IEEE 802.11

Danielle Lopes Ferreira Gonçalves Vieira *UFRJ*

***Abstract*— O presente trabalho descreve detalhadamente o principal padrão das redes locais sem fio (WLAN), o padrão IEEE 802.11. Suas principais variações, a família IEEE 802.11x, também são estudadas, comparadas e avaliadas, quando for o caso. O padrão 802.11 baseia-se na utilização de um protocolo de acesso aleatório, o CSMA/CA, e conta também com o método de acesso baseado em interrogação. Não suportando diferenciação de serviços e qualidade de serviço, assim, será estudado um protocolo capaz de prover qualidade e diferenciação de serviços. Apesar de amplamente utilizado, o padrão para redes sem fio, IEEE 802.11, oferece diversas vulnerabilidades que colocam em risco a confidencialidade, integridade, autenticidade e disponibilidade da comunicação, este trabalho apresenta a implementação e a segurança no padrão IEEE 802.11. Apresentam-se ainda dois novos padrões de segurança que irão substituir o atual modelo (WEP), o 802.11I e 802.1X.**

***Index Terms*— IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11e, IEEE 802.11i, IEEE 802.11n, QoS, OFDM, segurança.**

I. Introdução

AS redes sem-fio estão sendo cada vez mais utilizadas na comunicação entre dispositivos dos mais variados tipos e tamanhos (computadores pessoais, portáteis e de mão, telefones, eletrodomésticos, máquinas industriais, sensores e outros) em diferentes ambientes, como residências, edifícios, cidades, florestas e campos de batalha. Por permitirem a mobilidade, estas redes facilitam a ubiqüidade do poder computacional, tornando transparente a disseminação da informação e a cooperação dos dispositivos na realização das mais variadas tarefas. Diferentes padrões e tecnologias de rede sem-fio surgiram nos últimos anos para acomodar esta vasta gama de aplicações e coberturas. Neste cenário, dentre as tecnologias atuais que vêm contribuindo para o futuro das comunicações ubíquas, destaca-se o padrão 802.11, que devido a sua popularidade, altas taxas e baixo custo tem conseguido uma grande penetração no mercado. Pela sua diversidade em termos de capacidade e cobertura e devido ao baixo custo dos dispositivos de rede, o padrão 802.11 tem sido usado nos mais variados cenários, desde redes de acesso para redes celulares 2G/3G, como solução para redes residenciais e de campus (redes locais e metropolitanas), ou mesmo, em enlaces ponto-a-ponto de média distância em soluções corporativas. Esta vasta aplicabilidade do padrão 802.11 tem sido a chave do seu sucesso comercial.

Os primeiros produtos para redes locais sem fios, utilizando tecnologia proprietária, foram introduzidos no início da década de 90, aproveitando a disponibilidade das bandas ISM para operação sem necessidade de licença. Estes produtos operavam na banda ISM de 900 MHz, disponível na América do Norte. Algum tempo depois, surgiram produtos operando na banda ISM de 2.4 GHz e, mais para o final da década, começaram a aparecer produtos que utilizam a banda de frequências de 5 GHz. O principal problema das soluções proprietárias de redes sem fios foi a moderada aceitação no mercado, por falta de um padrão que garantisse a compatibilidade entre os produtos disponibilizados pelos diversos fabricantes. Para resolver este problema, após vários anos de discussão, o IEEE *(Institute of Electrical and Electronics Engineers)* aprovou a primeira versão das normas IEEE 802.11, publicada em 1997.

O IEEE desenvolveu uma série de padrões para redes de transmissão de dados sem fio. O padrão IEEE 802.11 foi o primeiro a ser desenvolvido e permite taxas de transmissão brutas de 1 até 2Mbit/s nas bandas ISM. O padrão evoluiu da seguinte forma, não necessariamente nesta ordem:

- IEEE 802.11a: permite atingir taxas de transmissão de até 54 Mbit/s na banda de 5 GHz, utilizando a técnica OFDM (*Orthogonal Frequency Division Multiplexing*), a distância máxima entre duas estações é de 20 metros.
- IEEE 802.11b: utiliza a faixa de freqüência de 2.4 Ghz, e a técnica DSSS (*Direct-Sequence Spread Spectrum*) para espalhamento de espectro. Possui uma taxa de transmissão de até 11 Mbps, e a distância máxima entre duas estações é de 100 metros.
- IEEE 802.11g: utiliza a faixa de freqüência de 2.4 Ghz, e a técnica DSSS (*Direct-Sequence Spread Spectrum*) para espalhamento de espectro. Possui uma taxa de transmissão de até 54 Mbps, e a distância máxima entre duas estações é de 100 metros. Utiliza a faixa de frequência de 2.4 GHz, e a técnica DSSS permite taxas de transmissões brutas de até 11 Mbit/s nas bandas ISM.
- IEEE 802.11e Provê QoS através de melhorias na camada MAC
- IEEE 802.11i Inclui mecanismos de segurança e autenticação na camada MAC.
- IEEE 802.11n Aumentar a vazão obtida na camada MAC.

Este trabalho está organizado da seguinte forma: Na seção II, o padrão 802.11 será apresentado detalhadamente. As próximas seções estudarão as variações do 802.11 e apresentarão comparações e desempenhos dos diversos padrões, quando for o caso.

II. O Padrão IEEE 802.11

O IEEE, em 1999, definiu uma norma para redes locais sem-fio chamada *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [1]. O padrão IEEE 802.11, como todos os protocolos da família 802.x, especifica as camadas física e de controle de acesso ao meio (MAC). Esse padrão continua em desenvolvimento através de vários grupos de trabalho que têm como objetivo prover melhorias no desempenho e novas aplicações.

A. A Arquitetura do 802.11

A arquitetura do IEEE 802.11 consiste em vários componentes que interagem para prover uma rede local sem-fio com suporte à mobilidade de estações de modo transparente para as camadas superiores.

O conjunto básico de serviços *(Basic Service Set - BSS)* é o bloco fundamental de construção da arquitetura do 802.11 [1]. Um BSS é definido como um grupo de estações que estão sob o controle direto de uma única função de coordenação, que determina quando uma estação pode transmitir e receber dados.

No 802.11 existem dois tipos de redes sem fio: *Ad Hoc* ou infra-estruturada. Uma rede *Ad Hoc* é composta somente por estações dentro de um mesmo BSS que se comunicam entre si sem a ajuda de uma infra-estrutura. Qualquer estação pode estabelecer uma comunicação direta com outra estação no BSS sem a necessidade que a informação passe por um ponto de acesso centralizado [4]. O padrão 802.11 refere-se a uma rede *Ad Hoc* como um BSS independente. Já em uma rede infra-estruturada, é utilizado um ponto de acesso que é responsável por quase toda a funcionalidade de rede. De modo a aumentar a cobertura de uma rede infra-estruturada, vários pontos de acesso podem ser interligados através de um *backbone* chamado sistema de distribuição *(distribution system - DS)*. O conjunto dos pontos de acesso e dos sistemas de distribuição é definido com um conjunto estendido de serviços *(Extended Service Set - ESS)*.

A Figura 1 representa os componentes da arquitetura da rede IEEE 802.11 na configuração baseada em infra-estrutura. Este modo de operação requer a presença de uma estação especial no BSS, denominada ponto de acesso *(AP, Access Point)*, que serve de interface entre o BSS e o sistema de distribuição (DS) e possibilita a comunicação entre as estações (STA) do BSS e entidades externas. O sistema de distribuição (DS) permite interligar múltiplos BSSs formando um conjunto estendido de serviço, que aparenta ser um único BSS alargado para a subcamada de ligação lógica (LLC) das estações que compõem o ESS. Normalmente, utiliza-se uma rede local convencional como sistema de distribuição, embora outras redes possam ser utilizadas, visto que as normas não entram em detalhes quanto à implementação do sistema de distribuição.

B. A Camada Física do 802.11

O padrão 802.11 [1] define três tipos de camada física: espalhamento de espectro por salto em freqüências (*Frequency Hopping Spread Spectrum* - FHSS), espalhamento de espectro por seqüência direta (*Direct Sequence Spread Spectrum* - DSSS) e infravermelho. Todas as camadas físicas do 802.11 incluem a provisão de um sinal de avaliação de canal livre (*Clear Channel Assessment signal* - CCA) que é utilizado pela camada MAC para indicar se o meio está livre. Além disso, cada camada física oferece uma taxa de 1 ou 2 Mbps.

O FHSS é uma técnica de espalhamento de espectro que divide a banda passante total em vários canais de pequena banda e faz com que o transmissor e o receptor fiquem em um desses canais por um certo tempo e depois saltem para outro canal. Com isso, permite-se a coexistência de várias redes

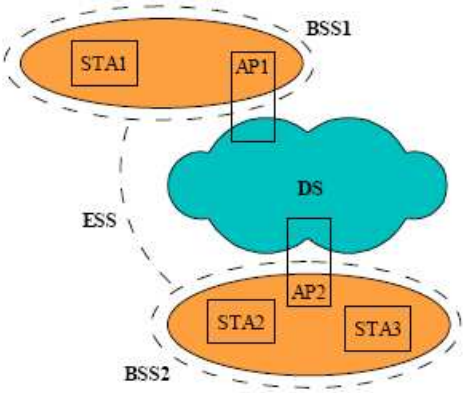

Fig. 1. Componentes da arquitetura da rede IEEE 802.11. Fonte [13]

em uma mesma área através da separação dessas redes por diferentes padrões pseudo-aleatórios de uso do canal chamados seqüências de saltos. O FHSS usa a banda ISM (*Industrial, Scientific and Medical*) de 2,4000 a 2,4835 GHz. Nos EUA e em quase toda a Europa, são definidos 79 canais. O primeiro canal tem uma freqüência central de 2,402 GHz e os canais subseqüentes estão separados por 1 MHz. Cada canal possui uma banda de 1 Mbps. Três diferentes conjuntos com 26 seqüências de saltos são definidos. As diferentes seqüências de saltos permitem que vários BSSs coexistam em uma mesma área geográfica e os três conjuntos de saltos existem para evitar períodos de colisões entre diferentes seqüências de saltos em um conjunto. O acesso básico de 1 Mbps usa uma modulação gaussiana por chaveamento de freqüência *Gaussian Frequency Shift Keying* (GFSK) de dois níveis, na qual o dado passa por um filtro gaussiano em banda base e é modulado em freqüência (um 1 lógico é codificado usando uma freqüência $Fc + f$ e um 0 lógico usa uma freqüência $Fc - f$). A taxa de acesso opcional de 2 Mbps usa um GFSK de quatro níveis, no qual dois bits são codificados por vez usando quatro freqüências.

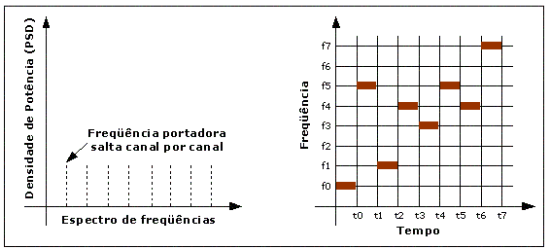

Fig. 2. Espalhamento de Espectro por Salto em Freqüências. Fonte [14]

O DSSS é um método alternativo de espalhamento de espectro, no qual códigos são separados. O DSSS também usa a banda ISM de 2,4 GHz. A taxa básica de 1 Mbps é gerada através de uma modulação diferencial binária por chaveamento de fase (*Differential Binary Phase Shift Keying* - DBPSK) e a taxa de 2 Mbps usa uma modulação diferencial quaternária por chaveamento de fase (*Differential Quadrature Phase Shift Keying* - DQPSK). O espalhamento é feito através da divisão da banda disponível em 11 subcanais, cada um com 11 MHz, e do

espalhamento de cada símbolo de dados usando uma seqüência de Barker de 11 chips dada por (+1,1,+1,+1,1,+1,+1,+1,1,1,1). A largura de um canal DSSS é de 20 MHz, ou seja, no máximo três canais não sobrepostos podem ser usados.

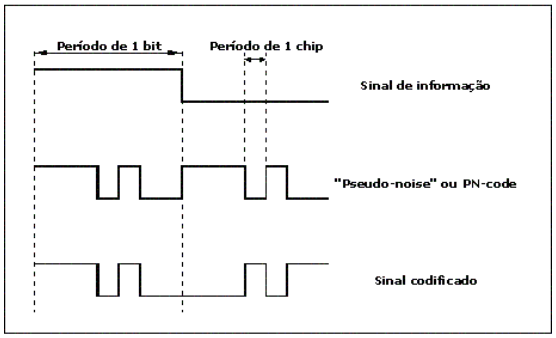

Fig. 3. Espalhamento de Espectro por Seqüência Direta. Fonte [14]

A especificação de infravermelho utiliza comprimentos de onda de 850 a 950 nm. O infravermelho foi projetado para ser usado em áreas fechadas e opera com transmissões não direcionadas com alcance máximo de aproximadamente 10 m caso não existam fontes de calor ou luz do sol interferindo ou 20 m caso sejam utilizados receptores mais sensíveis. As estações podem receber dados em suas linhas de visada e por transmissões refletidas. A codificação da taxa básica de 1 Mbps é realizada através de uma modulação por posição de pulso (16-*Pulse Position Modulation* - PPM), na qual quatro bits de dados são mapeados em 16 bits codificados para transmissão [1]. A taxa opcional de 2 Mbps usa uma 4-PPM, na qual dois bits de dados são mapeados em 4 bits codificados para transmissão.

