UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Proposta de um mecanismo de policiamento de tráfego baseado em *token bucket* para redes IEEE 802.16

Henaldo Barros Moraes

Uberlândia – 2013

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Proposta de um mecanismo de policiamento de tráfego baseado em *token bucket* para redes IEEE 802.16

Dissertação apresentada ao Programa de Pós-graduação em Engenharia Elétrica da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de Mestre em Ciências, submetida em 01 de Março de 2013 à banca examinadora:

Prof. Dr. Paulo Roberto Guardieiro – Orientador (UFU)

Prof. Dr. Márcio Andrey Teixeira - (IFSP)

Prof. Dr. Éderson Rosa da Silva - (UFU)

Proposta de um mecanismo de policiamento de tráfego baseado em *token bucket* para redes IEEE 802.16

Henaldo Barros Moraes

Dissertação apresentada ao programa de Pós-graduação em Engenharia Elétrica da Universidade Federal de Uberlândia, como parte dos requisitos à obtenção do grau de Mestre em Ciências.

Prof. Paulo Roberto Guardieiro, Dr. Orientador	Prof. Alexandre Cardoso, Dr. Coordenador do Curso de Pós-Graduação

Dedicatória

Dedico este trabalho aos meus pais, Joaquim Gabriel e Luzia Barros, que me propiciaram uma vida digna onde eu pudesse crescer, acreditando que tudo é possível, desde que sejamos honestos, íntegros de caráter e tendo a convicção de que desistir nunca seja uma ação contínua em nossas vidas; que sonhar e concretizar os sonhos só dependerá de nossa vontade.

A minha esposa, Luana, que sempre acreditou em mim apoiando os meus sonhos, ideias e aceitando minhas ausências.

Agradecimentos

Agradeço primeiramente a Deus por ter me dado força, saúde e sabedoria até a conclusão deste trabalho.

Ao meu orientador Prof. Dr. Paulo Roberto Guardieiro pela oportunidade que me foi dada de realizar um sonho na minha vida. Obrigado pelos ensinamentos e a paciência transmitida ao longo deste trabalho.

A Meu pai, Joaquim Gabriel de Moraes, e minha mãe, Luzia Barros Moraes, que tanto acreditaram na minha pessoa e tantas oportunidades me ofereceram. Sem o apoio de vocês não teria realizado este trabalho. Com vocês aprendi que na simplicidade podemos conquistar muito com o pouco que temos.

À Faculdade de Engenharia Elétrica da Universidade Federal de Uberlândia pelos recursos oferecidos na execução deste trabalho.

Aos meus colegas do Laboratório de Redes de Computadores que dividiram tantos momentos alegres ao longo do desenvolvimento desta dissertação.

Ao Centro Universitário de Patos de Minas – UNIPAM pelo apoio oferecido durante o desenvolvimento deste trabalho, em especial ao diretor Milton Roberto de Castro Teixeira.

Enfim agradeço a todos que de forma direta ou indiretamente tenham contribuído para realização deste trabalho.

“Embora ninguém possa voltar atrás e fazer um novo começo, qualquer um pode começar agora e fazer um novo fim.”

Chico Xavier

Resumo

Moraes, H, B., P*roposta de um mecanismo de policiamento de tráfego baseado em token bucket para redes IEEE 802.16,* UFU, Uberlândia, Brasil, 2013.

O padrão IEEE 802.16, também conhecido como *WiMAX (Worldwide Interoperability for Microwave Access),* é uma tecnologia promissora responsável por oferecer acesso banda larga sem fio para usuários finais, fixos, móveis e com alta taxa de transmissão de dados. A principal característica fornecida por este padrão aos usuários finais é o provimento de qualidade de serviço (QoS - *Quality of Service*) através de mecanismos de escalonamento, controle de admissão de conexões (CAC - *Control Admission Connection*) e policiamento tanto na estação base (BS - *Base Station*) quanto na estação do assinante (SS - *Subscriber Station*). Como esses mecanismos não são definidos pelo padrão IEEE 802.16 e afetam diretamente o desempenho das redes *WiMAX*, um número considerável de pesquisas focalizando estes tópicos tem sido propostas. Neste contexto é proposto e avaliado nesta dissertação um mecanismo de policiamento de tráfego para o tráfego *uplink* baseado na técnica *token bucket* para controlar o fluxo de dados gerado pelas estações presentes na rede. O mecanismo de policiamento de tráfego é aplicado a todas as classes do padrão IEEE 802.16d. Uma fila de espera foi adicionada ao mecanismo proposto com o objetivo de oferecer aos pacotes das classes nrtPS e BE, que não foram admitidos na rede na primeira oportunidade de transmissão, uma nova possibilidade de serem admitidos. Os resultados obtidos, baseados em modelagem e simulação, permitiram concluir que o mecanismo de policiamento proposto apresenta desempenho satisfatório.

Palavras-chave: IEEE 802.16, WiMAX, Policiamento, QoS.

Abstract

Moraes, H, B., *Proposal of a traffic policing mechanism based on token bucket for IEEE 802.16 networks*, UFU, Uberlândia, Brasil, 2013.

The IEEE 802.16 standard also known as WiMAX (Worldwide Interoperability for Microwave Access) is a promising technology responsible for providing wireless broadband access to end users, fixed, mobile and with high-rate data transmission. The main feature provided by this standard to end users is the provision of quality of service (QoS - Quality of Service) through scheduling mechanisms, connection admission control (CAC - Connection Admission Control) and policing in both the base station (BS - Base station) and the subscriber station (SS - Subscriber Station). As these mechanisms are not defined by IEEE 802.16 and directly affect the performance of WiMAX networks, a considerable number of studies focusing on these topics has been proposed in the areas of scheduling and CAC. In this context it is proposed and evaluated in this work a mechanism for traffic policing based on the token bucket technique for controlling data flow generated by the stations in the network. The traffic policing mechanism is applied to all classes of IEEE 802.16d standard. A temporary storage queue was added to the proposed mechanism in order to offer to the packages of nrtPS and BE classes, which were not admitted to the network transmission at the first opportunity, a new chance of being admitted. Results based on modeling and simulation showed that the proposed policing mechanism has satisfactory performance.

Keywords: IEEE 802.16, WiMAX, Policing, QoS.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ADSL	*Asymmetric Digital Subscriber Line*
AP	*Access Point*
ATM	*Asynchronous Transfer Mode*
BE	*Best Effort*
BPSK	*Binary Phase Shift Keying*
BS	*Base Station*
BWA	*Broadband Wireless Access*
CAC	*Connection Admission Control*
CBR	*Constant Bit Rate*
CI	*CRC Indicator*
CID	*Connection Identifier*
CPS	*Common Part Sublayer*
CRC	*Ciclic Redundancy Check*
CS	*Convergence Sublayer*
DFS	*Dynamic Frequency Selection*
DL-MAP	*Downlink Map*
EC	*Encriptation Control*
EDF	*Earliest Deadline First*
EKS	*Encriptation Key Sequence*
EPON	*Ethernet Passive Optical Network*
ertPS	*Extended Real-Time Polling Service*
FDD	*Frequency Division Duplexing*

FTP	*File Transfer Protocol*
HCS	*Header Check Sequence*
HT	*Header Type*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
ISM	*Industrial Scientific and Medical*
ISP	*Internet Service Provider*
LEN	*Length*
LMDS	*Local Multipoint Distribution*
LOS	*Line of Sight*
LSB	*Least Significant Bit*
MAC	*Medium Access Control*
MIB	*Management Information Base*
MIMO	*Multiple Input Multiple Output*
MMS	*Multimedia Messaging Service*
MPG	*Mecanismo de Policiamento Ghazal*
MRTR	*Minimum Reserved Traffic Rate*
MSB	*Most Significant Bit*
MSTR	*Maximum Sustained Traffic Rate*
NLOS	*Non Line of Sight*
nrtPS	*Non Real-Time Polling Service*
NS-2	*Network Simulator-2*
OFDM	*Orthogonal Frequency Division Multiplexing*
OFDMA	*Orthogonal Frequency Division Multiple Access*

OMNet ++	*Objetive Modular Network Testbed in C++*
PDU	*Protocol Data Unit*
PHY	*Physical Layer*
PMP	*Point to MultiPoint*
PS	*Physical slots*
QAM	*Quadrature Amplitude Modulation*
QoS	*Quality of Service*
QPSK	*Quadrature Phase Shift Keying*
RR	*Round Robin*
RRM	*Radio Resource Management*
RS	*Relay Station*
RSV	*Reserved*
rtPS	*Real-Time Polling Service*
SAP	*Service Access Point*
SC	*Single Carry*
SDU	*Service Data Unit*
SFID	*Service Flow Identifier*
SLA	*Service Level Agreement*
SS	*Subscriber Station*
SSTG	*Subscriber Station Transition Gap*
TCP	*Transmission Control Protocol*
TDD	*Time Division Duplexing*
TDM	*Time Division Multiplexing*
TDMA	*Time Division Multiple Access*

TTG	*Transmit Transition Gap*
UGS	*Unsolicited Grant Service*
UL-MAP	*Uplink Map*
VCI	*Virtual Channel Identifier*
VBR	*Variable Bit Rate*
VoIP	*Voice Over Internet Protocol*
VPI	*Virtual Path Identifier*
xDSL	*Various Digital Subscriber Line Technologies*
WFQ	*Weighted Fair Queuing*
WG	*Work Group*
WiMAX	*Worldwide Interoperability for Microwave Access*
Wi-Fi	*Wireless Fidelity*
WirelessHUMAM	*Wireless High-Speed Unlicensed Metropolitan*
WLAN	*Wireless Local Area Network*
WMAN	*Wireless Metropolitan Area Network*
WPAN	*Wireless Personal Area Network*

Capítulo 1

INTRODUÇÃO

Com o aumento da demanda por acesso residencial e comercial de alta velocidade à Internet, novas tecnologias de redes de acesso banda larga têm surgido no mercado. Comparativamente, as redes de acesso banda larga utilizando a infraestrutura cabeada, tais como fibra óptica, DSL e *Cable Modem* apresentam custo mais elevado e podem ser até mesmo inviáveis do ponto de vista financeiro, para atender áreas rurais e a periferia das grandes cidades. A demanda dos usuários por serviços no que se refere à mobilidade e flexibilidade proporcionou um grande aumento na utilização de tecnologias de comunicação de redes sem fio. Estas tecnologias apresentam várias vantagens em relação às redes cabeadas, no entanto para transmissão de dados, voz e vídeo sobre IP (*Internet Protocol*) os requisitos aumentam, tornando a transmissão um processo bastante desafiador [11], [30].

Dentre as tecnologias citadas o surgimento do padrão IEEE 802.11, comumente conhecido como *WiFi* (*Wireless Fidelity*), pode ser considerado um processo chave para o desenvolvimento das redes de acesso sem fio de "última milha" e ultimamente tem se tornado muito popular e bastante difundido devido aos baixos custos de implantação em termos de infraestrutura, fácil instalação e pouca manutenção. Modificações e novas versões desse padrão foram vistas nos últimos anos com o intuito de melhorar a qualidade do sinal de transmissão. No entanto, ele não foi criado com o objetivo de cobrir regiões metropolitanas, muito menos para alcançar longas distâncias. O padrão IEEE 802.11e foi desenvolvido com objetivo de introduzir suporte a QoS (*Quality of*

Service) para que as WLANs (*Wireless Local Area Network*) possam atender as necessidades das aplicações multimídia e em tempo real. Estes requisitos são fundamentais para atender as necessidades básicas dos usuários finais[12].

Com o objetivo de solucionar os problemas enfrentados pelas tecnologias citadas anteriormente, é que surgiu o padrão IEEE 802.16. Este padrão foi desenvolvido pelo IEEE (*Institute of Electrical and Electronics Engineers*) com a finalidade de padronizar a tecnologia BWA (*Broadband Wireless Access*), e definir a interface aérea e o protocolo de acesso ao meio para redes WMAN (*Wireless Metropolitan Area Network*), fornecendo altas taxas de transmissão para o acesso comercial e residencial à Internet. As redes existentes e que são baseadas neste padrão são comumente denominadas de *WiMAX* em referência a um consórcio denominado *WiMAX Forum.* Este consórcio surgiu por volta do ano de 2001 com a finalidade de certificar os produtos baseados no padrão IEEE 802.16, sendo composto por milhares de membros incluindo operadoras de telecomunicações e companhias fabricantes de dispositivos de sistemas de comunicação [13], [16], [30] e [40].

O padrão IEEE 802.16 define mecanismos de sinalização entre a BS (Base Station) e as SSs (*Subscriber Station*), com o único objetivo de dar suporte às variadas aplicações que podem ser executadas pelas SSs, baseadas em voz, vídeo e dados. No sentido *uplink* e *downlink* os pacotes são associados a um fluxo de serviço específico pela camada de controle de acesso ao meio e um conjunto de parâmetros de QoS é associado a cada fluxo. Neste sentido, aplicações com necessidades distintas podem receber tratamento diferenciado para alcançar o desempenho esperado. A estrutura em

camadas do padrão IEEE 802.16 permite a interoperabilidade com outras tecnologias, tais como as redes ATM e as redes baseadas na arquitetura TCP/IP.

A arquitetura para provisão de QoS definida pelo padrão IEEE 802.16 não define políticas ou mecanismos de escalonamento de pacotes, controle de admissão de conexões e policiamento de pacotes. No entanto, apesar destes mecanismos serem obrigatórios na provisão de QoS, as políticas e algoritmos específicos que devem ser utilizados são deixados em aberto pelo padrão para permitir que os fabricantes de dispositivos de redes possam diferenciar seus produtos [11], [30].

Baseado no fato do padrão IEEE 802.16 não definir os mecanismos para a provisão de qualidade de serviço, neste trabalho propõe-se implementar um algoritmo de policiamento de tráfego no sentido *uplink* na estação do usuário, para atender as classes de serviços definidas pelo padrão IEEE 802.16d. O mecanismo de policiamento proposto se baseia na técnica do *token bucket* para monitorar os pacotes que são gerados pelas aplicações das SSs antes de serem transmitidos pela rede. Ademais, no mecanismo de policiamento proposto uma fila de espera foi adicionada para permitir que pacotes pertencentes as classes nrtPS e BE que não foram admitidos na rede na primeira oportunidade de transmissão por falta de *tokens* no *bucket*, possam ter uma segunda oportunidade de serem enviados.

Este trabalho se concentrou no estudo de mecanismos para prover QoS ao padrão IEEE 802.16 além de apresentar uma proposta de policiamento de tráfego baseada na técnica *token bucket*. Além disso, destacam-se neste trabalho o levantamento bibliográfico e as análises comparativas realizadas com resultados de outros trabalhos relacionados com mecanismos de provisão de QoS. A proposta apresentada está em

acordo com as especificações do padrão IEEE 802.16, sendo capaz de prover QoS as aplicações da rede conforme os estudos de avaliação da proposta. O restante desta dissertação está organizado da seguinte forma:

No Capítulo 2 são apresentadas as principais características presentes no padrão IEEE 802.16, tais como o modo de operação, a arquitetura e o modelo de implementação. São apresentadas as principais limitações do padrão IEEE 802.11 que são superadas pelo *WiMAX*, além disso, é descrito a evolução do padrão IEEE 802.16 desde sua publicação em 2001 até os dias atuais. Na descrição da evolução são apresentadas as principais características, recomendações solicitadas e exigidas que foram publicadas em 2004 quando o projeto do padrão IEEE 802.16d foi concluído. Ademais, é apresentado um resumo detalhado a respeito da arquitetura de funcionamento, onde são especificados os modos de operação, Ponto-Multiponto (PMP – *Point to MultiPoint*) e *Mesh*.

O Capítulo 3 apresenta os principais aspectos referentes à provisão de QoS nas redes do padrão IEEE 802.16. São descritas as classes de serviços especificadas pelo padrão IEEE 802.16 bem como suas principais funcionalidades. Como componentes importantes na provisão de QoS no padrão, os fluxos de serviços são detalhados bem como suas classificações. Para os mecanismos de provisão de QoS no padrão IEEE 802.16 foram apresentadas sucintamente as características de escalonamento, CAC e policiamento. Por fim é apresentado o método *token bucket* que é uma das técnicas mais utilizadas nos algoritmos de policiamento de tráfego.

O Capítulo 4 descreve o problema a ser tratado nesta dissertação e apresenta a solução proposta a qual consiste num mecanismo de policiamento de tráfego

implementado para as SSs com utilização de uma fila de espera. São apresentadas as principais técnicas de policiamento utilizadas, e finalizando são apresentados os principais trabalhos relacionados ao tema desta dissertação e que foram considerados relevantes na melhoria desta pesquisa.

No Capítulo 5 são descritos os procedimentos que foram utilizados para avaliar o desempenho do mecanismo, bem como os resultados obtidos através de simulação. Finalizando, foram apresentados os resultados obtidos através de modelagem e simulação utilizando experimentos variados.

Por fim, no Capítulo 6 são apresentadas ás conclusões gerais a respeito da pesquisa desenvolvida, os resultados obtidos bem como sugestão para estudos futuros relacionados à melhoria dos resultados apresentados nesta dissertação.

Capítulo 2

REDES DE ACESSO BANDA LARGA SEM FIO IEEE 802.16

2.1 - Introdução

Nos últimos anos, a demanda por Internet móvel e aplicações multimídia tem motivado o desenvolvimento de tecnologias de redes de acesso banda larga sem fio [1]. Tradicionalmente, as tecnologias que permitem acesso e navegação em alta velocidade utilizam cabos físicos, e apresentam altos custos de implementação e manutenção, especialmente em áreas rurais e suburbanas [7]. O padrão IEEE 802.16, comumente conhecido como *WiMAX*, surge como uma alternativa extremamente viável para fornecer o acesso à Internet sem fio para a "última milha", em extensas áreas geográficas e regiões de difícil acesso para atender as necessidades de diferentes usuários, com QoS e custo acessível. O padrão IEEE 802.16 permitirá acelerar a introdução da tecnologia de banda larga sem fio no mercado, bem como aumentar o desempenho e a confiabilidade dos serviços oferecidos pelos provedores de acesso. [11].

Baseado neste contexto, o objetivo deste capítulo é apresentar as principais características do padrão IEEE 802.16. Para isso, o conteúdo aqui apresentado está organizado da seguinte maneira: A Seção 2.2 descreve o padrão IEEE 802.16 e suas principais características. A Seção 2.2.1 apresenta a evolução do padrão IEEE 802.16 desde a sua publicação até a última versão. A Seção 2.3 relata a arquitetura de rede utilizada pelo WiMAX e suas principais características. A Seção 2.4 descreve de forma

detalhada o modelo de referência do padrão IEEE 802.16, mostrando as principais funções de cada uma das subcamadas pertencente à camada MAC. A Seção 2.5 descreve os detalhes da camada física, e a Seção 2.6 finaliza com considerações finais a respeito do assunto abordado neste capítulo.

2.2 - Padrão IEEE 802.16

O padrão IEEE 802.16 é uma das tecnologias mais promissoras, atualmente, para redes de acesso de banda larga sem fio, sendo uma solução bastante atrativa em relação às tecnologias de banda larga cabeada, tais como: as linhas de assinantes digitais assimétricas (ADSL – *Asymetric Digital Subscriber Line*), *Cable Modem* ou E1. O padrão IEEE 802.16 veio para consolidar o conceito de WMAN, e para isto precisa apresentar altas taxas de transmissão em área extensa para um grande número de usuários.

O padrão IEEE 802.11 chamado de *WiFi* foi projetado para redes locais em pequenas localidades e apresenta várias limitações com relação a seus concorrentes diretos. Por isso, mesmo possuindo bons projetos para expansão de área de cobertura, este padrão possui diversos problemas, tais como: conexão entre os pontos de acesso ou APs (*Access Points*) de diferentes fabricantes, segurança, QoS e serviços limitados [12].

É baseado neste contexto que surge o *WiMAX* para suprir estas carências com altas taxas de transmissão, baixos custos e qualidade superior em praticamente todos os aspectos relacionados à "última milha" e longo alcance, podendo apresentar uma plataforma comum para o transporte de dados, voz, imagem e vídeo com segurança e QoS em um ambiente sem fio. O padrão IEEE 802.16 é capaz de prover acesso á Internet com altas taxas de transferência de dados, alto nível de escalabilidade e baixo

custo de manutenção para acesso residencial, comercial ou rural [19]. O padrão IEEE 802.16 é um conjunto de padrões de tecnologias de telecomunicações destinados a prover acesso à longa distância sem fio sobre dois modos, podendo ser em uma conexão Ponto-a-Ponto ou senão em uma conexão PMP, conforme pode ser visto na Figura 2.1 [9].

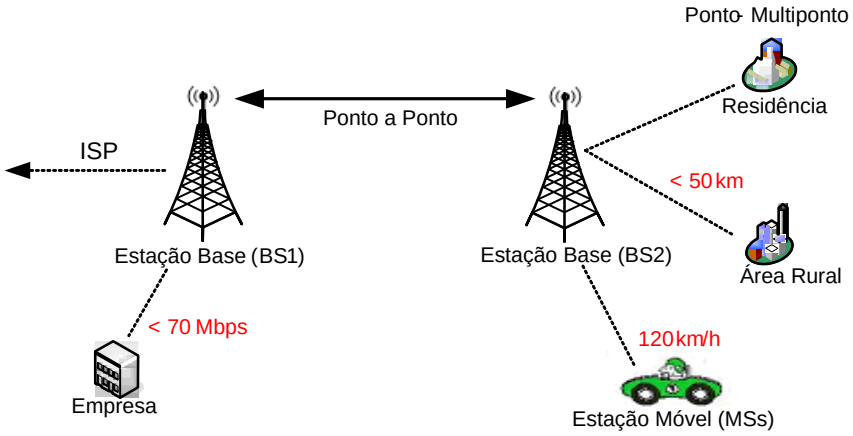

Figura 2.1: Modelo de implementação do *WiMAX*.

