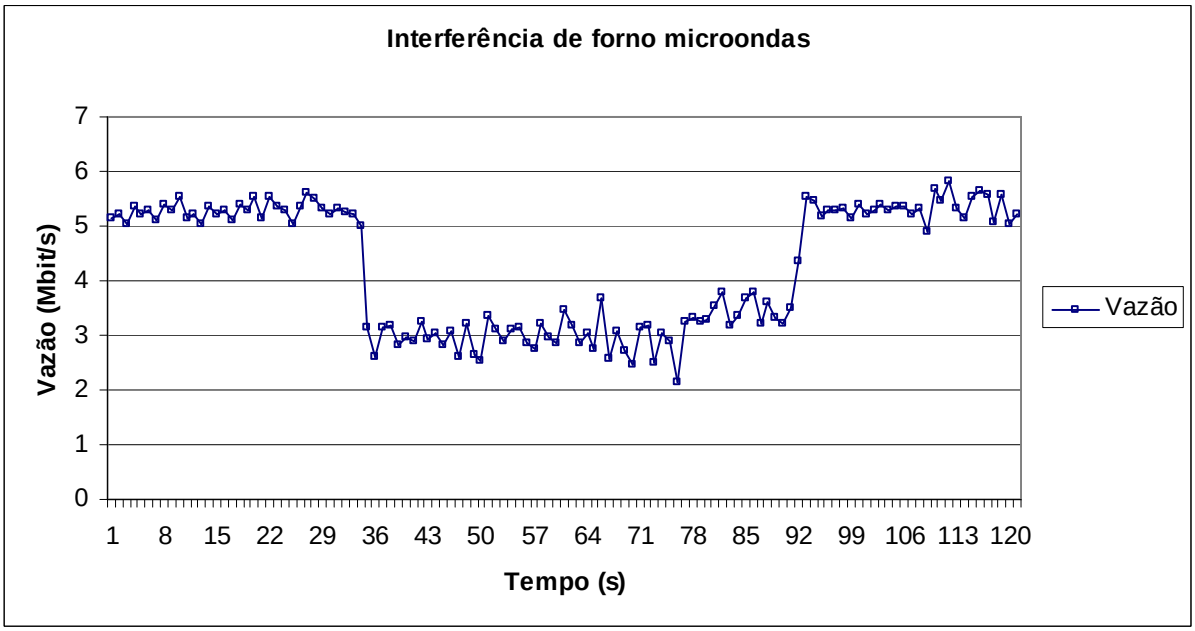

Ilustração 7: Interferência gerada por forno microondas em transmissão de dados

Para assegurar que não havia outros tipos de interferência durante o experimento e que o canal utilizado não estava sendo utilizado por nenhuma outra rede, o espectro eletromagnético foi monitorado com o uso da ferramenta Chanalyser e um processo de varredura foi efetuado pelos dois dispositivos utilizados no teste.

A Ilustração 8 mostra o espectro eletromagnético durante a realização do experimento, enquanto a transmissão de dados era efetuada, sem a interferência do forno microondas. Como pode ser observado, a rede utilizada no teste foi configurada para utilizar o canal 11.

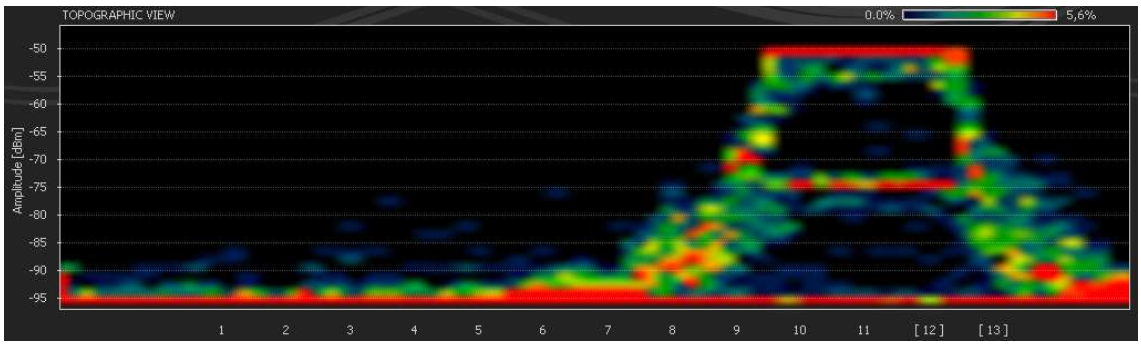

Ilustração 8: Espectro eletromagnético durante uma transmissão sem interferência

A Ilustração 9 mostra a interferência gerada pelo um forno microondas isoladamente, ou seja, com a rede sem fio de teste desativada. Observa-se que a maior parte da energia das

ondas eletromagnéticas liberadas pelo forno ocupa o espectro na faixa de freqüências utilizada pelo canal 11, estendendo-se com intensidade menor até o canal 1.

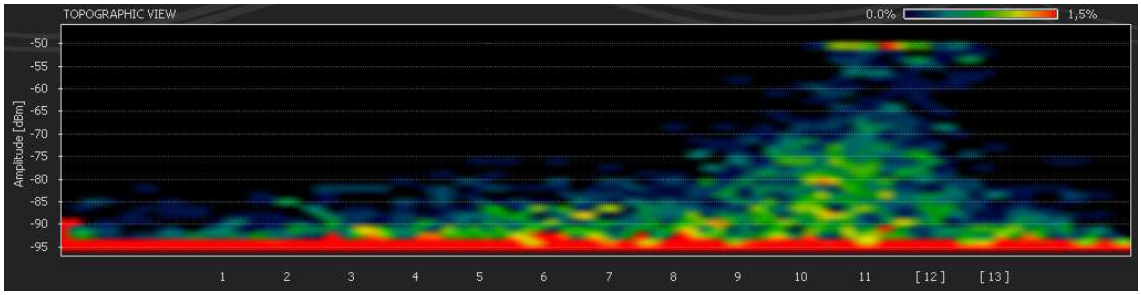

Ilustração 9: Interferência gerada por forno microondas

Finalmente, observamos na Ilustração 10 o espectro eletromagnético durante a transmissão de dados, com a interferência do forno microondas.

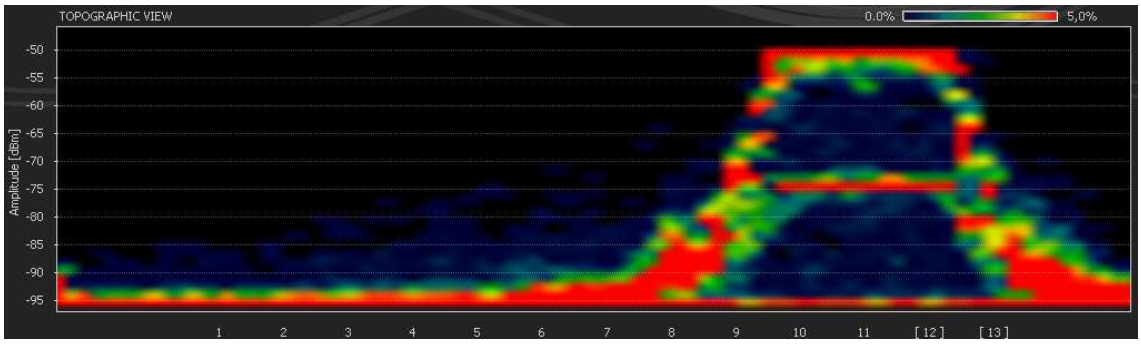

Ilustração 10: Transmissão de dados sofrendo interferência de um forno microondas

3.1.3.2 Interferência de redes Bluetooth

O Bluetooth é um padrão de redes sem fio de curta distância, que também opera na faixa dos 2.4 GHz. A perda de desempenho ocasionada por redes Bluetooth, porém, é menor devido ao método de transmissão por ele utilizado, o *Frequency Hop Spread Spectrum* (FHSS). Neste método, a freqüência utilizada pelo transmissor é alterada 1600 vezes por segundo dentre um número de canais pré-definidos pelo padrão, com o intuito de evitar-se a interferência com outros dispositivos Bluetooth. Desta forma, a interferência com redes 802.11 acaba sendo reduzida também.

A interferência ocorre quando os dispositivos Bluetooth, durante o processo de mudança de freqüência, passam a transmitir na mesma freqüência da rede 802.11. Como isto, ocorre por um curto espaço de tempo a interferência. Este tipo de interferência degrada de

forma mais significativa apenas aplicações com baixa tolerância à perda, como transmissão de fluxos de vídeo.

3.1.3.3 Interferência de telefones, mouses, teclados e outros dispositivos sem fio

Uma enorme gama de dispositivos sem fio tais como mouses, teclados, *joysticks*, além dos tradicionais telefones, têm invadido o mercado recentemente. Porém, muitos deles operam na faixa de freqüência de 2.4 GHz e também são responsáveis pela degradação do desempenho de redes 802.11. Estes dispositivos utilizam uma freqüência fixa e quando estão ativos são capazes de reduzir a taxa de transmissão da rede 802.11.

3.2 DESVANECIMENTO

Como comenta o próprio padrão 802.11, as áreas de cobertura não são bem definidas. As características de propagação das ondas eletromagnéticas são imprevisíveis e mudam a todo instante. O perfil da intensidade do campo é capaz de mudar drasticamente mesmo a partir de pequenas alterações de localização da estação. Isto ocorre em grande parte porque os sinais transmitidos por um canal de rádio experimentam o fenômeno de desvanecimento (*fading*). Alguns dos principais tipos de desvanecimento são descritos a seguir.

3.2.1 Devido à distância (*path loss*)

Trata-se do desvanecimento ocasionado pela atenuação da densidade de potência da onda eletromagnética a medida em que ela se propaga no espaço. Ocorre devido à expansão da frente de onda á medida em que aumenta a distância percorrida. Este tipo de perda é diretamente proporcional à distância e seu valor pode ser dado por d^n, onde n depende do tipo de ambiente considerado.

3.2.2 Desvanecimento lento, log-normal, long-term ou shadowing

Gerado devido a obstáculos entre origem e destino, é normalmente representado por uma distribuição log-normal e afeta o valor da potência média do sinal.

3.2.3 Desvanecimento multi-percurso, rápido, *short-term*

Este fenômeno é produzido pela soma de componentes de um mesmo sinal que chegam ao destino por diferentes percursos e com diferentes fases. O valor resultante da soma destas componentes pode ser maior ou menor que o sinal original, gerando um desvanecimento seletivo em freqüência. Quando apenas as componentes multi-percurso chegam ao destino, o desvanecimento é representado por uma distribuição de Rayleigh, sem a presença do raio em visada direta. Quando o receptor recebe além dos sinais multi-percurso a onde de linha de visada direta, denominada neste caso de componente dominante, a distribuição de Rice é utilizada. Além destas, existem outras distribuições que descrevem de forma mais detalhada o desvanecimento rápido como as distribuições de Weibull e a de Nakagami.

Um dos recursos utilizados no esquema de modulação do padrão 802.11 é a diversidade em freqüência que tem o intuito de oferecer uma maior robustez frente ao problema de desvanecimento.

3.3 VIOLAÇÃO DO PADRÃO POR PARTE DOS FABRICANTES

Não é garantido que todos os dispositivos 802.11 irão se comportar conforme é estabelecido pelo padrão. Na realidade existem diferenças significativas entre o padrão 802.11 e as implementações reais efetuadas pelos fabricantes. Alguns, por exemplo, utilizam diferentes valores para a janela mínima de contenção CWmin ou diferentes valores de IFS, bem como diferentes implementações dos mecanismos de controle de potência definidos no padrão. A diferença no comportamento dos dispositivos ocorre tanto quando ocupam isoladamente o canal quanto competem entre si. Alguns estudos conduzidos recentemente [22][23] verificaram a existência de inúmeras violações ao padrão por parte da maioria dos fabricantes, demonstrando de forma experimental o comportamento heterogêneo de tais dispositivos.

Dos diversos adaptadores de rede sem fio estudados, nenhum apresentou um comportamento satisfatório em relação à operação do *backoff*. Em alguns casos, a implementação deste mecanismo chega a afetar algumas funcionalidades do dispositivo.

Algumas partes do padrão 802.11 não são mandatórias, sendo, portanto implementadas de forma diversificada pela indústria. Diferenças significativas com relação à adaptação da taxa de transmissão, por exemplo, são encontradas. Os algoritmos de adaptação

de taxa não são especificados pelo padrão 802.11. Assim, cada fabricante implementa uma solução proprietária, levando a diferenças de comportamento nos dispositivos.

O comportamento heterogêneo das implementações dos dispositivos 802.11 pode ter impacto sobre a operação das redes, como por exemplo, alocações de banda injustas, falhas nos mecanismos de detecção de portadora e redução de desempenho na presença de terminal escondido.

3.4 SATURAÇÃO

A alocação de banda em uma rede 802.11 está relacionada com o nível de congestionamento da rede. Conforme descrito anteriormente, dependendo da carga de tráfego da rede podem ser considerados três estados: saturado, não-saturado e semi-saturado. Uma rede está saturada quando todas as estações têm sempre pacotes para transmitir. Isto significa que as estações estão sobrecarregadas. Em uma rede não-saturada, as estações não estão sobrecarregadas. Uma rede semi-saturada possui estações saturadas e não saturadas. Pode ser demonstrado que a probabilidade de colisão de uma rede 802.11 aumenta com o aumento do número de nós vizinhos compartilhando o meio ou com o aumento do tráfego destes nós [24] [25]. O estudo conduzido em [40] revela que a medida que o tráfego total da rede aumenta, aumenta a probabilidade de colisão dos pacotes transmitidos. Enquanto a probabilidade de colisão mantém-se abaixo de um determinado limiar, os valores de perda, atraso e *jitter* permanecem com valores reduzidos. Quando a probabilidade de colisão atinge o limiar, a vazão atinge seu valor máximo. A partir deste limiar de probabilidade de colisão, os valores de atraso e *jitter* aumentam significativamente e a vazão reduz-se drasticamente.

Estes resultados sugerem que para o suporte das aplicações de voz, que requerem baixos valores de atraso, *jitter* e perda, a rede deve ser mantida em um estado de não saturação. O ponto ótimo de operação da rede é então obtido se o valor limiar de probabilidade de colisão não é ultrapassado. Uma das formas de se obter isto é através da utilização de mecanismos de controle de banda que podem ser implementados na origem dos fluxos, ou seja, na aplicação que gera os dados transmitidos, ou nos elementos intermediários da rede.