C. Gestão de consumo de energia

O IEEE 802.11 proporciona suporte para gestão de consumo de energia das estações. O ponto de acesso armazena os dados destinados às estações que estão operando em modo de conservação de energia e difunde informação nos quadros *Beacon*, identificando estas estações. Para esse efeito, os quadros *Beacon* contêm um mapa de indicação de tráfego (TIM, *Traffic Indication Map*). As estações que operam no modo de conservação de energia acordam periodicamente para escutar o quadro de *Beacon*. Quando uma estação recebe indicação de que o ponto de acesso tem quadros armazenados para si, ela interroga o ponto de acesso, requisitando o envio dos quadros armazenados.

D. A camada MAC do 802.11

A camada MAC do 802.11 define dois tipos de funções de acesso ao meio: a função de coordenação distribuída (*Distributed Coordination Function* - DCF) e a função de coordenação em um ponto (*Point Coordination Function* - PCF). O DCF é o mecanismo básico de controle de acesso ao meio do IEEE 802.11, sendo um protocolo de acesso aleatório do tipo CSMA/CA *(Carrier Sense Multiple Access/Collision Avoidance)*. O PCF, por outro lado, é um protocolo de *polling* que permite às estações o acesso ao meio livre de contenção, o que torna sua utilização mais adequada para o transporte de tráfego de tempo real. Entretanto, a sua implementação não é obrigatória, ao contrário do DCF.

Os modos DCF ou PCF são multiplexados no tempo em um superquadro, o qual é formado por um período livre de contenção (CFP), seguido por um período de contenção (CP) posicionado em intervalos regulares (vide figura 4). O ponto de acesso transmite quadros de *beacon* periódicos de forma a gerenciar a entrega das informações nos terminais. Os limites entre CFPs e CPs são marcados por *beacons* transportando um DTMI (*Delivery Traffic Indication Message*). Os terminais podem usar das informações presentes nos *beacons* para se associar com o ponto de acesso, o qual é executado durante o CP. Essa associação é obrigatória se o terminal precisa ter suas transmissões comandadas pelo PCF, que é normalmente requisitada por um dado sensível ao QoS.

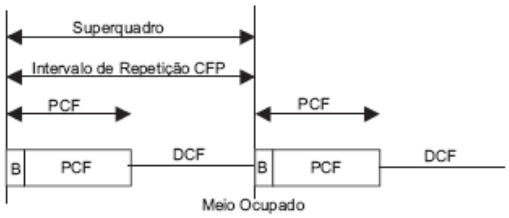

Fig. 4. *Beacons* e períodos livres de contenção. Fonte [15]

As prioridades de pacotes são implementações definindo IFSs (*Interframe Spaces*) de três diferentes tamanhos:

- SIFS *Short Interframe Space* - este é o menor IFS. É usado para transmissões de quadros de alta prioridade: pacotes de ACK (confirmação de recebimento de pacotes) de quadros de dados, quadros CTS, quadros PCF e todo quadro de DCF DATA quadros, exceto o primeiro fragmento de uma rajada.
- PIFS PCF *Interframe Space* - maior que SIFS. Depois de expirado o intervalo, quadros de qualquer modo de PCF podem ser transmitidos. É usado para o controle de *polling* no modo PCF.
- DIFS DCF *Interframe Space* - maior do que PIFS. Depois que o intervalo expirar, qualquer modo de quadros DCF assíncrono podem ser transmitidos de acordo com o mecanismo de *backoff* do CSMA. Utilizado para a transmissão de dados em geral, incluindo o de aplicações multimídia.

Dependendo do tamanho do intervalo entre as transmissões, é possível para os dispositivos, identificar qual é o próximo passo a ser seguido.

Cabe observar que o modo de operação DCF pode ser utilizado tanto no modo infra-estruturado, quanto no modo *Ad Hoc*, enquanto que o modo de operação PCF apenas pode ser utilizado no modo de funcionamento infra-estruturado.

1) A Função de Coordenação Distribuída - DCF: O DCF, mecanismo básico de acesso ao meio no 802.11, é de modo simples, um acesso múltiplo com detecção de portadora evitando colisões (*Carrier Sense Multiple Access with Collision*

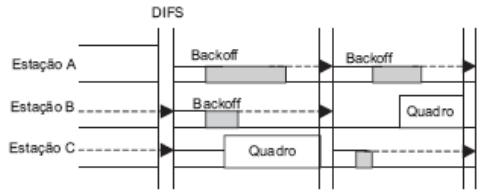

Fig. 5. Mecanismo de *Backoff* no DCF. Fonte [15]

Avoidance - CSMA/CA) com reconhecimento positivo. Embora o método de acesso CSMA/CD (CSMA com detecção de colisão) seja muito utilizado nas redes IEEE 802.3 ele não é adequado às redes 802.11, pois nesse caso a detecção de colisões é muito difícil por assumir que todas as estações ouvem as outras, por requerer um rádio full-duplex de custo elevado e porque a taxa de erro de bit na camada MAC do 802.11 é de 10^{-5}. Existem dois tipos de DCF no padrão: o baseado em CSMA/CA (obrigatório) e outro (opcional) que também utiliza pedidos e permissões para transmitir dados (Request To Send - RTS e Clear To Send - CTS). O funcionamento básico do DCF é apresentado na Figura 6.

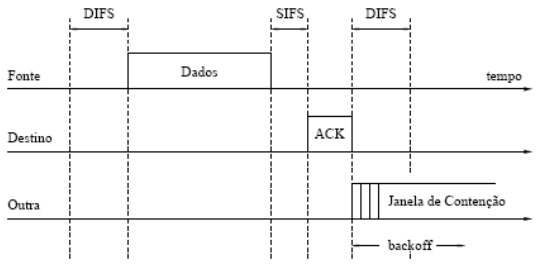

Fig. 6. Esquema básico de acesso no DCF. Fonte [16]

Quando um pacote chega à camada MAC, a estação primeiramente espera que o meio permaneça livre durante um intervalo de tempo igual ao *interframe space* em questão. Em seguida, para pacotes de dados, a estação começa a contar o tempo, com o auxílio de um *backoff counter* (BC), até que ele se iguale ao *backoff time*, que foi escolhido aleatoriamente entre 1 e a janela de contenção (CW) corrente. Ao passar o tempo de *backoff* a estação transmite o pacote, porém, caso o meio volte a ficar ocupado antes disso, a estação pára a contagem de tempo, espera até que o meio permaneça desocupado durante o *interframe space* novamente e então continua a contagem do tempo de *backoff*, decrescido de uma unidade. É justamente o tempo de *backoff* que garante a uniformidade de oportunidades entre os fluxos de mesma prioridade. Além dos já citados parêmetros SIFS, PIFS e DIFS, esse procotolo ainda usa o parâmetro PF para aumentar a janela de contenção em caso de colisões. Ao ocorrer uma colisão, a janela de contenção corrente é multiplicada por PF para que um novo tempo de *backoff* seja escolhido. No padrão 802.11 o valor de PF é 2. A figura 6 mostra a estrutura do acesso ao meio no modo DCF. Devido ao meio de transmissão sem fio estar sujeito a erros e colisões, a técnica de ARQ é implementada na camada MAC. Sempre que um pacote é transmitido, é aguardado um pacote de ACK após um determinado intervalo de tempo, e quando este pacote não chega assume-se que houve colisão, o que ocasiona a retransmissão do pacote, após a alteração do valor da janela de contenção (até que este chegue ao valor máximo definido), e do incremento do contador de colisões consecutivas.

A operação do protocolo no modo DCF pode ser resumida nos seguintes passos:

1) Escuta o meio até que ele permaneça livre durante DIFS, logo após transmite o pacote e vai para (2);
2) Aguarda um ACK que é enviado pelo receptor após SIFS (contando a partir do fim do envio do pacote);
   a) Caso não receba, houve colisão. Dobra o valor da janela de contenção atual (se permanecer abaixo do valor máximo), incrementa o contador de colisões consecutivas e se este não tiver atingido o valor máximo vai para (3), caso contrário vai para (2b);
   b) Caso o contador de colisões consecutivas tenha atingido o valor máximo, descarta o pacote, zera o contador, e caso ainda existam pacotes a serem transmitidos vai para (3);
   c) Recebido o ACK se ainda existirem pacotes a serem transmitidos vai para (3);
3) Escolhe aleatoriamente um valor de *backoff* dentro da janela de contenção atual e continua escutando o meio;
   a) Ao sentir o meio livre durante um intervalo de tempo igual a DIFS, inicia (ou continua) a contagem do tempo de *backoff*;
   b) Se durante este *backoff* o meio é sentido ocupado pausa a contagem, permanece escutando o canal e volta para (3a);
   c) Ao terminar o tempo de *backoff* transmite o pacote e vai para (2).

O segundo tipo de DCF (Figura 7), que é opcional, inclui pacotes RTS e CTS para evitar problemas gerados por terminais ”escondidos”. Esse tipo de problema surge, por exemplo, quando uma estação B é capaz de receber quadros de dois diferentes transmissores, A e C, porém estes transmissores não podem se comunicar entre si. Diz-se que A está escondido para C e vice-versa. Nesse caso, o transmissor A pode achar que o meio está livre mesmo que C esteja transmitindo, o que resulta em colisão no receptor B.

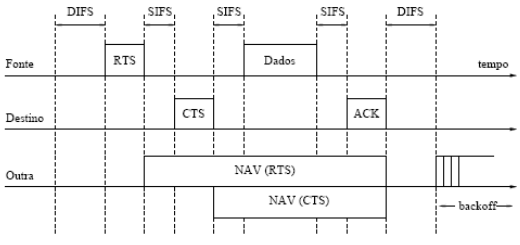

Fig. 7. DCF utilizando RTS e CTS. Fonte [16]

Nesse tipo de DCF, a detecção de portadora pode ser feita através de mecanismos físico (CCA) e virtual. O mecanismo de detecção virtual usa uma distribuição de informação de

reserva do meio através da troca de quadros RTS e CTS antes do envio do dado. Os pacotes RTS e CTS contêm informações a respeito do nó de destino e de um tempo relativo ao envio do pacote de dados e de seu respectivo ACK. O uso de RTS e CTS é controlado por estação através de um limiar de RTS *(RTSthreshold)*, através do qual uma estação pode não usar o RTS e o CTS, pode sempre utilizá-los ou ainda usá-los somente na transmissão de quadros maiores que o tamanho pré-determinado. Uma estação envia um RTS, após sentir o meio livre por pelo menos DIFS segundos, ao receptor antes da transmissão de um quadro para reservar o meio (Figura 5). A colisão de um quadro RTS de 20 bytes é menos severa e menos provável que uma colisão de quadros de dados que podem ter até 2346 bytes. O receptor responde com um CTS, após o meio estar livre por SIFS segundos, caso esteja pronto para receber. Todas as estações que ouvirem o RTS, o CTS, ou ambos, irão utilizar a informação da duração relativa ao pacote de dados para atualizar o vetor de alocação de rede (*Network Allocation Vector* - NAV), que é utilizado para uma detecção virtual da portadora (Figura 5). Essa informação indica o período de tempo pelo qual uma transmissão não é iniciada pela estação, não importando se o CCA indique que o meio está livre. Desse modo, qualquer terminal escondido poderá adiar a sua transmissão para evitar colisões. Ao receber o CTS e esperar o meio estar livre por SIFS segundos (Figura 5), o transmissor inicia o envio do quadro, como no DCF básico. Caso não receba o CTS, o transmissor entra na fase de *backoff* e retransmite o RTS.

2) Função de Coordenação em um ponto - PCF: Outro tipo de acesso da camada MAC do 802.11 é o PCF. Apesar da implementação do DCF ser obrigatória pelo padrão, esse não é o caso do PCF. No modo PCF um único ponto controla o acesso ao meio, através de consulta a cada estação, proporcionando a oportunidade de transmitir sem contenção.

O PCF fornece dois tipos diferentes de serviços:

1) Acesso ao canal livre de contenção para o AP entregar quadros somente no *downlink*. Esse serviço é usado para permitir ao AP transmitir tráfego armazenado no *buffer*, vindo da rede cabeada para rede móvel;
2) Acesso ao canal livre de contenção para terminais móveis suportarem tráfego limitado no tempo.

O coordenador de ponto, que pertence ao ponto de acesso, divide o tempo de acesso em períodos de superquadros. Cada superquadro compreende um período livre de contenção (modo PCF) e um período com contenção (modo DCF), como na Figura 8. Durante os períodos nos quais as estações estão no modo PCF, o coordenador de ponto consulta se cada estação tem algo a transmitir. As estações recebem dados quando são consultadas pelo coordenador de ponto.