O *WiMAX* Fórum é um consórcio formado por várias corporações que foi criado no ano de 2001 para dar suporte às tecnologias *WiMAX* e promover o uso comercial deste padrão. É responsável pelos testes de interoperabilidade para assegurar que as implementações de diferentes fabricantes possam ser compatíveis entre si. A primeira versão do padrão IEEE 802.16 foi publicada em 2001 e, desde então, várias outras têm surgido tratando de questões tais como: operação sem linha de visada (NLOS - *NON Line of Sight)*, mobilidade, classes de serviço e operação em banda licenciada e não licenciada [10].

2.2.1 - Evolução do Padrão IEEE 802.16

O IEEE 802.16-WG é o grupo de trabalho responsável pelo desenvolvimento, documentação e definição das recomendações para o padrão IEEE 802.16. Para melhoria deste padrão, várias recomendações solicitadas e exigidas foram elaboradas, documentadas, e publicadas finalmente em 2004, quando o projeto do padrão IEEE 802.16 foi concluído. A família de padrões que compõe a tecnologia *WiMAX* é descrita a seguir [5], [14] e [16].

802.16: Esta versão foi concluída no ano de 2001, mas foi publicada somente no ano de 2002, sendo projetada para acessos fixos e locais em sistema de distribuição multiponto (LMDS - *Local Multipoint Distribution System*) utilizando faixas de frequências de 10 a 66 GHz e exigindo linha de visada (LOS - *Line of Sight*). A camada física apresentava apenas uma especificação com uma única portadora e topologia do tipo Ponto-Multiponto.

802.16a: Publicada em 2003, esta normalização fez algumas alterações nas especificações da camada física e camada de acesso ao meio (MAC - *Medium Access Control*), sendo que na camada física foram incluídas especificações permitindo tecnologias de múltiplas portadoras. A partir desta recomendação passou-se a permitir frequências na operação não licenciada de 2 a 11 GHz, ocasionando competição com as tecnologias que fornecem acesso para usuários residenciais, tais como o *Cable Modem* e *xDSL*. Além disso, propôs oferecer taxas de transmissão teóricas de até 100 Mbps e alcance máximo de até 50 km utilizando antenas estacionárias sem linha de visada entre as estações do assinante (SS - *Subscriber Station*) e as estações base (BS - *Base*

Station). Esta versão permite topologia do tipo *Mesh*, onde as SSs podem funcionar como repetidoras transferindo informações da BS para outras SSs.

802.16c: Trata da interoperabilidade entre os dispositivos de diferentes fabricantes que operam em faixas de frequências entre 10 e 66 GHz com linha de visada.

802.16d: Este padrão foi ratificado em junho de 2004, sendo conhecido como *WiMAX* fixo ou Nomádico. Dentre as alterações presentes pode-se destacar a provisão de suporte as antenas de múltiplas entradas e múltiplas saídas (MIMO - *Multiple-Input Multiple-Output*), o que possibilita o aumento da confiabilidade quanto ao alcance em multipercurso e suporte a tipos de camadas físicas adicionais, tais como: multiplexação por divisão na frequência ortogonal (OFDM - *Orthogonal Frequency Division Multiplexing*) e acesso múltiplo por divisão na frequência ortogonal (OFDMA - *Orthogonal Frequency Division Multiple Access*). Esta versão permite a concatenação das unidades de dados do protocolo (PDUs - *Protocol Data Units*) com as unidades de dados de serviço (SDUs - *Service Data Units*), permitindo com isso a redução de *overhead* na camada MAC. Apresenta um alcance de 8 a 12 km de cobertura com sinalização do tipo NLOS, podendo chegar até 50 km com sinalização do tipo LOS e atingir uma taxa de transmissão de até 70 Mbps. Pode ser considerado o primeiro concorrente direto das tecnologias banda larga cabeadas em regiões onde o acesso via cabo metálico é prejudicado pela topografia. É a primeira versão capaz, verdadeiramente, de fornecer acesso para usuários em zonas rurais e de difícil acesso.

802.16e: Foi ratificado em Dezembro de 2005, sendo o primeiro padrão a introduzir totalmente a mobilidade, e por isso é conhecido como *WiMAX* móvel. Este padrão apresenta compatibilidade com as especificações do padrão IEEE 802.16 e as

especificações de mobilidade em WMANs, além de oferecer suporte a dispositivos para operar na faixa de frequências entre 2 e 6 GHz, e permitir a realização de *Handoff* a uma velocidade média de até 100 km/h.

802.16f: Responsável pelas definições da base de informações de gerenciamento ou MIB (*Management Information Base*), sendo esta uma base de dados responsável pelo gerenciamento de todos os dispositivos da rede.

802.16g: Outro padrão que descreve suporte a mobilidade.

802.16h: Descreve o suporte a contenção de acesso ao meio que permite a operação em bandas para indústria médica e científica ou ISM (*Industrial Scientific and Medical*) na faixa de 2,4 GHz e 5,8 GHz.

802.16i: Inclui o conceito de base de informação de gerência que especifica quais variáveis são mantidas pelos elementos da rede.

802.16j: Especifica as operações de retransmissões e a interoperabilidade entre as estações retransmissoras ou RS (*Relay Station*) e a BS.

802.16m: O padrão IEEE 802.16m é projetado para prover melhorias significantes de desempenho comparado com outros sistemas de redes celular em banda larga. Opera com taxa de 100 Mbps para estações móveis e 1Gbps para estações fixas. O Acesso ao enlace é rápido devido ao uso de um super quadro.

2.3 - Arquitetura de Rede

O padrão IEEE 802.16 foi desenvolvido com objetivo de oferecer acesso banda larga sem fio em áreas geográficas extensas bem como um meio para a interligação de redes heterogêneas. A arquitetura de uma rede que utiliza o padrão IEEE 802.16 é composta basicamente de uma estação base e várias estações de assinantes, conforme

pode ser visto na Figura 2.2. A BS é interconectada ao provedor de serviços de Internet através de uma rede cabeada, passando a ser a responsável pelo fornecimento de serviços de Internet às estações que estão sob o seu raio de cobertura.

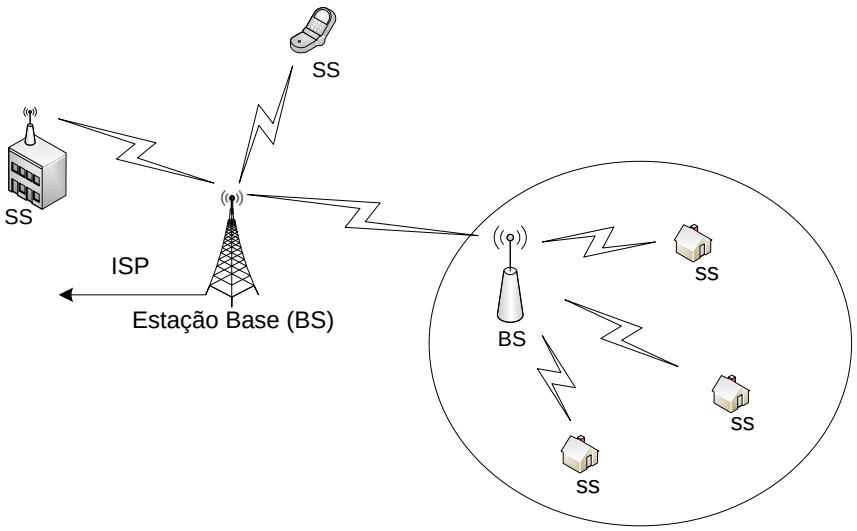

Figura 2.2: Arquitetura de uma rede padrão IEEE 802.16.

A BS interopera com redes IP, ATM, *Ethernet* e E1/T1. A SS é a responsável por permitir acesso dos clientes à Internet através do estabelecimento de conexão com a BS em uma topologia PMP ou *Mesh*. O padrão IEEE 802.16 especifica dois modos de operação para definir como as SS irão se comunicar na rede. O modo mais utilizado é o PMP, sendo que neste caso os recursos disponíveis serão compartilhados entre as SSs e o tráfego de dados ocorre apenas entre BS e SS. O segundo modo de operação é o malha ou *Mesh*, onde o tráfego de dados pode ser roteado através das SSs ou ocorrer diretamente entre duas estações clientes [11], [25]. Nas seções a seguir são apresentadas as principais características dos modos de operação anteriormente citados do padrão IEEE 802.16.

2.3.1 - Modos de Operação

2.3.1.1 - Ponto-Multiponto

Uma rede com topologia PMP é composta por uma BS e de uma ou várias SSs. A BS é provida de antenas setorizadas de forma que possa realizar o tratamento simultâneo da comunicação com as estações dos usuários localizadas nos múltiplos setores [1]. Esta arquitetura, comparada com a *Mesh*, apresenta redução de custos e facilidade na adição de novos usuários. No enlace de *downlink*, todas as estações de assinantes que estiverem em um determinado setor e utilizam um determinado canal de rádio frequência, recebem a mesma transmissão. Neste modo de operação as mensagens podem ser direcionadas pela BS para todas as SSs que pertencerem ao mesmo setor, normalmente este tráfego é vindo do provedor de serviços de Internet (ISP – *Internet Service Provider)*. Este processo de envio é denominado de *broadcast*, e cada SS precisa capturar e processar apenas o tráfego endereçado a ela [20]. A Figura 2.3, adaptada de [25], descreve a topologia PMP.

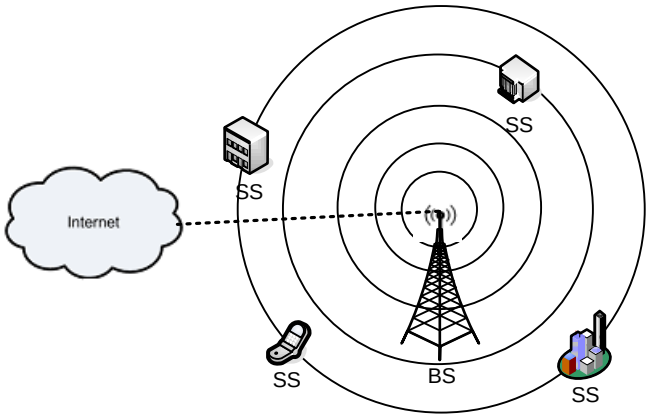

Figura 2.3: Topologia Ponto-Multiponto.

A BS é responsável pelo controle e coordenação da comunicação com todas as SSs da rede. Em ambientes rurais o acesso é tipicamente do tipo LOS, porém em áreas urbanas as conexões podem ser do tipo NLOS.

2.3.1.2 - Topologia Mesh

As redes *Mesh* surgem como uma alternativa às restrições impostas pelo modo de operação PMP, pois oferece maior flexibilidade e eficiência de expansão de comunicação. Diferentemente do modo de operação PMP, onde uma SS se comunica somente com a BS, nas redes *Mesh* todas as SSs apresentam uma conexão redundante para outras SSs da rede podendo funcionar como um *Access Point*, conforme pode ser visto na Figura 2.4. Neste modo de operação não existe a necessidade de investimento em infraestrutura extra para prover escalabilidade, uma vez que com a existência de conexões redundantes entre as SSs a área de cobertura é automaticamente ampliada.

Os aspectos de roteamento existente entre as SSs são fundamentais no sentido de permitir que uma SS específica encontre a melhor rota de comunicação com as outras SSs da rede. Dentro de uma rede *Mesh*, um sistema que possui uma estação com conexão direta para interligar serviços para fora da rede é denominada estação base *Mesh*, e apresenta um processo de comunicação mais complexo. Apesar de ser considerada mais complexa, a topologia *Mesh* se mostra mais adequada para os sistemas de telecomunicações sem fio atuais, visto que não impõe limitações quanto a posição das estações nem requer equipamentos adicionais para funcionar em ambientes que apresentam dificuldades na propagação do sinal [15].

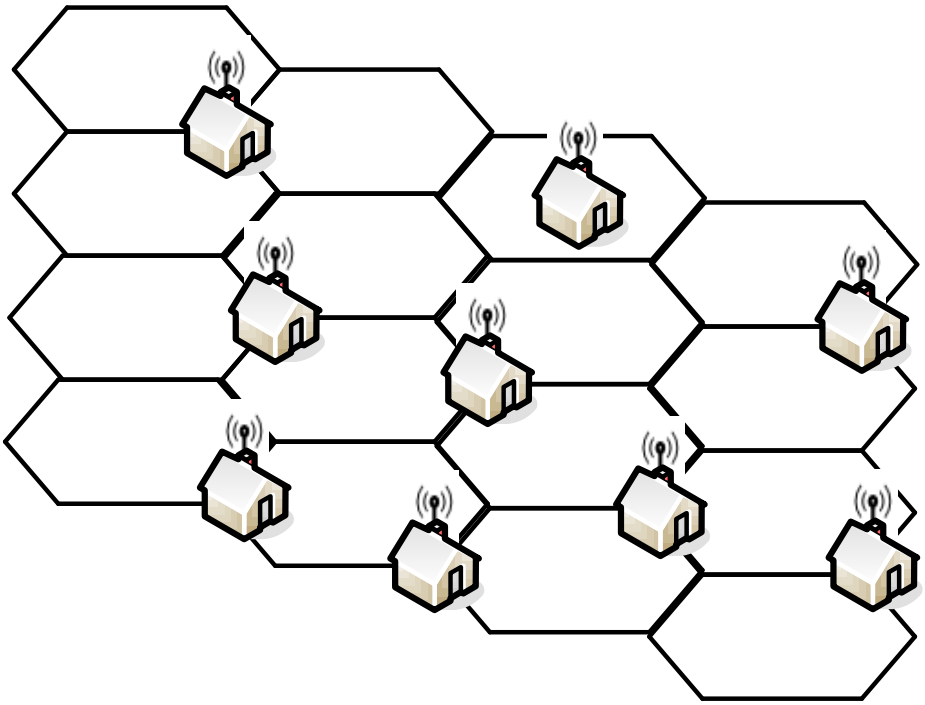

Figura 2.4: Topologia Mesh (adaptado de [15]).

A vantagem da topologia *Mesh* em relação à PMP é que ela não possui um único ponto de falha e se houver algum problema que impossibilite a BS de rotear o tráfego, as SSs podem transmitir os dados, entre elas se tornando uma opção de roteamento de tráfego para a célula. No entanto esta topologia apresenta problemas de latência, pois com o aumento do número de saltos, entre origem e destino, pode ocorrer a degradação da QoS das aplicações sensíveis á latência que surge, tais como tráfego de voz.

2.4 – Modelo de Referência do Padrão IEEE 802.16

O modelo de referência do padrão IEEE 802.16 que é empregado tanto na BS quanto na SS é ilustrado na Figura 2.5 [15]. O padrão IEEE 802.16 é baseado no modelo OSI (*Open Systems Interconnection*) e define a camada MAC e uma camada física (PHY - *Physical Layer*) para redes de banda larga de acesso fixo e móvel para

possibilitar o acesso à Internet em banda larga sem fio e interconectar com outros padrões de redes [30], [39]. Segundo [15], os principais componentes do modelo de referência responsáveis em organizar as funções dentro das duas camadas citadas são: Plano de Dados, Plano de Controle e Plano de Gerência.

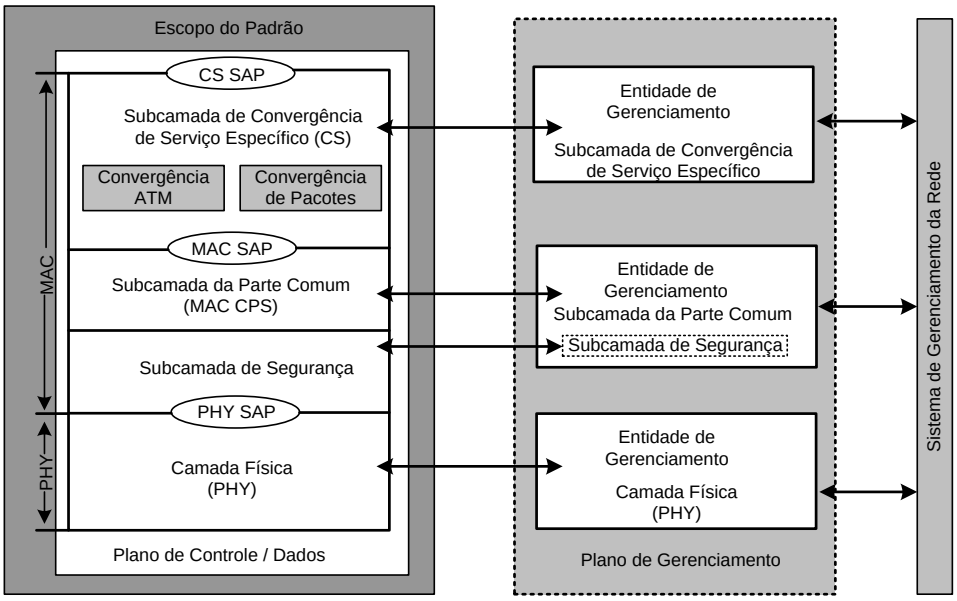

Figura 2.5: Modelo de referência do padrão IEEE 802.16.

O plano de dados define a forma como as informações dos usuários irão ser transportadas pela rede. O plano de controle apresenta as funções de controle de admissão de conexão, controle de recursos, controle de congestionamento e balanceamento de carga. O plano de gerenciamento apresenta as funções de engenharia de tráfego e monitoração de parâmetros de rede. Tanto o plano de dados como o de controle são desempenhados automaticamente pela rede e o plano de gerenciamento é executado pelo administrador da rede.

2.4.1 - Camada de Controle de Acesso ao Meio

A camada MAC é uma interface que está localizada acima da camada física no modelo de referência do padrão IEEE 802.16, cuja função é prover uma interface entre as camadas superiores e a camada física com objetivo de possibilitar a transferência de dados. No padrão IEEE 802.16, a camada MAC é projetada para dar suporte principalmente à topologia PMP, porém o modo *Mesh* tornou necessário o suporte a várias camadas físicas diferentes operando simultaneamente. A camada MAC possui as funções de controle de acesso, que determinam quais estações podem acessar o meio físico, garantias de QoS através de mecanismos de alocação dinâmica de recursos, e finalmente, atribuição de prioridade de tráfego. Outras funções desta camada são a multiplexação dos fluxos de tráfego em conexões, escalonamento e suporte na segurança de comunicação. O protocolo MAC lida com altas taxas de *bits*, tanto para *downlink* quanto para *uplink* e os algoritmos de acesso e alocação de banda podem reservar centenas de terminais por canal para que vários usuários possam fazer o compartilhamento do mesmo [8], [17] e [18]. A estrutura da camada MAC do padrão IEEE 802.16 com suas subcamadas e funções especificas pode ser vista na Figura 2.6.

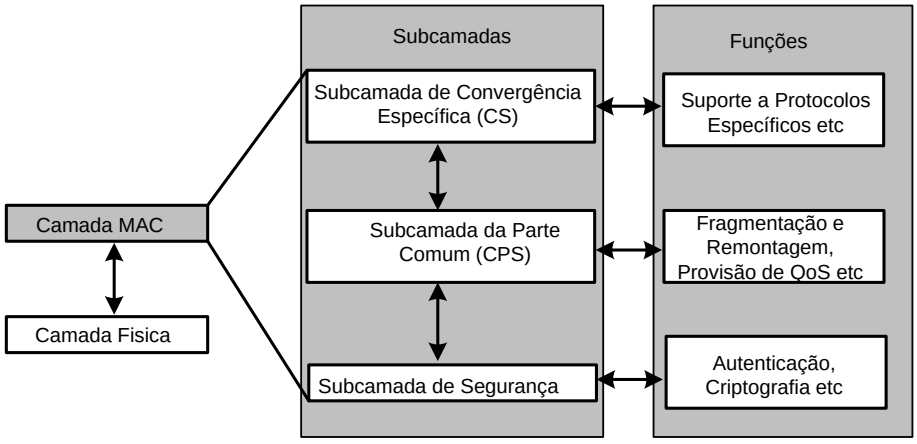

Figura 2.6: Subcamadas do padrão IEEE 802.16 e suas funções.

2.4.2 - Subcamada de Convergência Específica

A subcamada de convergência específica (CS - *Specific Convergence Sublayer*) de pacotes está localizada acima da subcamada da parte comum (CPS - *Commom Part Sublayer*) sendo a responsável pela interface entre a rede externa e a camada MAC. Os pacotes que chegam da rede externa são mapeados e recebidos através do ponto de acesso ao serviço ou CS-SAP (*Service Access Point*) em SDUs específicas para o padrão IEEE 802.16, e que serão recebidas na CPS através do MAC-SAP. Dentre os serviços oferecidos pela camada CS podem ser citados [15]:

- Classificação das PDUs das camadas superiores;
- Entrega das CS PDUs resultante para o MAC SAP associado com o fluxo de serviço para o transporte ao MAC SAP da entidade par;
- Recebimento da CS PDU a partir do MAC SAP das entidades pares;
- Classificação das SDUs e associação com o identificador do fluxo de serviço (SFID - *Service Flow Identifier*) e ao identificador de conexão (CID - *Connection Identifier*) apropriado.