3.5 TERMINAL ESCONDIDO

O problema do terminal escondido ocorre quando duas estações que estão longe do alcance uma da outra tentam transmitir para uma terceira que se situa dentro do alcance de transmissão das duas primeiras. Como mostra a Ilustração 11, o nó 2 é capaz de ouvir a portadora dos nós 1 e 3, porém os nós 1 e 3 não são capazes de perceber a portadora um do outro. Neste caso, a estação 3 poderá não perceber uma transmissão no nó 1 para o nó 2 e inadvertidamente interferir nesta transmissão [26]. Neste caso os mecanismos do CSMA/CA não funcionam e a capacidade da rede é reduzida.

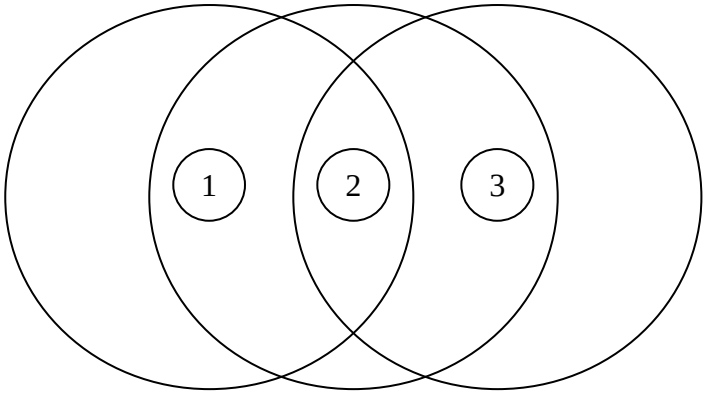

Ilustração 11: Problema do terminal escondido

Alguns trabalhos, porém, argumentam que com os ajustes adequados de potência, este efeito não é tão significativo. Se o nó 3, apesar de não estar dentro do limiar de transmissão do nó 1, estiver dentro do seu limiar de interferência, os dois nós serão capazes de observar a portadora um do outro e os mecanismos do CSMA/CA irão funcionar [26].

O mecanismo de RTS/CTS foi proposto para amenizar os efeitos do problema do terminal escondido. Porém, argumenta-se que a redução da vazão em conseqüência do aumento de overhead e sua pouca eficiência tornam seu uso desaconselhável, principalmente com pacotes pequenos [27].

3.6 TERMINAL EXPOSTO

Este fenômeno ocorre quando uma estação é impedida de transmitir devido a um transmissor vizinho. Tomando como exemplo os 4 nós exibidos na Ilustração 12, os nós receptores estão fora do alcance um do outro, enquanto os nós transmissores sofrem

interferência mútua. Enquanto o nó 2 estiver transmitindo para o nó 1, o nó 3 não consegue transmitir para o nó 4. Apesar do nó 4 estar apto a receber a transmissão do nó 3, este, após a detecção da portadora, conclui que sua transmissão causará interferência.

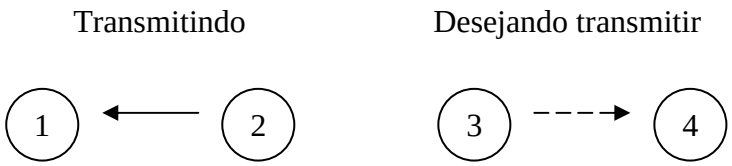

Ilustração 12: Problema do terminal exposto

4 ALTERNATIVAS PARA AUMENTO DE CAPACIDADE

Na mesma velocidade em que cresce a demanda de utilização de serviços VoIP, também cresce a necessidade de soluções que viabilizem seu uso em grande escala. Como visto anteriormente, a vazão, o atraso, o *jitter* e a perda de pacotes são parâmetros que afetam diretamente a qualidade das chamadas de voz e, conseqüentemente, reduzem a capacidade máxima de chamadas com qualidade aceitável na rede. Um grande problema enfrentado em redes em malha é que estes parâmetros podem ser profundamente afetados por elementos externos, conforme descrito no capítulo anterior, sobre os quais, na maioria das vezes, não há controle algum.

Os protocolos de sinalização de VoIP como SIP e H.323 não oferecem mecanismos de QoS. O protocolo utilizado no controle de fluxo de voz, o RTP, possui recursos como o *timestamp* e a numeração de quadros com o objetivo de amenizar os efeitos do *jitter* e da chegada de pacotes fora de ordem. Porém, estes recursos não são suficientes para uma garantia efetiva de QoS na rede. Assim, a rede deve prover mecanismos com a finalidade de assegurar os requisitos mínimos de QoS para sustentar os serviços de voz.

Uma enorme gama de soluções têm sido propostas para a provisão de QoS em redes cabeadas LANs, MANs e WANs. Uma grande quantidade de alternativas para provisão de QoS em redes sem fio também têm sido desenvolvidas. Esta seção apresenta algumas destas propostas aplicáveis em redes em malha.

4.1 DIFFSERV

A *Internet Engineering Task Force* (IETF) [28] gerou várias RFCs em meados de 1994 para o provimento de modelos de serviços integrados para a Internet. Destes esforços surgiu o *Integrated Services* (IntServ) [29], baseado no protocolo RSVP, que utiliza sinalização para reserva de recursos nos elementos da rede para cada fluxo estabelecido. Porém, o principal problema do IntServ era concernente à escalabilidade do plano de sinalização do RSVP quando aplicado à Internet. A IETF redirecionou, então, os esforços com o objetivo de desenvolver um novo modelo para o provimento de QoS. Surgiu, então, o *Differentiated Service* (DiffServ) ou serviços diferenciados, que foi definido inicialmente em 1998 pelo IETF na RFC 2475 [30]. Uma de suas principais diferenças em relação ao Intserv é a ausência de componentes de sinalização, o que possibilita uma maior escalabilidade.

A estrutura do DiffServ (DS) divide-se em dois elementos principais, as funções de borda e as funções de núcleo. Na borda da rede são aplicadas as funções de marcação, classificação e condicionamento de tráfego. Os pacotes que chegam no domínio DS são marcados nos nós de entrada. A marcação que os pacotes recebem identificam sua classe de serviço. Baseado nesta classificação, os pacotes formam fluxos agregados que recebem um tratamento específico no núcleo da rede. Na terminologia Diffserv, estes fluxos agregados são denominados *Behavior Aggregate* (BA), pois o comportamento dos nós é idêntico para todo o tráfego associado a determinado fluxo agregado. A forma como os pacotes serão encaminhados no núcleo da rede é definida pelo *Per-Hop-Behavior* (PHB), o comportamento associado à classe de serviço do pacote. Alguns PHBs padrões foram definidos, como o *Expedited Forwarding* (EF) descrito na RFC 2598 [31] e o *Assured Forwarding* (AF) documentado na RFC 2597 [32]. O PHB EF foi concebido para ser aplicado em tráfego que requer baixa perda, baixo atraso, baixo jitter e garantia de largura de banda, sendo apropriado para aplicações de voz. Os mecanismos que implementam o EF devem prover, além disso, meios para que haja uma limitação nos danos causados pelo tráfego EF em outros tipos de tráfego. O PHB AF, por sua vez, tem a finalidade de propiciar a chegada dos pacotes no destino com uma largura de banda assegurada, porém sem garantias com relação ao atraso.

Na arquitetura Diffserv, o campo *Type of Service* (TOS) do IPv4 [33] é redefinido para atuar como um campo Diffserv (DS) de 6 bits, como pode ser observado na Ilustração 13. A parte superior da ilustração mostra a composição do campo TOS conforme definido na RFC 791. Na parte inferior encontra-se como o campo TOS foi redefinido na RFC 2474. O campo DS é utilizado para transportar um código denominado *Diffserv Code Point* (DSCP)

[34], que identifica o BA de cada pacote e ocupa os 6 bits mais significativos do compo TOS. Conforme a definição do IETF, um BA é, portanto, uma coleção de pacotes com o mesmo DSCP atravessando um enlace em uma determinada direção. Com 6 bits disponíveis é possível a formação de 64 DSCPs. Entretanto, a maioria dos DSCPs não foi ainda padronizada.

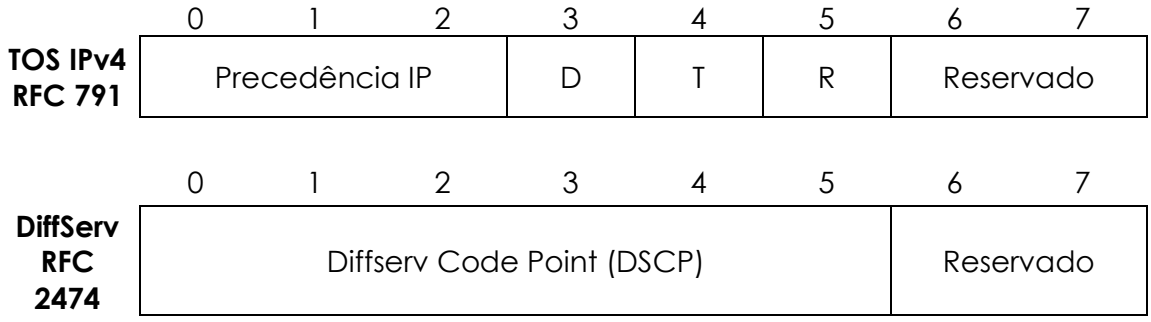

Ilustração 13: Campos TOS e DSCP no IPv4

As RFCs 2598 e 2597 recomendam que o fluxo de voz seja marcado como EF (DSCP 46) e que o tráfego associado à sinalização de voz seja marcado como AF31 (DSCP 26).

O domínio DiffServ é outro conceito importante e representa uma coleção de nós sob um mesmo controle administrativo e habilitados a suportar Diffserv. Este domínio é composto de nós de borda e nós de núcleo. Para o entendimento desta distinção algumas das principais funções executadas pelos nós de um domínio Diffserv são descritas a seguir.

a) Marcação – Consiste em definir o conteúdo do campo DSCP de um pacote. Pode ser definido como pré-marcação, quando ocorre antes do pacote entrar em um fluxo do domínio Diffserv, ou remarcação quando o conteúdo do campo DS é alterado dentro de domínio Diffserv.

b) Classificação – O processo de classificação consiste em selecionar pacotes com base no conteúdo do cabeçalho de acordo com regras preestabelecidas. A classificação pode ocorrer baseada na combinação de múltiplos campos do cabeçalho do pacote ou baseada no BA, ou seja, tomando como referência apenas o conteúdo do campo DS do pacote;

c) Policiamento - É o processo de descarte de pacotes dentro de um dado fluxo de acordo com uma métrica definida, forçando o tráfego a manter um determinado perfil. Existem duas formas de se implementar o policiamento, através de *Traffic Policing* (ou *dropping*) e *Traffic Shaping*. O *Traffic Policing* consiste em descartar os pacotes que excederem a um limite de rajada especificado, podendo ser aplicado na entrada e na saída das interfaces. Já o *Traffic Shaping* limita a emissão de pacotes a uma taxa média, através do retardamento do envio de pacotes que excedam a um limiar médio ou máximo, até que possam ser enviados ou descartados. O *Traffic Shaping* pode ser aplicado somente à saída das interfaces.

d) Escalonamento – Cada pacote que chega a um roteador é examinado e colocado em uma determinada fila onde irá aguardar até ser transmitido para o próximo nó da rede. O processo de enfileiramento (*Queuing*) ou escalonamento consiste na implementação de um algoritmo que irá controlar qual fila será atendida para a realização da transmissão de pacotes. Existem diversos modelos de escalonamento, dentre os quais destacam-se: *First-in, First out* (FIFO); *Fair Queuing* (FQ); *Priority Queuing* (PQ); *Weighted Fair Queuing* (WFQ) e diversos outros.

De uma maneira geral os nós de borda tendem a possuir funções de manipulação de pacotes mais complexas quando comparados aos nós de núcleo. As funções de classificação baseadas em campos múltiplos, policiamento (*Traffic Policing* e *Traffic Shaping*) e escalonamento são normalmente executadas pelos nós de borda. Em contrapartida, os nós de núcleo geralmente realizam a classificação baseada em BA e o escalonamento baseado em PHB. Em uma rede cabeada os nós podem ser facilmente categorizados como nós de núcleo e nós de borda, porém em uma rede em malha sem fio esta classificação não se aplica. Na verdade, todos os nós do *backbone* atuarão como nós de borda e nós de núcleo concomitantemente.

Vários métodos têm sido propostos para a provisão de Diffserv em redes 802.11 [35] [36] [37] [38] [39]. Algumas abordagens são focadas em sua implementação na camada MAC, realizando, por exemplo, ajustes no tamanho da janela de contenção para priorização de classes de serviço. Nesta abordagem, em cada nó do núcleo da rede os pacotes são colocados em diferentes filas de acordo com sua classe. Pacotes de classes com maior prioridade possuem uma fila com tempo médio de janela de contenção menor, tendo com isto uma chance maior de obter o meio que pacotes de classes com menor prioridade. Outras

abordagens utilizam diferentes esquemas para ajustar a janela de contenção após colisões ajustando valores menores para classes com maior prioridade.

A implementação do Diffserv na camada de rede deve levar em conta algumas peculiaridades da camada física e de enlace das redes 802.11. Enquanto nas redes cabeadas a largura de banda entre os nós é fixa, o mesmo não ocorre nas redes 802.11. Devido às características de compartilhamento do meio pelos nós e dos diversos fatores mencionados no capítulo anterior que degradam a capacidade da rede, a vazão máxima obtida em um enlace tem um perfil aleatório. Isto sugere que os mecanismos utilizados para a implementação do Diffserv na camada de rede como o policiamento e o escalonamento devem considerar a variação que ocorre nas camadas inferiores.

Conforme descrito na seção 3.4, a vazão máxima é obtida com a rede não saturada. Estudos conduzidos por [40] revelam que os parâmetros de atraso fim a fim, *jitter* e perda de pacotes são afetados diretamente pelo estado de saturação da rede. O que ocorre é que no estado de saturação, a probabilidade de colisão aumenta substancialmente, o que gera a redução da vazão máxima do enlace, além de aumentar de forma significativa os valores de atraso, *jitter* e perda de pacotes. Desta forma, para um melhor desempenho, é recomendável que a rede opere no seu estado de não saturação. Uma das maneiras de se obter isto é a realização do policiamento descrito anteriormente.