O coordenador de ponto inicia e controla o tempo livre de contenção. Ele escuta o meio por PIFS segundos e então começa um período livre de contenção (*Contention Free Period* - CFP) através da difusão de um sinal de *beacon* (Figura 8). Como, por definição, PIFS é menor que DIFS, nenhuma estação pode começar a enviar dados no modo DCF antes do coordenador de ponto. Todas as estações adicionam a duração máxima do período de contenção ($CFP_{maxduration}$) aos seus respectivos NAVs. O período livre de contenção pode terminar a qualquer momento através do envio de um pacote CF_{end} pelo coordenador de ponto. Isso ocorre freqüentemente quando a rede está com pouca carga. Além disso, o início de um período livre de contenção pode ser adiado por causa da transmissão de alguma estação no modo DCF (atraso na Figura 8).

Quando chega a vez de uma estação transmitir, o coordenador de ponto envia um pacote de dados, caso exista algum a ser enviado, dentro de um pacote de consulta (*piggyback*). O receptor envia de volta um ACK, também com dados se for o caso, depois de SIFS segundos. Após encerrar a transmissão a todas as estações contidas em uma lista de consultas, o coordenador de ponto reinicia o processo de consulta após PIFS segundos. Os usuários que estão sem transmitir por alguns ciclos são retirados da lista de consultas e são consultados de novo no início do próximo período livre de contenção.

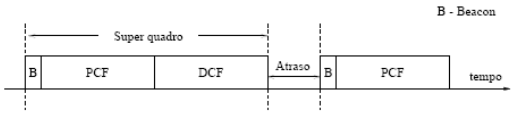

Fig. 8. DCF utilizando RTS e CTS. Fonte [16]

3) Fragmentação: Para lidar com o problema de canais ruidosos, diminuindo a probabilidade de erros devido ao enfraquecimento do sinal e ao ruído, o 802.11 permite que os quadros sejam fragmentados em partes menores. Os fragmentos são numerados individualmente e confirmados de acordo com o uso de um protocolo do tipo *stop-and-wait*, isto é, o transmissor não pode enviar o fragmento $k+1$ enquanto não receber a confirmação do fragmento k.

A fragmentação aumenta a vazão, restringindo as retransmissões aos fragmentos defeituosos, em vez de tranmitir o quadro inteiro. O MAC 802.11 provê suporte para a fragmentação de quadros em transmissões ponto-a-ponto e é responsável por remontar o quadro, o que torna o processo transparente para a camada superior. O padrão obriga que todos os receptores tenham suporte para a fragmentação, mas deixa como opcional a fragmentação nos transmissores. Um limiar de fragmentação ($Fragmentation_{threshold}$) é estabelecido, ou seja, um quadro é fragmentado se for maior que o limiar e o tamanho máximo de um fragmento também é dado por $Fragmentation_{threshold}$.

Caso não haja interrupção devido a limitação de ocupação do meio para uma camada física, os fragmentos de um quadro são enviados em rajada durante um período de contenção, utilizando uma única invocação do procedimento de acesso ao meio do DCF. Um fragmento é enviado SIFS segundos após o recebimento do ACK relativo ao fragmento anterior. A informação da duração no pacote de um fragmento indica o tempo necessário para a recepção do ACK do próximo fragmento, fazendo com que as outras estações que obtiverem essa informação não transmitam. O campo duração nos quadros de dados e no ACK especifica a duração total do próximo fragmento e do seu ACK. No caso do período livre de contenção os fragmentos são enviados como quadros individuais.

III. Comparação do desempenho do DCF e PCF

De acordo com os resultados obtidos em [2], observa-se que para um tráfego baixo, os protocolos de acesso aleatório possuem um baixo retardo de acesso ao canal, enquanto que protocolos baseados em interrogação possuem maior *overhead*. Porém, a medida que o tráfego cresce protocolos baseados em interrogação permitem a manutenção de um baixo retardo de acesso, enquanto que os protocolos baseados em acesso aleatório passam a sofrer de um retardo excessivamente grande.

O modo DCF trabalha bem em condições de carga baixa, mas sofre de alta degradação da vazão em condições de carga alta, esta perda da largura de banda é devida ao aumento do tempo gasto na negociação do acesso ao canal. Esse modo é o mais utilizado comercialmente e possui a característica de ser melhor esforço *(best-effort)* e não suportar nenhuma diferenciação de serviços. Já o modo PCF, por ser baseado em *polling*, suporta alguma diferenciação através da priorização de determinadas estações, porém, o tipo de interrogação *(polling)* realizado é bastante limitado. Dentre estas limitações é possível destacar a restrição da interrogação ao período CFP, a falta de um gerenciamento da interrogação, isto é, a utilização de uma disciplina com parâmetros adequados (pode acontecer do período máximo de interrogação terminar antes que uma estação tenha encerrado sua transmissão, ou alguma estação com um tráfego alto monopolizar o canal no período CFP), e a imprevisibilidade do início do superquadro, e conseqüentemente do CFP, devido à variação do intervalo de transmissão de *beacons*.

A. Considerações do Modelo

- 15 estações móveis com taxa de dados de 2 Mbps
- AP com taxa de dados de 11 Mbps
- Sistema de transmissão DSSS
- Modulação DQPSK

Modelo da Fonte

- Tráfego misto - 15% de dados em tempo real, e 85% baseado em melhor esforço
  - Tráfego em tempo real, voz, modelado por uma cadeia de Markov de dois estados com distribuição exponencial de períodos *on* e *off* com valores médios de $\lambda_{TALK} = 1.35ms$ e $\lambda_{SILENCE} = 1.15ms$ [6];
  - Tráfego baseado em melhor esforço modelado usando uma cadeia de Markov de dois estados [7], o tráfego é gerado durante o estado de TRANSMISSÃO com tempo entre chegadas de zero, considera-se ainda que pacotes não são enviados ao canal durante o tempo entre as ”rajadas”. O tempo de permanência em ambos os estados é dado por uma distribuição de Pareto com função densidade de probabilidade $f(x) = \frac{ak^a}{x^{1+a}}$. Uma fila bloqueante é usada para armazenar os pacotes antes da transmissão.

B. Acesso ao meio com carga-adaptativa

Como mostrado anteriormente, o 802.11 fornece mecanismos de acesso ao meio centralizado e distribuído. Escolhendo o resultado mais recente pode-se melhorar a vazão e o tempo de espera médio em condições de carga alta. *Hosts* numa célula sem fio irão monitorar o canal e evitar o modo DCF e comutar exclusivamente para o modo PCF quando a carga do canal excede um valor máximo. Assim, o objetivo é encontrar o ponto de comutação ótimo dependendo da carga oferecida, do número de estações e do tamanho dos pacotes.

Durante um CFP todas as estações são interrogadas usando um mecanismo *Round Robin* e depois finaliza-se a lista de interrogação, o tempo de vida residual do intervalo do superquadro é usado para transmissão assincrona. Modifica-se esse sistema para o tempo do modo DCF para no máximo um pacote. Após terminar o CFP, o AP se retira do canal por pelo menos $= DIFS + CW_{min} * tsegmento$ para permitir o acesso ao canal das estações em modo DCF (garantindo que ocorra pelo menos uma tranmissão em modo DCF). Se uma transmissão foi finalizada, o AP reinicia o CFP imediatamente enviando um *beacon* indicando o início do próximo CFP. Para encontrar o ponto de comutação ótimo executou-se a simulação usando DCF e PDF, respectivamente, assumindo um tamanho de pacote fixo de 1500 bytes.

C. Resultados

Fig. 9. Comparação do tempo de espera médio do pacote e *goodput* entre DCF e PCF a 2 Mbps. Fonte [2]

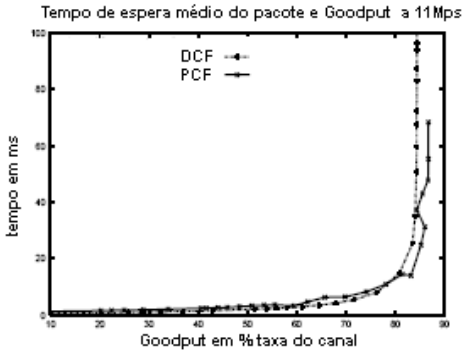

Fig. 10. Comparação do tempo de espera médio do pacote e *goodput* entre DCF e PCF a 11 Mbps. Fonte [2]

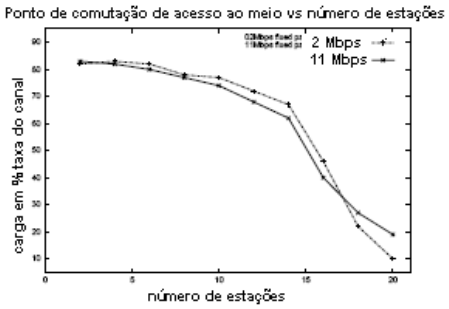

Fig. 11. Ponto de comutação ótimo dependendo do número de estações a 2 e 11 Mbps. Fonte [2]

O impacto da carga no *goodput* e no tempo de espera médio do pacote para DCF e PCF é mostrado na figura 9 e 10. As curvas revelam o seguinte fato: no modo DCF o retardo é limitado até cerca de 10ms para 2Mbps (3ms para 11Mbps) e aumenta levemente para condições de carga baixa. Além de 60% (75% para 11Mbps) de carga agregada o retardo aumenta exponencialmente. O PCF inicia com o tempo de espera dos pacotes aumentando suavemente, todavia o retardo permanece baixo e constante até um *goodput* de 80%.

Além disso, a máxima vazão alcançada para o modo DCF é cerca de 83% da largura de banda do canal para ambas as taxas, enquanto no modo PCF é de 89% para 2Mbps vs 87% em 11Mbps são alcançados. Comutando para o modo PCF ganha-se uma capacidade do canal adicional de 6% a 2Mbps e cerca de 4% a 11Mbps.

O ponto de interseção no gráfico do retardo mostra o ponto ótimo para trocar de DCF para PCF e vice-versa. Se a carga ultrapassa 66% o modo PCF deverá ser usado para alcançar retardos baixos. O ponto de comutação DCF-PCF depende do número de estações e da carga oferecida. Com o aumento do número de móveis numa célula sem fio, o ponto de comutação móvel é deslocado para uma carga baixa como mostra a figura 11.

IV. IEEE 802.11A

Com a necessidade de se obter taxas de transmissão mais elevadas, criou-se então um novo padrão que foi adicionado ao IEEE 802.11. O IEEE 802.11a definiu um novo padrão para redes sem-fio, que utiliza a faixa de freqüência de 5 GHz, ao invés da faixa ISM de 2,4 GHz. Isso trouxe algumas vantagens, como um menor nível de interferência, por não haver tantos equipamentos utilizando essa faixa, mas também trouxe alguns problemas que fizeram com que o 802.11a não obtivesse tanto sucesso, como problemas de padronização da faixa de freqüência e de propagação.

Nesse novo padrão, optou-se por utilizar um esquema de modulação totalmente diferente do anterior, não mantendo assim compatibilidade entre as duas especificações. O 802.11a utiliza como técnica de modulação o OFDM *(Orthogonal Frequency Division Multiplexing)*, que usa várias sub-portadoras, moduladas em BPSK, QPSK, 16-QAM ou 64-QAM. Também utiliza um código convolucional corretor de erros (FEC), com taxas de 1/2, 2/3 ou 3/4. Na sua configuração máxima, o 802.11a pode chegar a 54 Mbps, possuindo várias configurações possíveis a partir de 6 Mbps.

A técnica de transmissão OFDM (Multiplexação por Divisão de Freqüências Ortogonais) surgiu como uma evolução da técnica convencional de Multiplexação por Divisão em Freqüência - FDM, onde no lugar de se utilizar banda de guarda para a separação das subportadoras na recepção do sinal, trabalha-se com uma particular sobreposição espectral de subportadoras. Em técnicas normais de FDM, o espaçamento entre canais deve ser maior que a taxa de símbolos para evitar a sobreposição dos espectros. Na OFDM as subportadoras se sobrepõem mas são escolhidas subportadoras ortogonais, ou seja, que mantêm uma certa relação matemática de modo que não haja interferência entre elas. Como elas possuem um espectro do formato [sen (x) / x], colocam-se as subportadoras de modo que elas estejam centradas nos zeros das subportadoras adjacentes.

Embora a técnica leve o termo multiplexação em sua denominação, deve-se ter em mente que a rigor não ocorre multiplexação num sistema OFDM, mas sim a transmissão paralela de uma seqüência de bits originalmente única.

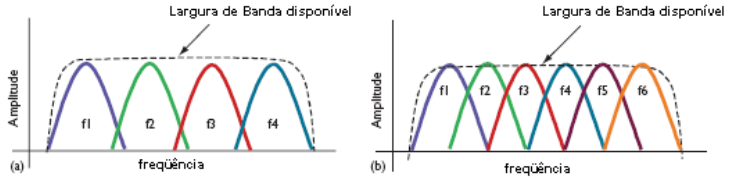

Fig. 12. Técnicas de tranmissão de sinal: (a) FDM usa múltiplas portadoras para transmitir a informação. (b) OFDM técnica *spread spectrum* permite o uso mais eficiente da largura de banda eliminando a necessidade da banda de guarda do FDM. Fonte [8]

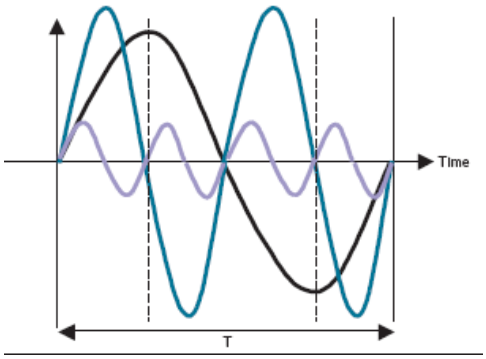

Fig. 13. Ortogonalidade das várias portadoras de freqüências. Freqüência base = 1/T, onde T=símbolo por período. Fonte [8]

No 802.11a, as subportadoras são espaçadas de 312,5 kHz. Como um símbolo é representado por 48 subportadoras de dados, 4 sub-ortadoras piloto, mais uma subportadora nula, resultando em 53 subportadoras, que multiplicadas pelo espaçamento de 312.5 kHz, resulta em uma banda ocupada de 16,6 MHz.