A camada CS ao receber um pacote faz a remoção de algumas informações que são redundantes e que estão contidas no cabeçalho. Posteriormente este pacote é classificado num fluxo de serviço específico de acordo com sua classe de serviço para facilitar o processo de provisão de QoS. Para prover este serviço, a CS necessita de várias especificações para tratar de maneira diferenciada os pacotes de acordo com o protocolo utilizado, para que todo o tráfego seja adequado num só formato. Neste sentido o padrão IEEE 802.16 define atualmente duas especificações para a subcamada de convergência específica: Subcamada de Convergência ATM ou ATM CS e

Subcamada de Convergência de Pacotes ou (CS *Packet*), conforme pode ser visto na Figura 2.7, adaptado de [15].

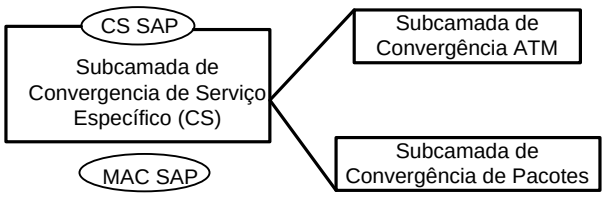

Figura 2.7: Subcamadas de convergência ATM e de pacotes.

A subcamada de convergência ATM é uma interface lógica que associa diferentes serviços ATM juntamente com seus parâmetros de conexão, como o identificador de caminho virtual (VPI - *Virtual Path Identifier*) e o identificador de canal virtual (VCI - *Virtual Channel Identifier*), e com a subcamada de convergência comum a fim de que os requisitos de QoS sejam garantidos [15].

A subcamada de convergência de pacotes ou *CS Packet* é responsável pela compatibilidade entre uma rede *WiMAX* com qualquer outra rede baseada em comutação por pacotes, pois permite que exista uma troca de dados entre as camadas independentemente do protocolo que está sendo utilizado [15].

Além das funções, anteriormente citadas, as subcamadas de convergência ATM e de pacotes podem realizar funções mais complexas, tais como: supressão e a reconstrução de cabeçalho da carga útil para melhorar a eficiência do *link*.

2.4.3 - Subcamada da Parte Comum

A CPS constitui a segunda camada do padrão IEEE 802.16, está localizada entre a subcamada CS e a subcamada de segurança. Esta camada faz o tratamento das funcionalidades centrais da camada MAC, podendo ser destacadas as seguintes:

- Fragmentação e remontagem dos pacotes;
- Alocação de largura de banda;
- Estabelecimento de Conexão, e;
- Manutenção das conexões entre os lados origem e destino.

A CPS inclui vários procedimentos para QoS e gerenciamento dos recursos do *link* (RRM - *Radio Resource Management*). A comunicação entre a CS e a MAC CPS é mantida pelo MAC SAP. Todos os serviços na camada MAC são mapeados para uma conexão, caracterizando a CPS como orientada a conexão.

Cada estação que entra na rede possui um endereço MAC universal de 48 *bits*, que é único e define a estação dentro de um conjunto de equipamentos e fabricantes. Este endereço é usado durante o processo de definição de largura de banda para estabelecer as conexões apropriadas, e como parte do processo de autenticação, onde a BS e a SS verificam suas autenticidades. As conexões são endereçadas através de CID com 16 *bits*, e podem necessitar de largura de banda fornecida constantemente ou senão de acordo com a demanda [15], [17].

A CPS é responsável pela criação da MAC PDU que será transmitida para sua entidade par. O tamanho máximo da MAC PDU é de 2048 *bytes* sendo que cada pacote padrão MAC consiste de um cabeçalho de tamanho fixo (6 *bytes*), um *payload* opcional de tamanho variável e um código de redundância cíclica (CRC - *Ciclic Redundancy Check*) opcional (4 *bytes*). O padrão IEEE 802.16 especifica os cabeçalhos da MAC PDU, que são distinguidos pelo campo tipo de cabeçalho (HT - *Header Type*) e podem ser do tipo genérico ou de requisição de banda. O formato genérico do cabeçalho da MAC PDU é visto na Figura 2.8 [17].

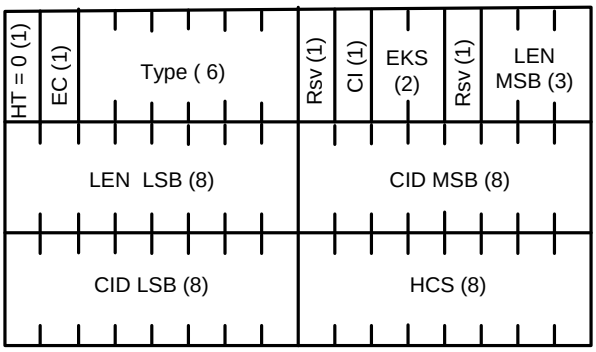

Figura 2.8: Formato do cabeçalho genérico da MAC PDU.

Para o cabeçalho do tipo genérico (HT = 0), tem-se a presença de um *payload* qualquer na PDU, enquanto com HT = 1, indica que o cabeçalho é de requisição de banda. Em seguida o cabeçalho apresenta o campo de controle de criptografia (EC - *Encriptation Control*) que é o responsável por indicar se o *payload* será ou não criptografado. O campo *Type* informa o tipo de carga que está sendo carregado pelo *payload*, podendo os valores deste campo variar de "0" a "5". Os campos Rsv, de 1 bit cada um, são reservados para uso futuro. O campo indicador do CRC (CI - *CRC Indicator*) informa se existe (CI = 1) ou não (CI = 0) um CRC no final da MAC PDU. O campo de sequência de chaves de criptografia (EKS - *Encriptation Key Sequence*) informa o tipo de chave que foi utilizada na criptografia, sendo usada para PDUs com EC = 1. O campo LEN (*Length*), informa o tamanho total do quadro da MAC PDU. Já o campo identificador de conexão ou CID, identifica as conexões atribuídas pela BS. E por fim, o campo sequência de checagem de cabeçalho (HCS - *Header Check Sequence*) é responsável por detectar possíveis erros presentes no cabeçalho [18].

Além das especificações citadas anteriormente, na camada CPS são implementados os mecanismos para a requisição de largura de banda que são especificados pelo padrão IEEE 802.16. O padrão define intervalos de *polling*

periódicos nos quais as SSs podem requerer largura de banda individualmente através do campo *type.* As mensagens de requisição de banda também podem ser enviadas através dos dados transmitidos no sentido *uplink,* sendo este processo denominado de *piggyback.*

2.4.4 - Subcamada de Segurança

Com o grande crescimento da demanda por redes sem fio, as questões relativas à segurança têm aumentado nas mesmas proporções. No geral as redes sem fio são pouco seguras devido à falta de infraestrutura física, e neste caso uma atenção especial deve ser dada aos aspectos de segurança. Estas redes são mais vulneráveis com relação a acessos indevidos e aos dados que trafegam, necessitando por isso de mecanismos que garantam maior segurança. Com o aumento da popularidade da Internet banda larga sem fio, o mercado para novas tecnologias de redes tem aumentado na mesma proporção, e o *WiMAX* é uma tecnologia emergente de redes banda larga, WMAN, que chega para suprir problemas existentes nos outros padrões de redes sem fio.

Como a parte de segurança do padrão IEEE 802.11 foi desenvolvida após a publicação da versão inicial, este padrão apresenta muitas vulnerabilidades. No padrão IEEE 802.16, porém, a segurança foi considerada como ponto essencial durante os projetos de protocolos, mas alguns pontos ainda precisam ser resolvidos quando se trata de riscos e vulnerabilidade em situações reais. Para atender estes requisitos, o padrão IEEE 802.16 especifica uma subcamada de segurança, localizada logo abaixo da CPS da MAC. Esta subcamada é responsável pelo controle de e criptografia, com o intuito de prover segurança no nível de enlace.

A subcamada de segurança oferece as estações comunicantes, uma grande proteção contra roubo de informações, e a BS é responsável pela proteção contra os acessos não autorizados aos serviços de transporte de dados. Esta subcamada emprega um protocolo de gerenciamento de chave cliente/servidor autenticado, onde a BS é responsável por controlar a distribuição de chaves aos clientes. A subcamada de segurança define um protocolo de encapsulamento para criptografar os pacotes de dados que trafegam por uma rede do padrão IEEE 802.16. Ademais, também é responsável por definir um conjunto de normas de criptografia, algoritmos de autenticação e regras para aplicar os algoritmos na carga útil das MAC PDUs [15], [22].

2.5 - Camada Física

O principal propósito da camada física do padrão IEEE 802.16 é o transporte físico de dados gerados nas camadas superiores em forma de *bits* entre as estações da rede. Pode-se destacar ainda, dentre suas funções, as seguintes características:

- Definição das técnicas de transmissão digital: Modulação e Codificação;
- Definição do espectro;
- Correção de erro;
- Definição da técnica de duplexação; e
- Construção dos *frames* e *subframes* de transmissão.

No padrão IEEE 802.16 a camada física opera em duas faixas de frequência, sendo que na faixa de 2 a 11 GHz existem 4 especificações para WirelessMAN e uma para WirelessHUMAM (*Wireless High-Speed Unlicensed Metropolitan Area Network*). As especificações variam com os seguintes parâmetros [21]:

- Faixa do espectro – é permitido operações nas faixas de 10 a 66 GHz licenciadas, e faixas abaixo de 11 GHz licenciadas e não licenciadas com restrição de potência e utilização de seleção dinâmica de frequência (DFS - *Dynamic Frequency Selection*) que evita interferência;
- Propagação de sinais - existe a possibilidade de operação em sistemas LOS e NLOS, dependendo do comprimento de ondas e das aplicações;
- Tipo de aplicação – dependendo da aplicação será necessária a utilização de determinada tecnologia como, por exemplo, para as redes *Mesh* são possíveis apenas as especificações WirelessMAN – OFDM e WirelessHUMAN.

As especificações da camada física estão divididas de acordo com a tecnologia de portadora utilizada: Portadora Simples (SC - *Single Carry*) ou OFDM. As especificações baseadas na tecnologia SC utilizam apenas uma portadora, enquanto aquelas baseadas no OFDM utilizam várias portadoras ortogonais entre si. Em 2004, foi publicada a versão do IEEE 802.16-2004 que acrescenta as características do padrão IEEE 802.16a e especifica as regras para interoperabilidade nas frequências até 66 GHz [24]. Cinco tipos de camada física que podem ser utilizadas em conjunto com a camada MAC são especificadas nesta versão e são divididas como se segue [18]:

- WirelessMAN-SC – versão com portadora única. Foi projetada para operação em frequências entre 10 e 66 GHz, com linha de visada direta, sendo que nesta faixa de frequência não existe suporte a propagação sem linha de visada. Permite operação nas configurações: duplexação por divisão no tempo (TDD - *Time Division Duplexing*) e duplexação por

divisão da frequência (FDD - *Frequency Division Duplexing*). Em ambas as configurações, os parâmetros de transmissão, como os esquemas de modulação e codificação, podem ser definidos para SS a cada novo frame;

- WirelessMAN-SCa – esta especificação utiliza modulação de portadora única na frequência de 2 a 11 GHz, sendo direcionada para operações do tipo NLOS, tais como: estrutura de quadros robusta a multi percurso, estimativa e equalização de canal, modulação adaptativa, múltiplos esquemas de codificação, antenas adaptativas, diversidade de transmissão e controle de potência. Esta especificação deve suportar configurações TDD e FDD;
- WirelessMAN-OFDM – é baseada na tecnologia OFDM e projetada principalmente para SSs fixas em residências e/ou escritórios. Opera sem linha de visada com frequência abaixo de 11 GHz. Suporta topologia *Mesh* e subcanalização no *uplink* com 16 subcanais. O controle de acesso ao meio é através da técnica de acesso multiplo por divisão no tempo (TDMA - *Time Division Multiple Access*). Os tipos de modulação suportados são BPSK, QPSK, 16-QAM e 64-QAM. Esta interface aérea é obrigatória em bandas não licenciadas;
- WirelessHUMAM – inclui funcionalidades para operação em bandas não licenciadas na faixa espectral entre 5 e 6 GHz. Esta especificação da camada física permite a utilização de 200 canais com frequências centrais separadas por 5 MHz com canais de 10 e 20 MHz de largura.

- WirelessMAN-OFDMA – é baseada na tecnologia de múltiplas portadoras OFDM com uma transformada de 2048 subportadora e suporta a estrutura de frame TDD e FDD. Realiza subcanalização dos enlaces no sentido *uplink* e *downlink*, permitindo com isso que mensagens sejam trocadas ao mesmo tempo. Projetado para faixas de frequência inferiores a 11 GHz e operação NLOS.

A camada física opera num formato de *frames* e a duração de cada um pode variar de 0,5 a 20 ms dependendo da tecnologia em uso. Os *frames* são divididos em intervalos de tempo chamado *slots* físicos. A quantidade de *slots* físicos (PS - *Physical Slots*) em um *frame* é uma função da taxa de símbolo e da duração do *frame*.

O acesso ao meio físico pode ser feito sobre duas maneiras: FDD ou TDD. No modo FDD, Figura 2.9 [15], os canais de *uplink* e *downlink* operam em frequências diferentes e de forma simultânea.

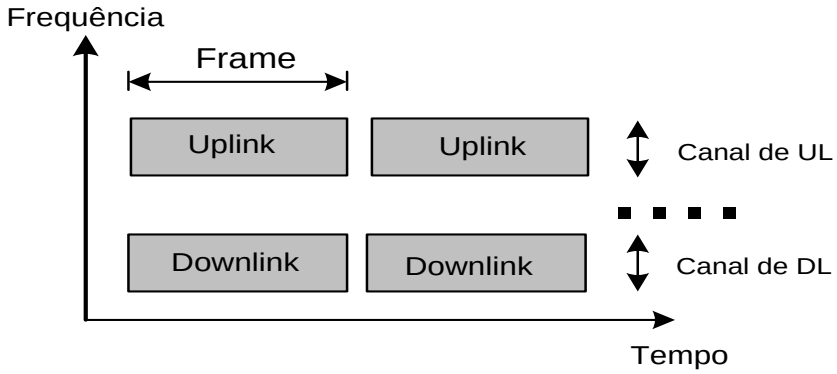

Figura 2.9: Estrutura do frame FDD.

Diferentemente do modo FDD, no modo TDD os subframes de *uplink* e *downlink* compartilham a mesma faixa de frequência, porém cada um faz sua transmissão em tempos diferentes. Cada *frame* é dividido em 2 *subframes*: *downlink* e

uplink. O subframe de *downlink* é utilizado pela BS para o envio de dados e informações de controle para as SSs, e o subframe de *uplink* é compartilhado entre todas as SSs. A estrutura do *frame* TDD apresenta um subframe de *downlink* seguido por um subframe de *uplink*, conforme pode ser visto na Figura 2.10 [15], [11].

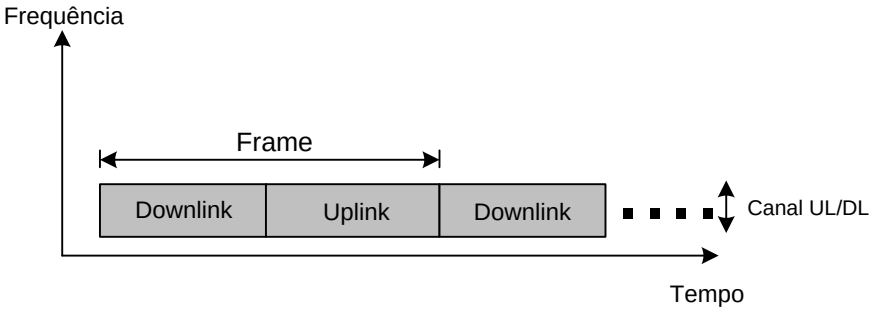

Figura 2.10: Estrutura do frame TDD.

2.5.1 - Subframe Uplink

A estrutura do *subframe* de *uplink* utilizado pelas SSs para realizar transmissões para BS é mostrado na Figura 2.11 [18].

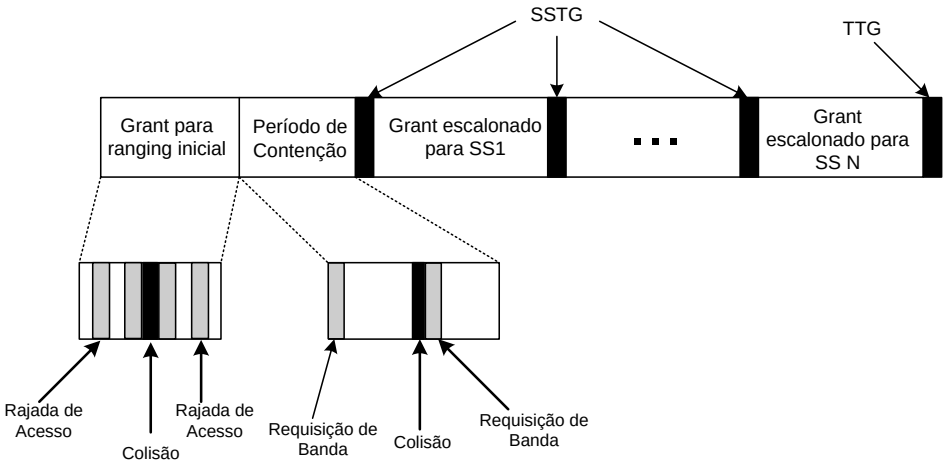

Figura 2.11: Estrutura do subframe *uplink*.

Três tipos de rajadas podem ser transmitidas pelas SSs durante o subframe de *uplink*.

- Aquelas que são transmitidas em *slots* de contenção reservados para *ranging* inicial;
- Aquelas que são transmitidas em *slots* de contenção reservado para mensagens de requisição de banda;
- Aquelas que são transmitidas em intervalos definidos e alocados individualmente para as SSs realizarem transmissões no sentido *uplink.*

Essas rajadas podem ocorrer em qualquer quantidade e em qualquer ordem no *frame*, a critério do escalonador de *uplink* da BS.

2.5.2 - Subframe Downlink

A estrutura do subframe *downlink* do padrão IEEE 802.16 é apresentado na Figura 2.12 [18].

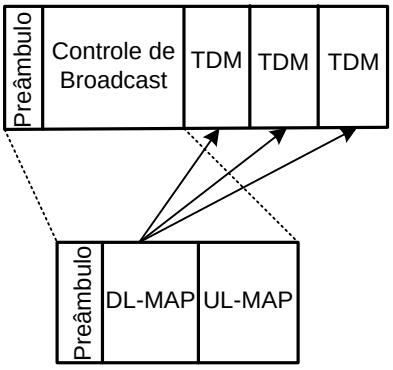

Figura 2.12: Estrutura do *subframe downlink.*

Este *subframe* inicia com um preâmbulo que é utilizado na sincronização pela camada física. O preâmbulo está contido no campo juntamente com a seção de controle do *frame* que contém um mapa *downlink* (DL-MAP - *Downlink Map*), para o subframe *downlink* e um mapa *uplink* (UL-MAP - *Uplink Map*), para o *subframe uplink.*

Após a seção de controle, são contidas as porções TDM que são responsáveis por carregar os dados organizados em rajadas com diferentes perfis. Os perfis são negociados entre as SSs e a BS antes do início da transmissão.

2.6 – Considerações Finais

Este capítulo apresentou algumas considerações importantes sobre as camadas MAC e física do padrão IEEE 802.16. Foram descritas as recomendações do padrão, sua evolução e seus modos de operação, sendo mostradas as formas de comunicação entre as SSs e as BSs. Também, foram apresentadas as principais características das 3 subcamadas pertencentes à camada MAC do padrão. Foram vistos detalhes importantes da Subcamada da Parte Comum, uma vez que é nesta subcamada que são implementados serviços fundamentais, tais como QoS, CAC dentre outros. Quanto à camada física, foram apresentadas as especificações utilizadas bem como a estrutura do *frame* usada na troca de informações entre BS e SSs. Também foram explicadas sucintamente as estruturas e principais características dos subframes *uplink* e *downlink* do padrão IEEE 802.16. Por fim, este capítulo apresentou as características fundamentais que fazem do padrão IEEE 802.16, não somente um complemento e expansão das redes cabeadas de “última milha”, mas um competidor com capacidade de oferecer altas taxas de transmissão de dados, com QoS para atender aos requisitos das aplicações de multimídia atuais.

Capítulo 3

QUALIDADE DE SERVIÇO EM REDES IEEE 802.16

3.1 - Introdução

Nos últimos anos tem ocorrido um crescimento significativo nas comunicações que utilizam redes sem fio. Neste sentido, o provimento de QoS passou a ser uma questão primordial. O termo QoS surgiu originalmente na área de telecomunicações com o objetivo de descrever um conjunto de características técnicas que se observa nas transmissões de dados [47], [42]. Segundo os autores em [31], QoS refere à capacidade da rede em prover os melhores serviços para o tráfego selecionado sobre várias tecnologias, e possui como meta, prover a prioridade requerida por tráfegos interativos e em tempo real, enquanto garante que a taxa de outras transmissões não seja degradada.

Para dar suporte a uma variedade de aplicações que utilizam os recursos de uma rede, tais como, voz sobre IP (VoIP - *Voice Over Internet Protocol*) e serviços de multimídia, o provimento de QoS passou a ser um ponto fundamental. Várias tentativas de prover QoS sobre a arquitetura TCP/IP foram realizadas, mas uma série de desafios adicionais surge quando se trata de prover QoS em redes de acesso sem fio devido às instabilidades que são observadas no meio de comunicação.