Realizar o policiamento significa limitar a vazão máxima de determinados fluxos gerados por cada nó da rede em prol do bem estar da rede como um todo. Um grande desafio, porém, é estabelecer os valores que servirão de referência para este controle. Como uma das características das redes em malha é possuir um comportamento aleatório da capacidade de tráfego, um requisito essencial para uma implementação eficiente de policiamento é uma estimativa de banda disponível o mais precisa possível. Esta estimativa serve de ponto de partida para a determinação do valor limite da vazão de cada nó.

Outro problema enfrentado quando se deseja implementar o policiamento é a ação dos fatores externos descritos na seção 3.1. O resultado do controle de tráfego poderá ser comprometido se o mesmo for realizado sem considerar-se a redução de capacidade da rede ocasionada por estes fatores.

4.1.1 Controle de tráfego no Linux

A rede de testes na qual foram realizados os experimentos que serão descritos no próximo capitulo foi configurada de forma a utilizar uma distribuição Linux denominada OpenWRT [41]. Uma grande variedade de funções de controle de tráfego pode ser encontrada nas versões mais recentes de kernel do Linux como parte de uma arquitetura denominada *Linux Traffic Control* [42]. Os trabalhos desenvolvidos nesta área produziram os mecanismos necessários para o suporte à arquitetura Intserv e podem servir de base para a implementação do Diffserv. O controle de tráfego no Linux pode ser configurado através do utilitário **tc**, que é parte integrante do pacote iproute2. Os componentes básicos do controle de tráfego no Linux são os seguintes:

a) Disciplinas de enfileiramento (*Queuing disciplines* – qdisc): É o bloco maior no qual o *Linux Traffic Control* está estruturado e constitui-se de algoritmos que controlam como os pacotes são tratados. Oferece as funcionalidades de enfileiramento, desenfileiramento, re-enfileiramento, descarte e fornece informações de diagnóstico. Os qdiscs são subdivididos em *classful*, que pode conter um conjunto de classes, e *classless*, que não possuem classes a eles associadas.

b) Classes: As classes existem em um *qdisc classfull* e podem conter múltiplas classes filhas. Cada classe tem um número arbitrário de filtros associados a ela.

c) Filtros: O filtro é o componente mais complexo na arquitetura do *Linux Traffic Control*. Uma das funções do filtro é classificar os pacotes.

d) Policiamento: Executa uma ação específica para valores de tráfego acima de determinado valor e outra para valores abaixo deste limiar.

Na estrutura do *Linux Traffic Control*, cada dispositivo de rede tem uma disciplina de enfileiramento associada a ele, que irá decidir como será realizado o tratamento dos pacotes que serão enfileirados em seus *buffers*. As disciplinas de enfileiramento por sua vez têm classes associadas a elas. Os filtros encarregam-se de agrupar os pacotes nestas classes. Porém, as classes não manipulam os pacotes, em vez disso, utilizam outras disciplinas de enfileiramento para realizarem esta tarefa. A Ilustração 14 mostra um exemplo da estrutura de

uma disciplina de enfileiramento no *Linux Traffic Control*. No exemplo considerado aqui, os pacotes entram na disciplina de enfileiramento principal pelo lado esquerdo da ilustração e em seguida são classificados através da utilização dos filtros, de forma a serem colocados na classe apropriada. A partir daí, os pacotes serão tratados por disciplinas de enfileiramento específicas definidas para cada classe.

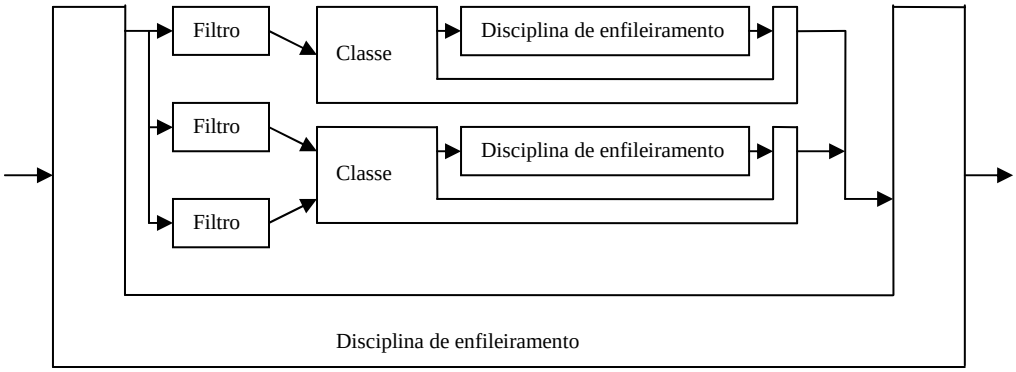

Ilustração 14: Um modelo simples de disciplina de enfileiramento no Linux

4.2 AJUSTE NO TAMANHO DOS PACOTES

O tamanho dos cabeçalhos dos pacotes em uma comunicação VoIP tem um impacto significativo na banda ocupada. Na transmissão de um fluxo de voz, quanto menor for a taxa de transmissão de pacotes, maior será a quantidade de bytes que o pacote irá comportar. Porém, isto acarretará no aumento do atraso de empacotamento. Isto significa que o receptor deverá esperar mais para receber os pacotes. Por outro lado, o aumento da taxa de transmissão de pacotes gera um aumento da carga na rede devido ao acréscimo de bytes de cabeçalho transmitidos, significando um aumento da banda ocupada pelo fluxo de voz. Se o fluxo consome mais banda então, menor será a quantidade máxima de fluxos suportada pela rede. Portanto, o ajuste no tamanho dos pacotes dos fluxos pode aumentar a eficiência do uso da banda. Isto deve ser feito levando-se em consideração o atraso máximo fim a fim aceitável para o fluxo, ou seja, há uma relação de compromisso entre atraso fim a fim e banda ocupada pelos fluxos.

4.3 COMPRESSÃO DE CABEÇALHO

A compressão de cabeçalho RTP, realizada pelo protocolo *Compressed Real-Time Transport Protocol* (CRTP) [43] padronizado pelo IETF, consiste na diminuição do tamanho do cabeçalho RTP com o intuito de aumentar a eficiência de uso da largura de banda. A compressão pode reduzir de 40 para 2 bytes o tamanho do cabeçalho, o que significa uma diminuição de 95 % em seu tamanho. Seu uso é amplamente difundido em redes WAN. Quando aplicado em redes em malha pode proporcionar um aumento de capacidade de tráfego.

4.4 SUPRESSÃO DE SILÊNCIO

A supressão de silêncio ou *Voice Activity Detection* (VAD) é uma técnica utilizada para redução do consumo de banda na rede. Considera-se que normalmente uma conversação consiste em 50 % de silêncio de cada lado transmissor. A supressão de silêncio consiste em monitorar a atividade do sinal de voz e na detecção de momentos de silêncio, a partir de um certo intervalo de tempo, evitar a transmissão de pacotes de silêncio pela rede. Isto resulta numa diminuição da ocupação da largura de banda. Porém, como depende dos instantes em que os locutores encontram-se em silêncio, esta redução é aleatória.

4.5 CONTROLE DE ADMISSÃO DE CHAMADAS - CAC

Na telefonia tradicional o controle de acesso dos usuários à rede telefônica é realizado através do controle de admissão de chamadas. A quantidade de chamadas simultâneas é limitada pela quantidade de circuitos disponíveis, definida na fase de dimensionamento do sistema telefônico.

A maioria das redes IP não implementa nenhum mecanismo de controle de admissão de tráfego de voz. Assim um novo tráfego pode entrar na rede mesmo que não haja mais recursos disponíveis para ele, comprometendo o desempenho tanto dos tráfegos existentes quanto do novo. Para se evitar isto, mecanismos de controle de admissão devem ser utilizados.

O mecanismo de controle de admissão deve levar em conta os parâmetros de desempenho da rede como atraso, *jitter* e perda de forma a atender os requisitos de QoS da rede. Seu papel é determinar se um novo fluxo de voz pode ser aceito ou rejeitado de tal

forma que a manutenção do QoS das chamadas existentes seja garantida. Por outro lado ele deve garantir que uma nova chamada não será rejeitada se a rede tem recursos disponíveis.

A eficiência do controle de admissão depende de quão precisa a capacidade da rede é aferida e esta é uma tarefa difícil. Existem duas abordagens principais para a realização do controle de admissão.

4.5.1 Controle de admissão baseado em parâmetros

Este esquema de controle de admissão utiliza as informações de tráfego, tais como atraso e perda, para tomar decisões quanto à admissão de chamadas. O mecanismo de controle de admissão pode, por exemplo, avaliar o atraso na rede e comparar com valores de referência para tomar decisões de admissão de forma apropriada.

Este método de controle de admissão pode não ser apropriado para tráfegos que possuam um perfil em rajadas, pois neste caso é difícil estimar um valor de atraso adequado. O que pode ocorrer então é um processo de decisão de admissão que subestima a capacidade da rede, reduzindo sua utilização.

4.5.2 Controle de admissão baseado em medição

Constitui-se de duas partes: medição, que tem o objetivo de estimar a carga da rede, e o controle de admissão baseado na carga da rede estimada. As medições podem ser realizadas localmente ou fim a fim. Nos métodos que utilizam medição local, cada nó da rede no caminho do fluxo efetua a medição e o controle de admissão. Já no caso de medição realizada fim a fim, os nós finais podem avaliar ativamente os recursos da rede através do envio de mensagens com o intuito de sondar o estado da rede. A maior desvantagem deste tipo de abordagem é que variações muito bruscas no estado da rede podem não ser devidamente percebidas. Para se evitar isto o tempo de sondagem pode ser reduzido, porém tendo como conseqüência um aumento de utilização dos recursos da rede. Outra desvantagem é que em alguns casos, as mensagens de sondagem não possuem *payload* de voz, logo a avaliação de como a rede irá tratar os pacotes de voz pode não ser a mais fiel.

5 AVALIAÇÃO

O grande desafio no processo de estimativa da capacidade de uma rede em malha é discriminar e modelar os fatores responsáveis pela degradação da qualidade das aplicações. Cada aplicação possui seus pré-requisitos e existem diversos fatores capazes de afetá-los, muitos dos quais possuem um comportamento aleatório.

Este capítulo apresenta uma avaliação das abordagens para estimativa de capacidade de chamadas de voz em redes em malha que foram descritas até aqui. A análise toma como base a comparação entre os métodos analíticos abordados e experimentos realizados por meio de dois processos distintos: simulação e medição em uma rede em malha real.

5.1 METODOLOGIA DOS EXPERIMENTOS

Os experimentos foram efetuados por meio de simulação e através de medições em uma rede em malha real. Algumas das vantagens da utilização de simulação para avaliação dos modelos analíticos apresentados são a possibilidade de visualização da simulação através do *Network Animator* (NAM) [44] e a facilidade na montagem de cenários variados. Em conjunto com as simulações foram realizadas medições em uma rede em malha com o objetivo de obter resultados mais próximos aos encontrados no mundo real. A seguir, são descritos os detalhes da metodologia adotada nos experimentos.

5.1.1 Simulação

Foi utilizada a ferramenta *Network Simulator* NS-2 [12] para realização das simulações. O NS-2 é um simulador para eventos discretos, muito conhecido no meio acadêmico. Os resultados obtidos são altamente dependentes dos modelos de camada física e MAC implementados na ferramenta.

5.1.2 Medição em uma rede em malha

Os experimentos de medição em um ambiente real foram realizados em uma rede sem fio Faixa Larga com configuração em malha, em ambiente *indoor*, desenvolvida por meio de um projeto da Universidade Federal Fluminense e localizada no Prédio de Engenharia da Universidade Federal Fluminense, na cidade de Niterói, estado do Rio de Janeiro. Um total de 5 roteadores foram distribuídos ao longo do 3º pavimento do prédio e um sexto roteador foi instalado em uma sala do andar superior. Uma planta baixa simplificada dos dois pavimentos é apresentada na Ilustração 15.

No desenvolvimento desta rede optou-se pela utilização de roteadores que oferecessem baixo custo de instalação, sistema operacional e ferramentas de código aberto e protocolos de roteamento já disponíveis. Os nós da rede de teste são compostos de roteadores Linksys, modelos WRT54G, que opera na faixa de freqüência de 2,4GHz segundo os padrões 802.11b e 802.11g, e WRT55AG, nas faixas de 2,4 GHz e de 5GHz, conforme o padrão 802.11a. Foi utilizado nos roteadores o sistema operacional OpenWRT, uma distribuição Linux desenvolvida para roteadores sem fio. Para o roteamento na rede foi utilizado o protocolo OLSR com uma métrica modificada, denominada ML [45].

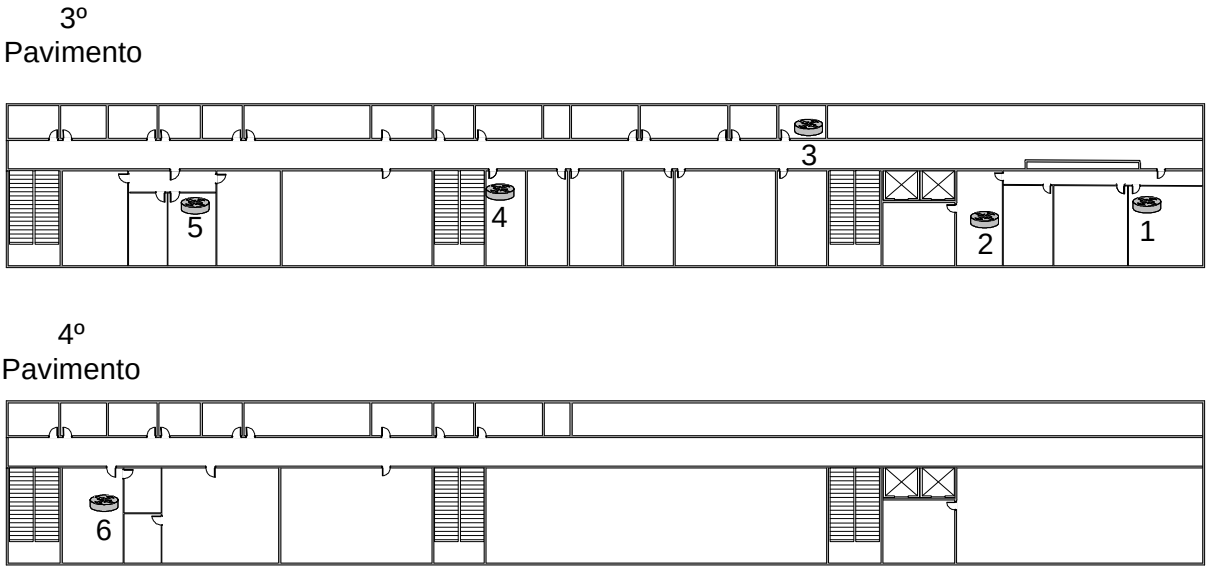

Ilustração 15: Planta baixa dos pavimentos do prédio de Engenharia da UFF

A Ilustração 16 mostra a topologia lógica da rede de testes. Para a medição de capacidade de tráfego, *jitter* e perda, foi utilizada a ferramenta de medição de desempenho de redes Iperf, versão 2.0.2 [46]. Esta ferramenta gera tráfego UDP e TCP, fornecendo relatórios de vazão para os dois tipos de tráfego, disponibilizando também informações de *jitter* e perda para tráfego UDP. Para as medições de qualidade de chamadas de voz, foram geradas chamadas simultâneas destinadas a um PC conectado diretamente ao *Gateway*. Para tanto, foi utilizado um *softphone* denominado callgen, no qual foram realizadas modificações de forma a gerar relatórios contendo diversos parâmetros referentes às chamadas, dentre os quais perdas e atraso [47] [48]. Estes relatórios foram posteriormente manipulados com o intuito de aplicar o modelo E para a obtenção do fator R das chamadas e posterior conversão para o valor referente de MOS. Todos os testes foram efetuados em um número entre 10 a 30 repetições, realizadas em horários e dias da semana diferentes. A variação nos horários em que foram obtidas as amostras se deu com o intuito de obter uma amostra representativa da variação do comportamento da rede.