V. IEEE 802.11B

Uma iniciativa para se aumentar as taxas de transmissão do padrão 802.11, mas mantendo a compatibilidade com o padrão original, foi a criação do 802.11b. Esse padrão utiliza a mesma faixa de freqüência de 2,4 GHz, e mantém os modos de operação a 1 Mbps e 2 Mbps utilizando-se DSSS (FHSS foi descartado) com o código Barker, sem nenhuma alteração. Além disso, ele adiciona dois novos modos, com uma nova técnica de codificação, possibilitando chegar então a 5,5 Mbps e 11 Mbps.

Para se atingir velocidades maiores, o 802.11b utiliza, ao invés da seqüência de Barker, uma técnica de codificação chamada de *Complementary Code Keying* (CCK), que consiste em um conjunto de 64 palavras de 8 bits, que irão formar o código, e mantém as propriedades de ortogonalidade. A modulação utilizada será novamente o DQPSK, para os dois modos, que já faz o mapeamento de 2 bits por símbolo. A diferença agora estará no código CCK, que ao invés de mapear um código para um bit como fazia o código de Barker, irá mapear cada palavra do código em 2 ou 6 bits, de acordo com a taxa utilizada, resultando em um total de 4 bits por símbolo para 5,5 Mbps, e 8 bits por símbolo para 11 Mbps.

Esta versão opera com os mesmos protocolos de controle de acesso ao meio, embora os seus parâmetros sejam diferentes em função da camada física utilizada.

No cenário do 802.11b, o desempenho das STAs torna-se um requisito essencial, uma vez que aplicativos multimídia, de acesso móvel a informações ou jogos em rede, necessitam de grande largura de banda. Sendo assim, grandes esforços têm sido empregados por parte dos fabricantes e pesquisadores em identificar e resolver problemas que possam degradar o desempenho dos protocolos e redes desta tecnologia. Um exemplo de diminuição de performance pode ser observado no 802.11 com o aumento da distância entre os pontos em comunicação ou na presença de interferências e/ou ruídos no meio. Nesta condição, há um diminuição da relação sinal/ruído e conseqüente elevação da taxa de erros dos pacotes transmitidos pelas STAs. Tais situações adversas são solucionadas com esquemas de modulação mais robustos que têm como inconveniente a redução da taxa de transmissão das STAs. Para o 802.11b, são previstas as taxas de 11Mbps e 5.5Mbps, em adição as taxas de 1Mbps e 2Mbps já existentes no padrão original. Embora o 802.11b tenha sido criado com o objetivo de proporcionar maiores taxas de transmissão, seu funcionamento pode ainda ser degradado na presença de STAs transmitindo a taxas de bits menores. Conforme observado em [3], uma STA mais lenta, ao transmitir um pacote de tamanho T, ocupa o meio por um período maior quando comparada a uma STA mais rápida. Neste cenário, a STA de maior taxa terá sua vazão decrescida para um valor próximo ao da STA que transmite a uma taxa de bits menor. Esta diminuição de desempenho ocorre em função do método CSMA/CA, o qual atribui igual probabilidade de acesso ao meio para todas as STAs, independente de suas taxas. Em [10] estabelecem-se critérios para fornecer um melhor desempenho das STAs de maior taxa, de maneira que elas não sejam tão prejudicadas pelas STAs mais lentas. Tais critérios têm como objetivo fazer o compartilhamento da banda disponível e ir ao encontro das definições de justiça.

VI. LIMITES DO RETARDO E VAZÃO DO IEEE 802.11

A família de protocolos IEEE 802.11 estudada até agora fornece taxas de dados de até 54Mbps, ao passo que a indústria procura taxas de dados ainda maiores. Em [9] mostra-se que existe um limite superior da vazão teórico e um limite inferior do retardo teórico para os protocolos IEEE 802.11. A existência de tais limites indica que simplesmente aumentando a taxa de dados sem reduzir o *overhead*, o acentuado desempenho, em termos do retardo e da vazão, está limitado mesmo quando a taxa de dados aumenta infinitamente. Reduzir o *overhead* é vital para um bom desempenho.

A. Limites do retardo e vazão

Considera-se somente o mecanismo básico de acesso ao meio (DCF sem RTS/CTS). Para encontrar o limite superior da vazão (TUL) e o limite inferior do retardo (DLL), é preciso derivar duas métricas de desempenho: a vazão máxima alcançável (MT) e o retardo minímo alcançável (MD). Para derivar MT e MD, o sistema deve estar no cenário do melhor caso - 1) o canal é um canal ideal sem erros e 2) em qualquer ciclo de transmissão, há uma e somente uma estação ativa a qual sempre tem um pacote a enviar e as outras estações podem somente aceitar pacotes e fornecer reconhecimento. Note que em um canal com ruído, a vazão é esperada ser menor que a MT e o retardo é esperado ser maior que o MD.

Um ciclo de transmissão DCF consiste de DIFS, *backoff*, transmissão de dados e transmissão do ACK, assim de [9]

$$MT = \frac{8L_{DATA}}{T_{D_{DATA}} + T_{D_{ACK}} + 2\tau + T_{DIFS} + T_{SIFS} + C\bar{W}}$$

$$MD = T_{D_{DATA}} + \tau + T_{DIFS} + C\bar{W}$$

Teorema do limite: Para o mecanismo de acesso básico, o TUL e o DLL existem, independente da taxa de dados, para um dado tamanho de carga útil fixo e um dado conjunto de parâmetros de overhead, e é dado como segue:

$$TUL = \frac{8L_{DATA}}{2T_P + 2T_{PHY} + 2\tau + T_{DIFS} + T_{SIFS} + \frac{CW_{min}T_{slot}}{2}}$$

$$DLL = T_P + T_{PHY} + \tau + T_{DIFS} + \frac{CW_{min}T_{slot}}{2}$$

onde,

L_{DATA} é o tamanho da carga útil em bytes $T_{D_{DATA}}$ é o retardo da transmissão de dados $T_{D_{ACK}}$ é o retardo da transmissão do ACK τ é o retardo de propagação T_{DIFS} é o tempo de DIFS T_{SIFS} é o tempo de SIFS $C\bar{W}$ é o tempo médio de *backoff* T_P é o tempo de transmissão do preambulo físico T_{PHY} é o tempo de transmissão do cabeçalho físico CW_{min} é o tamanho mínimo da janela de *backoff* T_{slot} é o tempo de um segmento

A figura 14 mostra o limite superior TUL e os MTs para o IEEE 802.11a. Quando o tamanho da carga útil é de 1000

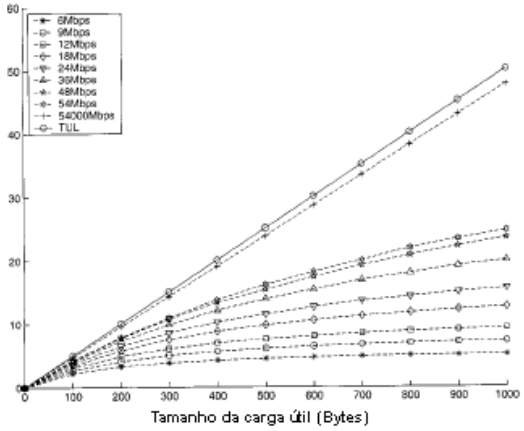

Fig. 14. Vazão máxima e TUL (Mbps) do 802.11a. Fonte [9]

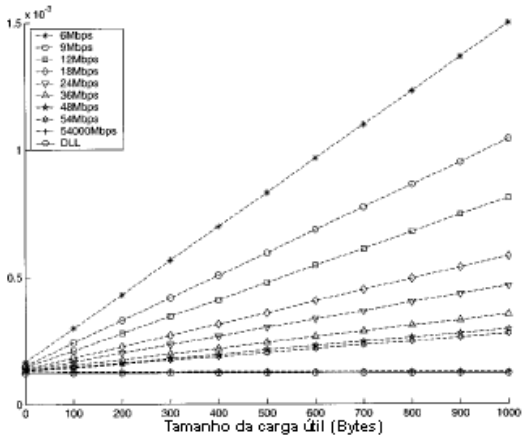

Fig. 15. Retardo mínimo e DLL (segundos) do 802.11a. Fonte [9]

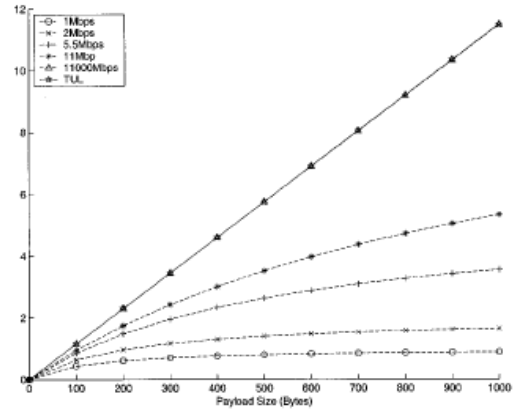

Fig. 16. Vazão máxima e TUL (Mbps) do 802.11b. Fonte [9]

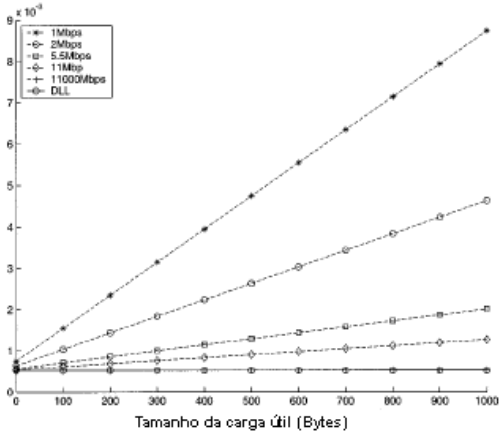

Fig. 17. Retardo mínimo e DLL (segundos) do 802.11b. Fonte [9]

bytes, o MT para 54 Mbps é 24.7 Mbps e o TUL é 50.2 Mbps. O MT para 54000 Mbps com o mesmo conjunto de parâmetros de *overhead* quase alcança o TUL. A figura 15 mostra que o limite inferior DLL e os MDs para o 802.11a. O DLL é o mesmo para todos os tamanhos de carga útil, i.e., 122.5 μs. Quando o tamanho da carga útil é de 1000 bytes, o MD para 54 Mbps é 278.5 μs. O MD para 54000 Mbps com o mesmo conjunto de parâmetros de *overhead* quase alcança o DLL.

A figura 16 mostra o limite superior TUL e os MTs para o IEEE 802.11b. Quando o tamanho da carga útil é de 1000 bytes, o TUL é 11.49 Mbps. O MT para 11000 Mbps com o mesmo conjunto de parâmetros de *overhead* quase alcança o TUL. A figura 17 mostra que o limite inferior DLL e os MDs para o 802.11b. O DLL é o mesmo para todos os tamanhos de carga útil, i.e., 523 μs. O MD para 11000 Mbps com o mesmo conjunto de parâmetros de *overhead* quase alcança o DLL.

VII. IEEE 802.11G

O 802.11g é uma evolução do 802.11b, já que opera na mesma faixa de freqüência de 2,4 GHz, e mantém a compatibilidade com esse padrão. Porém, ele pode ser visto também como uma fusão dos dois padrões, o 802.11a e o 802.11b. Ele usa o que cada um tem de melhor, sendo a modulação do 802.11a, o OFDM, e a faixa de freqüência do 802.11b, a ISM de 2,4 GHz. Assim, o padrão 802.11g funciona identicamente ao 802.11b para as taxas de 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps, e também funciona de modo similar ao 802.11a, mas na faixa de 2,4 GHz, possibilitando também todas as suas configurações de velocidade.

Para manter a compatibilidade com o 802.11b, o 802.11g também suporta todos os seus modos, podendo funcionar normalmente em uma rede 802.11b. Porém para um dispositivo 802.11b detectar o sinal de um 802.11g de modo que não haja colisões, usa-se o mecanismo de RTS/CTS, que é o mesmo mecanismo utilizado para solucionar o problema do terminal escondido o qual é similar a esse problema. Sempre que uma estação quiser utilizar o meio, ela envia uma mensagem de RTS para o ponto de acesso, e só terá direito a transmitir sua menssagem ao receber o CTS. Assim, o ponto de acesso pode controlar quem irá acessar o meio, evitando colisões entre dispositivos b e g.