Diante disso, o objetivo deste capítulo é descrever os principais mecanismos adotados pelo padrão IEEE 802.16 para prover QoS para as aplicações dos usuários

finais. Neste sentido na Seção 3.2 são apresentadas as características gerais a respeito da QoS nas redes sem fio existentes. A Seção 3.3 faz uma introdução da QoS aplicada às redes IEEE 802.16, onde são apresentados os mecanismo que auxiliam no provimento da QoS, tais como as classes de serviços e suas principais características bem como os fluxos de serviços e suas classificações. A Seção 3.4 apresenta de forma sucinta os mecanismos existentes para o gerenciamento de largura de banda nas redes do padrão IEEE 802.16, e a Seção 3.5 apresenta os mecanismos de tratamento de tráfego com suporte a QoS de forma breve. A Seção 3.6 apresenta os mecanismos de provisão de QoS onde são apresentadas sucintamente as técnicas de policiamento existentes com detalhes para a técnica do *token bucket*. Na Seção 3.7 são realizadas as considerações finais a respeito do assunto abordado neste capítulo.

3.2 - Qualidade de Serviço nas Redes sem Fio

A grande popularidade que a Internet vem alcançando nos últimos anos tem despertado o interesse de diversas empresas de telecomunicações, o que tem levado a se pensar na Internet sem fio como a rede do futuro para atender as necessidades de usuários que ainda não podem ser atendidos pela rede cabeada. As tecnologias sem fio têm ganhado cada vez mais popularidade devido a sua mobilidade e agilidade, e a expectativa é que num futuro próximo os usuários que utilizam redes móveis possam acessar a Internet de qualquer lugar do mundo a qualquer momento. As redes de acesso sem fio apresentam um grande número de questões técnicas que precisam ser solucionadas, dentre elas a QoS que impõe muitos desafios devidos aos seguintes fatores: a dinâmica do ambiente em função da mobilidade dos usuários, as limitações da largura de banda disponível e altas taxas de erros. Com estes fatores podem ocorrer

constantes flutuações na disponibilidade de recursos que são fundamentais nas redes sem fio [12], [43].

Uma estrutura de redes de telecomunicações sem fio necessita de alguns cuidados para garantir desempenho, segurança e disponibilidade, tais como:

- Obstáculos na área de cobertura podem causar uma diminuição da distância no alcance do sinal;
- Vários usuários na mesma área podem influenciar no desempenho e;
- A proximidade com fontes geradora de sinais indesejados.

Por conseguinte o provisionamento de QoS em redes sem fio é bastante desafiador, uma vez que a dinâmica do ambiente em função da mobilidade dos usuários provoca variações na capacidade do canal e na taxa de erros [12], [6].

3.3 - Qualidade de Serviço no padrão IEEE 802.16

A QoS é o efeito coletivo do desempenho do serviço que determina o grau de satisfação do usuário. As três principais características das redes que proveem QoS são [6], [12], [31]:

- Qualidade da Informação - As informações são recebidas com baixa taxa de erros conforme os requisitos da aplicação;
- Disponibilidade de Serviço – O serviço é disponibilizado imediatamente ou adiado por um período de tempo aceitável dependendo do *status* do usuário.

A disponibilização é mais rápida para os usuários que possuem uma prioridade mais alta [45];

- Entrega Consistente - Os dados serão entregues a uma taxa e com uma qualidade consistente, garantindo que a percepção do usuário permaneça sempre a mesma.

O provimento de QoS em uma rede é essencial para as aplicações em tempo real, pois estas demandam por largura de banda e serviços diferenciados. Existem aplicações para as quais é necessário garantir que a transmissão de dados seja feita sem interrupção ou perda de pacotes [46]. Segundo os autores em [11], QoS é caracterizada como um efeito coletivo do desempenho do serviço que determina o grau de satisfação e cujos valores são estabelecidos nos contratos de nível de serviço (SLA - *Service Level Agreement*).

Uma rede deve utilizar mecanismos para gerenciar seus recursos para que possa oferecer um nível de QoS que satisfaça aos anseios dos usuários enquanto maximiza a utilização dos recursos da rede. Para alcançar esta meta, a rede analisa os requisitos de aplicação, gerencia os recursos e aplica vários mecanismos de QoS. Os parâmetros de QoS que quantitativamente representam requisitos de QoS das aplicações são [27]:

- Atraso – É o tempo decorrido desde o instante em que o processo de aplicação de origem envia uma mensagem até o momento em que o usuário de destino receba a mensagem por inteiro;
- Vazão – Quantidade de dados que são recebidos por unidade de tempo;
- Taxa de Transmissão – Capacidade de dados que um determinado meio pode transmitir em um determinado tempo;

- *Jitter* – Representa a variação do atraso entre os pacotes de dados que são enviados sucessivamente;
- Taxa de Erros – É a razão entre a quantidade de pacotes perdidos ou recebidos com erros pela quantidade de pacotes enviados.

O padrão IEEE 802.16 pode suportar variados serviços de comunicação (voz, dados e vídeo) com diferentes requisitos de QoS, e a camada MAC é responsável por especificar os mecanismos de sinalização de QoS a fim de suportar as requisições e alocações de largura de banda. Num canal é possível acomodar diferentes conexões que são usadas por uma variedade de aplicações que necessitam de diferentes requisitos de QoS. As aplicações dos usuários podem apresentar requisições variadas de largura de banda e latência, deste modo o padrão IEEE 802.16 deve apresentar flexibilidade e eficiência sobre uma quantidade variada de diferentes modelos de tráfegos [15].

No padrão IEEE 802.16 o mecanismo utilizado para prover QoS consiste em associar pacotes que passam pela camada MAC, mais especificamente na camada CPS, a um fluxo de serviço que fornece um transporte unidirecional aos dados. Esta associação consiste em fornecer um tratamento diferenciado aos tráfegos que são gerados pelas aplicações. Os fluxos de serviços ativos são identificados por um valor numérico exclusivo de 32 *bits* (SFID) e durante a fase de estabelecimento da conexão estes fluxos são criados e ativados pela BS e pela SS. Cada conexão é identificada por um número inteiro de 16 *bits* em cada direção (CID). Segundo [11], [18], cada fluxo de serviço é caracterizado por um conjunto de parâmetros de QoS, que são os seguintes:

- MRTR (*Minimum Reserved Traffic Rate*) – Determina a taxa de tráfego mínima que foi reservada para um fluxo de serviço. De acordo com o padrão

IEEE 802.16 se a quantidade de banda requisitada for menor do que o valor da MRTR a BS deve alocar a banda excedente para outras conexões. O valor da MRTR garante uma vazão mínima para cada aplicação.

- MSTR (*Maximum Sustained Traffic Rate*) – Determina a taxa de pico máxima do serviço no sentido *downlink* e *uplink*. A SS deve controlar o serviço no sentido *uplink* para que a taxa seja igual ao valor definido pelo parâmetro, enquanto na BS no sentido *downlink*, assume-se que o tráfego é controlado na entrada da rede não sendo necessário realizar um controle adicional;

- *Maximum latency* – Define a latência máxima entre a recepção do pacote na interface de rede da BS ou da SS e a transmissão do pacote para a interface de radio frequência;

- *Maximum traffic burst* – Define o tamanho máximo da rajada a ser permitida e disponibilizada para o serviço;

- *Tolerated jitter* - Define a variação máxima permitida para a latência da conexão;

- *Service flow scheduling type* – Um fluxo deve ser associado com um tipo de serviço baseado no valor deste parâmetro. O serviço de melhor esforço deve ser usado quando o valor deste parâmetro é omitido;

- *Unsolicited Grant interval* – Intervalos entre alocação sucessiva de largura de banda ou *grants*, para as classes de serviços UGS e ertPS;

- *Unsolicited polling interval* - Intervalo máximo entre *grants* sucessivos alocados para um fluxo de serviço rtPS enviar requisição de banda;

- *Traffic priority* – Especifica a prioridade atribuída ao tráfego. Dados dois fluxos de serviço idênticos em todos os parâmetros de QoS exceto na prioridade, o fluxo de serviço com maior prioridade deve ter latência menor e prioridade maior no processo de armazenamento no *buffer*.

3.3.1 - Classes de Serviço

O padrão IEEE 802.16 define cinco classes de serviços, ou categorias de serviço, as quais devem ser tratadas de forma diferenciada pelo mecanismo de escalonamento da camada MAC e estão relacionadas à provisão de QoS na rede de acesso. As classes de serviços são as seguintes: UGS (*Unsolicited Grant Service*), rtPS (*Real Time Polling Service*), nrtPS (*Non Real Time Polling Service*) e BE (*Best Effort*). A partir do padrão IEEE 802.16e foi especificada e fundamentada na eficiência do UGS e do rtPS uma nova classe denominada ertPS (*Extended Real Time Polling Service*). Estas cinco classes de serviços são descritas com mais detalhes a seguir [9], [15], [21].

- UGS – É voltada para tráfego em tempo real com a geração de pacotes de dados de tamanho fixo em intervalos periódicos, ou seja, tráfego com taxa de *bits* constantes ou CBR (*Constant Bit Rate*). Pode ser representada por tráfego gerado por emulação de circuitos T1/E1 e por aplicação VoIP sem supressão de silêncio. O serviço oferece periodicamente concessões de tamanho fixo em tempo real, o que elimina a sobrecarga e a latência das requisições dos pedidos das SSs e

assegura que concessões sejam disponibilizadas para atender as necessidades dos fluxos em tempo real. Fluxos UGS não podem utilizar *slots* reservados para requisição de banda. A SS é proibida de usar qualquer requisição de contenção e a BS não oferece qualquer oportunidade de requisição unidirecional para a SS. Para classe UGS pedidos de banda utilizando o *piggyback* não são permitidos.

- rtPS – É projetada para oferecer suporte aos fluxos de serviço em tempo real que geram pacotes de tamanho variável em intervalos periódicos, tais como transmissão de vídeo sob demanda. São fornecidas *polling* para requisição de banda em apenas uma direção e que atendem as necessidades das conexões em tempo real, permitindo a SS especificar o tamanho da concessão que ela deseja. Deste modo a BS deve alocar periodicamente largura de banda para que as conexões rtPS requisitem banda de acordo com seus requisitos. Nesta classe ocorre o mecanismo de *polling unicast*. Os métodos de requisição de contenção ou de *piggyback* não podem ser utilizados pela SS.
- nrtPS – Projetada para aplicações que não são sensíveis ao atraso, portanto não são em tempo real e que geram pacotes de tamanho variável em intervalos periódicos, tais como o tráfego gerado pelo protocolo de transferência de arquivos (FTP - *File Transfer Protocol*), *email*, e os serviços de mensagens de multimídia (MMS - *Multimedia Messaging Service*). A oferta periódica de *polling unicast* é fornecida nesta classe. O mecanismo de *polling* empregado também pode ser do tipo *multicast polling* ou *broadcast polling* sendo regular e não periódico.

- ertPS – Esta classe de serviço foi introduzida a partir do padrão IEEE 802.16e-2005. Apresenta como função o gerenciamento das taxas de tráfego e as políticas de transporte, bem como melhora a latência e o *jitter*. Suporta serviços em tempo real que utilizam pacotes de tamanho variável em períodos fixos, tais como, serviços VoIP com supressão de silêncio. Nesta classe de serviço a BS provê *grants* para a transmissão dos dados sem a necessidade de mecanismos explícitos para requisição de banda, o qual economiza largura de banda do canal e diminui a latência. As alocações de banda feitas por esta classe são dinâmicas como no rtPS, e por *default* o tamanho destas alocações corresponde ao valor corrente da taxa de tráfego máxima sustentável de cada conexão. A SS pode alterar o tamanho da alocação dinamicamente.
- BE – É um tipo de serviço que é oferecido para tráfegos na *Web* e navegação pela Internet, ou seja, de melhor esforço. É definido para aplicações que não possuem nenhum requisito de atraso específico. Nesta classe, os parâmetros de QoS são escolhidos de tal forma que eles possam fornecer suporte aos serviços de escalonamento de fluxos de dados, para os quais nenhuma alocação mínima de recurso foi concedida. Para os serviços da classe BE não existe garantia de QoS.

A Tabela 3.1 [11] apresenta os parâmetros de QoS que cada classe de serviço deve informar durante o estabelecimento da conexão.

Tabela 3.1 - Parâmetros de QoS fornecidos por cada tipo de serviço [11].

	UGS	ertPS	rtPS	nrtPS	BE
Minimum reserved traffic rate		٧	٧	٧	
Maximum sustained traffic rate	٧	٧	٧	٧	
Maximum traffic burst	٧	٧	٧	٧	٧
Maximum latency	٧	٧	٧		
Tolerated jitter	٧	٧			
Service flow scheduling type	٧	٧	٧	٧	٧
Unsolicited grant interval	٧	٧			
Unsolicited Polling interval			٧		
Traffic priority	٧	٧	٧	٧	

3.3.2 - Fluxos de Serviço

Os fluxos de serviços são componentes importantes na provisão de QoS da camada MAC. Toda conexão possui um fluxo de serviço associado, sendo possível que vários pacotes possam usar um mesmo fluxo. Um fluxo de serviço fornece um transporte unidirecional de pacotes oriundos da BS destinados para SS ou da SS destinados para BS. É caracterizado por um conjunto de parâmetros ou atributos de QoS, tais como: latência, retardo e garantias de vazão [14]. Fluxo de serviço cria um mecanismo para o gerenciamento de QoS nos canais de *downlink* e *uplink*, sendo fundamental para o processo de alocação de banda. O padrão IEEE 802.16 define que os fluxos de serviços sejam caracterizados por seis atributos conforme pode ser visto na Tabela 3.2 [15], [18].

Os fluxos de serviços são divididos em três estados [15], [18]:

- Provisionado – Este tipo de fluxo de serviço é conhecido pelo provisionamento, é caracterizado por parâmetros de QoS fornecido por mecanismos externos definidos pelo padrão IEEE 802.16;

- Admitido – Define um conjunto de recursos reservados de QoS pela BS para *AdmittedQoSParamSet*, no entanto estes parâmetros não são ativos, ou seja, o *ActiveQoSParamSet* é nulo. Os fluxos de serviço admitido podem ter sido provisionado ou sinalizado por algum outro mecanismo;
- Ativo – Este tipo de fluxo de serviço apresenta recursos comprometidos pela BS para o conjunto de parâmetros *ActiveQoSParamSet*. Somente um fluxo de serviço ativo pode enviar pacotes.

O padrão IEEE 802.16 especifica os principais objetos que compõem a arquitetura de provisão de QoS. Cada objeto é representado por um retângulo que contém vários atributos, conforme pode ser visto na Figura 3.1 [15], [18].

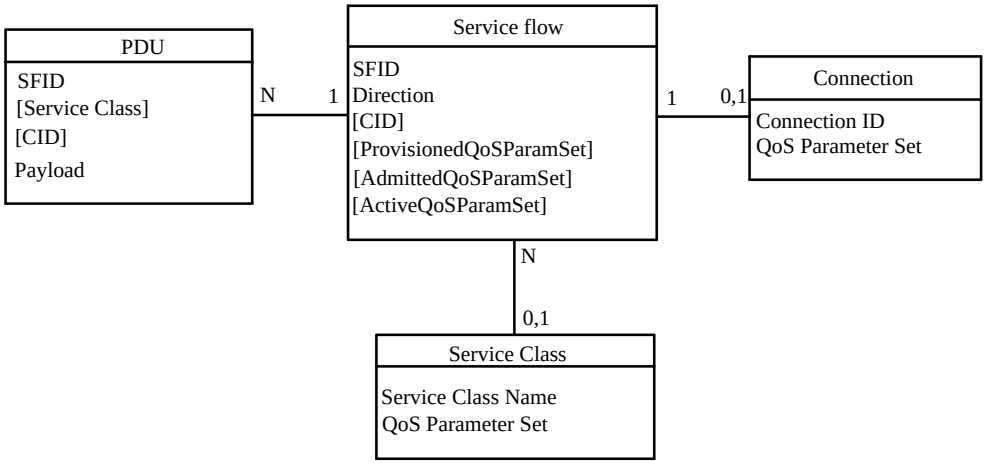

Figura 3.1: Teoria do modelo de objeto de operações (adaptado de [15]).

Cada objeto é identificado unicamente por um atributo sendo que os atributos opcionais estão listados entre colchetes. Um fluxo de serviço é um conceito central do protocolo MAC sendo identificado unicamente por um SFID de 32 bits, podendo estar tanto no sentido *uplink* quanto no sentido *downlink* [15].

Tabela 3.2 – Atributos de um fluxo de Serviço.

Atributos	**Características**
Identificador Fluxo de Serviço (SFID)	Identificador que é atribuído a cada fluxo de serviço existente. Cada fluxo de serviço deve ter no mínimo um SFID
Identificador de Conexão (CID)	O identificador da conexão de transporte somente existe quando o fluxo de serviço é admitido ou ativo. Quando presente, o relacionamento entre um SFID e um CID é único.
ProvisionedQoSParamSet	Define um conjunto de parâmetros de QoS que é provisionado através de meios que o padrão assume ser externo, podendo ser uma parte do sistema de gerenciamento de rede.
AdmittedQoSParamSet	Define um conjunto de parâmetros de QoS para os quais a BS e possivelmente a SS estão reservando recursos. O principal recurso para ser reservado é a largura de banda, mas inclui outros baseados no tempo ou na memória requeridos para posteriormente ativar o fluxo.
ActiveQoSParamSet	Especifica um conjunto de parâmetros de QoS definindo o serviço que atualmente está sendo provido para o fluxo de serviço.
AuthorizationModule	É uma função lógica internamente a BS que é responsável por aprovar ou bloquear as trocas nos parâmetros de QoS e nos classificadores associados com um fluxo de serviço.

3.3.2.1 - Classificação dos Fluxos de Serviços

A classificação dos fluxos de serviços é o principal mecanismo de provisão de QoS no padrão IEEE 802.16 sendo o responsável pela associação dos pacotes com um fluxo de serviço específico. O mecanismo de classificação pode ocorrer tanto no sentido *uplink* quanto no sentido *downlink.* Uma aplicação deve, primeiramente, efetuar o registro na rede para ser associada com um fluxo de serviço específico através da distribuição de um identificador SFID. Cada pacote de uma conexão deve ser identificado pelo SFID atribuído, para que a rede tenha condições de aplicar a QoS adequada. Toda vez que uma aplicação deseja enviar pacotes, primeiramente deve ser estabelecida uma conexão com a BS para receber um CID. Assim, no padrão IEEE 802.16 os pacotes de dados em uma transmissão incluem identificadores por fluxo e por conexão o que torna a camada MAC do padrão IEEE 802.16 orientada a conexão [18].

O conjunto de ferramentas que oferecem suporte de QoS para tráfegos *downlink* e *uplink* são as seguintes:

- Funções de configuração e registro dos fluxos;
- Sinalização para o estabelecimento dinâmico de QoS;
- Escalonamento;
- Agrupamento de propriedade do fluxo de serviço em classe de serviço.

O canal de comunicação entre a BS e a SS do padrão IEEE 802.16, utiliza TDM no sentido *downlink* e TDMA no sentido *uplink*. O módulo de escalonamento de pacotes apresenta as seguintes funções: Alocação de largura de banda para as conexões em função do número de *slots* alocados por conexão pelo canal TDM, e determinação

de quando uma conexão terá permissão para transmitir, caracterizando a conexão como ativa ou inativa [18], [21] e [23].

3.4 Mecanismos de Gerenciamento de Largura de Banda nas Redes do Padrão IEEE 802.16

Os mecanismos de gerenciamento de largura de banda são responsáveis pelo gerenciamento dos recursos da rede através da configuração dos dispositivos existentes, e pelos mecanismos de manipulação de tráfego. Os principais mecanismos de gerenciamento de largura de banda são os seguintes [6], [27], [11]:

- Reserva de recursos – informa as entidades da rede a respeito dos requisitos das aplicações usando os recursos de rede. As informações serão usadas pelos dispositivos de rede a fim de gerenciar os recursos para encontrar os requisitos;
- CAC – consiste num procedimento que visa limitar o número de conexões, de forma que a rede não fique sobrecarregada com um número excessivo de usuários. Sempre que um usuário deseja estabelecer uma nova conexão, uma requisição é enviada para a BS, pela SS, para que o mecanismo de CAC decida se a nova conexão pode ou não ser aceita;
- Mecanismo de gerenciamento de largura de banda que utiliza abordagem *Cross-Layer* - quando o fluxo de uma nova aplicação chega na camada IP, ele é primeiramente analisado de acordo com as definições obtidas no caminho, sendo classificada e mapeada dentro de um dos tipos de classes de serviços.

3.5 - Mecanismos de Tratamento de Tráfego com Suporte à QoS nas Redes do Padrão IEEE 802.16

São mecanismos responsáveis pela classificação, tratamento, policiamento e monitoração do tráfego dentro da rede. Os principais mecanismos de tratamento de tráfego são:

- Classificação de tráfego
- Acesso ao canal
- Policiamento
- Gerenciamento de *Buffer*
- Controle de Congestionamento
- Escalonamento de Pacotes

Da Seção 3.5.1 até a Seção 3.5.7 são especificadas as principais características destes mecanismos [15], [21] e [27].

3.5.1 - Mecanismo de Classificação de Tráfego

Este mecanismo é responsável por identificar e separar os diferentes tráfegos de fluxos ou grupos de fluxos, deste modo, cada fluxo ou grupo de fluxo pode ser tratado de maneira diferenciada. O tráfego de aplicações é identificado pelo mecanismo de classificação, sendo encaminhado para a fila de espera de serviço adequado a partir de outros mecanismos, dentre eles o escalonamento de pacotes. Para identificar e classificar um tráfego, o mecanismo de classificação requer algumas formas de marcação nos pacotes [15], [27].