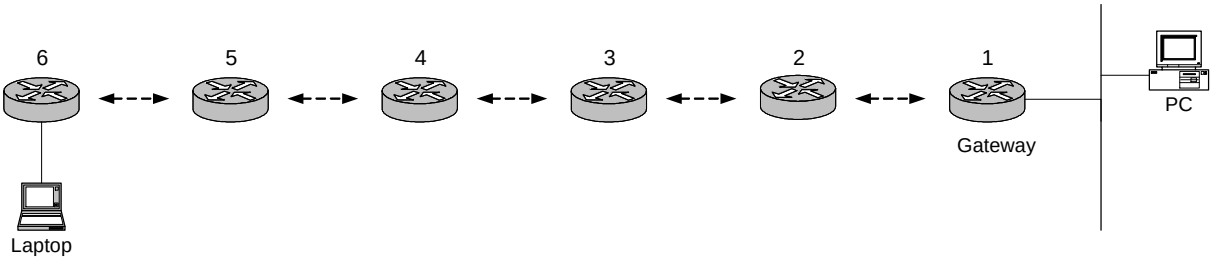

Ilustração 16: Diagrama lógico da rede de testes

Foi utilizado o codec G.729 para a realização das chamadas, pois era o único com o mecanismo de avaliação de qualidade da chamada disponível. Cada chamada teve um tempo de duração de 10 minutos. As chamadas foram efetuadas através do envio de arquivos com extensão wav, gerados previamente, nos dois sentidos da conversação, com gravações de fala, seguindo as recomendações do padrão ITU-T P.59 [49].

Para evitar a presença de tráfego indesejado durante os experimentos, o acesso dos usuários à rede foi bloqueado com a utilização do utilitário iptables, um *firewall* integrante do *kernel* Linux, uma vez que a rede de teste é também utilizada por usuários comuns da Universidade Federal Fluminense.

5.3 AVALIAÇÃO DA CAPACIDADE DE TRÁFEGO

Conforme descrito no capítulo 2, apenas uma fração da taxa nominal do canal em uma rede 802.11 é efetivamente utilizada para a transmissão de dados devido à grande quantidade de bytes de cabeçalho, à troca de mensagens de sinalização e aos mecanismos de alocação do meio do CSMA/CA. Além disto, a vazão é diretamente proporcional ao tamanho do pacote transmitido. Para averiguar isto, um experimento foi conduzido com a utilização de dois nós da rede de teste, onde um nó transmitia um fluxo de dados UDP segundo a taxa máxima comportada pelo canal. As medições foram realizadas com diversos tamanhos de pacote. A Ilustração 17 mostra os valores obtidos em contraste com os resultados obtidos com a metodologia apresentada na seção 2.3.2.1.

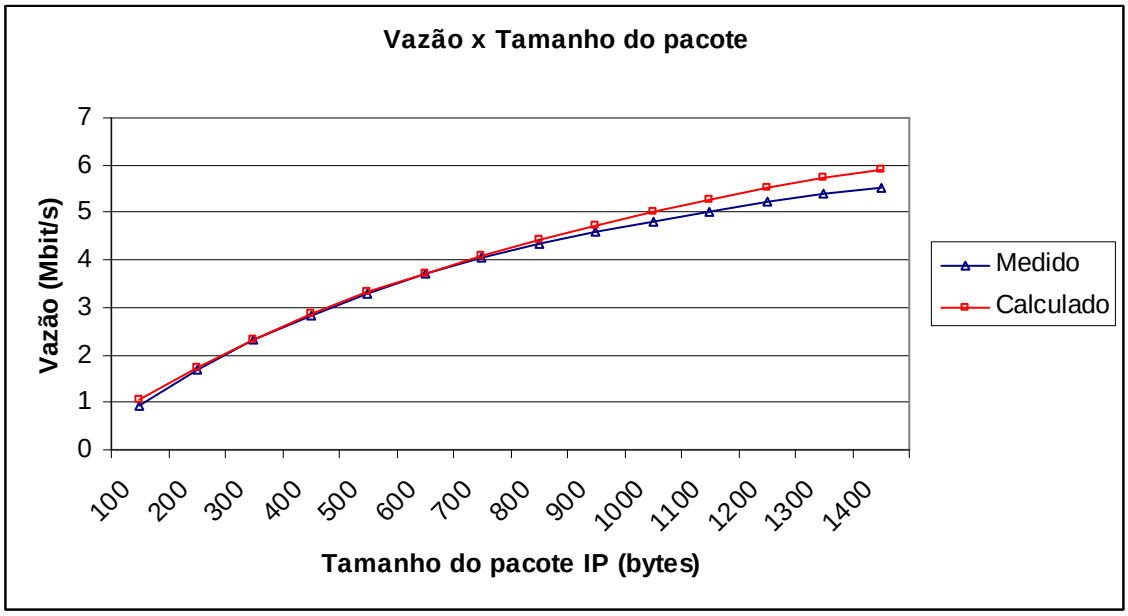

Ilustração 17: Vazão máxima em função do payload

Pode ser observado que os valores obtidos nas medições aproximam-se dos resultados obtidos analiticamente. A banda ocupada por um fluxo é diretamente proporcional ao tamanho do pacote transmitido. Os parâmetros utilizados na análise foram propositalmente ajustados para coincidir com os parâmetros configurados na rede de teste. A pequena diferença entre os valores analítico e medido deve-se principalmente às variações nos valores da janela de contenção na camada MAC, ocasionadas pela disputa do meio com o tráfego de roteamento utilizado, por colisões na transmissão ou perda de quadros devido aos efeitos de *fading*, que por simplificação não foram consideradas na abordagem analítica. Quanto maior o valor médio da janela de contenção em uma transmissão menor a vazão do fluxo. A Tabela 7 mostra o intervalo de confiança obtido a partir da realização do experimento. Neste cálculo foi considerado o nível de significância de 0,05 num total de 10 amostras para cada medição.

Pacote IP (bytes)	Desvio Padrão	Intervalo de Confiança
100	0,008343327	0,005171150
200	0,015491933	0,009601817
300	0,016633300	0,010309230
400	0,020000000	0,012395893
500	0,020138410	0,012481679
600	0,037771241	0,023410413
700	0,018408935	0,011409760
800	0,046200048	0,028634543
900	0,043525216	0,026976696
1000	0,281669625	0,174577328
1100	0,070938158	0,043967091
1200	0,054170513	0,033574594
1300	0,053427001	0,033113770
1400	0,056025788	0,034724484

Tabela 7: Intervalo de confiança do experimento vazão x tamanho do pacote IP

Uma das principais limitações das redes em malha é a redução da vazão dos nós em função do número de saltos até o destino da transmissão dos dados. O comportamento da vazão em uma configuração linear abordado no item 2.3.2.2 também foi verificado através de simulação e medições realizadas na rede de teste. Inicialmente, foi medida a vazão máxima em função do número de saltos, através da geração de tráfego UDP, com um tamanho de pacotes fixado em 1470 bytes. O resultado dos experimentos de medição e simulação é apresentado na Ilustração 18, junto com os valores estimados analiticamente.

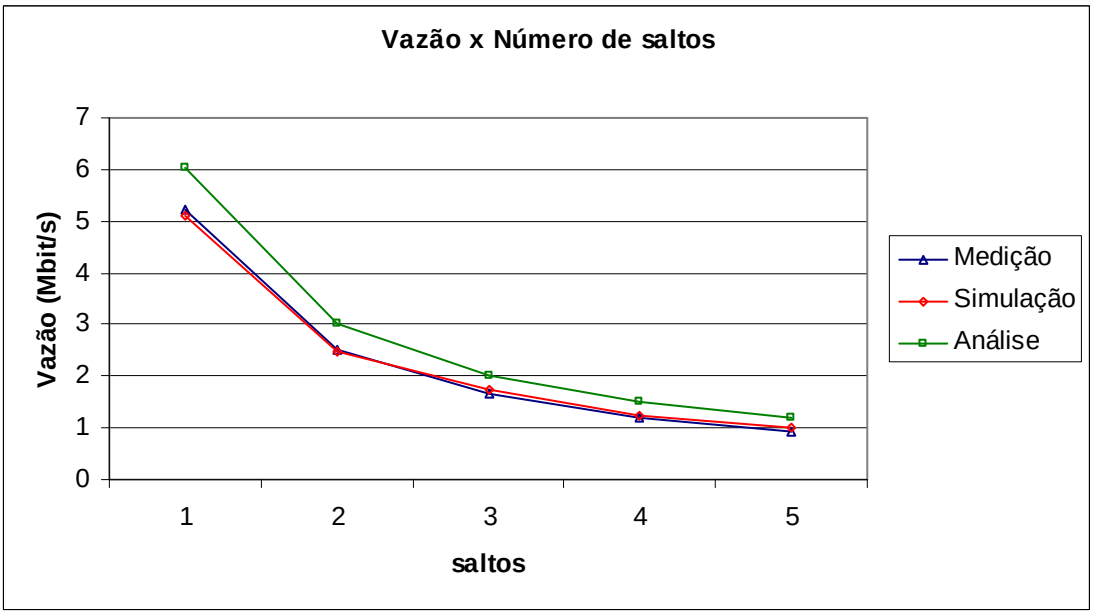

Ilustração 18: Capacidade máxima de banda por saltos – pacotes de 1470 Bytes

Conforme pode ser observado, os valores obtidos por experimentação são muito semelhantes aos valores analíticos. Como esperado, a vazão máxima é inversamente proporcional ao número de saltos entre origem e destino da transmissão de dados. Conseqüentemente, quanto mais distante determinado nó estiver do gateway da rede, menor a capacidade de chamadas de voz deste nó sendo um dos motivos à limitação de banda disponível. A Tabela 8 mostra o intervalo de confiança para o experimento. Para a simulação, é mostrado na tabela a média da vazão no estado estacionário, considerando um nível de confiabilidade de 0,95.

Saltos	Simulação		Medição	
	Média	Intervalo de Confiança	Média	Intervalo de Confiança
1	5,106635	0,007826	5,229778	0,030072
2	2,481620	0,005831	2,499640	0,048557
3	1,731633	0,011818	1,668012	0,015381
4	1,222053	0,009838	1,217886	0,009582
5	0,995004	0,043554	0,927479	0,018767

Tabela 8: Intervalo de confiança do experimento Vazão x Saltos para 1470 bytes

O mesmo experimento foi realizado entre dois nós da rede, porém com o tamanho dos pacotes fixado em 100 Bytes. Novamente, os valores medidos são condizentes com os valores obtidos pelo método analítico, conforme mostrado na Ilustração 19. Como previsto, a

vazão máxima obtida por cada nó é consideravelmente menor do que a vazão com pacotes de 1470 bytes, devido ao aumento do número de bytes de cabeçalho, de mensagens de controle e de intervalos entre os quadros (IFS) do CSMA/CA.

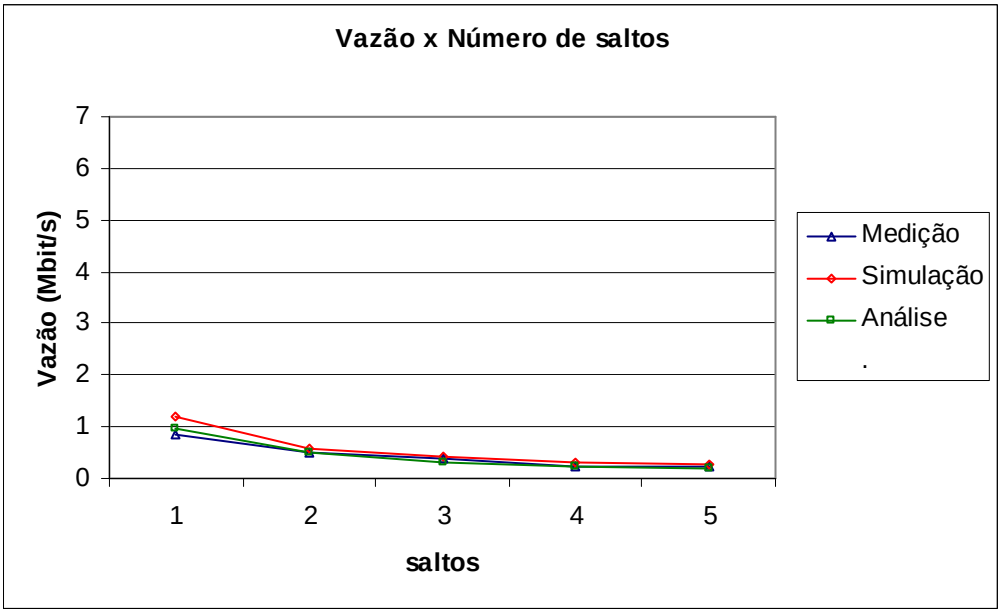

Ilustração 19: Capacidade máxima de banda por saltos – pacotes de 100 Bytes

A Tabela 9 mostra o intervalo de confiança do experimento a partir das amostras obtidas na simulação e nas medições.