Uma outra solução para esse problema, seria a utilização de uma nova técnica de modulação opcional no 802.11g, que é o CCK/OFDM, que combina as duas técnicas. Nessa modulação, o cabeçalho dos pacotes é enviado utilizando a modulação CCK, enquanto a área de carga *(payload)* é enviada utilizando

OFDM. Com isso, os equipamentos 802.11b da rede podem escutar o cabeçalho do pacote, que é enviado em CCK, e desse cabeçalho podem obter a informação de quanto tempo o pacote vai levar para ser enviado, esperando então esse tempo mínimo antes de tentar enviar novamente, evitando assim colisões.

Vale a pena lembrar que os dois mecanismos, RTS/CTS e CCK/OFDM, adicionam alguma *overhead* à capacidade da rede, mas é um *overhead* aceitável para que se mantenha a compatibilidade com os sistemas atuais.

Já o PBCC é uma outra técnica de modulação opcional incluída no 802.11g. Ele foi criado pela *Texas Instruments*, e consiste em uma técnica de uma portadora, com modulação 8-PSK, e uma estrutura de código convolucional (o CCK usa uma estrutura em bloco). Assim como o CCK/OFDM, ele também transmite o cabeçalho do pacote com modulação CCK para manter a compatibilidade com sistemas 802.11b, e a máxima taxa de transmissão definida para o PBCC é de 33 Mbps.

A. Desempenho da Vazão no IEEE 802.11g

Em teoria, ambos 802.11a e 802.11g utilizam quase a mesma especificação PHY e podem ter desempenho de vazão similares. Na realidade, o desempenho da vazão do 802.11g será significantemente diferente do 802.11a pelas seguintes razões:

1) 802.11 tem 20 μs segmentos de tempo, para ser compatível com os dispositivos 802.11b; o uso de 9 μs segmentos de tempo como usado no 802.11a é opcional
2) 802.11g compartilha o mesmo espectro de 2.4 GHz dos dispositivos 802.11b; o impacto no desempenho pode ser significante se não for empregada coordenação
3) Perda por propagação dependendo da freqüência favorece o 802.11g. Entretanto, os dispositivos predominantes de não-WLAN em 2.4GHz, e.g., dispositivos *Bluetooth*, telefones sem fio, forno de microondas, aumentam a probabilidade de interferência
4) Menos canais disponíveis na banda de 2.4 GHz que na banda de 5 GHz. Por exemplo, somente três canais estão disponíveis na banda de 2.4 GHz comparados com 13 na banda de 5GHz. Interferência co-canal devido ao reuso da freqüência pode ser significante se poucos canais estão disponíveis.

Observa-se que a vazão depende de muitos fatores tais como Taxa de Erro de pacotes (PER), tamanho do pacote e taxa de dados. A figura 18 mostra a vazão da camada MAC com diferentes PER para o tamanho do pacote de dados de 1500 bytes onde colisões não são assumidas. Uma das principais diferenças entre o 802.11a e o 802.11g é a duração do segmento de tempo. Para o 802.11a, o segmento de tempo é igual a 9 μs. Para o 802.11g, por ser compatível com o 802.11b, o segmento de tempo é de 20 μs e um segmento de 9 μs é opcional. Na figura 18 está claro que o maior segmento de tempo resulta em maior DIFS e menor vazão. A degradação também depende do esquema da taxa de dados.

Como visto anteriormente, a melhor vazão pode somente ser encontrada se a opção do segmento de 9μs puder ser

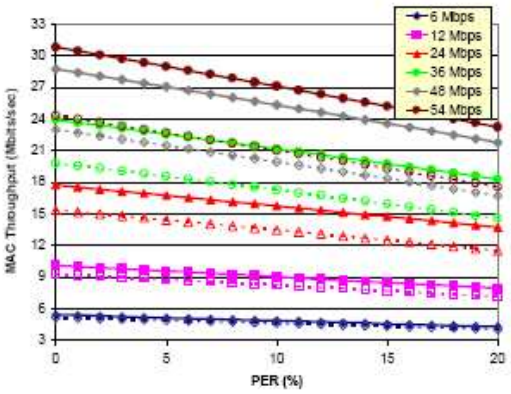

Fig. 18. Vazão MAC para diferentes taxas de dados variando a PER, linha sólida denota tempo de segmento=9μs e linha pontilhada tempo de segmento=20μs. Fonte [5]

utilizada, mas isso pode somente ser utilizado em ambientes g-apenas, onde todos os dispositivos são capazes de transmitir frames OFDM. Os usuários 802.11b podem iniciar um processo de *roaming* enviando quadros de requisição intermitentemente, esses quadros podem possivelmente colidir com pacotes 802.11g. A figura 19 mostra a degradação no desempenho do 802.11g causado por diferentes números de usuários 802.11b não-coordenados. A comparação foi feita com respeito a um sistema 802.11g com a opção do tempo de segmento de 9μs. Os parâmetros usados são quadros de requisição de duração=0.1ms e esses quadros são enviados em 10tempos/seg. Observe que a vazão diminui quando o número de usuários não-coordenados aumenta.

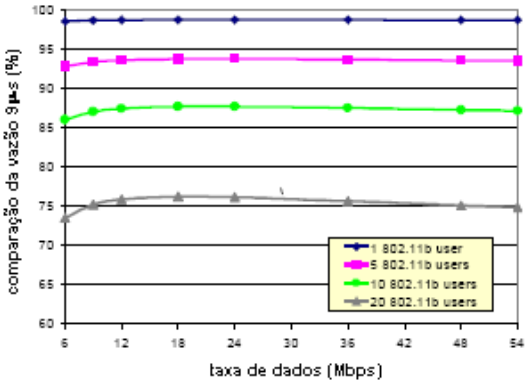

Fig. 19. Redução da vazão devido a usuários 802.11b não-coordenados, PER=10%, tamanho do pacote=1500 bytes

Como já foi visto, para resolver o problema dos usuários não-coordenados, pode ser usado o mecanismo RTS/CTS, estudado acima. A figura 20 mostra a degradação da vazão devido ao maior tempo de segmento e a implementação do mecanismo de proteção (RTS/CTS) comparado com a opção do tempo do segmento de 9μs. A opção CTS-apenas e para o tráfego *downlink* (AP para móvel) e a opção RTS/CTS é usada para tráfego *uplink* (móvel para AP)

Analisando-se as figuras 19 e 20, pode-se notar que:

1) Ao contrário da figura 2, a magnitude do impacto

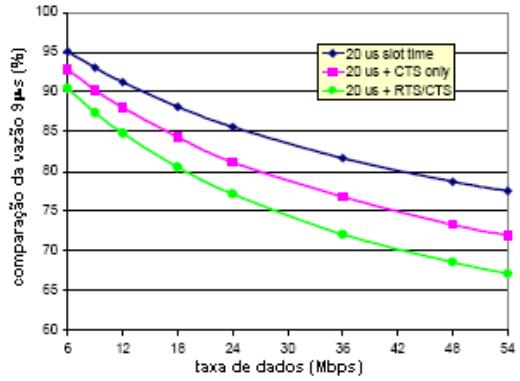

Fig. 20. Redução da vazão devido ao maior tempo de segmento(20μs), CTS, RTS, PER=10%, tamanho do pacote=1500. Fonte[5]

RTS/CTS é dependente da taxa de dados. Quanto maior a taxa de dados maior é a penalidade do *overhead*;

2) O uso da opção CTS-apenas pode ser útil para disposição em espaços públicos desde que a penalidade do *overhead* não exceda o impacto causado por numerosos usuários 802.11b não-coordenados;
3) Para aplicações empresariais com usuários controlados, a implementação RTS/CTS pode ser considerada significante

.

A penalidade do mecanismo de proteção 802.11g pode ser maior que 30% para operações com taxa de dados alta.

VIII. IEEE 802.11e e Qualidade de Serviço

Algumas aplicações são relativamente insensíveis à degradação transitória da qualidade de serviço oferecida pela rede. Por exemplo, num serviço de transferência de arquivos, a redução da largura de banda disponível ou o aumento do atraso dos pacotes podem afetar o desempenho da aplicação, mas não comprometem a sua operação. Devido à capacidade de adaptação a variações na disponibilidade de recursos. Essas aplicações contentam-se com um serviço do tipo melhor esforço, no qual a rede compromete-se apenas a tentar transmitir o tráfego gerado pela aplicação, sem no entanto oferecer garantias de desempenho. Já no caso de aplicações em tempo real, a diminuição da largura de banda disponível ou o aumento do atraso podem inviabilizar a sua operação. Neste caso, a rede necessita reservar recursos para as aplicações de modo que, mesmo em momentos de maior carga na rede, os requisitos mínimos de desempenho destas aplicações sejam atendidos, ou seja, a rede deve fornecer um serviço com garantias de qualidade de serviço (QoS).

A forma de se obter qualidade de serviço, envolve a inclusão de mecanismos que buscam racionalizar o uso dos recursos disponíveis na rede. Esses mecanismos estabelecem níveis de serviço e permitem a convivência na mesma rede de tráfegos com requisitos distintos de qualidade. Tráfegos pertencentes a níveis de serviço diferentes são tratados de forma que o nível mais prioritário possa sempre dispor dos recursos de que necessita, ainda que em detrimento dos níveis menos prioritários. Ao mesmo tempo, tráfegos pertencentes a um mesmo nível de serviço são tratados de forma que suas demandas sejam atendidas de forma justa.

Dentre as métricas de QoS mais utilizadas na literatura destacam-se o retardo médio, o jitter, a taxa de perda e a banda obtida.

A. Escalonamento

A disciplina de escalonamento diz respeito à política de transmissão de pacotes utilizada. Uma das principais formas de prover qualidade de serviços numa rede de computadores é incorporar disciplinas de escalonamento ao protocolo de acesso ao meio, para que seja obtida a diferenciação de serviços na camada MAC. Conforme será apresentado, o 802.11e atinge a diferenciação de serviços através da aplicação de uma disciplina de escalonamento que prioriza o tráfego de determinados fluxos. Diversas são as disciplinas de escalonamento propostas na literatura, por exemplo:

Exaustiva, *Gated* e Limitada: Estas são as disciplinas mais básicas, utilizadas principalmente em protocolos de interrogação *(polling*). A disciplina exaustiva consiste em transmitir até que o *buffer* da estação considerada esteja completamente vazio, passando em seguida para a próxima estação. A disciplina *gated* consiste em transmitir todos os pacotes que estavam no buffer da estação no momento em que ela recebeu a permissão para acessar o canal, porém os pacotes que chegarem ao buffer após o início da transmissão serão transmitidos apenas no próximo ciclo. Já a disciplina limitada consiste em respeitar um limite de transmissão, seja em tempo ou em número de pacotes, onde no momento em que o limite de transmissão é atingido, a estação corrente deixa de transmitir e a permissão de transmissão passa para a próxima estação, independente do estado do *buffer* da estação corrente.

Head of The Line: Em uma descrição inicial, a disciplina consiste em respeitar as prioridades de cada pacote, ou seja, pacotes de classe k serão transmitidos sempre na frente dos pacotes de classe j, sendo k $<$ j (a classe k é mais prioritária que a classe j). Esta disciplina encontra-se descrita também em [9].

B. Serviços Integrados e Diferenciados

Existem duas abordagens genéricas na literatura para o provimento de QoS em redes de computadores. A primeira, denominada serviços integrados, é orientada à conexão, e nela existe um controle por fluxo dos dados que estão trafegando. Na segunda, denominada serviços diferenciados, o controle do tráfego não é feito por fluxo, mas sim por classe, ou conjunto de fluxos.

As técnicas utilizadas em ambas as abordagens são similares, variando-se apenas a granularidade (tratamento por fluxo ou por conjunto de fluxos). Com a abordagem de serviços integrados é possível obter níveis de QoS por aplicação, o que é importante em redes multimídia devido às diferentes características de cada tipo de tráfego. No caso da diferenciação por conjunto de fluxos (sem um controle de admissão, que seria feito por fluxo) existe a possibilidade dos fluxos individuais sofrerem um efeito parecido com o de *starvation*, ou seja,

aplicações de vídeo e voz terem um retardo excessivo, assim como aplicações de dados terem uma alta taxa de perdas, devido ao tráfego de cada classe estar muito alto.

C. Eficiência

A eficiência de um protocolo de controle de acesso ao meio é uma medida do aproveitamento da largura de banda disponível, sendo normalmente expressa pela razão entre a taxa útil e a capacidade do canal. Um protocolo de controle de acesso ao meio deve procurar maximizar a eficiência sem comprometer a qualidade de serviço oferecida às conexões. Para isso, deve procurar minimizar o *overhead* que introduz.

D. Justiça (fairness)

Um protocolo de controle de acesso ao meio é considerado justo se não exibir preferência por nenhuma estação em particular quando múltiplas estações competem pelos recursos, no caso das diferentes conexões pertencerem a uma mesma classe de tráfego. Entre diferentes classes de tráfego, o protocolo deve atribuir recursos na proporção de suas alocações.