3.5.2 - Mecanismo de Acesso ao Canal

A comunicação entre os dispositivos, numa rede *Wireless*, ocorre através de um meio compartilhado. Quando uma grande quantidade de estações tenta acessar e transmitir pacotes num canal de comunicação compartilhado é possível que haja colisão. Deste modo, redes *wireless* necessitam de um mecanismo de acesso ao canal onde exista o controle ao meio compartilhado [15], [23], [27], [55].

3.5.3 - Mecanismo de Policiamento de Tráfego

Quando uma chamada é admitida, a rede se protege de fontes abusivas através de um controle de parâmetros denominado de Policiamento. Deste modo garante que uma fonte de tráfego não violará os parâmetros negociados antes do estabelecimento da conexão, tais como: taxa máxima, taxa média e comprimento de rajada. Caso alguma violação seja encontrada, o mecanismo regulador é forçado em ajustar e bloquear o tráfego em excesso para garantir o cumprimento dos acordos do contrato [15], [36], [57].

3.5.4 - Mecanismo de Gerenciamento de *Buffer*

Refere-se a alguma disciplina particular usada para regular a ocupação de uma fila de dados, onde os pacotes devem ser armazenados ou bloqueados. Um *buffer* é definido como um dispositivo capaz de melhorar a utilização e o desempenho de um sistema, podendo aumentar o atraso dos pacotes na fila de transmissão. O mecanismo de gerenciamento de *buffer* é importante para definir atrasos mínimos na transmissão de

dados em uma rede, principalmente para transmissões em tempo real que requerem pequenos atrasos na garantia de QoS [15], [27].

3.5.5 - Mecanismo de Controle de Congestionamento

O congestionamento é a necessidade agregada de largura de banda que excede a capacidade disponibilizada pela linha, causando deste modo a degradação de desempenho e ocasionando perda múltipla de pacotes, baixa utilização do meio, tempo de atraso alto e colapso. Nas redes onde prevalece o melhor esforço, o congestionamento causa prejuízo considerável na QoS, inviabilizando o atendimento a requisitos de QoS das aplicações [27], [31].

Segundo os autores em [36] o congestionamento pode ter duas causas básicas:

- Insuficiência para acomodar a carga presente;
- Desbalanceamento do tráfego nos nós da rede.

Este problema causa o descarte de pacotes nos roteadores, e uma vez descartados os recursos que foram utilizados são desperdiçados, levando os pacotes a alocarem novos recursos diminuindo a vazão e aumentando o atraso na rede.

3.5.6 - Mecanismo de Escalonamento de Pacotes

Este mecanismo refere-se ao processo de decisão que é usado para escolher os pacotes que devem ser transmitidos ou bloqueados nas interfaces de *uplink* ou *downlink* da BS ou na interface de *uplink* da SS. Estes algorítmos são os responsáveis por decidir qual o próximo pacote que será servido na fila de espera, determinação da largura de banda entre o usuário e suas ordens de transmissões e promover o uso eficiente do

enlace sem fio. Uma das tarefas mais importantes executadas pelos algoritmos de escalonamento é satisfazer os requisitos de QoS enquanto utiliza eficientemente a largura de banda disponível [27], [29], [34], [32].

3.5.7 - Mecanismo para Requisição e Alocação de Banda

No padrão IEEE 802.16 a reserva de recursos é feita sob demanda, e quando uma SS deseja requisitar banda para uma conexão ela envia uma mensagem para a BS contendo o pedido. A requisição de banda pode ser enviada como pacote, onde no cabeçalho um campo indica que existe uma solicitação de banda, ou pode ser enviada juntamente com pacotes de dados. Esta técnica é denominada de *Piggyback* e pode ser incremental ou agregada. Para uma requisição incremental a BS deve adicionar a quantidade de banda solicitada a sua percepção atual sobre a banda que deve ser alocada. Quanto à requisição agregada a BS deve substituir a largura de banda que deve ser alocada para a conexão pela quantidade de banda requisitada pela conexão. Todas as requisições feitas pelas SSs devem indicar o número de *bits* necessários para transmitir o pacote completo [11], [29].

Uma BS destina parte da largura de banda disponível para as SSs enviarem suas requisições, e a alocação de *grants* pode ser para uma SS particular ou para um grupo de SSs. A alocação é informada para as SSs através de mensagens UL-MAP. Este processo recebe o nome de *polling* e define dois mecanismos [54]:

- Unicast – As SSs são interrogadas individualmente para informar se desejam transmitir, caso positivo recebe um *grant* cujo tamanho é suficiente para o envio de uma mensagem de requisição de banda.

- Baseado em Contenção – É utilizado quando não existe largura de banda disponível para fazer o *polling* para cada uma das SSs individualmente. Nesta técnica, a BS aloca um *grant* para um grupo de SSs que devem competir pela oportunidade de enviar mensagens de requisição. Apenas as SSs que necessitam de largura de banda usam a contenção, com isso a probabilidade de colisão, no meio, é menor. A resolução da contenção se dá com um algoritmo de *backoff* exponencial [11], [18]. A reserva de recursos nas redes do padrão IEEE 802.16 é feita por escalonadores localizados nas SSs e BSs, conforme Figura 3.2 [27].

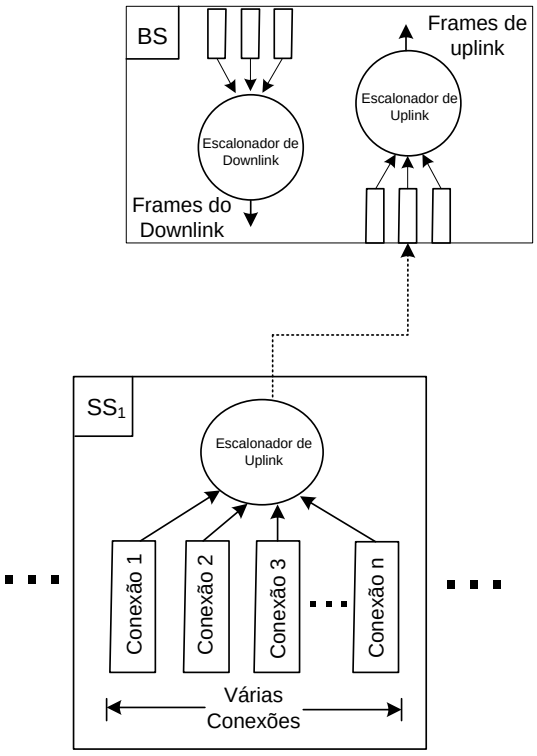

Figura 3.2: Arquitetura base do padrão IEEE 802.16 (adaptado de [27]).

A estação base possui dois escalonadores, sendo um de *uplink* e outro de *downlink.* O escalonador de *uplink* localizado na SS é o responsável por decidir quais

serão os pacotes a serem enviados nas oportunidades de transmissão que forem recebidas no *subframe* de *uplink*. Para a BS, o escalonador de *downlink* irá decidir quais conexões terão o direito de transmitir em cada *subframe* de *downlink*, diferentemente, o escalonador de *uplink* irá atribuir *grants* para que as estações clientes possam enviar requisições e pacotes no *subframe* de *uplink* [11], [27].

3.6 - Mecanismos Para Provisão QoS no Padrão IEEE 802.16

O padrão IEEE 802.16 foi projetado para dar suporte a QoS e está associado a conceitos como: classificação, escalonamento por fluxos de serviço, CAC e policiamento. As classes e fluxos de serviços definidos no padrão IEEE 802.16 não são suficientes para garantir QoS para as aplicações. O provimento de QoS implica na execução de alguns mecanismos, tais como, o gerenciamento eficiente dos recursos do enlace, execução de políticas de CAC, escalonamento e técnicas de policiamento tanto na SS quanto na BS [15], [30], [61].

O padrão IEEE 802.16 define uma arquitetura base para a provisão de QoS, conforme pode ser visto na Figura 3.3 [28]. No entanto, o padrão deixa em aberto os mecanismos de escalonamento, CAC e policiamento para que os fabricantes de produtos tenham liberdade na implementação dessas técnicas e diferenciarem seus produtos.

Nas Seções 3.6.1, 3.6.2 e 3.6.3 são apresentadas as principais características das técnicas de CAC, escalonamento e policiamento. Será dado um enfoque maior para as técnicas de policiamento utilizadas, uma vez que este é o foco principal no desenvolvimento desta pesquisa.

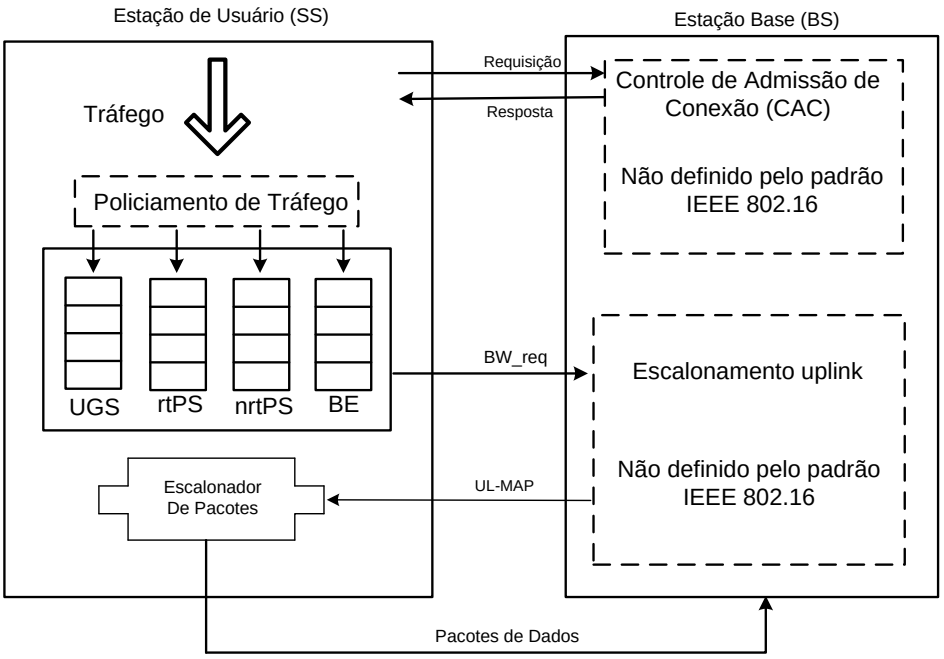

Figura 3.3: Arquitetura base do padrão IEEE 802.16.

3.6.1 - Escalonamento de Pacotes

Os pacotes de dados de uma rede do padrão IEEE 802.16 precisam ser escalonados de acordo com o tráfego e os requisitos de QoS. O escalonamento de pacotes é um processo que determina quando e como os pacotes em uma fila serão transmitidos nos canais *upstream* e *downstream*, o que pode ocorrer tanto na SS como na BS, porém de forma diferenciada. A função mais importante dos escalonadores é satisfazer os requisitos de QoS dos usuários enquanto busca utilizar de forma eficiente os recursos escassos de uma rede [15], [29], [56].

3.6.2 - Controle de Admissão de Conexões

Os algoritmos de CAC asseguram que uma conexão será aceita em uma rede se e somente se os requisitos de QoS puderem ser satisfeitos e o desempenho das conexões já estabelecidas não for prejudicado. Um mecanismo de CAC deve ser o mais eficiente

possível, pois caso seja aceito um número excessivo de conexões, o sistema não poderá garantir QoS para todas as conexões e, contrariamente, se for admitido um número menor do que a rede tem capacidade de suportar, os recursos da rede serão desperdiçados [29], [30].

3.6.3 - Mecanismos de Gerenciamento de Tráfego

O padrão IEEE 802.16 é uma tecnologia que permite a implementação de redes de acesso banda larga sem fio com garantia de QoS. Nos últimos anos, a quantidade de aplicações nas redes IP tem aumentado de forma vertiginosa, e muitas destas aplicações apresentam requisitos de atraso máximo limitado e largura de banda mínima. Por existir diferentes tipos de aplicações de rede com cargas de tráfego heterogêneas, tem se tornado desafiador implementar mecanismos de controle de congestionamento enquanto se mantêm os requisitos de QoS. Deste modo, as políticas de gerenciamento de tráfego são fundamentais para assegurar justiça e desempenho adequado nas redes de computadores.

Conforme citado na Seção 3.6.2, os mecanismos de CAC são fundamentais para controlar a entrada de conexões na rede, uma vez que novas conexões somente serão aceitas baseadas nas informações contidas nos contratos de tráfegos e nas condições atuais da rede. Mesmo com a utilização do CAC é possível ocorrer congestionamento na rede, uma vez que conexões já estabelecidas podem violar o contrato de tráfego aceito no início da conexão. Diante disso conclui-se que um mecanismo de CAC deve ser o mais eficiente possível para não tomar decisões que prejudiquem o desempenho do sistema [4], [26], [30].

Baseado neste contexto é essencial realizar o controle e o monitoramento, regulando assim, todo o tráfego que adentrar a rede com o objetivo de detectar a violação de parâmetros que foram negociados na fase do estabelecimento da conexão, fazendo com que os tráfegos que não estejam em acordo obedeçam aos contratos assumidos. A principal tarefa a ser realizada por uma técnica de monitoramento é fazer o encaminhamento de pacotes de forma controlada e compartilhar os recursos de uma rede de maneira inteligente a fim de prevenir futuros congestionamentos com tráfegos indesejáveis.

Segundo [26] o tráfego em rajadas é a principal causa de congestionamento numa rede sendo caracterizado pela chegada de pacotes de dados em pequenos intervalos de tempo, e pela variação da quantidade de pacotes de dados de um instante para outro, conforme pode ser visto na Figura 3.4.

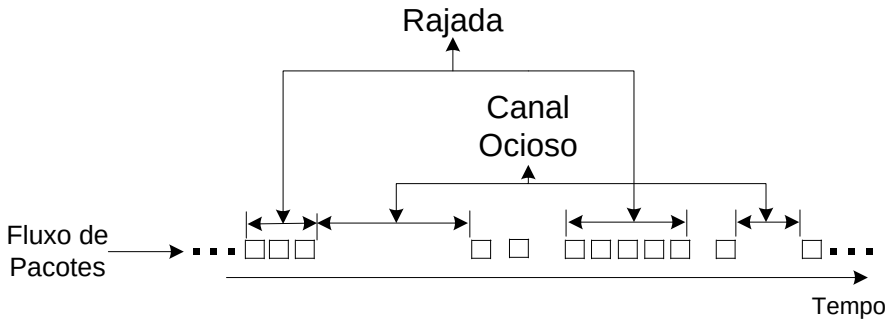

Figura 3.4: Fluxo de pacotes em rajada.

A fim de solucionar este problema, técnicas que forneçam suporte para o controle do tráfego em rajadas podem ser utilizadas para restringir a variação no tempo de chagada dos pacotes, monitorar a taxa de fluxo de dados e descartar pacotes que não obedeçam ao contrato de tráfego estabelecido.

3.6.3.1 - Policiamento de Tráfego

O policiamento de tráfego ou *Traffic Policing* é um método utilizado para monitorar e controlar o tráfego das conexões já admitidas numa rede para que não violem os contratos de QoS, além de garantir que todo tráfego de dados que passar pelas regras de policiamento estará em acordo com os parâmetros de tráfego definidos. Em caso de violação, o mecanismo policiador é forçado a ajustar o tráfego e descartar ou marcar os pacotes em excesso [4]. O policiamento é realizado pela rede através do controle dos seguintes parâmetros: taxa máxima, taxa média e comprimento de rajadas. Por fim, as classes de serviços com maior sensibilidade ao atraso apresentam prioridade no mecanismo. A parcela de tráfego que excede os limites estabelecidos no contrato é descartada ou simplesmente marcada para tratamento futuro [36], [41]. Os autores em [27] citam que as fontes de tráfego que assumirem um acordo de contrato de tráfego antes do estabelecimento de uma conexão, esporadicamente podem aplicar um ajuste de tráfego a fim de assegurar que o tráfego gerado esteja dentro dos limites máximos permitidos, evitando deste modo descarte de pacotes.

Devido ao fato de que o policiamento de tráfego ajusta o tráfego baseado em parâmetros de tráfego quantitativos conhecidos, as aplicações em tempo real são naturalmente compatíveis com policiamento de tráfego. Segundo [27], a maioria do tráfego de dados das aplicações multimídia, tempo real, é gerado por um *codec* padrão que geralmente fornece certo conhecimento dos parâmetros de tráfego quantitativos. Enquanto isso, o tráfego não tempo real não provê parâmetros de tráfego quantitativos e usualmente necessita de uma largura de banda o quanto maior possível. Deste modo o policiamento de tráfego força o tráfego em tempo não real aos acordos de contrato de

tráfego da rede, e quando a taxa de tráfego atinge um valor máximo configurado pelo usuário o tráfego em excesso é totalmente descartado pelo mecanismo policiador.

3.6.3.1.1 – Mecanismos de Policiamento de Tráfego

Nesta seção são apresentados os principais mecanismos de policiamento encontrados na literatura.

3.6.3.1.1.1 – Mecanismo da Janela Saltitante

Este mecanismo considera as janelas com os tempos fixos e duração igual a T segundos. Cada janela apresenta o seu início após o término da janela anterior e somente “C” pacotes poderão ser submetidos à rede, conforme mostrado na Figura 3.5.

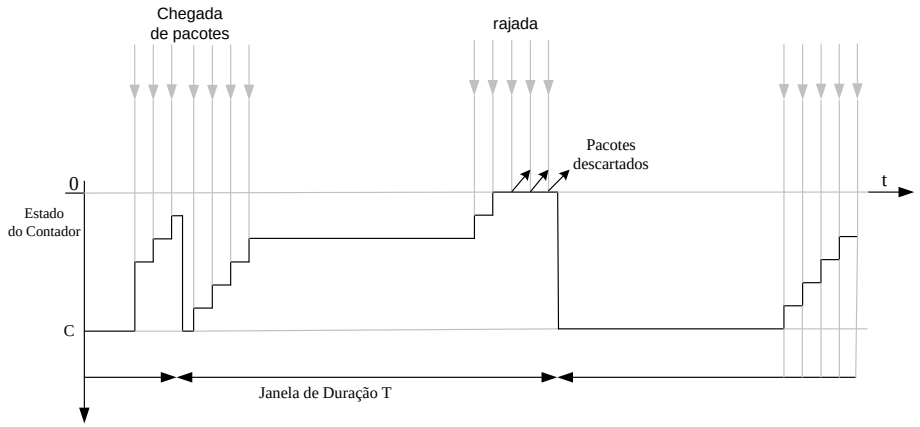

Figura 3.5: Mecanismo de policiamento de tráfego da janela saltitante (adaptado de [36]).

Caso “C” pacotes já tenha sido recebido pela rede durante uma janela, os pacotes seguintes serão considerados fora do contrato de tráfego e serão descartados [36], [37], [38], [59].

3.6.3.1.1.2 – Mecanismo de Janela Saltitante Sincronizada

Este mecanismo é semelhante ao mecanismo de janela saltitante, descrito na subseção anterior, no entanto, neste mecanismo o início de uma janela ocorre com a chegada de um pacote. Este procedimento evita o período de silêncio no início de uma janela permitindo assim maior controle do tráfego [36].

3.6.3.1.1.3 – Mecanismo de Janela Deslizante Continua

É um mecanismo que igualmente aos anteriores limita em "C" o número máximo de pacotes na rede durante um período de tempo. Neste mecanismo o início de uma janela está associado ao instante de chegada de cada pacote e seu término é constante, ou seja, "T" unidades de tempo depois, conforme pode ser verificado na Figura 3.6 [36], [37].

Verifica-se que várias janelas sobrepostas vão sendo abertas e fechadas ao longo do tempo e cada uma separadamente restringindo o tráfego em "C" pacotes no máximo em qualquer período de tempo "T".

3.6.3.1.1.4 – Mecanismo de Janela Deslizante Discretizada

Este mecanismo é semelhante ao mecanismo de janela deslizante continua, com diferença no fato dos instantes entre as chegadas de pacotes serem aferidos em segmentos de tempo com duração igual ao tempo de transmissão de um pacote, ou seja, a aferição das chegadas é feita em intervalos de tempo discreto [36].

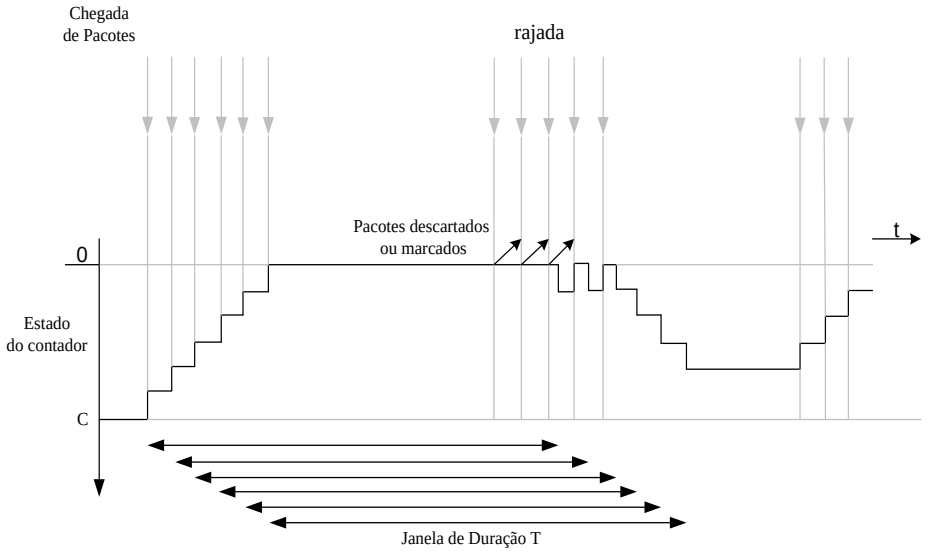

Figura 3.6: Mecanismo de policiamento de tráfego janela deslizante continua (adaptado de [36]).