Saltos	Simulação		Medição	
	Média	Intervalo de Confiança	Média	Intervalo de Confiança
1	1,194624	0,001542	0,857870	0,002630
2	0,576311	0,000738	0,492391	0,006289
3	0,427091	0,002305	0,370043	0,003832
4	0,319381	0,000840	0,243783	0,006249
5	0,282594	0,003165	0,214696	0,001683

Tabela 9: Intervalo de confiança do experimento Vazão x Saltos para 100 bytes

5.4 AVALIAÇÃO DA CAPACIDADE DE CHAMADAS DE VOZ

Conforme discutido anteriormente, a capacidade máxima de chamadas de voz em uma rede em malha é limitada inicialmente pela vazão máxima que pode ser obtida pelos nós. Foi obtido o valor nominal do número máximo de chamadas suportadas pelos nós caso a vazão máxima fosse a única limitação infligida pela rede. Porém diversos fatores afetam a qualidade das chamadas, reduzindo a capacidade real da rede. Segundo a recomendação P.114 [17], o atraso fim a fim deve ser menor que 150ms em uma direção. A violação deste limite gera degradação da qualidade de voz. A influência deste e outros parâmetros na qualidade das chamadas precisa ser modelada de forma a traduzir a percepção dos usuários do serviço de VoIP. Diversos métodos têm sido propostos para a medição fim a fim desta qualidade. A seguir é apresentado o modelo escolhido para esta finalidade.

5.4.1 Métodos de medição de qualidade

Um dos métodos mais conhecidos para medição de qualidade de chamadas é o MOS (Mean Opinion Score) descrito nas Recomendações ITU-T (ITU P.800 [50] e P.830 [51]). É um método de avaliação subjetiva em que é solicitado a um determinado número de ouvintes que classifiquem a qualidade de amostras de voz de forma objetiva, atribuindo uma pontuação que varia de 1 a 5 conforme a Tabela 10.

Qualidade da voz	**Pontuação**
Excelente	5
Boa	4
Regular	3
Insatisfatória	2
Ruim	1

Tabela 10: Pontuação MOS

A dificuldade de se utilizar os métodos subjetivos, no entanto, conduziu a propostas de aferição da qualidade de chamadas através de métodos objetivos. Um deles é o Modelo-E (*E-Model*), definido na Recomendação ITU-T G.107 [52]. Este modelo avalia os efeitos de diversos parâmetros que afetam a qualidade da conversação. Foi adotado o modelo proposto por esta recomendação para a avaliação de chamadas VoIP neste trabalho, sendo os resultados posteriormente convertidos para o valor de MOS.

O *E-Model* resulta em um valor numérico denominado fator R, que varia de 0 a 100. O fator R pode ser convertido para um valor de MOS, conforme as seguintes expressões:

$$\begin{gathered} \textit{Para } R < 0\textit{: MOS} = 1 \\ \textit{Para } 0 \leq R \leq 100\textit{: MOS} = 1 + 0{,}035\ R + 7.10\text{-}6\ R\ (R\text{-}60)\ (100\text{-}R) \\ \textit{Para } R > 100\textit{: MOS} = 4{,}5 \end{gathered} \qquad (12)$$

Os valores estão resumidos na Tabela 11.

Fator R	**Satisfação do Usuário**	**MOS**
$90 \leq R < 100$	Muito Satisfeito	4,34 – 4,50
$80 \leq R < 90$	Satisfeito	4,03 – 4,34
$70 \leq R < 80$	Alguns Insatisfeitos	3,60 – 4,03
$60 \leq R < 70$	Muitos Insatisfeitos	3,10 – 3,60
$0 \leq R < 60$	Quase todos Insatisfeitos	1,00 – 3,10

Tabela 11: Relação entre Fator R e MOS

5.4.2 Resultados

Um experimento para a avaliação da capacidade de chamadas foi realizado na rede de testes. Para isto, foram geradas chamadas de voz bidirecionais a partir de um *Laptop* conectado diretamente ao nó avaliado, com destino a um PC conectado diretamente ao *Gateway*, conforme mostra a Ilustração 16. Diversas chamadas simultâneas foram geradas e para cada chamada foi computado um valor de MOS. Assim, um valor médio de MOS foi obtido para cada grupo de *n* chamadas simultâneas geradas. Aumentando-se gradativamente o número de chamadas simultâneas, o valor resultante de MOS é reduzido. Desta forma, foi obtida a quantidade máxima de chamadas com MOS $\geq$ 3,5, valor estabelecido como limiar de qualidade aceitável. Os resultados obtidos nas medições são apresentados na Tabela 12, juntamente com os valores encontrados de forma analítica a partir das abordagens apresentadas no Capítulo 2.

	Número de chamadas	
Nó	**Análise**	**Medição**
2	61	57
3	30	23
4	20	16
5	15	6
6	12	4

Tabela 12: Número de chamadas obtido analiticamente e por experimento

Observa-se que valores medidos são consideravelmente menores do que os valores calculados. Quanto maior o número de saltos, maior também é a disparidade entre os valores. Isto sugere que os efeitos da perda de pacotes e atraso, os maiores responsáveis pela degradação da qualidade das chamadas segundo o modelo de avaliação utilizado, são muito mais significativos nos nós que se situam mais distantes do *gateway*.

5.6 TRÁFEGO CONCORRENTE

Um experimento realizado na rede de teste foi conduzido para averiguar o comportamento de um fluxo UDP na presença de tráfego TCP concorrente. Inicialmente, um tráfego UDP com taxa constante de 100 Kbit/s foi enviado do nó 3 para o nó 6. Após 30 segundos, um tráfego concorrente TCP foi gerado do nó 6 para o nó 3. O tráfego TCP, neste caso, utiliza seus mecanismos de ajuste de banda até alcançar sua vazão máxima. Foram realizadas 10 repetições do experimento e observou-se em todas um aumento significativo no *jitter* e na quantidade de pacotes perdidos enquanto os dois tráfegos eram gerados simultaneamente. A Ilustração 20 exibe uma amostra representativa do experimento. Observa-se que na transmissão do fluxo TCP é obtida uma vazão média de 1,5 Mbit/s. Após os 60 segundos do experimento, sem a concorrência do tráfego UDP, o tráfego TCP alcança uma vazão média de 1,7 Mbit/s.

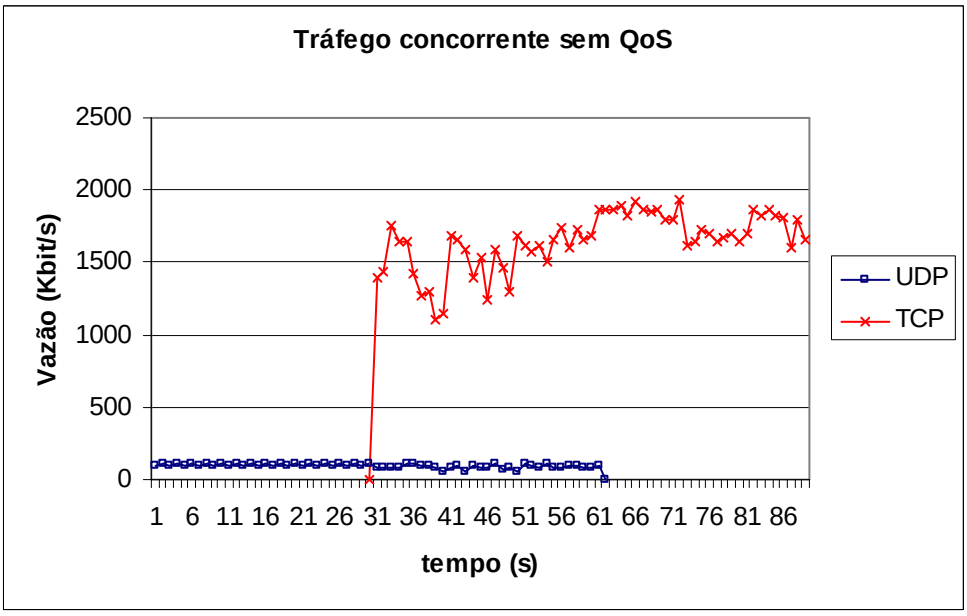

Ilustração 20: Tráfego UDP com tráfego TCP concorrente

Os valores de *jitter* do tráfego UDP coletados nesta amostra podem ser observados na Ilustração 21. Enquanto somente o tráfego UDP cursa na rede, o valor médio do *jitter* é de 1,38 ms. Após o início da transmissão do tráfego TCP, aos 30 segundos, o valor médio de *jitter* tem seu valor aumentado para algo em torno de 20 ms.

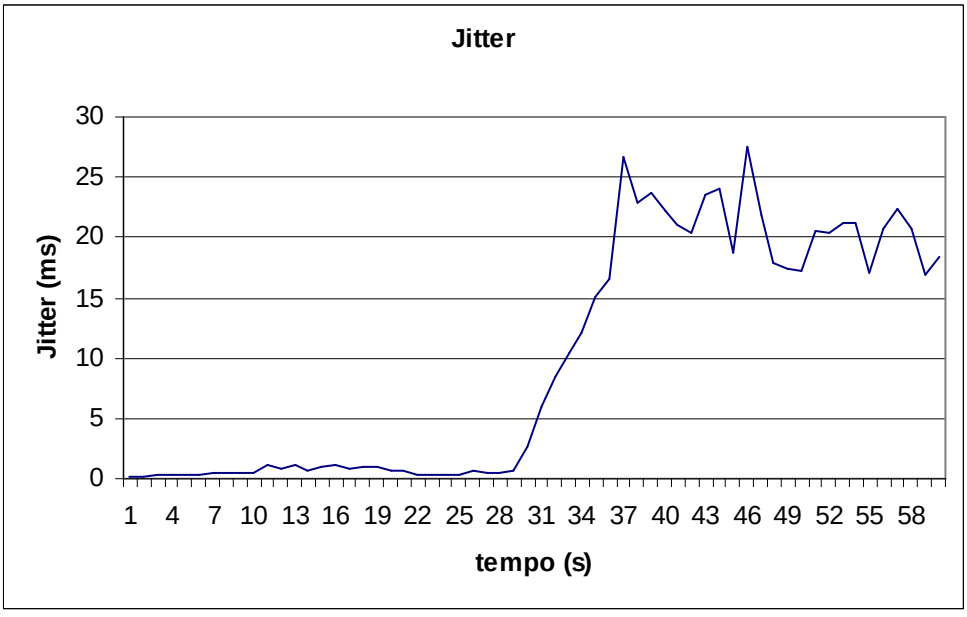

Ilustração 21: Valores de jitter do tráfego UDP com tráfego TCP concorrente

Na Ilustração 22 é mostrada a porcentagem de pacotes UDP perdidos por segundo durante a amostra. Observa-se que não há perda até o surgimento do tráfego TCP aos 30

segundos do experimento. Com a presença na rede dos dois tráfegos, há uma perda de pacotes significativa, chegando a um valor de quase 45% aos 40 segundos do experimento. A perda de pacotes UDP neste caso é justificada pela presença do tráfego TCP. Os mecanismos de ajuste da janela de transmissão do TCP fazem com que sua taxa de transmissão tente alcançar sempre o valor máximo possível, o que leva a rede a um estado de saturação. Os dois tráfegos passam a disputar não só o meio sem fio, mas também os buffers dos roteadores da rede.

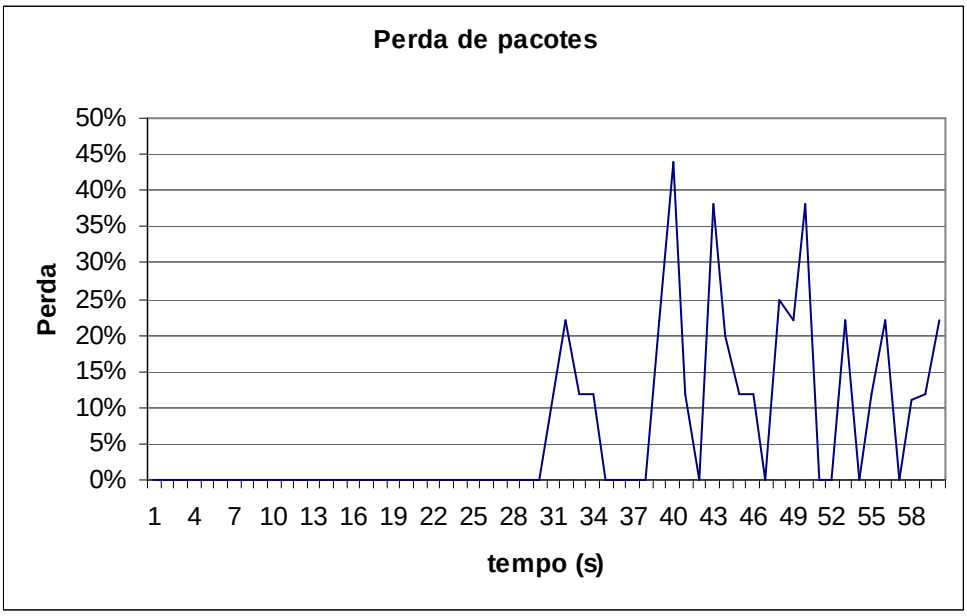

Ilustração 22: Valores de perda de pacotes UDP com tráfego TCP concorrente

Valores tão altos de perda afetam significativamente a qualidade das chamadas de voz. Percebe-se, então, a necessidade de provisão de mecanismos que priorizem o tráfego de voz na presença de tráfego TCP concorrente.

5.7 DIFFSERV COM LINUX TRAFFIC CONTROL – TC

A utilização do sistema operacional OpenWRT, uma distribuição Linux, permite a realização de experimentos de controle de tráfego através do uso do *Linux Traffic Control*. Uma avaliação do policiamento do tráfego TCP concorrente foi conduzida. Para isto, uma disciplina de enfileiramento foi aplicada à interface sem fio da rede de testes e foram criadas duas classes, uma para o tráfego TCP e outra para o tráfego UDP. Devido à importância do tráfego do protocolo de roteamento utilizado, o OLSR, foi criada uma terceira classe, com o intuito de evitar que este seja penalizado, o que comprometeria o resultado dos testes.