IX. IEEE 802.11E

Afim de criar um protocolo capaz de prover qualidade e diferenciação de serviços em redes sem fio, o IEEE *(Institute of Electronics and Electrical Engineers)*, criou um grupo de trabalho chamado 802.11e. O objetivo era melhorar a camada MAC para suportar os requisitos de Qualidade de Serviço. Esses melhoramentos, adicionados às mudanças feitas na camada física com os resultados dos grupos 802.11a e 802.11b, de uma forma geral capacitarão o desempenho do sistema, e expandirão as ofertas para aplicações no padrão 802.11. Como exemplos para essas aplicações, citam-se a transmissão de voz, vídeo e dados sobre redes sem fio, conferências multimídia, distribuição de *streams* de vídeo, melhoria de segurança das aplicações, e o surgimento de aplicações móveis.

O 802.11e é formado basicamente por duas funções de coordenação, ou modos de operação: O EDCF (*Enhanced Distributed Coordination Function*), que é uma extensão do modo DCF, descrito na seção anterior, implementa mecanismos de diferenciação de serviços, e o HCF (*Hybrid Coordination Function*), que é uma melhoria do modo PCF. Apesar dos modos EDCF e HCF serem baseados, respectivamente, no DCF e PCF, considera-se que a função de coordenação principal do 802.11e é o modo HCF, e que o EDCF faz parte do modo HCF. Este fato contrasta com a organização do 802.11 atual, onde o modo DCF é justamente a função de coordenação principal, e o PCF é um modo opcional e pouco implementado comercialmente.

A. EDCF

O modo EDCF, assim como o DCF do atual 802.11, é baseado no protocolo de acesso aleatório CSMA/CA. No entanto, o protocolo suporta 8 níveis de prioridade, que são mapeados em 4 categorias de acesso. Cada pacote que chega à camada MAC vem das camadas superiores marcado com sua respectiva prioridade, variando entre 0 e 7. Ao chegar na camada MAC, esta prioridade é mapeada em uma categoria de acesso, denominada AC (*access category*), de acordo com a figura 21.

Prioridade	Categoria de Acesso	Tipo
1	0	*Best Effort*
2	0	*Best Effort*
0	0	*Best Effort*
3	1	*Video Probe*
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Fig. 21. Mapeamento de Prioridade para AC. Fonte [15]

Cada categoria de acesso utiliza determinados parâmetros da camada MAC, cujos valores são utilizados para obter a diferenciação de serviços do protocolo. Os parâmetros utilizados por cada categoria são: $AIFSD[AC], C_{Wmin}[AC] e CW_{max}[AC]$, onde AC varia entre 0 e 3, conforme a tabela 1. AIFSD[AC] é calculado da seguinte forma: $AIFSD[AC] = SIFS + AIFS[AC] \times SlotTime$, onde $AIFS[AC]$ é um inteiro maior que zero. O valor de *backoff* é escolhido aleatoriamente entre [1, 1+CW[AC]], onde CW[AC] é o valor da janela de contenção corrente, que está entre CW_{min}[AC] e CW_{max}[AC]. O fator multiplicativo, PF, utilizado para aumentar a janela de contenção no caso de colisões, assume o valor 2.

A diferenciação é obtida por categoria de acesso, justamente através da diferença de valores dos parâmetros descritos, denominados de parâmetros do EDCF. Estes parâmetros são enviados pelo ponto de acesso para todas as estações através de quadros de *beacon*. Basicamente, quanto menor forem os parâmetros descritos, menor será o retardo para que a estação acesse o meio. No entanto, é importante observar que estes valores também influenciam a probabilidade de colisões. A figura 22 exibe a estrutura do acesso ao meio quando o EDCF é utilizado.

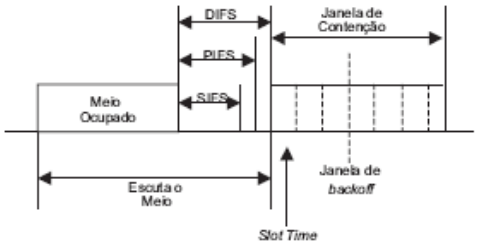

Fig. 22. Estrutura do acesso ao meio no modo EDCF. Fonte [15]

Da forma que foi estruturado o protocolo, cada categoria de acesso compete com as demais mesmo em uma única estação, ou seja, podem acontecer colisões denominadas co-

lisões virtuais ou colisões internas, quando duas ou mais categorias existentes em uma única estação tentam transmitir simultaneamente. Neste caso, a categoria prioritária tem sua transmissão realizada e as demais assumem que ocorreu uma colisão no acesso ao meio, ou seja, são tomadas as medidas com relação ao incremento da janela de contenção e escolha de um novo tempo de *backoff*. A figura 23 mostra a estrutura das categorias de acesso presentes em todas as estações que suportam o protocolo. A estação pode transmitir um pacote de cada vez ao conquistar o direito de acessar o meio, mas existe ainda a possibilidade de uma estação transmitir mais de um quadro de forma consecutiva, com um espaço de SIFS entre cada quadro. Através dos quadros de *beacon* a estação informa o parâmetro EDCF TXOP, que determina o limite de tempo que uma estação possui para transmitir quadros de uma categoria, a partir do momento em que ela adquire o acesso ao meio.

Desta forma, observa-se que o modo EDCF suporta a diferenciação de serviços através de suas quatro categorias de acesso. No entanto, por ser baseado em um protocolo de acesso aleatório, garantias não podem ser feitas. Com o objetivo de melhorar a diferenciação de serviços foi definido o modo HCF.

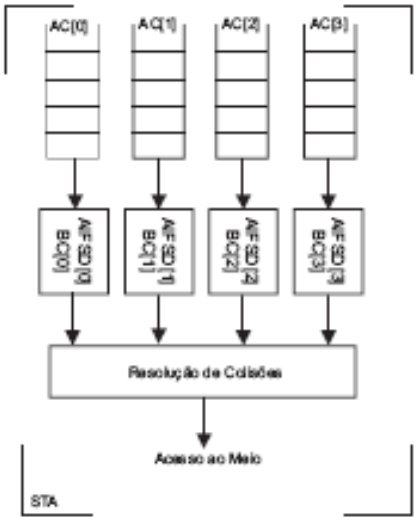

Fig. 23. Categorias de acesso utilizadas no modo EDCF. Fonte [15]

B. HCF

O modo HCF é descrito como a função de coordenação primária da proposta IEEE 802.11e, caracterizada por alternar entre períodos de acesso aleatório, regidos pelo EDCF, e períodos de interrogação *(polling)*, conforme funcionamento descrito a seguir. A entidade principal deste modo é o HC (*Hybrid Controller*) que possui duas funções principais: realizar o controle de admissão de conexões (CAC) e gerenciar a interrogação, desta forma coordenando o acesso ao meio.

No 802.11e, o tempo também é segmentado em segmentos denominados superquadros, delimitados pela transmissão de quadros de *beacon*. O HC realiza a interrogação das estações em qualquer ponto do superquadro, não se limitando a um período específico como no modo PCF do 802.11. Para manter a compatibilidade com o 802.11, a proposta prevê a possibilidade de um período de CFP após a transmissão do *beacon*, porém recomenda-se que este período seja igual a zero, e que apenas as regras do HCF sejam utilizadas.

A figura 24 mostra o funcionamento do 802.11e neste modo, ou seja, o período CFP opcional, seguido de períodos alternados de interrogação, denominados CAPs (*Controlled Access Periods*), e de contenção, seguindo as regras do EDCF. Observa-se que a qualquer momento o HC pode interromper a contenção (EDCF) e iniciar o período de acesso controlado (CAP), transmitindo mensagens de interrogação. O período de contenção é retomado após o término do CAP.

Fig. 24. Estrutura do acesso ao meio no modo HCF. Fonte [15]

A disciplina de interrogação utilizada no 802.11e modo HCF é a limitada, ou seja, cada estação tem um período máximo de tempo por superquadro em que pode acessar o canal. A determinação do valor deste limite é responsabilidade do escalonador utilizado.

O escalonamento das transmissões é feito em dois níveis. Um escalonador presente no HC determina a duração máxima do acesso ao meio por superquadro de cada estação e um outro escalonador presente em cada estação determina, dentro deste limite, quanto tempo será utilizado para cada fluxo admitido no HCCA (HCF Controlled Channel Access). O HC realiza então a interrogação das estações de acordo com o escalonador central, enquanto que ao receber mensagens de interrogação as estações transmitem dados de suas aplicações de acordo com seu escalonador. Basicamente cada estação envia ao HC uma requisição de admissão de conexão para cada fluxo que deseja transmitir no modo HCCA, assim como o TSPEC (Traffic Specification) de cada um deles, informando a respectiva característica estatística de cada fluxo de dados assim como seus requisitos de QoS. Com estes dados o HC realiza o CAC, e caso esta conexão seja admitida estes dados também são utilizados para a determinação de dois parâmetros, que são o SI (*Service Interval*), que diz respeito ao intervalo entre interrogações sucessivas de uma mesma estação, e a duração do TXOP (*Transmission Opportunity*), período pelo qual a estação pode transmitir pacotes sucessivamente em um superquadro. Para uma melhor coexistência da interrogação e do EDCF no modo HCF, a proposta prevê a utilização de parâmetros que limitem a duração máxima do período de interrogação em cada superquadro. Os parâmetros são o DOT11CAPRATE e o DOT11CAPMAX, que juntos definem um *time token bucket* que limita o período CAP dentro de cada superquadro.

X. IEEE 802.11I E SEGURANÇA

Como foi visto as redes sem fio estão em franca expansão, por oferecem inúmeras vantagens. Uma das grandes vantagens deste tipo de rede é a flexibilidade oferecida. Sem a necessidade de cabos, os usuários estão livres para se moverem livremente enquanto estão conectados à rede de forma transparente. Em locais onde não é permitida a passagem de cabos, como em prédios históricos, ou o custo do cabeamento é significante, redes sem fio são, sem dúvida, uma solução de menor custo. Apesar de amplamente utilizada, o padrão para redes sem fio, IEEE 802.11, oferece diversas vulnerabilidades que colocam em risco a confidencialidade, integridade, autenticidade e disponibilidade da comunicação.

A confidencialidade, também referenciada como privacidade ou sigilo, impede que pessoas não autorizadas tenham acesso à informação. A integridade do conteúdo é a garantia que a informação está consistente, ou seja, não foi criada, alterada ou eliminada sem autorização. A autenticidade garante a identidade de quem está executando uma determinada ação. A partir da identificação do usuário, é possivel implementar o controle de acesso aos recursos disponíveis. O controle de acesso define quais usuários podem realizar determinadas tarefas em determinados objetos. Por sua vez, o controle de acesso permite que se implemente o log, auditoria e contabilização de acesso aos objetos. Outra conseqüência da autenticação é a não-repudiação. O não-repúdio ou irretratabilidade previne que alguém negue a autoria de uma determinada ação. A disponibilidade garante que uma informação estará disponível para acesso no momento desejado. Apesar de amplamente utilizada, o padrão para redes sem fio, IEEE 802.11, oferece diversas vulnerabilidades que colocam em risco a confidencialidade, integridade, autenticidade e disponibilidade da comunicação. Esta seção apresenta como é implementada a segurança no padrão IEEE 802.11, além das vulnerabilidades encontradas na sua implementação. É apresentado dois novos padrões de segurança que irão substituir o atual modelo (WEP), o 802.11I e 802.1X.

A. Problemas em Redes Sem Fio:

as redes *wireless* apresentam problemas de segurança semelhantes aos das redes cabeadas, além dos problemas específicos decorrentes da forma de conexão sem fio. Neste item, serão apresentados apenas os problemas relacionados com as redes sem fio e as possíveis conseqüências na rede cabeada.

O principal problema da ausência de um meio de transmissão ligado é a grande facilidade em implementar ataques do tipo *eavesdropping*, comprometendo a confidencialidade da comunicação. Com software e hardware apropriados, é possível capturar facilmente *logins*, senhas, endereços de servidores e estações de usuários.

Além do problema de confidencialidade, existe o risco de perda de integridade e autenticidade. Mensagens podem ser alteradas e reencaminhadas comprometendo a integridade da informação. Redes sem fio podem ser acessadas por pessoas não autorizadas, ignorando as possíveis restrições existentes no *firewall*. Desta forma, a rede sem fio pode ser uma porta de entrada para a rede corporativa cabeada, tornando o problema de segurança ainda mais crítico.

As redes sem fio também podem ser alvos de ataques DoS (*Denial of Service*), o que pode tornar os serviços da rede indisponíveis. Além de alvo direto, é cada vez mais comum a utilização de redes sem fio como ponto de partida para ataques DDoS (*Distributed Denial of Service*) contra outras redes e para o envio de emails não autorizados (*spam*). Neste caso, a rede pode ter sua largura de banda seriamente comprometida.

B. Segurança no IEEE802.11:

as falhas de segurança conhecidas no 802.11 podem ser divididas em 3 grupos, são eles:

- Uso do 802.11 sem criptografia
- Falhas no WEP
- Falta de autenticação nas mensagens de gerência

1) WEP: O padrão de segurança para WLANs IEEE 802.11 é conhecido como WEP (*Wired Equivalent Privacy*). O WEP atua na camada de enlace entre estações e o ponto de acesso (AP), oferecendo, basicamente, três serviços: confidencialidade, integridade e autenticação.