3.6.3.1.1.5 - Mecanismo *token bucket*

A técnica do *token bucket* é descrito no RFC 2215 [50], sendo um dos mecanismos mais utilizados para controlar a taxa de pacotes que são injetados numa rede. É caracterizado como um filtrador ou policiador de tráfego apresentando bom desempenho para tráfego em rajada. Este mecanismo necessita de dois parâmetros para realizar sua tarefa de controle: O tamanho do *bucket* (b) e a taxa de *tokens* (Tr). O *bucket* é um dispositivo lógico que armazena os *tokens* que são gerados dentro de uma taxa (Tr). A taxa (Tr) especifica o número *bytes*, *bits* ou pacotes que são admitidos numa rede. O tamanho de um *bucket* define o tamanho da rajada a ser permitida de um fluxo de tráfego dentro de um intervalo de tempo. Os pacotes que chegarem ao mecanismo policiador somente serão transmitidos se tiverem *tokens* disponíveis dentro do *bucket*. Caso não tenha pacotes chegando ao mecanismo policiador os *tokens* gerados ficarão armazenados no *bucket* até atingirem o limite máximo definido pelo tamanho

máximo do *bucket* (b). Se o *bucket* estiver cheio, todos os outros *tokens* gerados serão imediatamente descartados [36], [41], [48].

Na técnica *token bucket* quando os pacotes são gerados dentro de uma taxa de pico que seja maior do que a taxa de geração de *tokens* (Tr), os *tokens* que estiverem armazenados dentro do *bucket* serão utilizados numa taxa (Tr). Um tráfego em rajadas pode ser bem manipulado usando o mecanismo do *token bucket* [4], [26], [32], [60]. O mecanismo *token bucket* é mostrado na Figura 3.7.

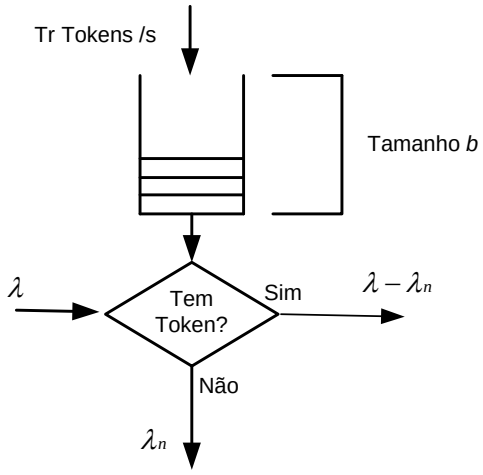

Figura 3.7: Escopo do policiamento de tráfego com *token bucket.*

A carga de tráfego que é injetada na rede é dada por λ e a taxa de pacotes de dados que passa pelo mecanismo policiador e obedece as regras do contrato de tráfego é dada por $\lambda - \lambda_n$. Enquanto isso, λ_n representa a taxa de pacotes de dados que não obedeceu aos parâmetros definidos pelo mecanismo policiador e por isso é descartado pelo mecanismo policiador de tráfego. Em redes de computadores que empregam um mecanismo policiador de tráfego baseado no *token bucket*, os parâmetros do *token bucket* devem ser selecionados de modo a alcançar uma melhor utilização dos recursos

disponíveis. No entanto, o RFC 2215 não especifica como determinar a taxa de *token* e o tamanho do *bucket* [48].

O uso do mecanismo *token bucket* em redes de computadores para controlar o tráfego de dados através do policiamento, deve ter os parâmetros Tr e *b* escolhidos de forma adequada para que os recursos da rede sejam utilizados da melhor forma possível [4].

3.7 – Considerações Finais

Este capítulo apresentou vários mecanismos que oferecem suporte a QoS nas redes de acesso IEEE 802.16. Foram apresentadas as principais especificações da QoS nas redes *wireless*, bem como as classes e fluxos de serviços com suas principais características e classificações. Também, foram apresentados os mecanismos de gerenciamento de largura de banda e suas principais características.

Para as redes sem fio foi apresentado na Seção 3.2 as principais características da QoS. Ademais na Seção 3.3 é apresentado os principais aspectos existentes no padrão IEEE 802.16 no que diz respeito a provisão de QoS. A Seção 3.4 apresenta os mecanismos de gerenciamento de largura de banda e que são essenciais no provimento de QoS. Os mecanismos de tratamento de tráfego do padrão IEEE 802.16 são exemplificados na Seção 3.5. Por fim a Seção 3.6 apresenta de forma sucinta os principais mecanismos de provisão de QoS do padrão IEEE 802.16 e apresenta os principais mecanismo de policiamento utilizados na literatura.

Capítulo 4

PROPOSTA DE UM MECANISMO DE POLICIAMENTO DE TRÁFEGO PARA REDES IEEE 802.16

4.1 - Introdução

O padrão IEEE 802.16 é uma tecnologia emergente que foi projetada para transmissão em altas velocidades com projetos flexíveis e desenvolvimento fácil e custo acessível. Este padrão provê acesso banda larga em área metropolitana sendo considerado por isso uma rede de "última milha". Devido à necessidade cada vez maior, por parte dos usuários finais, por acesso em banda larga em áreas suburbanas ou rurais, o padrão IEEE 802.16 se tornou uma alternativa extremamente interessante às tecnologias *DSL* e *Cable Modem*. Além disso, este padrão pode suportar tipos de tráfegos heterogêneos, tais como voz e vídeo em tempo real, os quais requerem diferentes níveis de QoS. O suporte diferenciado e garantido à QoS é uma tarefa complexa devido ao fato das aplicações de voz e vídeo apresentarem diferentes requisitos e comportamento de tráfego variados.

O escalonamento de pacotes, o CAC e o policiamento de tráfego são os principais mecanismos capazes de prover QoS no padrão IEEE 802.16 e estes não são definidos pelo padrão. Diante disso, este capítulo visa apresentar uma proposta básica de mecanismo de policiamento de tráfego na SS.

Este capítulo, além desta seção, está organizado da seguinte maneira: a Seção 4.2 descreve o problema e a motivação para a apresentação desta proposta. A Seção 4.3 apresenta a solução proposta para o problema e os objetivos do mecanismo de policiamento apresentado. A Seção 4.4 destaca de forma detalhada os principais trabalhos relacionados ao tema desta dissertação. E, finalizando, a Seção 4.5 apresenta as considerações finais a respeito deste capítulo.

4.2 - Descrição do Problema

Segundo os autores em [4], o CAC representa o primeiro passo no provimento de QoS para redes padrão IEEE 802.16, sendo responsável por decidir se uma nova solicitação de conexão deve ou não ser aceita pela rede, levando-se em conta os recursos já alocados para as conexões existentes e os requisitos de QoS para a nova conexão. Após o estabelecimento de uma conexão, o mecanismo de policiamento é o responsável por regular a taxa de tráfego com objetivo de prevenir futuros congestionamentos, caso contrário, isto deve resultar na saturação da rede e, como consequência, na rejeição de conexões solicitadas por outras fontes de tráfego. Ademais os requisitos de QoS das conexões já estabelecidas, tais como, *jitter*, *delay* e perda de dados não poderão ser mais atendidos.

Devido ao fato de algumas fontes de tráfego apresentarem uma natureza em rajadas, a implementação de mecanismos de controle de congestionamento, mantendo os requisitos mínimos de QoS têm se tornado desafiadora para os projetistas das redes WiMAX. Neste sentido os mecanismos de policiamento de tráfego são utilizados em redes de computadores, mais especificamente naquelas que suportam serviços multi-níveis com requisitos de QoS selecionáveis, e são capazes de permitir um tratamento

diferenciado de uma grande variedade de aplicações. Segundo os autores em [48] e [49], o principal objetivo de um mecanismo de policiamento de tráfego é controlar diferentes aplicações e compartilhar os recursos da rede de uma maneira inteligente, a fim de prevenir e recuperar possíveis congestionamentos, bem como monitorar fluxo de dados e descartar pacotes que não estejam em acordo com os contratos de tráfego.

Além disso, normalmente um mecanismo policiador pode descartar muitos pacotes de aplicações elásticas, uma vez que a chegada destes ao longo do tempo não é constante. Diante disso, um mecanismo policiador eficiente deve se adaptar às variações do tempo entre as chegadas de pacotes e tentar de alguma forma diminuir o descarte para as aplicações elásticas.

4.3 - Solução Proposta

Para solucionar o problema descrito na Seção 4.2, é de fundamental importância monitorar e controlar o tráfego que está sendo injetado na rede pelas conexões já admitidas, a fim de detectar possíveis violações dos parâmetros negociados, forçando o tráfego que não estiver em conformidade a respeitar o contrato de tráfego estabelecido.

Atualmente vários mecanismos de policiamento têm sido utilizados pela comunidade acadêmica para realizar o controle do tráfego na rede e que foram descritas na Seção 3.6.3.1.1. Para o desenvolvimento deste trabalho, o mecanismo de policiamento baseado em *token bucket* foi o escolhido como o filtrador, pois monitora o fluxo de tráfego garantindo conformidade com o contrato negociado, além de permitir fluxos contínuos e em rajadas.

O mecanismo de policiamento baseado em *token bucket* é caracterizado por dois parâmetros: O tamanho do *bucket* (b) e a taxa de *tokens* (Tr). A taxa de *tokens* (Tr)

representa a taxa na qual os *tokens* são gerados e adicionados ao *bucket* o que permite especificar o número máximo de *bits* ou *bytes* por segundos que podem adentrar a rede. Já o tamanho do *bucket* (b) define o tamanho máximo da rajada permitido para um fluxo de tráfego dentro de um intervalo de tempo definido. Os *tokens* gerados, numa taxa fixa e constante (Tr *tokens/s*), podem ser acumulados no *bucket* e são controlados pelo tamanho fixo (*b tokens*) do *bucket*. Quando um *bucket* atinge sua capacidade máxima, os *tokens* deixam de ser gerados ou simplesmente são descartados. A Figura 4.1 apresenta o módulo de policiamento de tráfego e o mecanismo de policiamento baseado em *token bucket*.

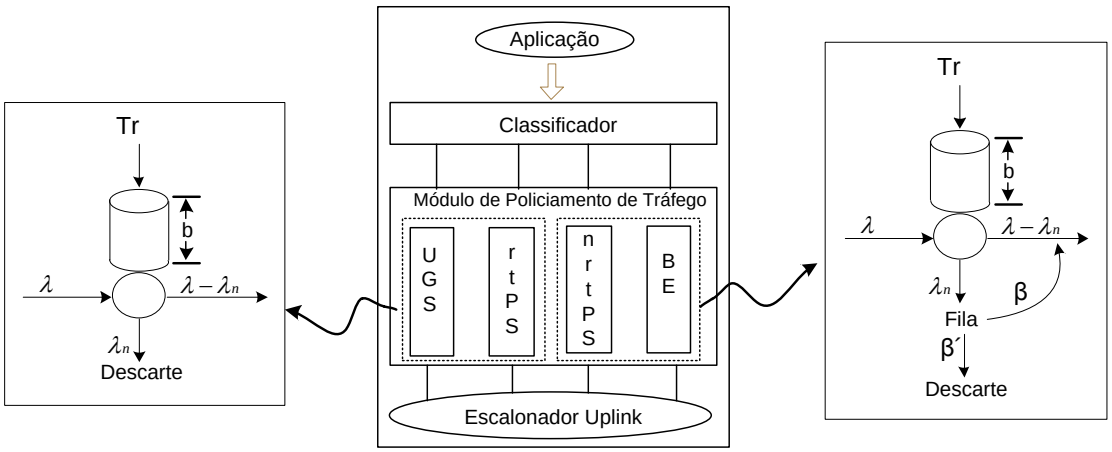

Figura 4.1: Módulo de policiamento de tráfego e o mecanismo de policiamento proposto (adaptado de [4]).

Cada pacote produzido pela aplicação, após ser classificado em uma das classes de serviço, retira um *token* do *bucket* antes de ser admitido pela rede. Portanto, um pacote somente irá passar pelo mecanismo de policiamento baseado em *token bucket* se houver *tokens* dentro do *bucket.* Pacotes de um fluxo de tráfego que não obtiverem *tokens* para serem admitidos na rede poderão ser descartados imediatamente ou armazenados num *buffer* para uma segunda oportunidade de transmissão, obedecendo a dois casos:

Caso 1: O pacote pertence aos fluxos de serviços rtPS ou UGS: Nesse caso, o pacote é descartado imediatamente, pois a aplicação não é tolerante a atrasos;

Caso 2: O pacote pertence aos fluxos de serviços nrtPS ou BE: Como as aplicações neste caso são elásticas, os pacotes serão armazenados em uma fila para a transmissão posterior ao invés de serem descartados imediatamente. Isso poderá minimizar as retransmissões TCP, aumentando-se dessa forma, a eficiência na utilização da largura de banda disponível.

O mecanismo de policiamento de tráfego baseado em *token bucket* proposto nesta dissertação será implementado na SS com o objetivo de monitorar e controlar os fluxos de dados que são encaminhados para a rede.

4.3.1 – Módulo de Policiamento de Tráfego

Nas redes sem fio, diferentes tipos de tráfego incluindo dados, voz, vídeo etc podem ser classificados em CBR ou VBR. Para o caso CBR, os pacotes são enviados numa taxa fixa e, neste caso, a alocação de capacidade na taxa de pico pode ser aplicada. Por outro lado, no caso VBR como o tráfego apresenta-se em rajadas, a taxa média pode ser muito pequena se comparada com a taxa de pico [48], [51]. Além disso, aplicando a taxa de pico tem-se como consequência, a prevenção de congestionamento na rede, mas isto causa baixa utilização dos recursos da rede, como a largura de banda [48], [52]. Neste trabalho um policiador de tráfego é aplicado para cada uma das classes de tráfego, num esquema multi-policiador. Portanto, a configuração de parâmetros apropriados do *token bucket* para o policiador de cada classe de serviço se faz necessário. A seguir são apresentados os parâmetros citados anteriormente para o *token bucket.*

4.3.1.1 – Policiador de Tráfego UGS

A classe de tráfego UGS é projetada para o suporte a fluxos em tempo real com taxa de *bits* constante (CBR). Para esta classe, a BS aloca largura de banda fixa periodicamente para cada uma das conexões presentes, cada qual caracterizada pelo parâmetro MSTR que foi definido nesta dissertação por Rmax. A MRTR, se existir, será igual ao Rmax. É essencial garantir que todos os fluxos de tráfego entrantes da classe UGS passem através do policiador de tráfego UGS. Neste sentido, a taxa de geração de *tokens* (Tr_u) deve ser igual à taxa máxima de chegada de pacotes das conexões UGS ($R_u max$), conforme a seguinte equação:

$$Tr_u = R_u max \tag{4.1}$$

A Figura 4.2 apresenta o esquema de policiamento proposto utilizando a técnica *token bucket* comum às classes de tráfego UGS e rtPS.

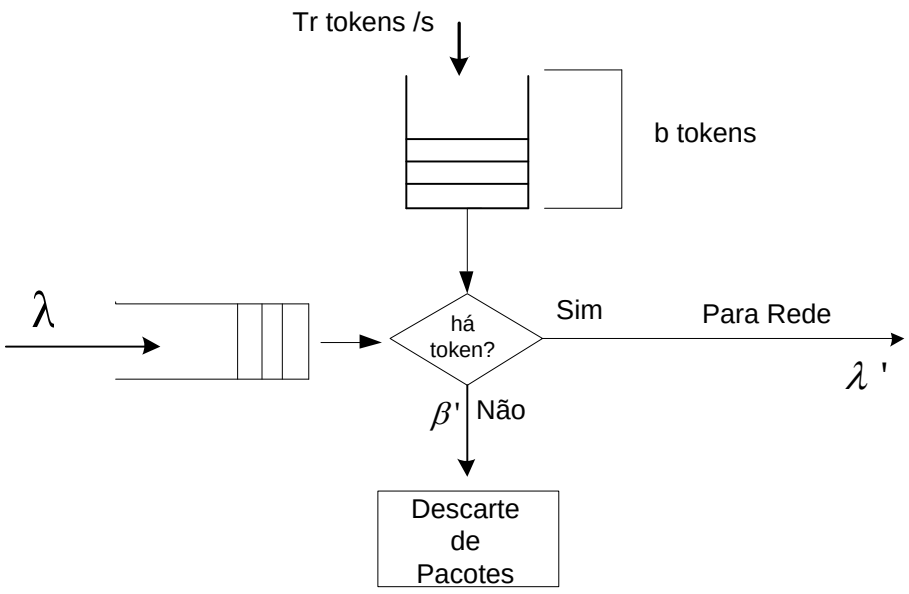

Figura 4.2: Esquema de policiamento utilizando *token bucket* (policiadores UGS e rtPS).

No esquema apresentado na Figura 4.2, caso tenha *tokens* no *bucket*, os pacotes que chegam a taxa λ serão admitidos na rede numa taxa λ'. β' representa a diferença entre os pacotes UGS ou rtPS que chegam à rede e aqueles que são admitidos.

O mecanismo de policiamento baseado em *token bucket* proposto é uma técnica de limitação de largura de banda ocupada de acordo com as especificações do padrão IEEE 802.16. O algoritmo 4.1 apresenta o mecanismo de policiamento baseado em *token bucket*, proposto para as classes de serviços UGS e rtPS.

Algoritmo 4.1 Policiamento de Tráfego

Entrada: pacote P, classe C
Saída: ------
1: Início
2: **se** (qde_tokens > 0) **então**
3: qde_tokens = qde_tokens - 1;
4: Admite o pacote P;
5: s**enão**
6 Descarta o pacote P;
7: **fim se**
8:**Fim**

O policiador recebe como entrada um pacote P com classe de tráfego definida pelo classificador. Primeiramente, o algoritmo verifica se existem *tokens* disponíveis no *bucket*. Se houver, o pacote é admitido na rede e um *token* é retirado do *bucket*. Caso contrário, se não houver *tokens no bucket*, o pacote é imediatamente descartado.

4.3.1.2 – Policiador de Tráfego rtPS

A classe de tráfego rtPS é projetada para o suporte de tráfego VBR com requisitos de atrasos limitados. Assim, os parâmetros do *token bucket* devem ser cuidadosamente definidos de forma que os pacotes de dados rtPS passem pelo mecanismo de policiamento sem atrasos adicionais. O parâmetro que especifica o

tamanho do *bucket* define o tamanho máximo da rajada permitido. Neste sentido, o parâmetro de MSTR para rtPS ($R_{rt}max$) vai especificar a taxa de pico que os fluxos rtPS podem transmitir. Com o objetivo de garantir que todo pacote de dados da classe rtPS tenha *tokens* suficientes para passar pelo mecanismo policiador, os *tokens* devem ser gerados na taxa máxima permitida. Neste sentido, a taxa de geração de *tokens* para classe rtPS (Tr_{rt}) é dada pela equação 4.2 a seguir:

$$Tr_{rt} = R_{rt}max \tag{4.2}$$

O esquema de policiamento e o algoritmo representando o mecanismo de policiamento utilizando o *token bucket*, para classe de serviço rtPS, são idênticos aqueles que foram apresentados na Seção 4.3.1.1.

4.3.1.3 – Policiador de Tráfego nrtPS

De acordo com o padrão *WiMAX*, a taxa de tráfego para classe nrtPS é controlada pelos valores de taxa máxima e taxa mínima. Diante disso, a taxa de tráfego que estiver acima do valor de $R_{nr}min$ e abaixo do valor atribuído à $R_{nr}max$ é permitida. O policiador deve ser capaz de controlar a quantidade e a duração das rajadas nrtPS. Segundo os autores em [48], o valor da taxa de geração de *tokens* para classe nrtPS pode ser escolhida empiricamente. Todavia, uma vazão satisfatória para os fluxos nrtPS pode ser obtida se a taxa de geração de *tokens* (Tr_{nr}) for definida como a média entre os valores de $R_{nr}max$ e $R_{nr}min$, dada pela equação 4.3 a seguir:

$$Tr_{nr} = \frac{R_{nr}\max + R_{nr}\min}{2} \tag{4.3}$$

O esquema de policiamento de tráfego proposto utilizando a técnica *token bucket* com fila de espera, comum às classes de tráfego nrtPS e BE, é apresentado na Figura 4.3.

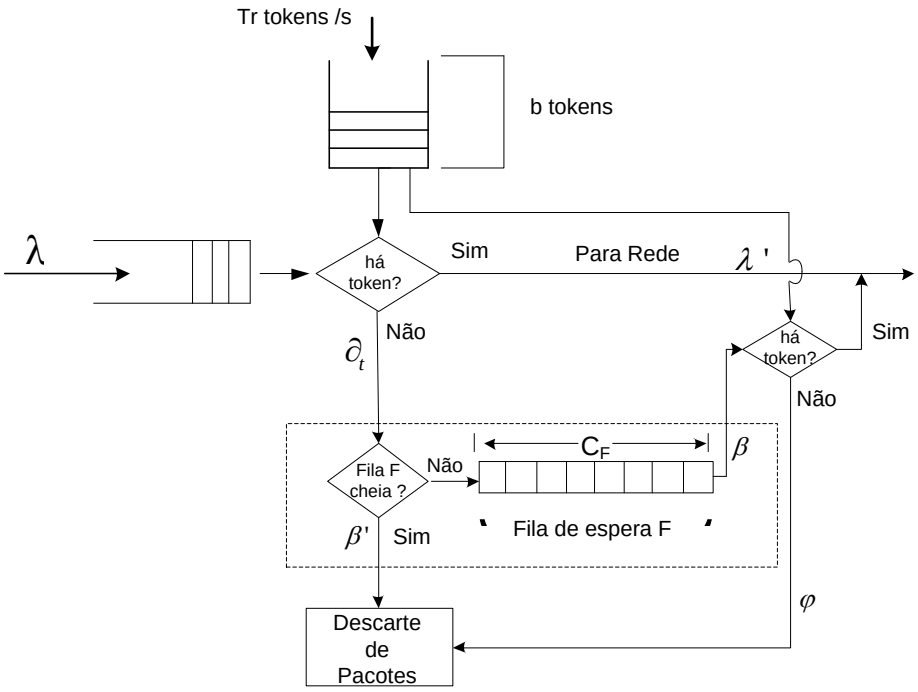

Figura 4.3: Esquema de policiamento utilizando *token bucket* com fila de espera (policiadores nrtPS e BE).