Para o dimensionamento do OLSR, foi realizada uma coleta de dados para levantamento de seu perfil de tráfego, conforme mostra a Ilustração 23. Aqui, observa-se o tráfego OLSR gerado pelo nó 2 da rede de teste e o tráfego recebido dos seus 2 nós adjacentes. O tráfego gerado por cada nó possui valores médios situados em torno de 2 Kbit/s, com um pico observado no intervalo de medição no valor de 6,5 Kbit/s. O OLSR utiliza a porta 698. Desta forma foi definida a marcação dos pacotes através da utilização de filtro. Verificou-se que os pacotes OLSR já saem dos nós marcados com o valor hexadecimal 0x18 no campo DS do pacote IP. Assim, foi estabelecida uma banda garantida de 150 Kbit/s para o tráfego OLSR.

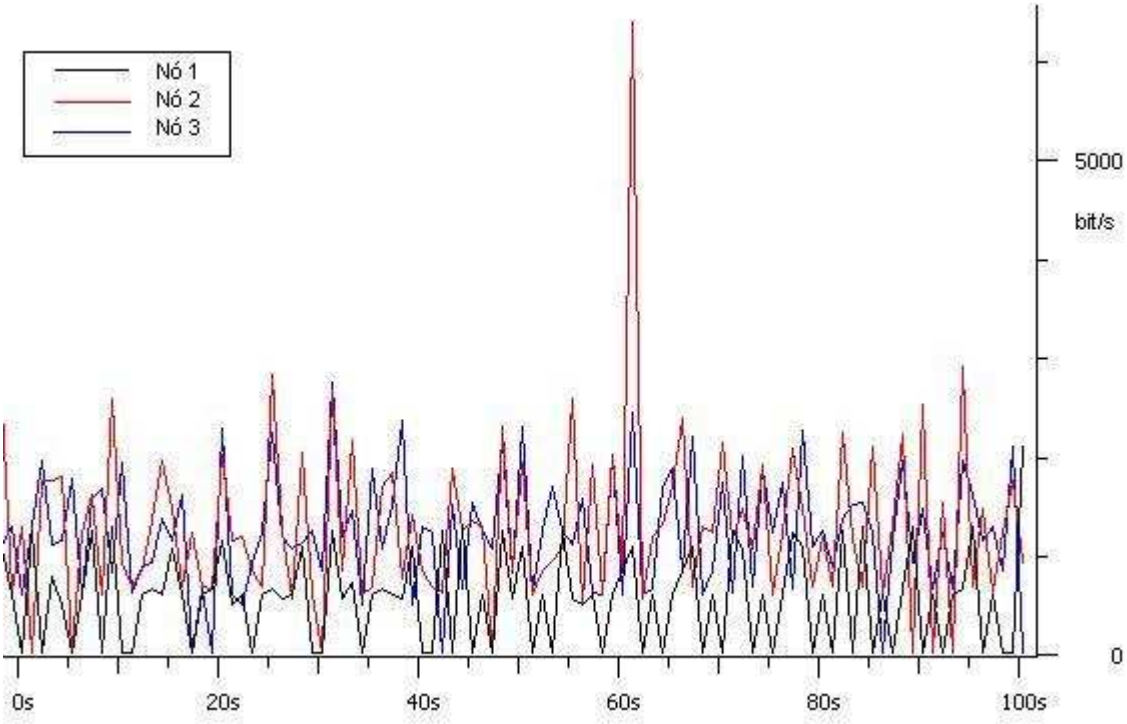

Ilustração 23: Perfil de tráfego do OLSR

À classe definida para o tráfego UDP foi associada uma disciplina de enfileiramento HTB, configurada de modo a prover um PHB EF. O tráfego UDP foi gerado com marcação no campo DS com o valor hexadecimal 0x28, conforme recomenda a RFC 2598 [31]. O tráfego UDP foi gerado com uma taxa de 300 Kbit/s e o mesmo valor de banda garantida foi configurada na rede. Na classe reservada para o tráfego TCP foi configurada uma disciplina de enfileiramento com tratamento de melhor esforço, com tráfego limitado a 64 Kbit/s.

Um tráfego UDP foi inicialmente gerado do nó 3 para o nó 6, com tamanho de pacote de 1470 Bytes, e aos 30 segundos um tráfego TCP foi transmitido do nó 6 para o nó 3 com tamanho de pacote também de 1470 Bytes. Novamente o experimento foi repetido 10 vezes e uma amostra representativa da vazão dos dois tráfegos é exibida na Ilustração 24.

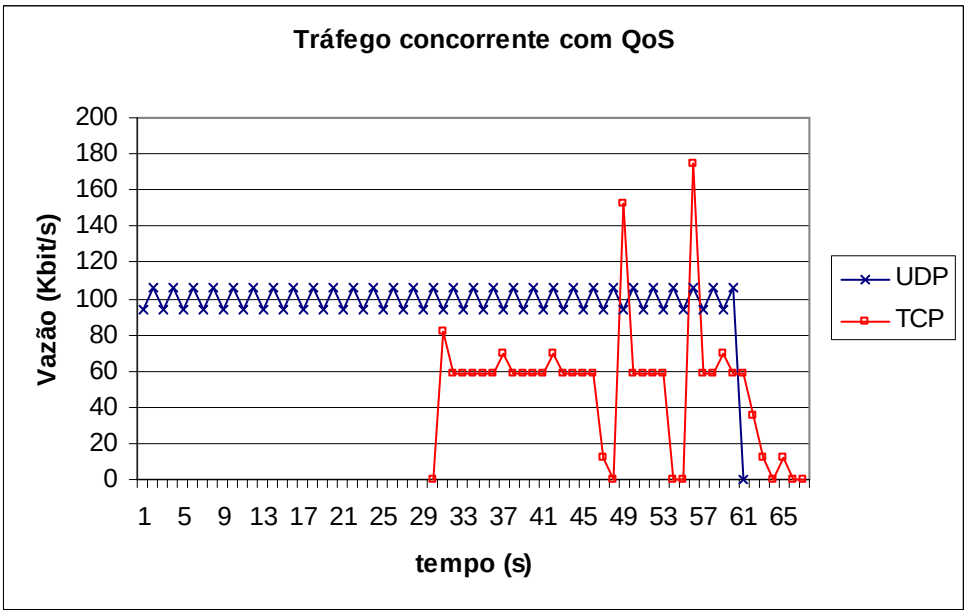

Ilustração 24: Tráfegos UDP e TCP concorrentes com controle de tráfego

A Ilustração 25 exibe os valores de *jitter* do tráfego UDP da amostra. O valor médio do *jitter* durante os primeiros 30 segundos do experimento, enquanto apenas o tráfego UDP cursava na rede, era de algo em torno de 1 ms. Observa-se que a partir dos 30 segundos do experimento, quando o tráfego TCP foi iniciado, houve um pequeno aumento no valor do *jitter*.

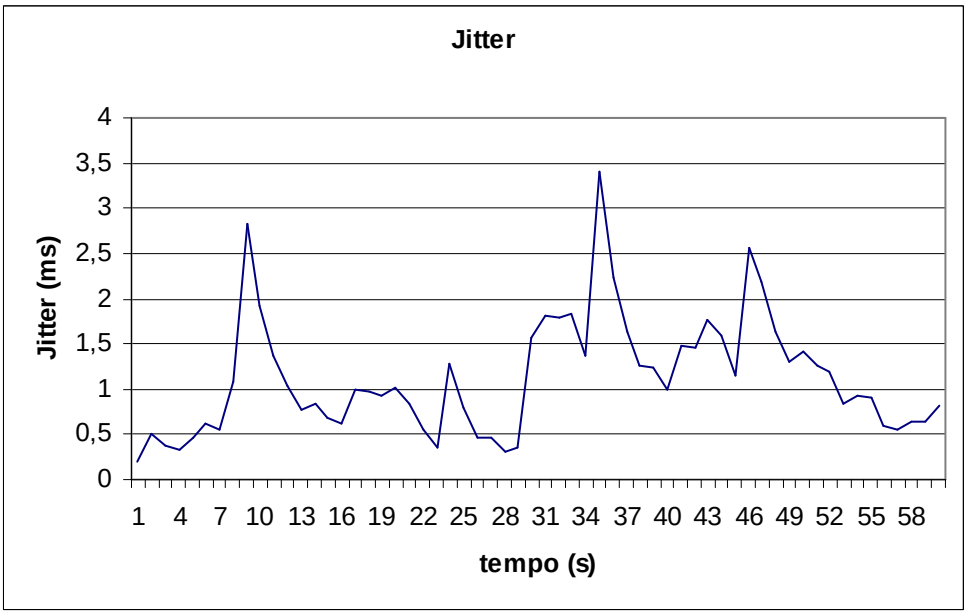

Ilustração 25: Jitter do tráfego UDP com tráfego TCP concorrente e controle de tráfego

Mesmo com o crescimento, após o início da transmissão do tráfego TCP, os valores de *jitter* do tráfego UDP mantiveram-se em um patamar aceitável para uma transação VoIP. Além disto, durante todas as repetições do experimento, não houve perda de pacotes UDP, mesmo na presença de tráfego TCP concorrente. Os resultados demonstram a viabilidade da utilização do *Linux Traffic Control* para o controle de tráfego na rede e priorização do tráfego de voz.

Para finalizar os experimentos, duas chamadas simultâneas foram geradas do nó 6 para o nó 1, com cinco saltos portanto, a fim de avaliar o comportamento do MOS na presença de tráfego concorrente e com a utilização de QoS com o *Linux Traffic Control*. Foi utilizado o codec G.723.a. Na primeira avaliação, as chamadas foram geradas tem nenhum tráfego concorrente e os valores de MOS foram medidos. Na segunda avaliação, um tráfego TCP foi gerado do nó 1 para o nó 6, durante todo o período em que as chamadas foram efetuadas. Na terceira avaliação, novamente foi gerado o tráfego TCP concorrente, porém os mecanismos de QoS foram aplicados na rede. Os resultados são apresentados na Tabela 13.

Características das chamadas	MOS
Sem tráfego TCP Concorrente – Sem QOS	4,3
Com Tráfego TCP Concorrente – Sem QOS	1,0
Com Tráfego TCP Concorrente – Com Qos	4,3

Tabela 13: Valores de MOS de 2 chamadas para avaliação de QoS com Linux Traffic Control

Observa-se que a utilização do *Linux Traffic Control* permitiu a realização das duas chamadas com boa qualidade, mesmo com a presença do tráfego concorrente TCP. O valor de MOS obtido com o QoS aplicado na rede, neste caso foi semelhante ao valor encontrado com as chamadas efetuadas sem tráfego concorrente.

6 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresenta uma avaliação da capacidade de tráfego e da capacidade de chamadas de voz em redes em malha. São apresentados alguns fatores responsáveis pela degradação da qualidade das aplicações de voz neste tipo de rede e são descritas algumas técnicas utilizadas para a obtenção de melhorias na qualidade e aumento na capacidade de chamadas. Através de uma série de experimentos realizados por meio de simulações e medições em uma rede em malha real, a capacidade de uma rede com topologia linear é avaliada. Os experimentos são utilizados para averiguar a degradação sofrida por chamadas de voz na rede e como a aplicação de mecanismos de QoS pode reduzir esta degradação. As simulações foram realizadas com a utilização da ferramenta *Network Simulator* e as medições efetuadas em uma rede em malha implantada na Universidade Federal Fluminense na cidade de Niterói, no Rio de Janeiro.

Uma das conclusões que podem ser obtidas neste trabalho é que a qualidade de chamadas de voz, bem como a capacidade de uma rede em malha em suportar este tipo de aplicação depende não somente do controle de parâmetros da rede. Diversas variáveis externas devem ser consideradas e algumas delas são de difícil controle, tais como interferências geradas por outras redes 802.11, por outras tecnologias sem fio ou até mesmo dispositivos eletroeletrônicos como o forno microondas.

Uma contribuição deste trabalho é a apresentação de diversos fatores que comprometem o desempenho de redes em malha sem fio, particularmente as aplicações de voz. Este estudo é significativo, pois apresenta informações úteis no processo de planejamento e implementação de redes em malha e no dimensionamento das aplicações de voz. O desempenho de uma rede em malha e o comportamento dos parâmetros vazão, atraso, *jitter* e perda depende de como estes fatores são tratados. Alguns destes, por sua vez, dependem das características da aplicação utilizada (ex.: tamanho de pacote e taxa de dados

transmitidos), outros dependem das condições em que se encontra a rede (ex.: número de nós disputando o meio, número de saltos até o destino, taxa de transmissão dos nós e obstruções), e alguns dependem de fatores externos (ex.: interferência de outras redes ou dispositivos eletro-eletrônicos). O atraso na camada de aplicação pode ser reduzido aumentando-se a taxa de transmissão de pacotes, reduzindo-se assim o atraso de empacotamento. Por outro lado, o aumento da taxa de transmissão de pacotes aumenta a carga na rede devido ao acréscimo de bytes de cabeçalho. Taxas mais altas geram mais colisões, aumentando a probabilidade de perda de pacotes e a janela de contenção da camada MAC, o que ocasiona um maior atraso na camada MAC. Observa-se então que todos estes parâmetros não podem ser analisados separadamente, pois estão inter-relacionados. Modelar o comportamento deles e assim, estimar a capacidade real de uma rede em malha, bem como a capacidade de chamadas de voz é, portanto, uma tarefa extremamente desafiadora.

Em futuros trabalhos, os diversos mecanismos de enfileiramento podem ser avaliados para a determinação dos que melhor se aplicam a cada tipo de aplicação nas redes em malha. Tais mecanismos têm ação direta sobre as métricas do tráfego cursado, como atraso, perda e *jitter*. Mesmo com a influência dos fatores externos é importante o tratamento adequado do tráfego que cursa na rede através da utilização de mecanismos de QoS. Outros experimentos também podem ser conduzidos para a avaliação dos mecanismos de compressão de cabeçalho e *dejjiter buffer* adaptativo, bem como o comportamento de outros tipos de *vocoder* (codec).

REFERÊNCIAS

[1] IEEE 801.11, Part 11: **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification**, IEEE, ago, 1999.

[2] IEEE 802.11b, Part 11: **Wireless LAN Medium Access Control(MAC) and Physical (PHY) Layer Specification**: High Speed Physical Layer Extensions in the 2.4 GHz Band, supplement to IEEE 802.11 Standard, set, 1999.

[3] IEEE 802.11g, Part 11: **Wireless LAN Medium Access Control(MAC) and Physical (PHY) Layer Specification**: Further Higher Data Rate Extension in the 2.4GHz Band. jun, 2003.

[4] LI, J.; BLAKE, C.; COUTO, D. S. J. De; LEE, H. I.; MORRIS, R.. **Capacity of ad hoc wireless networks**. ACM MobiCom, Rome, Italy, p. 61–69, jul, 2001.