Confidencialidade:A implementação da confidencialidade da transmissão é opcional, ou seja, pode ser habilitada ou não. Quando habilitada, a confidencialidade é garantida pela técnica de criptografia de chave simétrica, utilizando o algoritmo RC4. O RC4, projetado por Ron Rivest em 1987, é um algoritmo de chaves secretas, amplamente utilizado em aplicações comerciais, especialmente em transações na Internet que utilizam SSL. Para que seja possível o ciframento dos quadros, os participantes devem compartilhar a mesma chave secreta. A configuração das chaves é feita manualmente em cada estação. Um dos grandes problemas no WEP é a ausência de um mecanismo de gerência de chaves, o que introduz uma série de vulnerabilidades e não garante escalabilidade ao modelo. Por exemplo, se a chave secreta de uma estação for roubada, todas as estações terão que ter suas chaves alteradas. Para enviar uma mensagem, a estação transmissora, inicialmente, concatena a sua chave secreta (*shared key*) a um vetor de inicialização (IV). O resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios (PRNG) definido pelo RC4. O PRNG gera uma seqüência de bits do mesmo tamanho que a informação a ser cifrada, ou seja, o quadro MAC incluindo o CRC. Um XOR (OU exclusivo) é realizado entre o quadro e a seqüência de bits, gerando o quadro cifrado. Finalmente, o quadro é enviado juntamente com o IV para que o receptor possa fazer o processo inverso (Fig. 24).

O WEP utiliza um vetor de inicialização (IV) de 24 bits para proteger a chave secreta utilizada no processo de criptografia. A cada quadro enviado, o IV é gerado e concatenado à chave secreta, fazendo com que a chave utilizada no ciframento do quadro (*keystream*) mude a cada novo quadro. O vetor de inicialização faz com que o tamanho de chave passe de 40 bits para 64 bits e de 104 bits para 128 bits, porém como IV é passado em claro para a estação destino para realizar a decriptografia, os tamanhos das chaves continuam 40 bits e 104 bits para fins de criptografia. De qualquer forma,

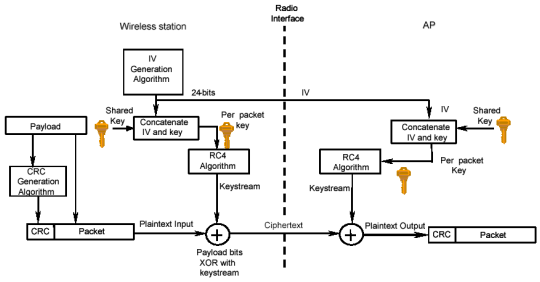

Fig. 25. Confidencialidade no 802.11. Fonte [11]

quanto maior o tamanho da chave criptográfica, mais seguro é processo de criptografia.

Um dos grandes problemas na implementação da confidencialidade no WEP é o esquema de geração das chaves criptográficas utilizadas pelo algoritmo RC4. O RC4 utiliza uma nova chave a cada quadro enviado, sendo que a chave é formada por uma parte fixa (chave secreta) e uma variável (IV). O problema está na parte variável da chave, que possui apenas 24 bits e pode repertir-se em pouco tempo, comprometendo a chave como um todo. Em uma rede com grande fluxo de mensagens, é possível derivar chaves de 128 bits após o envio de cerca de quatro milhões de quadros ou depois de quatro horas de monitoramento da rede. Esta vulnerabilidade torna o protocolo WEP sem qualquer utilidade prática. Apesar desta vulnerabilidade, o RC4 continua sendo utilizado na maioria das aplicações Web com base no SSL, mas implementando um outro esquema de geração de chaves.

Integridade: A integridade de um quadro, ou seja, a garantia que o quadro não será alterado entre o transmissor e o receptor é implementada a partir da técnica de CRC-32 (*Cyclic Redundancy Check*), que gera um ICV (*Integrity Check Value*) para cada quadro enviado. Ao receber o quadro, o destinatário executa a mesma função de CRC e compara o ICV obtido com ICV recebido. Caso o valor do ICV calculado seja igual ao ICV recebido, a mensagem está integra, caso contrário, o quadro sofreu alguma alteração. Figura 25.

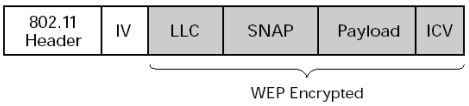

Fig. 26. Quadro WEP. Fonte [11]

A utilização da técnica de CRC para gerar a integridade do quadro, torna o WEP vulnerável à ataques do tipo *replay* e *bit-flipping*.

Autenticação: o WEP oferece dois tipos de autenticação: sistema aberto (*open system*) e chave compartilhada (*shared key*). A autenticação por sistema aberto é a opção *default* e, na verdade, funciona apenas como mecanismo de identificação, devendo ser evitado. Se o mecanismo de criptografia não estiver habilitado, qualquer dispositivo poderá ter acesso ao AP e, conseqüentemente, acesso à rede. Se a criptografia estiver habilitada e o cliente não possuir uma chave secreta, o cliente não consigará transmitir mensagens através do AP e nem recebê-las, mesmo que a estação seja autenticada.

A autenticação com base em chave compartilhada utiliza a técnica de *challenge-response*. Neste mecanismo, o ponto de acesso não é autenticado, apenas a estação. Na Fig. 26, a estação sem fio (*wireless station*) está solicitando ao AP sua autenticação (*authentication request*). O AP gera um número aleatório (*challenge*) e o envia para a estação. A estação recebe o número, criptografa-o utilizando o algoritmo RC4 e o envia de volta (*response*). O AP decripta a resposta e a compara com o número enviado. Se a comparação for positiva, o AP envia para a estação um mensagem confirmando o sucesso da autenticação.

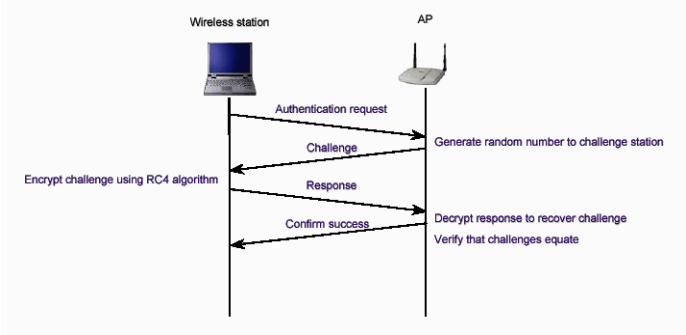

Fig. 27. Autenticação no 802.11. Fonte [11]

Um dos grandes problemas neste esquema de autenticação é que o processo de *challenge-response* é vulnerável a ataques do tipo *man-in-the middle*. Como é possível capturar tanto o texto cifrado como o texto original, a chave criptográfica pode ser facilmente derivada.

A autenticação por endereço MAC é uma outra forma de autenticação, porém não é padrão IEEE, mesmo sendo oferecida por alguns fabricantes, como a Cisco. Neste esquema, existe um servidor de autenticação que verifica, a partir de uma lista de endereços MAC, se a estação cliente está autorizada ou não a ter acesso à rede. Este mecanismo não oferece segurança, pois os endereços MAC podem ser interceptados e forjados, permitindo ataques do tipo *spoofing*.

C. IEEE 802.11i:

o padrão IEEE 802.11i será o substituto do protocolo WEP. Seu objetivo é resolver os diversos problemas encontrados no protocolo WEP, ligados a garantia da confidencialidade e da integridade da comunicação, como apresentados anteriormente. Desde quando o grupo de trabalho do 802.11i iniciou o seu estudo alguns fabricantes têm implementado algumas pré normas no mercado para prevenir alguns tipos de vulnerabilidade, como:

- Ataque de dicionário ao EAP: o quadro 802.11 é facilmente capturado, possibilitando que um intruso descubra uma senha usando o mecanismo de força bruta baseado em dicionário. É recomendado que seja utilizado métodos de autenticação como, EAP *(Extensible Authentication Protocol)* TLS, SRP TTLS and PEAP.
- Ataque a chave *default*: como 802.11 não implementa um mecanismo de troca de chaves aleatório descobrir a chave

é questão de tempo. É extremamente recomendado que se use algum mecanismo de troca dinâmica de chaves como SNMPv3 ou SSH.
- Ataque de DOS baseado no quadro *EAPOL-Logoff*: como esse tipo de quadro não é autenticado, alguém pode enviar um quadro *EAPOL-Logoff* e desconectar um usuário. Pode-se filtrar esse tipo de solicitação no ponto de acesso (AP).
- Ataque de DOS baseado no quadro *EAPOL-Styart*: o atacante pode fazer um envio maciço de quadro *EAPOL-Start* para sobrecarregar o ponto de acesso (AP) e tirá-lo de serviço. Isso pode ser evitado fazendo com que o AP não gaste muito recurso com o atendimento desse tipo de quadro.
- Ataque de DOS baseado no espaço de identificação do EAP: O atacante pode consumir o espaço de identificação do EAP, que vai de 0 a 255, e tirar o ponto de acesso fora de serviço.
- Ataque de DOS baseado no envio antecipado do pacote de sucesso do EAP: o atacante pode enviar um pacote de sucesso do EAP antecipado para permitir que uma estação possa ser vista na rede antes que o ponto de acesso complete o processo de autenticação.
- Ataque de DOS baseado no pacote de falha do EAP: o atacante pode enviar um pacote de falha do EAP antecipado para não permitir que uma estação seja vista na rede antes que o ponto de acesso complete o processo de autenticação.
- Ataque de DOS baseado na alteração do pacote EAP: o atacante pode modificar o conteúdo do pacote EAP. Para evitar esse tipo de ataque devem-se utilizar protocolos de criptografia como TLS, PEAP ou TTLS.

Basicamente, o 802.11i oferece dois esquemas de criptografia, que eliminam os problemas encontrados no WEP. O TKIP e o CCMP podem ser utilizados simultaneamente na mesma rede, permitindo que exista uma negociação entre o cliente e o AP para definirem qual protocolo criptográfico será utilizado.

1) TKIP: O TKIP (*Temporal Key Integrity Protocol*), também chamado de WEP2, foi projetado para resolver os problemas apresentados pelo WEP, ao mesmo tempo que mantém a compatibilidade com a base instalada. O TKIP pemite eliminar os problemas de confidencialidade e integridade apresentados pelo WEP.

A integridade no TKIP é garantida atravé do MIC *(Message Integrity Code)*, que tem a função de evitar ataques do tipo *bit-flipping* aplicados no WEP. O MIC é um campo do quadro 802.11i, calculado a partir de diversas informações contidas no próprio quadro, como, por exemplo, os endereços MAC de origem (SA) e destino (DA). O MIC é calculado a partir de uma função de *hashing*, conhecida como *Michael*. Além do campo MIC, o TKIP implementa um campo de seqüência (SEQ) no quadro 802.11i, para evitar ataques do tipo *replay*. O número de seqüência é incrementado a cada quadro enviado, sendo que o AP irá descartar quadros que estejam fora de ordem enviados por um mesmo cliente. O TKIP utiliza um vetor de inicialização (IV) de 48 bits, ao contrário dos 24 bits utilizados no WEP. Com 48 bits é possível enviar 2^{48} quadros sem que o IV se repita, o que permiti ampliar o tempo de vida da chave temporal, tornando desnecessária a geração de uma nova chave.

2) AES-CCMP: O protocolo CCMP (*CCM Protocol*) utiliza o novo padrão para criptografia simétrica AES (*Advanced Encryption Standard*), aprovado pelo NIST (*National Institute of Standardsand Technology*) em 2002. O AES trabalha com blocos de 128 bits e, no caso do 802.11i, chaves de 128 bits.

O AES trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado. Os modos de operação têm o objetivo de previnir que uma mesma mensagem quando criptografada gere o mesmo texto cifrado. O CCM utiliza o modo de operação conhecido como CBC (*Cipher Block Chaining*). Neste modo de operação, o texto cifrado no passo anterior é utilizado como entrada no processo de criptografia subsequente. No primeiro passo, como ainda não existe um texto cifrado, é utilizado o vetor de inicialização. O CCM é, na verdade, uma combinação de dois modos de operação: o CBC-CTR (*Cipher Block Chaining Counter mode*) e CBC-MAC (*Cipher Block Chaining Message Authenticity Check*), sendo que o CBC-CTR oferece criptografia, enquanto o CBC-MAC oferece integridade.

D. IEEE 802.1X

o padrão IEEE 802.1X foi concebido para oferecer autenticação, controle de acesso e distribuição de chaves criptográficas em redes locais com e sem fio. É importante destacar que o 802.1X não está ligado apenas ao padrão IEEE 802.11, mas a todos os padrões de redes locais e metropolitanas patrocinados pelo IEEE 802. Além disso, o padrão pode ser utilizado em conjunto com diversos protocolos de autenticação localizados nas camadas superiores. O grupo de trabalho 802.11i definiu que o mecanismo de autenticação a ser utilizado no IEEE 802.11 deverá seguir o modelo do IEEE 802.1X. A autenticação no IEEE 802.1X é realizada nos dois sentidos (*mutual autentication*) e utiliza o esquema de *challenge-response*. Existem três componentes a serem considerados no padrão: autenticador, *supplicant* e servidor de autenticação. Em uma rede sem fio, o autenticador é geralmente o AP e o *supplicant* uma estação que deseja conectar-se ao AP. O servidor de autenticação é o verdadeiro responsável por autenticar o *supplicant*, com base nas informações oferecidas por ele. O padrão não especifica qual servidor de autenticação deve ser utilizado, podendo ser, por exemplo, um servidor RADIUS (*Remote Authentication Dial-In User Service*). Na verdade, o servidor de autenticação não precisa ser necessariamente um elemento externo, podendo fazer parte do próprio AP.