No esquema apresentado na Figura 4.3 os pacotes que chegam à taxa λ somente serão admitidos pela rede se houver *tokens* no *bucket*. ∂t representa a quantidade de pacotes que não foram admitidos na primeira oportunidade por falta de *tokens*, mas que poderão ser armazenados numa fila de espera para uma segunda oportunidade de admissão. Os pacotes que excederem à capacidade máxima C_F da fila de espera F serão imediatamente descartados. β´ representa a diferença entre a quantidade de pacotes nrtPS ou BE que não foram admitidos na rede na primeira tentativa por falta de *tokens* e os pacotes que foram armazenados na fila de espera. β representa os pacotes que obtiveram uma segunda oportunidade de admissão na rede, mas somente serão

admitidos se houver *tokens* no *bucket*. φ representa a quantidade de pacotes das classes nrtPS ou BE descartados após uma segunda oportunidade de admissão na rede.

O algoritmo 4.2 apresenta o mecanismo de policiamento baseado em *token bucket* para as classes de serviços nrtPS ou BE.

Algoritmo 4.2 Policiamento de Tráfego

```
Entrada: pacote P, classe C, fila F
Saída: ------
1: Início
2:   se (qde_tokens > 0) então
3:        qde_tokens = qde_tokens - 1;
4:        Admite o pacote P;
5:    senão
6:         se (fila F não estiver cheia) então
7:              Insere o pacote P na fila F;
8:                se (qde_token>0) então
9:                   Admite o pacote P da fila de espera F;
10:                  qde_tokens = qde_tokens - 1;
11:               senão
12:                  Descarta o pacote P;
13:               fim se
14:            Descarta o pacote P;
15:         fim se
16:             Descarta o pacote P;
17:      fim se
18: Fim
```

O policiador recebe como entrada um pacote P com classe de tráfego definida pelo classificador e fila de espera de tamanho F. Primeiramente o algoritmo verifica se existem *tokens* disponíveis no *bucket.* Se houver, o pacote é admitido na rede e um *token* é retirado do *bucket.* Caso contrário, se não houver *tokens* e a fila F não estiver completamente cheia, o pacote é inserido nesta fila. Em seguida, quando o pacote se tornar cabeça da fila e houver *tokens* no *bucket,* então o pacote P será admitido na rede, caso contrário ele será descartado imediatamente.

4.3.1.4 – Policiador de Tráfego BE

A classe BE foi projetada para suportar fluxo de tráfego sem requisitos de largura de banda ou atraso limitado. No IEEE 802.16, a classe de tráfego BE possui apenas a taxa de tráfego mínima reservada (R_{be}min) como parâmetro de QoS e não possui parâmetro de taxa máxima. Assim, a taxa geração de *tokens* deve ser a mínima permitida e dada pela equação 4.4 a seguir:

$$Tr_{be} = R_{be}\text{min} \tag{4.4}$$

Todos os pacotes de dados BE que chegarem numa taxa maior que R_{be}min serão considerados fora de conformidade pelo mecanismo policiador, a menos que *tokens* suficiente estejam disponíveis no *bucket* no momento da chegada [48].

O esquema de policiamento e o algoritmo representando o mecanismo de policiamento utilizando o *token bucket*, para classe de serviço BE, são idênticos aos apresentados na Seção 4.3.1.3.

4.3.2 – Especificação dos Parâmetros do *bucket*

A equação geral apresentada a seguir (equação 4.5), baseada em [53] e [48], permite determinar o tamanho do *bucket* para cada policiador.

$$b[i] = N*M[i] \tag{4.5}$$

onde, M é o tamanho máximo do pacote, e N é um inteiro (N=1,2,3...), e $i \in$ {UGS, rtPS, nrtPS, BE}. Segundo os autores em [53], N=1 é recomendado para tráfego em tempo não real (nrtPS e BE) e N=2 para tráfego em tempo real (UGS e rtPS).

Caso a classe de tráfego tenha mais de uma conexão ativa, o tamanho do *bucket* e a taxa de *tokens* devem ser ajustados para levar em conta o número de conexões. O tamanho do *bucket* total da classe de tráfego i é dado pela equação 4.6 a seguir:

$$b'[i] = \sum_{j=1}^{c} bj[i] \tag{4.6}$$

onde c é o número de conexões ativas da classe i.

Da mesma forma, a taxa de *tokens* total (Tr') para uma classe de tráfego [i] com múltiplas conexões é dada pela equação 4.7 a seguir:

$$Tr'[i] = \sum_{j=1}^{c} Trj[i] \tag{4.7}$$

Segundo os autores em [4], os policiadores que controlam o tráfego de dados em tempo real devem ser configurados com parâmetros de taxa de *token* e tamanho de *bucket* de forma a permitir admissão de pacotes de dados sem nenhum atraso adicional. Este objetivo pode ser alcançado regulando o valor de N que é o responsável pelo controle do tamanho máximo do *bucket*, sem alterar as regras de definição do valor da taxa de *tokens* (Tr).

Os requisitos de taxa máxima, taxa mínima, tamanho do *bucket* e todos os outros parâmetros que são utilizados na modelagem do tráfego estão ilustrados na Tabela 4.1.

4.4 - Trabalhos Relacionados

Na literatura existe uma ampla variedade de trabalhos destinados ao padrão IEEE 802.16, no entanto, com poucas propostas de mecanismos de policiamento. Nesta

seção são discutidos e analisados trabalhos que são relacionados com o mecanismo de policiamento de tráfego apresentado nesta dissertação.

Tabela 4.1- Parâmetros utilizados na modelagem de tráfego [adaptado de 48].

Classe de Serviço	R_{max} (Kbps)	R_{min} (Kbps)	Intervalo de envio (ms)	Tr'	b'	R_{avg} (Kbps)	C_F
UGS	20	-	20	100	200	-	-
rtPS	10	-	20	50	100	-	-
nrtPS	12	8	20	50	60	10	80
	8	6	20	30	35	7	30
BE	-	2	20	10	10	-	10

No trabalho desenvolvido pelos autores em [3] o mecanismo é baseado na técnica *token bucket* para oferecer QoS para as conexões da classe de serviço BE. Como a maioria dos algoritmos de CAC utiliza prioridade estrita, as classes de serviços de menor prioridade acabam sendo penalizadas. Diante disso, os autores propõem a utilização de um mecanismo de policiamento para regular o número de conexões aceitas pelas classes rtPS e nrtPS. Os autores pretendem com isso melhorar de forma significativa o número de conexões aceitas para a classe de serviço BE. A proposta apresentada nesta dissertação usa o mecanismo de *token bucket* para todas as classes do padrão IEEE 802.16d, além de utilizar uma fila no mecanismo de policiamento conforme citado anteriormente.

Os autores em [4] propõem um mecanismo de policiamento baseado no mecanismo *token bucket* e aplicado às classes UGS, rtPS, nrtPS e BE. O mecanismo

utilizado visa oferecer QoS para conexões já estabelecidas e para aquelas que ainda pretendem entrar na rede. Foi implementado um esquema de gerenciamento de tráfego para as redes *WiMAX* com o objetivo de controlar a taxa de tráfego dos fluxos já admitidos permitindo rajadas e detectando violações dos parâmetros negociados. Os autores optaram pelo mecanismo *token bucket*, visto que não introduz atrasos adicionais nas transmissões e suporta tráfego em tempo real e rajadas, sendo isso uma característica do padrão IEEE 802.16. O mecanismo de policiamento foi implementado para ser aplicado às classes UGS, rtPS, nrtPS e BE e os parâmetros utilizados para definir a taxa em que os *tokens* são gerados e o tamanho do *bucket* são os mesmos definidos na Seção 4.3 desta dissertação. A proposta desta dissertação inclui uma fila adicional no mecanismo de policiamento para as classes nrtPS e BE com o objetivo de permitir que os pacotes que não forem transmitidos na primeira tentativa tenham uma segunda oportunidade de serem transmitidos.

Os autores em [28] utilizam os parâmetros do *token bucket* para aceitar ou rejeitar uma conexão baseado nos requisitos de QoS e na largura de banda disponível. O mecanismo de policiamento foi aplicado em 3 classes de serviço das redes *WiMAX:* UGS, rtPS, nrtPS, e os parâmetros do *token bucket* foram especificados para cada uma das classes de serviços separadamente. O autor fixa a taxa de geração de *tokens* igual à taxa média das conexões. O autor não especifica como foi escolhido o tamanho do *bucket*. Como as classes de maior prioridade podem utilizar toda a largura de banda disponível, impedindo desta maneira que as classes de menor prioridade acessem o meio, foi inserido em todas as SSs o mecanismo de policiamento com o objetivo de forçar as conexões a obedecerem aos contratos de tráfegos negociados antes do estabelecimento das conexões. Nesta dissertação, o tamanho do *bucket* e os parâmetros

de taxa máxima e taxa mínima permitida foram escolhidos baseados nos valores da MSTR, MRTR e no trabalho apresentado por [4], [48].

Os autores em [32] propõem um mecanismo que utiliza o *token bucket* para realizar o escalonamento de pacotes e o controle de conexões nas redes do padrão IEEE 802.16 para tráfegos em tempo real. É utilizado um modelo matemático para realizar a estimativa de largura de banda da classe rtPS a fim de respeitar os requisitos de atraso. O mesmo modelo matemático foi utilizado para realizar o cálculo dos parâmetros da taxa de *tokens* baseado em atraso de fila e perda de pacotes de um fluxo de tráfego. Nesta dissertação os valores atribuídos a taxa de *tokens* e tamanho do *bucket* foram utilizados com base no RFC 2215 [50], e no trabalho apresentado por [4], [48].

A proposta apresentada pelos autores em [33] propõe um modelo matemático para determinar os valores ideais para serem utilizados na técnica do *token bucket.* Os autores propõem um mecanismo para descobrir quais são os valores ideais para o tamanho do *bucket* (b), taxa de geração de *tokens* (Tr) e tamanho da fila (C_F) para um fluxo de dados de forma que não haja perda considerável de pacotes. Os autores propõem um tamanho de fila que insere um atraso mínimo nos pacotes armazenados para todos os fluxos de dados. Ademais, o mecanismo propõe definir qual o tamanho mínimo da fila de espera baseado nos valores do tamanho do *bucket* (b) e taxa de geração de *tokens* (Tr). Nesta dissertação foi utilizada a técnica do *token bucket* com fila de espera, onde os parâmetros do tamanho do *bucket* (b) e taxa de geração de *tokens* (Tr) foram baseados em [53]. O mecanismo utilizando a fila de espera foi aplicado para as classes de serviços nrtPS e BE do padrão IEEE 802.16d.

4.5 - Considerações Finais

Neste capítulo apresentou-se uma proposta de mecanismo de policiamento baseado na técnica *token bucket* visando a provisão de QoS em redes do padrão IEEE 802.16. A principal motivação para o desenvolvimento deste trabalho está relacionada ao fato do padrão IEEE 802.16 deixar em aberto as questões referentes à provisão de QoS. Outro fator, motivacional, é que atualmente não existe na literatura um mecanismo que ofereça uma segunda oportunidade de transmissão para os pacotes pertencentes às classes nrtPS e BE. Neste sentido, este trabalho apresenta uma proposta de tratamento diferenciado para tráfego de dados em não tempo real, permitindo uma nova tentativa de transmissão e diminuindo deste modo o descarte de pacotes e as retransmissões.

Os parâmetros do *token bucket* foram definidos baseados no trabalho apresentado por [4], [48] e pelo RFC 2215 [50].

Capítulo 5

AVALIAÇÃO DA PROPOSTA DE MECANISMO DE POLICIAMENTO DE TRÁFEGO PARA REDES IEEE 802.16

5.1 - Introdução

Neste capítulo, o mecanismo de policiamento de tráfego utilizando a técnica *token bucket*, proposto no Capítulo 4, é avaliado através de modelagem e simulação. Neste estudo considerou-se as 4 principais classes de serviço especificadas pelo padrão IEEE 802.16d. Para isso utilizou-se o simulador *Network Simulator-2* [35] acrescido do módulo desenvolvido por [2], o qual foi modificado para a realização de vários experimentos para avaliação do comportamento da proposta.

Inicialmente, na Seção 5.2 apresenta-se as ferramentas de simulação que foram analisadas no desenvolvimento desta pesquisa. Na sequência, na Seção 5.3 descreve-se o cenário de rede que foi utilizado para a obtenção dos resultados de simulação. Em seguida, na Seção 5.4 descreve-se os parâmetros de simulação que foram utilizados. Por fim, na Seção 5.5 é realizada a apresentação e análise dos resultados que foram obtidos nas simulações.

5.2 - Modelagem e Simulação

5.2.1 - Ferramentas de Simulação

Atualmente existe uma grande quantidade de ferramentas de simulação disponíveis, as quais auxiliam nos estudos de avaliação de desempenho de redes de computadores. Estes estudos apresentam um papel importante no projeto, análise e implementação de sistemas de comunicação, principalmente em sistemas que apresentam projetos de implantação caros e complexos. A utilização de modelagem e simulação é uma forma viável de analisar o comportamento de redes de computadores devido a sua flexibilidade com diferentes cenários que podem ser criados, incluindo o comportamento dos protocolos e o impacto de novas tecnologias sobre as redes [30].

Existem diversos simuladores de rede disponíveis, os que mais se destacam comercialmente e academicamente são o *OPNET*, o *OMNeT++* e o *Network Simulator* (NS).

A ferramenta de simulação OMNeT++ (*Objective Modular Network Testbed* in C++) é um simulador de eventos discretos e orientado a objetos, sendo muito utilizado na simulação de protocolos e redes de telecomunicações. Este simulador apresenta uma estrutura modular onde sempre que necessário é possível acoplar novos módulos ao sistema para que novas funções sejam disponibilizadas. Atualmente este simulador está sendo bastante utilizado pela comunidade acadêmica para estudos de avaliação de desempenho de redes de computadores.

Já a ferramenta *OPNET* é um simulador comercial bastante utilizado nos meios corporativos devido as suas funcionalidades e precisão nos resultados. Este simulador

permite a especificação de um grande número de componentes. É uma ferramenta comercial bastante restrita nos ambientes acadêmicos devido ao seu elevado custo [13].

Por sua vez, o NS-2 é um simulador de eventos discretos, escrito nas linguagens C++ e oTCL, sendo voltado para o desenvolvimento de pesquisas em redes de computadores com suporte à arquitetura TCP/IP, permitindo a inclusão de módulos que simulam protocolos de redes específicos [2]. Nesta dissertação é utilizado o NS-2 devido ao fato de ser uma ferramenta de código aberto, com a possibilidade de se criar e inserir novos módulos, além de ser bastante utilizado no meio acadêmico para pesquisas científicas.

5.3 – Cenário de Simulação

O cenário de simulação adotado neste estudo é composto de uma BS e 5 SSs distribuídas uniformemente ao redor da BS. A distância máxima permitida entre uma SS e a BS foi mantida em 500 metros e a modulação e codificação utilizada é a OFDM-64QAM ¾. A chegada de pacotes de dados obedece à distribuição de *Poisson* com taxa de tráfego variável entre os experimentos para cada uma das classes de serviços. O tempo entre as chegadas de pacotes são constantes e iguais a 20 ms para todas as conexões. O tráfego UGS foi gerado por uma fonte CBR, sendo que os pacotes são gerados a cada 20 ms. O tráfego rtPS utiliza um gerador VBR e o nrtPS utiliza uma fonte FTP com pacotes de tamanho variando entre 10 e 40 *bytes*. Por fim, para o tráfego de melhor esforço utilizou-se pacotes com tamanho de 10 *bytes* e uma fila com capacidade para 10 pacotes.

O *bucket* é iniciado completamente cheio e foram consideradas 4 classes de serviços com o número de conexões variável para cada experimento.

5.4 - Parâmetros de Simulação

As simulações foram realizadas considerando 5 conexões sendo uma conexão por estação. Os principais parâmetros de simulação referentes à camada MAC e física são apresentados na Tabela 5.1 e foram escolhidos por serem utilizados na maioria dos trabalhos apresentados na literatura [30], [48], [11].

Tabela 5.1 – Parâmetros de simulação referentes à camada MAC e física.

Parâmetros	**Valores**
Largura de Banda	5 MHz
Duplexação	TDD
Antena	Omnidirecional
Duração do *Frame*	20 ms
Prefixo Cíclico	0,25
Tempo de Simulação	50/60/80s
MCS Empregado	OFDM 64 QAM ¾
Taxa de Transmissão *uplink*	7,7 Mbps

Os seguintes parâmetros: taxa de *tokens* e tamanho do *bucket,* utilizam valores similares aos utilizados pelos autores em [4], [48] e [53]. Estes parâmetros apresentam seus valores alterados diferentemente entre os experimentos, conforme [48], com o objetivo de verificar o comportamento da rede em diferentes situações.

5.5- Apresentação e Análise de Resultados

Nesta seção são apresentados os resultados obtidos por meio de modelagem e simulação utilizando diferentes experimentos. O objetivo de cada experimento é analisar a eficiência do mecanismo de policiamento de tráfego proposto.

Para analisar os arquivos de *trace* gerados pelo *Network Simulator*-2 foi utilizado um aplicativo desenvolvido por [30], pelo fato de ser flexível no tratamento dos dados em relação a outras ferramentas existentes.

5.5.1 Avaliação do Mecanismo de Policiamento Proposto Considerando a Classe rtPS

O objetivo deste experimento é analisar o comportamento da taxa média de descarte de pacotes em função do intervalo de geração de *tokens* para classe rtPS, onde a carga de tráfego injetada na rede permaneceu constante. Neste sentido, os parâmetros utilizados são os seguintes: A carga de tráfego gerada por cada estação remetente é de 10 Kbps e o *bucket* teve seu tamanho fixado em 100 *tokens*. Conforme pode ser visto na Figura 5.1, o intervalo de geração de *tokens* varia de 10 ms a 100 ms em intervalos de 10 ms e, à medida que este valor aumenta, a taxa média de descarte de pacotes cresce exponencialmente, uma vez que menos *tokens* são inseridos no *bucket.*

Observa-se neste experimento, cujos resultados são mostrados na Figura 5.1, que o intervalo de geração de *tokens* influencia de forma significativa na taxa média de descarte de pacotes [63], [64], [65], [66].

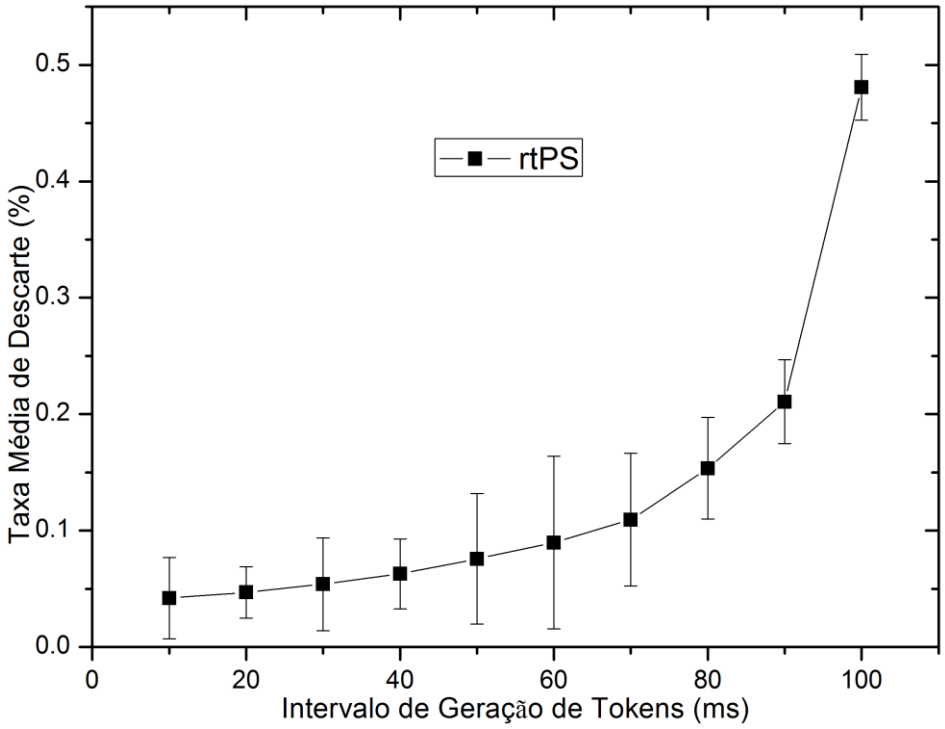

Figura 5.1: Taxa média de descarte em função do intervalo de geração de *tokens*.