[5] JUN, Jangeun; PEDDABACHAGARI, Pushkin; SICHITIU, Mihail. **Theoretical Maximum Throughput of IEEE 802.11 and its Applications**. Second IEEE International Symposium on Network Computing and Applications. Cambridge, Massachusette, USA: IEEE, p. 249.256, abr, 2003.

[6] MEDEPALLI, Kamesh; GOPALAKRISHNAN, Praveen; FAMOLARI, David; KODAMA, Toshikazu. **Voice Capacity of IEEE 802.11b, 802.11a and 802.11g Wireless LANs**. IEEE Global Telecommunications Conference (Globecom), Dallas, Texas, United States, nov, 2004.

[7] GARG, S; KAPPES, M.. **Can I add a VoIP call?.** IEEE Int. Conf. on Communications, (ICC ´3), p. 779-783, vol.2, Anchorage, Alaska, 2003.

[8] HOLE, David P.; TOBAGI, Fouad A.. **Capacity of an IEEE 802.11b Wireless LAN supporting VoIP**. IEEE Int. Conference on Communications (ICC), 2004.

[9] GUPTA, Piyush; KUMAR, P. R.. **The Capacity of Wireless Networks**. IEEE Transactions on Information Theory, mar, 2000.

[10] JUN, Jangeun; SICHITIU, Mihail L.. **The Nominal Capacity of Wireless Mesh Networks**. IEEE Wireless Communications, out, 2003.

[11] LEE, Bin Hong; CAI, Guan Yan; GE, Yu; SEAH, Winston K. G.. **VoIP capacity over Wireless Mesh Networks**. 31st Annual IEEE Conference on Local Computer Networks (LCN2006), p. 14-17, nov, 2006.

[12] **NS-2 Network simulator** (v2.31). Disponível em: <http://www.isi.edu/nsnam/ns/> Acesso em: 10 mar. 2008

[13] ITU-T Recommendation G.1010, **End-User Multimedia QoS Categories**, Geneva, nov, 2001.

[14] BERGER, A.; ROMASCANU, D.. **SIP**: Session Initiation Protocol. RFC 3621. IETF, 2002.

[15] ITU-T Recommendation H.323. **Packet-based multimedia communications systems**. Geneva, jun, 2006.

[16] SCHULZRINNE, H.; CASNER. S.; FREDERICK, R.; JACOBSON, V.. **RTP**: A Transport Protocol for real-Time Applications. RFC 3550, jul, 2003.

[17] ITU-T Recommendation G.114. **One-way transmission time**. Geneva, mai, 2003.

[18] HADZI-VELKOV, Zoran; SPASENOVSKI, Boris. **Saturation Throughput-delay analysis of IEEE 802.11 DCF in fading Channel**. IEEE ICC 2003, p.121–126, mai, 2003.

[19] TIA, **Telecommunications IP Telephony Equipment Voice Quality Recommendations for IP Telephony PN-4689**, TIA/EIA/TSB-116, TIA Engineering Committee, TR-41.1, 2001.

[20] ITU-T SG12. STUDY GROUP 12 – DELAYED CONTRIBUTION 98. **Analysis, measurement and modelling of Jitter**. Geneva, jan, 2003.

[21] GAST, Mattheu S.. **802.11 Wireless networks**: the definitie guide. O'Reilly, abr, 2002.

[22] BIANCHI, G; STEFANO, A. Di; GIACONIA, C.; SCALIA, L.; TERRAZZINO, G.; TINNIRELLO, I.. **Experimental assessment of the backoff behavior of commercial IEEE 802.11b network cards**. INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, mai, 2007.

[23] GOPINATH, K. N.; BHAGWAT, Pravin; GOPINATH, K.. **An Empirical Analysis of Heterogeneity in IEEE 802.11 MAC protocol implementations and its implications**. ACM MobiCom, set, 2006.

[24] Zhai, H.; FANG, Y.. **Performance of wireless LANs based on IEEE 802.11 MAC protocols**. IEEE Personal Indoor and Mobile Radio Communications (PIMRC), Beijing, p. 2586–2590, China, 2003.

[25] ZHAI, H.; Kwon, Y.; FANG, Y.. **Performance analysis of IEEE 802.11 MAC protocols in wireless LANs**. WileyWireless Commun. Mobile Comput., Special Issue on Emerging LAN Technologies and Applications, vol. 4, no. 8, p. 917–931, dez, 2004.

[26] RAHMAN, Ashikur; GBURZYNSKI, Pawel. **Hidden Problems with the Hidden Node Problem**. 23rd Biennial Symposium on Communications, p. 270- 273, jun, 2006.

[27] CHUNG, Ping; LIEW, Soung Chang; SHA, Ka Chi; TO, Wai Ting. **Experimental Study of Hidden-node Problem in IEEE802.11 Wireless Networks.** SIGCOMM, ago, 2005

[28] Internet Engineering Task Force (IETF). Disponível em <www.ietf.org> Acesso em 10 mar, 2008.

[29] BRADEN, R.; CLARK D.; SHENKER. S.. **Integrated Services in the Internet Architecture**: an Overview. RFC1633, IETF, jun, 1994.

[30] BLAKE, S., BLACK, D., CARLSON M., DAVIES, E., WANG Z., WEISS, W., **An Architecture for Differentiated Service**. RFC2475, dez. 1998.

[31] JACOBSON, V.; NICHOLS, K.; PODURI, K. **An Expedited Forwarding PHB**. RFC 2598. IETF, 1999.

[32] HEINANEN, J.; BAKER, F.; WEISS, W.; WROCLAWSKI, J.. **Assured Forwarding PHB Group**. RFC 2597. IETF, 1999.

[33] **INTERNET Protocol**. RFC 791. IETF, 1981.

[34] NICHOLS, K.; BLAKE, S.; BAKER, F.; BLACK, D.. **Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers**. RFC 2474. IETF, 1998.

[35] VERES, Andras; CAMPBELL, Andrew; BARRY, Michael. **Supporting Service Differentiation in Wireless Packet Networks Using Distributed Control**. IEEE Journal on Selected Areas in Communications, vol. 19, no 10, out, 2001.

[36] CHEN, Xiuzhong; WANG, Chunfeng; LI, Zhongchecg; MIN, Winghua; ZHAO, Wei. **Survey on QoS Managment of VoIP**. International Conference on Computer Networks and Mobile Computing (ICCNMC ‘03), 2003.

[37] AHN, Gahng-Seop; CAMPBELL, Andrew, VERES, Andras; SUN, Li-Hsiang. **SWAN**: Service Differentiation in Stateless Wireless Ad Hoc Networks. IEEE INFOCOM 2002, vol.2, p.457–466, jun, 2002.

[38] PERKINS, C.E; BELDING-ROYER, E.M.. **Quality of service for ad hoc on demand distance vestor**, Internet Draft, draft-perkins-manet-aodvqos-02.txt, 14 out, 2003

[39] XYLOMENOS, G.; POLYZOS, G.C.. **Link Layer Support for Quality of Service on Wireless Internet Links**. IEEE Personal Communications 6, p. 52–60, 1999.

[40] ZHAI, Hongqiang; CHEN, Xiang; FANG, Yuguang. **How well can the ieee 802.11 wireless LAN Support Quality of Service?**. IEEE Transactions on Wireless Communications, 2005.

[41] **OpenWRT**, Disponível em: <http://openwrt.org> Acesso em: 10 mar 2008.

[42] ALMESBERGER, Werner. **Linux Traffic Control**: Implementation Overview. nov, 1998.

[43] CASNER. S.; JACOBSON, V.. **Compressing IP/UDP/RTP Headers for Low-Speed Serial Links**. IETF, RFC 2508, 1999.

[44] **Network Animator - NAM**, Disponível em: <http://www.isi.edu/nsnam/nam/ > Acesso em: 10 mar 2008

[45] PASSOS, Diego; TEIXEIRA, Douglas Vidal; MUCHALUAT-SAADE, Débora C; MAGALHÃES, Luiz C. Schara; ALBUQUERQUE, Célio V. N.. **Mesh Network Performance Measurements**. 5th International Information and Telecommunicatios Technologies Symposium (I2TS 2006), p. 48-55, Cuiabá, MT, Brasil, dez, 2006.

[46] **Iperf**. Disponível em: < http://dast.nlanr.net/Projects/Iperf/> Acesso em: 10 mar 2008

[47] **Grupo de Redes de Computadores e Multimídia** (GRCM). Disponível em: <http://grcm.dcc.ufam.edu.br> Acesso em: 10 mar 2008

[48] LUSTOSA, L. C. G.; CARVALHO, L. S. G.; RODRIGUES, P. H. A. & MOTA, E. S. **Utilizacão do Modelo E para avaliação da qualidade da fala em sistemas de comunicação baseados em voz sobre IP**, in: Anais do XXII Simpósio Brasileiro de Redes de Computadores. Gramado, p.603-616, mai, 2004.

[49] ITU-T Recommendation P.59. **Artificial Conversational Speech**. Geneva, mar, 1993.

[50] ITU-T Recommendation P.800. **Methods for subjective determination of transmission quality**. Geneva, ago, 1996.

[51] ITU–T Recommendation P.830. **Subjective performance assessment of telephoneband and wideband digital codecs**. Geneva, fev, 1996.

[52] ITU-T Recommendation G.107, **The E-Model, a computational model for use in transmission planning**. Geneva, mar, 2003.

APÊNDICE

APÊNDICE A: Interferência gerada por outra rede 802.11

As ilustrações a seguir mostram os resultados obtidos em um experimento consistindo na utilização de duas redes, cada uma com dois nós, localizadas próximas uma da outra, utilizando canais adjacentes. Enquanto uma rede permanecia fixa no canal 11, a outra tinha seu canal gradativamente alterado do canal 11 ao canal 6. Inicialmente somente a primeira rede transmitia um fluxo udp em sua vazão máxima e aos 30 segundos a segunda também passava a transmitir. Aos 60 segundos o tráfego da primeira rede era interrompido e somente a segunda rede permanecia transmitindo. Com pode ser observado, A interferência ocorre nos canais adjacentes até o canal 7, reduzindo a vazão máxima das redes enquanto transmitem simultaneamente.