O IEEE 802.1X implementa o protocolo EAP (*Extensible Authentication Protocol*), em conjunto com o *EAP over LAN* (EAPOL). O EAP permite o encapsulamento de diversos protocolos de autenticação oferecidos nas camadas superiores e, consequentemente, não definidos pelo 802.1X. Estes protocolos oferecem diferentes métodos de autenticação, como Kerberos, senhas, certificados digitais e chaves públicas. Desta forma é possível que o usuário também seja autenticado e não apenas a estação. O IEEE 802.1X, apesar de ser uma

iniciativa de oferecer autenticação forte, apresenta algumas vulnerabilidades em função de alguns protocolos que fazem parte do padrão.

1) Protocolos de Autenticação: Os protocolos de autenticação mais comuns oferecidos pelas camadas superiores são o EAP-TLS, PEAP, EAP-TTSL e LEAP. É importante perceber, que o AP serve apenas como um meio para que as mensagens cheguem ao servidor de autenticação. Sendo assim, pode-se especificar qualquer mecanismo de autenticação sem a necessidade de alterar-se o AP. A Tabela I apresenta algumas das características dos diversos protocolos de autenticação disponíveis.

O EAP-TLS (*Transport Layer Security*) foi proposto pela Microsoft e hoje é um padrão Internet. O TLS é baseado no SSL (*Secure Sockets Layer*) versão 3.0 e oferece autenticação mútua utilizando certificados digitais e permite geração de chaves criptográficas. Os certificados digitais devem ser configurados individualmente em cada cliente da rede e no servidor de autenticação. O protocolo é suportado por default no MS-Windows XP e pode ser configurado nas demais versões do Windows. Já existem também versões do EAP-TLS para estações Linux e FreeBSD.

O PEAP (*Protected Extensible Authentication Protocol*) ainda está em processo de aceitação no IETF. O *Protect* EAP ofecere autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificados dos clientes. O protocolo foi adotado pela Microsoft no Windows XP e Windows Server 2003.

O EAP-TTLS (*Tunnuled Transport Layer Security*) também está em fase de aceitação pelo IETF. EAP-TTLS é uma extensão do EAP-TLS, pois utiliza a conexão segura TLS para trocar informações adicionais entre cliente e servidor. O EAP-TLS oferece autenticação mútua e unidirecional, na qual apenas o servidor é autenticado.

O LEAP (*Lightweight Extensible Authentication Protocol*) foi desenvolvido pela Cisco Systems e foi um dos primeiros protocolos de autenticação disponível para redes sem fio. O LEAP oferece diversas vantagens, como autenticação mútua, autenticação de usuário por senha e chaves dinâmicas.

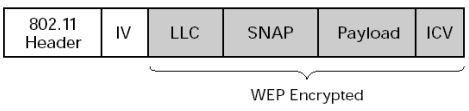

Fig. 28. Quadro WEP. Fonte [11]

XI. IEEE 802.11N

Em resposta à demanda cada vez maior do mercado por redes de área local sem Fio de desempenho superior, o IEEE aprovou a criação do IEEE 802.11 Task Group N (802.11 TGn) na segunda metade de 2003. O escopo do objetivo do TGn é definir modificações para as camadas PHY/MAC que ofereçam uma vazão mínima de 100 megabits por segundo (Mbps) no AP da camada MAC.

Essa exigência de vazão mínima representa um salto de aproximadamente o quádruplo do desempenho da vazão da WLAN, quando comparado às redes atuais do padrão 802.11a/g. O objetivo do TGn nessa próxima etapa do desempenho da WLAN é aprimorar a experiência do usuário com os atuais aplicativos de WLAN e ainda habilitar novos aplicativos e segmentos do mercado. Ao mesmo tempo, o TGn prevê uma transição suave da adoção, exigindo a compatibilidade com versões anteriores nas soluções da tecnologia prévia existente da WLAN do IEEE (802.11a/b/g)

Há três áreas importantes que precisam ser consideradas ao se tratar dos aumentos no desempenho da LAN sem fio. Primeiro, serão necessários aprimoramentos na tecnologia de rádio para aumentar a taxa de transferência física. Segundo, é necessário desenvolver novos mecanismos que implementem o gerenciamento eficaz dos modos de desempenho PHY. Terceiro, são necessários aprimoramentos na eficiência da transferência de dados para reduzir os impactos dos cabeçalhos PHY e atrasos de tempo de resposta via rádio sobre o desempenho, os quais, de outra forma, prejudicariam as otimizações alcançadas com os aumentos na taxa de transferência física.

Ao mesmo tempo, ao desenvolver novas propostas para se alcançar o desempenho, precisa-se da coexistência com os dispositivos da tecnologia prévia do 802.11a/b/g existentes. Todos esses aspectos devem ser tratados ao considerar as implementações práticas e eficazes para os segmentos do mercado sensíveis ao custo.

Uma proposta para aumentar a taxa de transferência física dos sistemas sem fio utiliza sistemas de várias antenas para o transmissor e receptor. Essa tecnologia é conhecida como MIMO (*Multiple-Input Multiple-Output*) ou sistemas de antenas inteligentes. A tecnologia MIMO explora o uso de múltiplos sinais transmitidos para o meio físico sem fio e múltiplos sinais recebidos desse meio, para aumentar o desempenho dos dispositivos sem fio.

A MIMO pode trazer vários benefícios, todos oriundos da possibilidade de processar simultaneamente diferentes sinais no espaço. Dois benefícios importantes explorados aqui são a diversidade de antenas e a multiplexação espacial. Ao usar várias antenas, essa tecnologia permite resolver com coerência as informações procedentes de diversos percursos de sinal por meio de antenas receptoras separadas no espaço. Sinais de vias múltiplas são sinais refletidos que alcançam o receptor algum tempo após o recebimento do sinal original ou sinal da linha de visão (LOS). Geralmente, os múltiplos percursos são percebidos como uma interferência que prejudica a possibilidade de um receptor recuperar a informação inteligente. A tecnologia MIMO permite resolver, conforme o espaço, os sinais de múltiplas vias, propiciando um ganho de diversidade que aumenta a possibilidade de um receptor recuperar a informação inteligente.

Outra oportunidade importante que a tecnologia MIMO pode oferecer é o SDM *(Spatial Division Multiplexing* Acesso Múltiplo por Divisão do Espaço). O SDM multiplexa no espaço diversos fluxos de dados independentes, transferidos simultaneamente dentro de um canal de largura de banda espectral. O SDM da MIMO pode aumentar muito a vazão dos dados à medida que aumenta o número de fluxos de dados espaciais resolvidos. Cada fluxo espacial exige seu próprio par de antenas de transmissão/recepção em cada ponta da trans-

missão. É importante saber que a tecnologia MIMO requer uma cadeia de radiofreqüência (RF) separada e um conversor analógico-digital (ADC *Analog-to-Digital Conversor*) para cada antena MIMO. Em última análise, essa complexidade crescente significa um aumento dos custos de implementação, uma vez que são necessários sistemas de desempenho mais altos.

Outra ferramenta importante que pode aumentar a taxa de transferência PHY são os canais com maior largura de banda. O aumento da largura de banda do canal não é um conceito novo. Pode ser facilmente encontrado na equação da capacidade de Shannon [C = B log2 (1+SNR)], a qual diz que os limites de capacidade teórica ”C”são imediatamente aumentados ao se considerarem os aumentos na largura de banda ”B”ocupada.

XII. Conclusão

Com esse trabalho espera-se contribuir para o melhor entendimento do padrão 802.11. Nessas páginas o leitor tem a sua disposição um detalhamento do padrão 802.11 e suas principais variantes.

O presente trabalho analisou detalhadamente o padrão 802.11, descrevendo sua arquitetura, camada física, e suas três técnicas de espalhamento. A camada MAC, com seus dois modos de operação, foi vista em detalhes. Na seção (III) foi comparado o desempenho do modo DCF e PCF, observando-se que para condições de carga alta, o mecanismo PCF otimiza a utilização da largura de banda do canal e diminui o tempo de espera médio do pacote. Foi estimado um ponto de comutação ótimo DCF-PCF em termos da carga oferecida.

Descreveram-se as melhorias do 802.11 para o aumento das taxas de dados, o 802.11a e 802.11b. Mostrou-se que existe um limite superior da vazão e um limite inferior para o retardo. A existência desses limites mostra que, simplesmente aumentando a taxa de dados sem diminuir o overhead, o acentuado desempenho, em termos do retardo e da vazão, está limitado mesmo quando a taxa de dados aumenta infinitamente. Ou seja, reduzir o overhead é fundamental para o padrão IEEE 802.11 encontrar maiores vazões.

A evolução do 802.11b, o 802.11g, tem seu mecanismo investigado, assim como o desempenho de sua vazão. Foram feitas considerações sobre o tempo de duração do segmento e o mecanismo RTS/CTS mostrou significante impacto no desempenho do 802.11g. O IEEE 802.11 não apresenta bons resultados quando utilizado para a taxa de tráfego multimídia, no que diz respeito à diferenciação e qualidade de serviços. Assim, estudou-se o protocolo IEEE 822.11e, os mecanismos de escalonamento, os serviços integrados e diferenciados e os protocolos da camada MAC.

Ainda analisou-se o problema da segurança em redes sem fio, como é implementada a segurança no padrão IEEE 802.11, além das vulnerabilidades encontradas na sua implentação. Foram apresentados dois novos padrões de segurança para substituir o atual modelo WEP, o 802.11i e 802.1x

Por último comentou-se brevemente o IEEE802.11n que preve fornecer uma vazão minima de 100Mbps

References

[1] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE Standard 802.11, 1999.

[2] Köpsel, A., Ebert, J.-P., and Wolisz, A. A, Performance Comparision of Point and Distributed Coordination Function of an IEEE 802.11 WLAN in the Presence of Real-Time Requirements. In 7th. Intl. Workshop on Mobile Multimedia Communications (MoMuC2000) (Tokyo, Japan, October 2000).

[3] Heusse, M., Rousseau, F., Berger-Sabbatel, G. e Duda, A. (2003). Performance anomaly of 802.11b. Em IEEE INFOCOM 2003.

[4] M-J. Ho, J. Wang, K. Shelby and H. Haisch, IEEE 802.11g OFDM WLAN Throughput Performance, IEEE, pp.2252-2256, 2003

[5] W. E. Leland, M. S. Taggu, W. Willinger, and D. V. Wilson, On the self similar nature of ethernet traffic (extended version). IEEE ACM Transactions on Networking, pp.1-15, 1994

[6] M. Visser and M. Elzaki, Voice and data transmission over an 802.11 wireless network, In proceedings of IEEE personal. Indoor Mobile Radio conf. (PIMRC) 1995. Toronto, Canada, pp.648-652, sept. 1995

[7] S. Kapp, 802.11a More Bandwidth without the Wires, IEEE Internet computing, pp.75-79, aug. 2002

[8] Xiao, Y. e Rosdahl, J. (2002). Throughput and delay limits of ieee 802.11. IEEE Communications Letters, 6(8):355.357, 2002.

[9] C. B. Carvalho and J. F. Rezende, Definindo Critérios no Compartilhamento de Banda em Redes 802.11b sob Degradãção de Performance, Grupo de Teleinformática e Automação (GTA)/Pós-Graduação em Engenharia (COPPE) Universidade Federal do Rio de Janeiro (UFRJ)

[10] R. Maia, Segurança em Redes Wireless 802.11i, Grupo de Teleinformática e Automação (GTA)/Pós-Graduação em Engenharia (COPPE) Universidade Federal do Rio de Janeiro (UFRJ)

[11] http://www.intel.com/portugues/update/contents/wi08041.htm

[12] J. A. Afonso, Acesso Local sem Fios em Redes de Comunicação Escalonamento de Tráfego de Tempo Real em Sistemas de Aquisição de Dados e Controlo, Universidade do Minho, Tese de Doutorado.

[13] www.wirelessbrasil.org

[14] F. C. A. Verissimo, Proposta e avaliação de Protocolos de Acesso Alternativos ao Padrão IEEE 802.11e. Tese de Mestrado, COPPE/UFRJ, Agosto 2005.

[15] B. P. Crow, I.Widjaja, J. G. Kim e P. T. Sakai, IEEE 802.11 wireless local area networks, IEEE Communications Magazine, vol. 35, no. 9, pp. 116126, setembro de 1997.

[16] Rubinstein, M. G., and Rezende, J. F. Qualidade de serviço em redes 802.11. Anais do XX Simpósio Brasileiro de Redes de Computadores (SBRC2002) (Maio 2002).

[17] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 GHz band. IEEE Standard 802.11a, 1999

[18] Y. Xiao, IEEE 802.11E: QoS Provisioning at the MAC Layer. IEEE Wireless Communications (June 2004), 7279.

Danielle Vieira (danielle@ravel.ufrj.br) recebeu o B.Sc. em engenharia de Telecomunicações da Universidade do Estado do Rio de Janeiro em 2004.