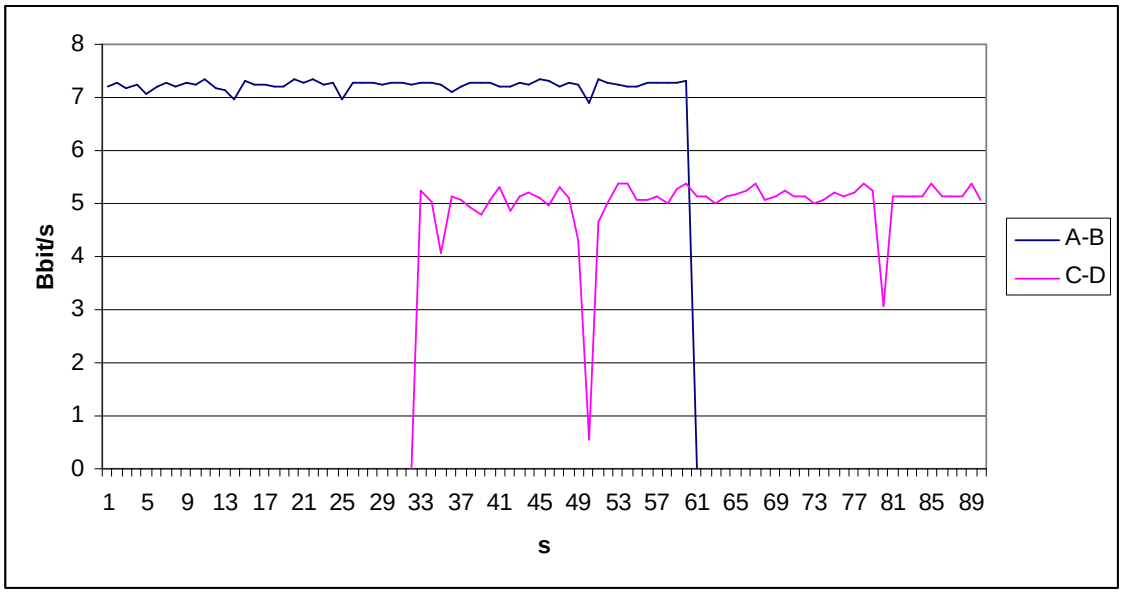

Ilustração 26: Transmissão de duas redes nos canais 11 e 6

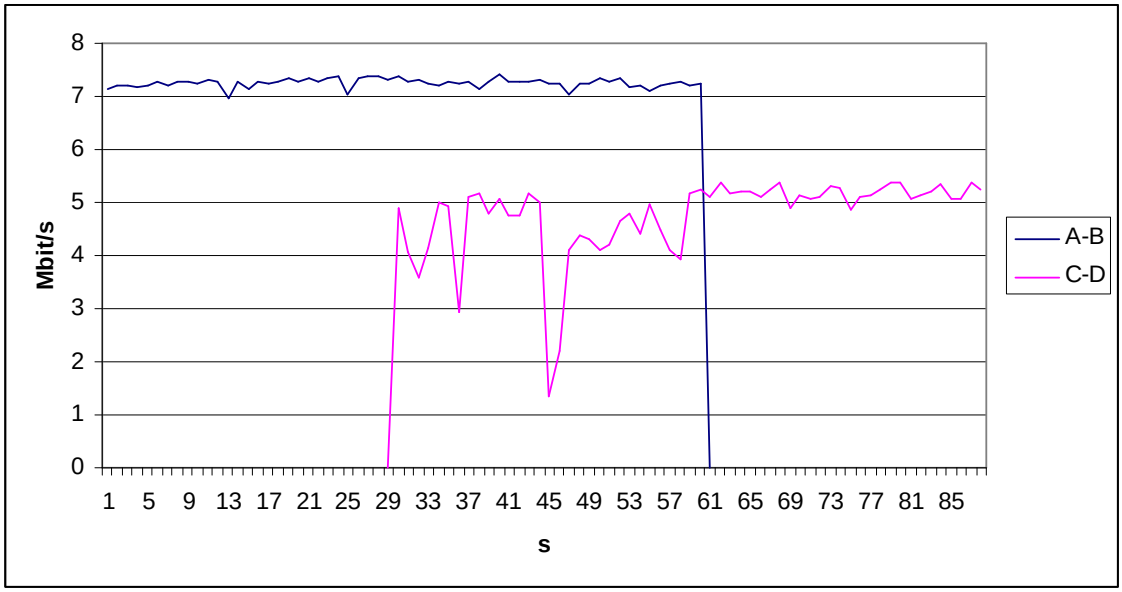

Ilustração 27: Transmissão de duas redes nos canais 11 e 7

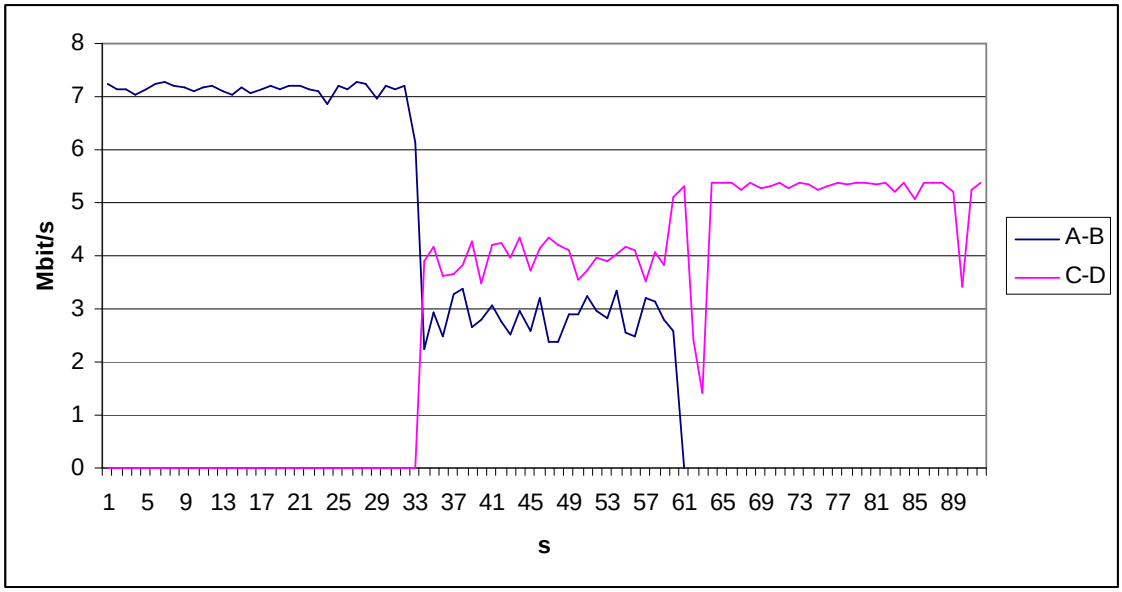

Ilustração 28: Transmissão de duas redes nos canais 11 e 8

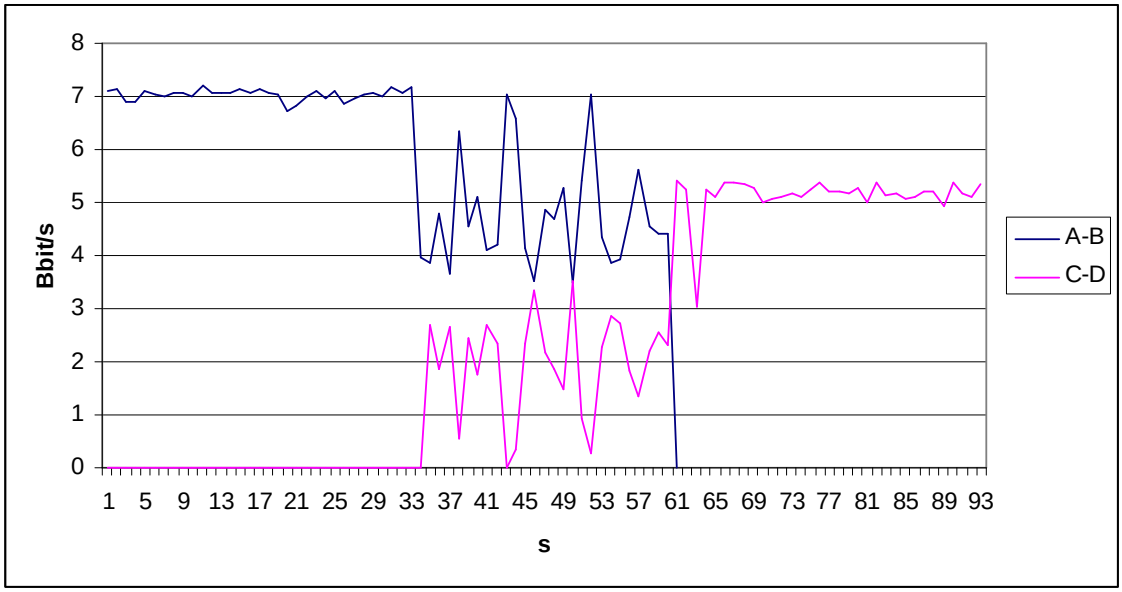

Ilustração 29: Transmissão de duas redes nos canais 11 e 9

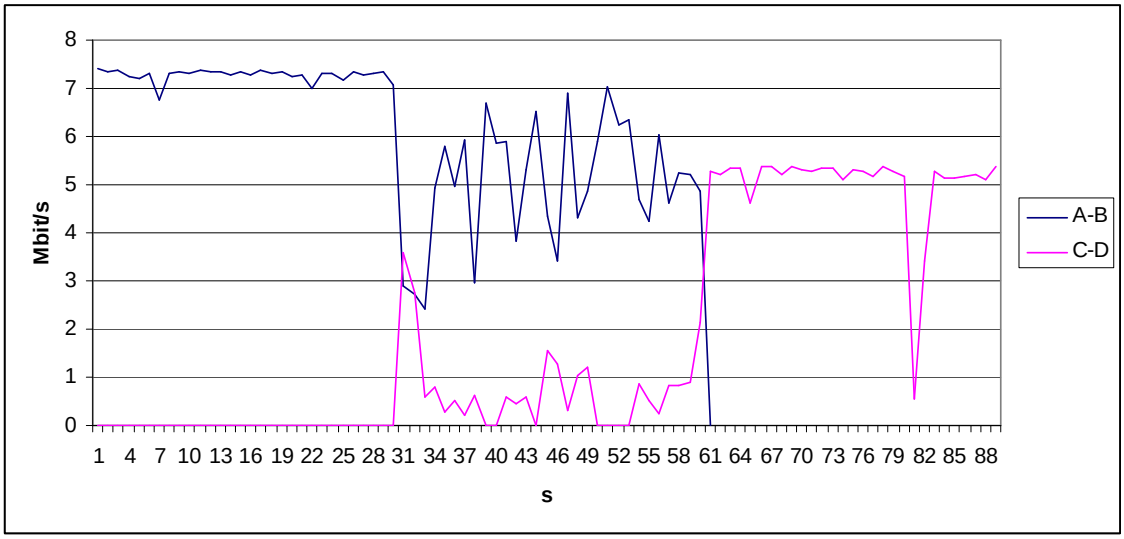

Ilustração 30: Transmissão de duas redes nos canais 11 e 10

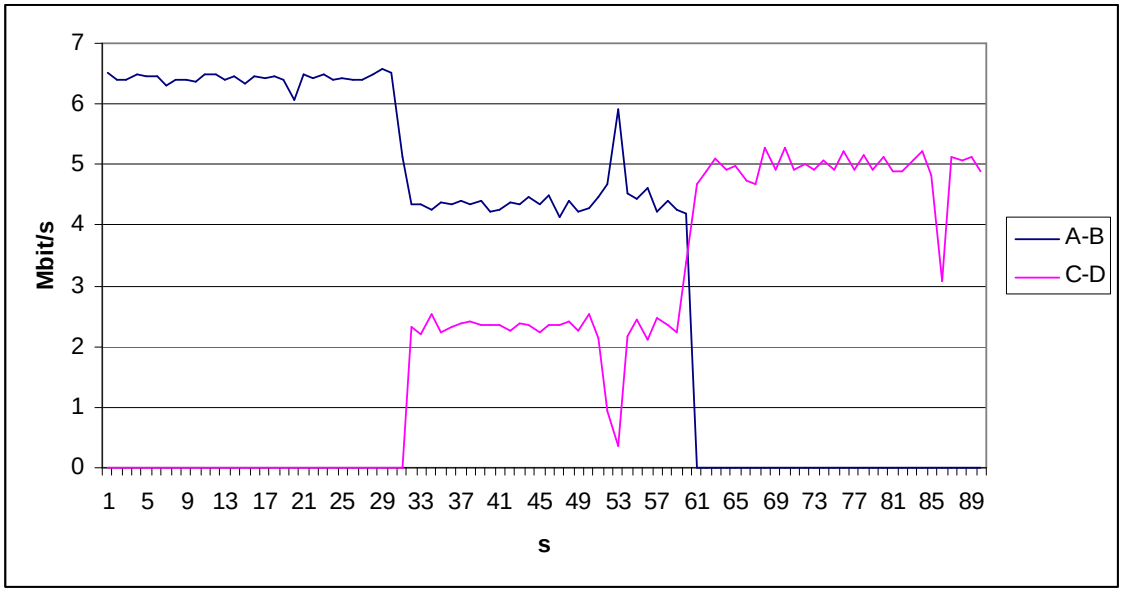

Ilustração 31: Transmissão de duas redes no canal 11

As ilustrações a seguir mostram o espectro eletromagnético enquanto as duas redes realizavam a transmissão de dados simultaneamente. Pode ser observada a sobreposição que ocorre nas componentes de freqüência dos dois sinais, o que gera a diminuição na relação sinal ruído e conseqüentemente a degradação na transmissão dos dados.

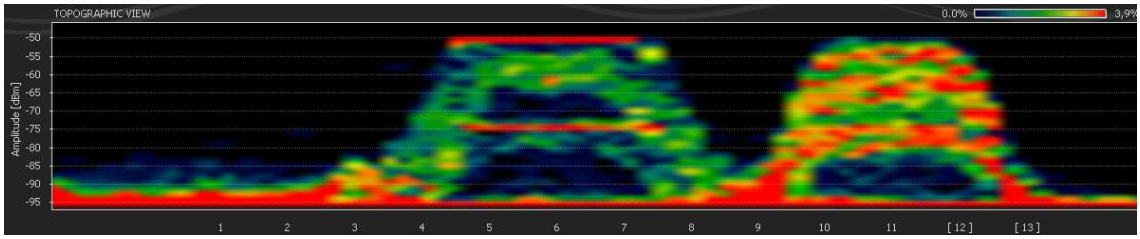

Ilustração 32: Espectro eletromagnético de duas redes utilizando os canais 11 e 6

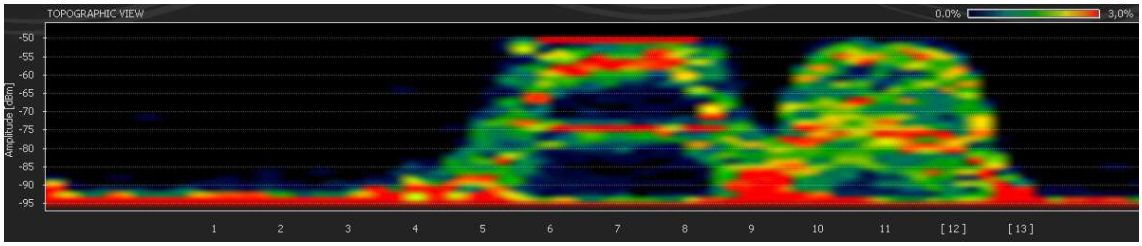

Ilustração 33: Espectro eletromagnético de duas redes utilizando os canais 11 e 7

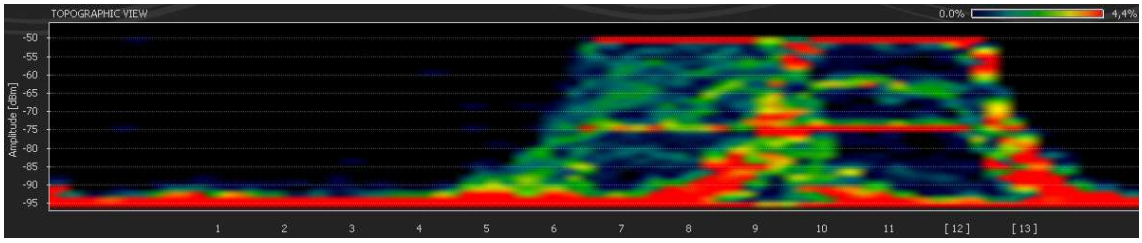

Ilustração 34: Espectro eletromagnético de duas redes utilizando os canais 11 e 8

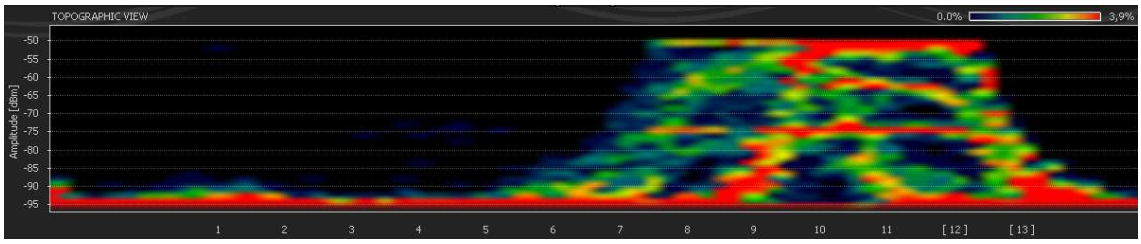

Ilustração 35: Espectro eletromagnético de duas redes utilizando os canais 11 e 9

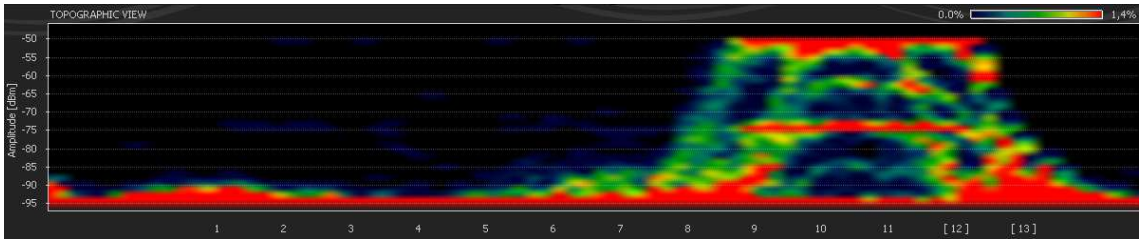

Ilustração 36: Espectro eletromagnético de duas redes utilizando o canal 11