5.5.2 Avaliação do Mecanismo de Policiamento Proposto Considerando as Classes rtPS e nrtPS

O objetivo deste experimento é analisar a taxa média de descarte de pacotes em função da carga de tráfego aplicada à rede pelos fluxos das classes de serviços rtPS e nrtPS. Neste experimento, o *bucket* possui um tamanho de 100 *tokens* com taxa de geração de 100 *tokens/s*. Para isso realizaram-se 6 diferentes simulações variando-se a carga de tráfego injetada na rede pelas conexões rtPS e nrtPS de 500 Kbps a 3500 Kbps. Pode-se observar através da Figura 5.2, que a taxa média de descarte de pacotes aumenta exponencialmente tanto para rtPS como para nrtPS. Isso se deve ao fato de que, como ambos, taxa de geração de *tokens* e tamanho do *bucket*, são constantes, a vazão média obtida na rede estará limitada a um valor máximo. Deste modo, o tráfego

em não conformidade será descartado pela rede justificando o gráfico apresentado na Figura 5.2.

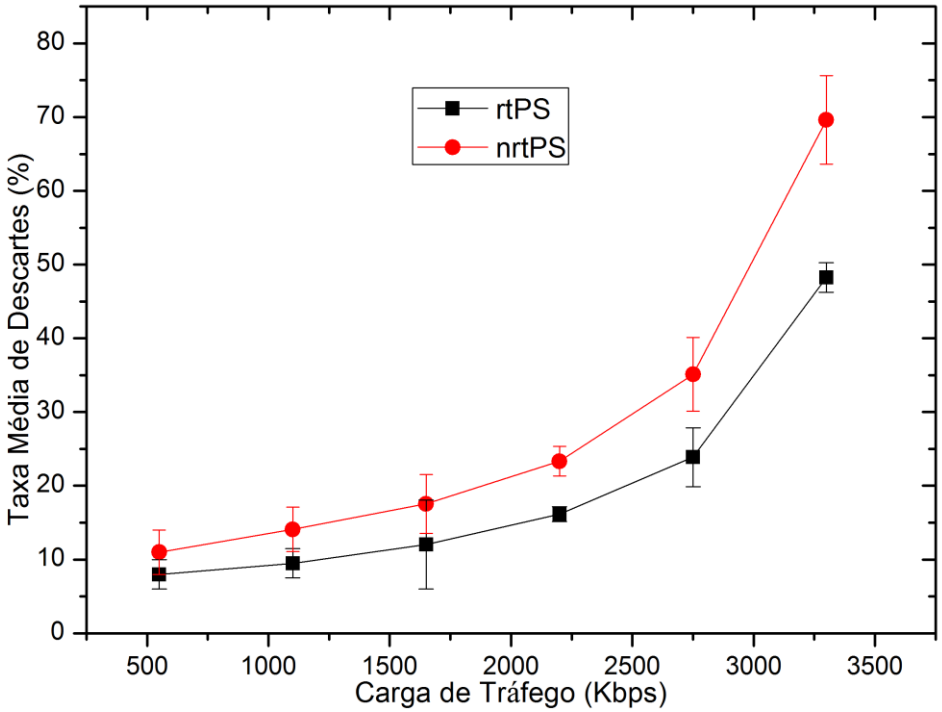

Figura 5.2: Taxa média de descarte em função da carga de tráfego.

Neste experimento observa-se que o descarte de pacotes é mais agressivo com a classe nrtPS devido ao fato da classe rtPS apresentar maior prioridade de tráfego sendo esse fato levado em consideração pelo escalonador, que escalona o tráfego rtPS antes do nrtPS [63], [64], [65], [66].

5.5.3 Avaliação do Mecanismo de Policiamento Proposto Considerando a Classe nrtPS

O objetivo do experimento considerado nesta seção é analisar a influência da inserção de uma fila de espera adicional e finita no mecanismo policiador nrtPS proposto. A fila será importante neste experimento, pois irá armazenar pacotes nrtPS

que não foram transmitidos na primeira oportunidade por falta de *tokens*. Como a fila apresenta um tamanho finito, nem todos os pacotes que não conseguiram ser transmitidos na primeira oportunidade serão armazenados na fila, mas aqueles pacotes enfileirados terão garantia de uma segunda oportunidade de transmissão. O gráfico apresentado pela Figura 5.3 descreve o comportamento da vazão média total em função do tempo de simulação para a classe nrtPS.

Neste experimento a fila apresenta um tamanho de 80 pacotes e o *bucket* um tamanho fixo de 60 *tokens*. A taxa de geração de *tokens* é de 50 *token*/s, e a carga média de tráfego gerada por cada estação remetente é de 10 Kbps. Este experimento foi realizado utilizando 5 SSs, sendo que a primeira entra na rede 12s após o início da simulação e as outras em intervalos regulares de 1s.

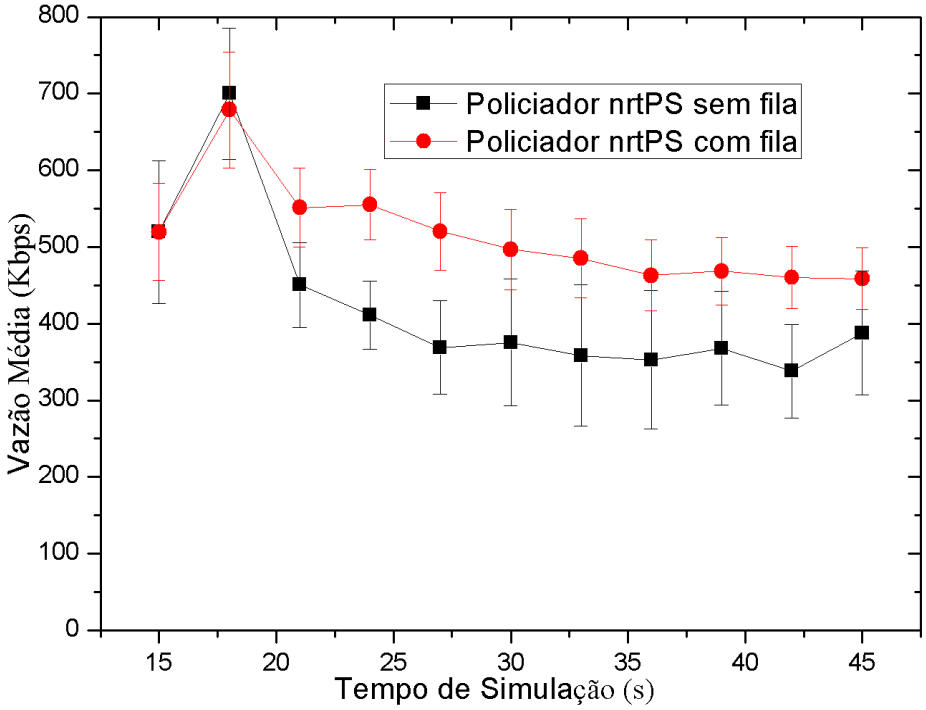

Figura 5.3: Vazão média total em função do tempo de simulação.

O tempo de simulação considerado é de 50s. Neste experimento quando o mecanismo policiador sem fila de espera é utilizado, a vazão atinge seu pico no tempo de 17s com valor aproximado de 700 Kbps, diminuindo posteriormente e sofrendo pequenas alterações devido à transmissão estar sendo regulada pelo mecanismo policiador.

Para o mecanismo policiador com fila observa-se um pequeno aumento da vazão. Isto ocorre devido à transmissão dos pacotes que foram armazenados na fila de espera. A partir do tempo de 17s observa-se, para o mecanismo policiador com a utilização da fila de espera, que houve um significativo aumento da vazão em comparação com o mecanismo convencional. Este fato é devido ao aproveitamento dos pacotes armazenados na fila de espera.

O gráfico mostrado na Figura 5.4 apresenta o atraso médio total obtido após a inserção da fila de espera no mecanismo de policiamento para classe nrtPS.

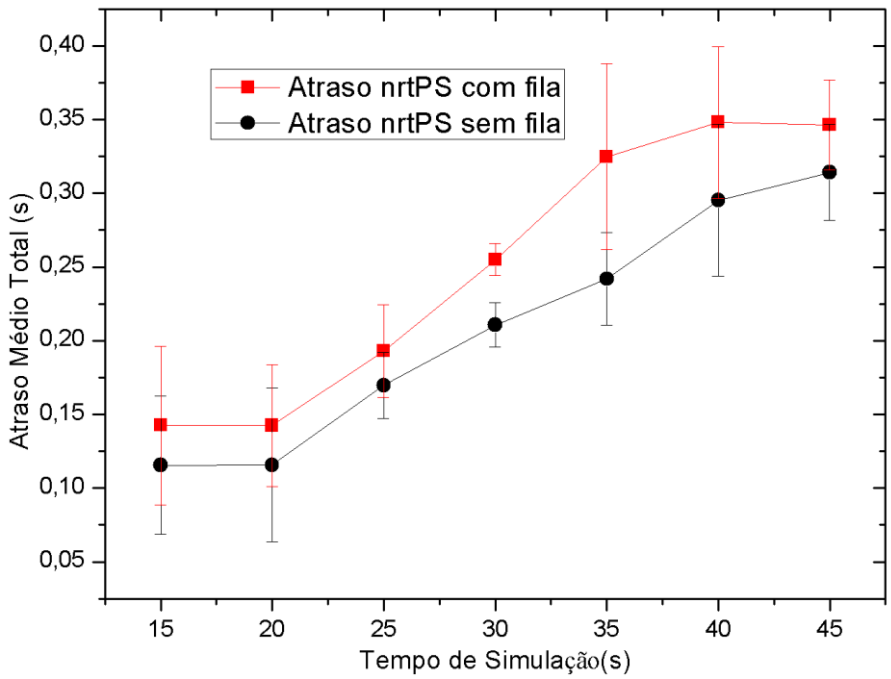

Figura 5.4: Atraso médio total em função do tempo de simulação.

Pode-se observar que a inserção da fila de espera adiciona um pequeno atraso nas transmissões da classe nrtPS. No intervalo de 15s a 20s, o atraso permaneceu praticamente constante para os dois experimentos, com pequeno acréscimo para o mecanismo com fila devido ao atraso imposto pela fila de espera. Com o tempo de simulação acima de 20s, o atraso aumenta linearmente nos dois experimentos. Para o policiador sem fila de espera, o atraso é crescente devido à limitação imposta pela taxa de geração de *tokens*, enquanto que no experimento com fila, o atraso médio total é maior devido à limitação imposta pela taxa de *tokens* e pelo atraso inserido enquanto os pacotes aguardam para serem transmitidos na fila de espera inserida no mecanismo de policiamento.

A Figura 5.5 descreve o comportamento da taxa média de descarte em função do tamanho da fila de espera classe nrtPS. O objetivo deste experimento é analisar a influência do tamanho da fila de espera na diminuição do descarte de pacotes que não foram transmitidos na primeira oportunidade.

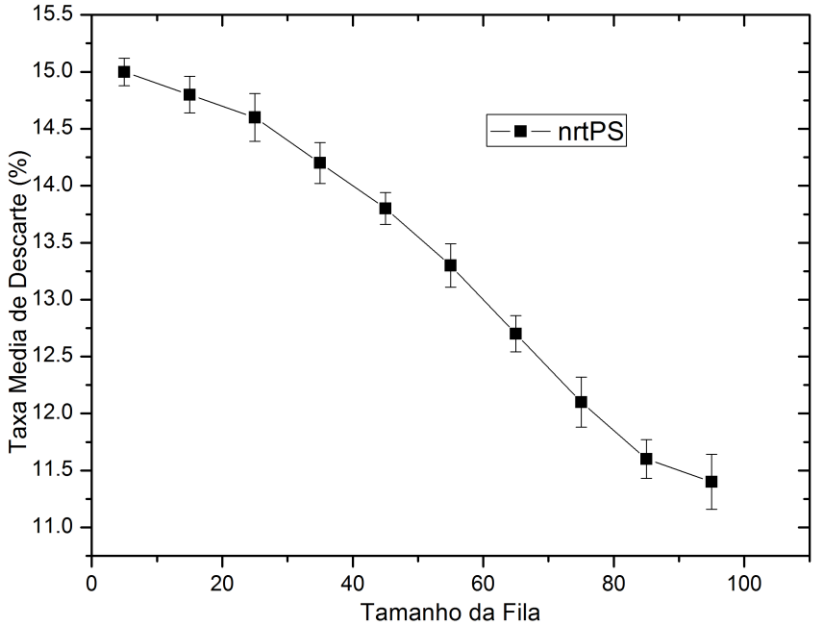

Figura 5.5: Taxa média de descartes em função do tamanho da fila de espera.

Diante disso, para este experimento, o *bucket* tem o seu tamanho definido em 300 *tokens* com taxa de geração de 12 *tokens/s*. Foram realizadas neste experimento 10 simulações diferentes, onde apenas o tamanho da fila de espera sofre um aumento em 10 pacotes entre cada simulação. O tamanho inicial da fila de espera é de 5 pacotes.

Conforme pode ser observado, com o aumento do tamanho da fila de espera a taxa média de descarte dos pacotes da classe nrtPS sofreu uma expressiva diminuição. Pode-se observar que mantendo os valores iniciais da taxa de *tokens*, tamanho do *bucket* e aumentando o tamanho da fila entre as simulações, a taxa média de descarte tende a diminuir significativamente.

5.5.4 Avaliação do Mecanismo de Policiamento Proposto Considerando a Classe BE

Nesta subseção apresentam-se os estudos de avaliação de desempenho do mecanismo de policiamento proposto em relação à classe BE. O objetivo principal é avaliar a influência causada pela inserção de uma fila de espera para pacotes que não foram transmitidos na primeira oportunidade. A carga de tráfego mínima gerada por cada estação remetente é de 2 Kbps. O tamanho do *bucket* foi fixado em 10 *tokens* e a taxa de geração de *tokens* é de 10 *tokens*/s. A fila de espera tem capacidade para 10 pacotes. A Figura 5.6 descreve o comportamento da vazão média em função do tempo de simulação.

Neste experimento foram utilizadas 5 SSs com conexões BE, sendo que a primeira entra na rede no tempo de 17s e as outras são adicionadas em intervalos

regulares de 1s. No tempo de 19s, após o início da simulação, pode-se verificar no gráfico da Figura 5.6 que a vazão atinge seu valor máximo.

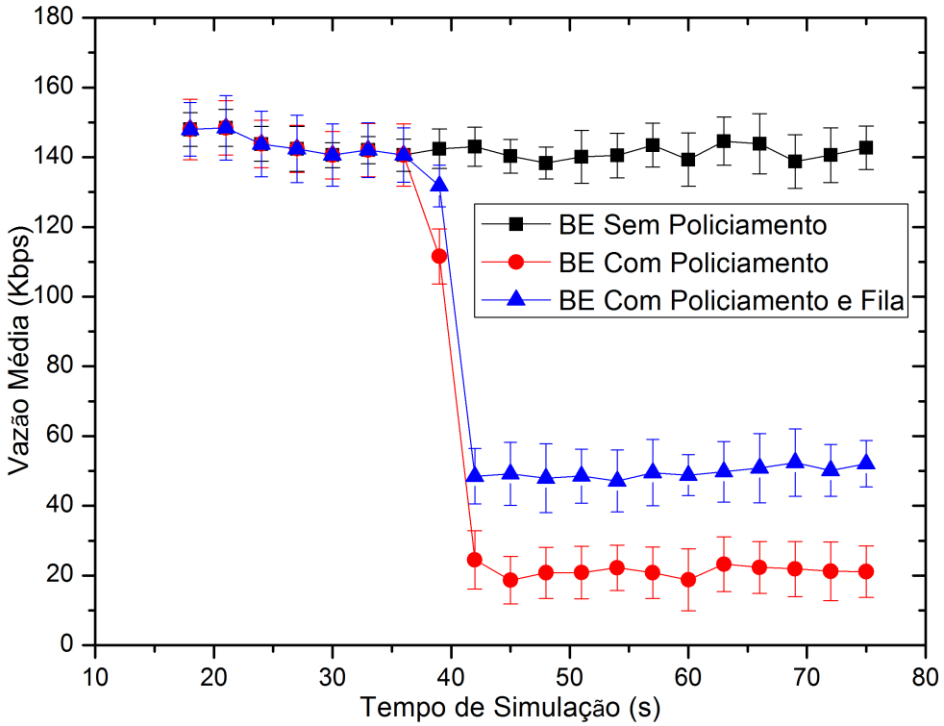

Figura 5.6: Vazão média em função do tempo de simulação.

Para o experimento onde não se utiliza policiamento a vazão sofre pequenas alterações, aumentando ou diminuindo, ao longo do tempo de simulação. Adicionando o mecanismo de policiamento percebe-se que a vazão é consideravelmente diminuída devido à conformação de tráfego imposta pelo mecanismo de policiamento. Com a utilização da fila de espera, pode-se observar que a vazão sofreu um aumento significativo em seus valores comparado ao experimento com policiamento sem fila. Este experimento mostra que utilizando uma fila de espera no mecanismo de policiamento é possível aumentar a vazão a partir da diminuição do descarte de pacotes e das retransmissões.

A Figura 5.7 mostra o comportamento do atraso médio em função do tempo para as conexões pertencentes à classe BE. Neste experimento todos os parâmetros utilizados são os mesmos do experimento anterior.

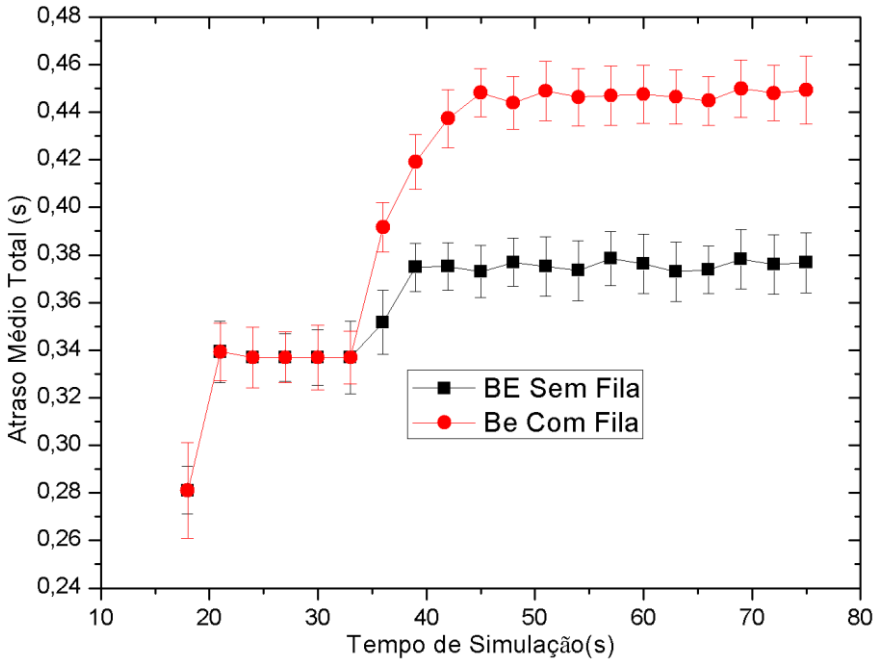

Figura 5.7: Atraso médio total em função do tempo de simulação.

Analisando os resultados apresentados na Figura 5.7 para o mecanismo sem fila, pode-se observar 2 fenômenos que ocorrem ao longo da simulação. De 17s a 40s o atraso sofreu um aumento devido à entrada das conexões na rede. A partir de 40s o atraso permaneceu praticamente constante ao longo da simulação. Isto ocorre porque os *tokens* que vão sendo gerado, imediatamente são retirados do *bucket* por um pacote que chega ao mecanismo, mantendo o atraso médio com pequenas variações ao longo do tempo. Para o mesmo experimento utilizando a fila, pode-se observar 3 fenômenos que ocorrem ao longo da simulação. De 17s a 35s o comportamento do atraso médio total foi similar ao experimento anterior. De 35s a 45s houve um aumento no atraso médio devido ao atraso imposto pela fila de espera. A partir do tempo de 45s de simulação,

verifica-se que o atraso médio permanece praticamente constante com pequenas variações. O fato do atraso médio permanecer praticamente constante justifica-se pela retirada imediata dos *tokens* que estão sendo gerado do *bucket*. Esta retirada de *tokens* do *bucket* pode ser realizada pelos pacotes que estão sendo injetados na rede ou por pacotes da fila de espera. O atraso médio é significativamente maior no experimento com fila devido ao atraso imposto pelo tempo de armazenamento em fila.

5.5.5 Avaliação do Mecanismo de Policiamento Proposto Considerando a Classe UGS

O objetivo deste experimento de simulação é avaliar a influência dos policiadores de tráfego rtPS no desempenho das conexões UGS.

Definiu-se o tamanho do *bucket* como sendo 200 *tokens* e uma taxa de geração de 100 *tokens*/*s*. Utilizaram-se 5 conexões rtPS e 5 conexões UGS. A primeira conexão UGS entra na rede 11s após o início da simulação e as outras conexões desta classe entram com intervalos regulares de 1s. A primeira conexão rtPS entra na rede aos 16s e as outras conexões rtPS entram com intervalos regulares de 1s. Para este experimento o mecanismo de policiamento proposto foi aplicado apenas aos fluxos da classe rtPS. A Figura 5.8 mostra a vazão média em função do tempo de simulação para classe UGS.

Pode-se observar na Figura 5.8 que a utilização ou não do mecanismo de policiamento proposto aplicado à classe rtPS não interfere na vazão do fluxo UGS, que permaneceu constante ao longo do tempo. Isso pode ser explicado pelo fato de todo o tráfego UGS ser escalonado antes do tráfego rtPS devido a prioridade existente. Esta

mesma avaliação é válida se o mecanismo de policiamento proposto for ativado para as classes nrtPS e BE.

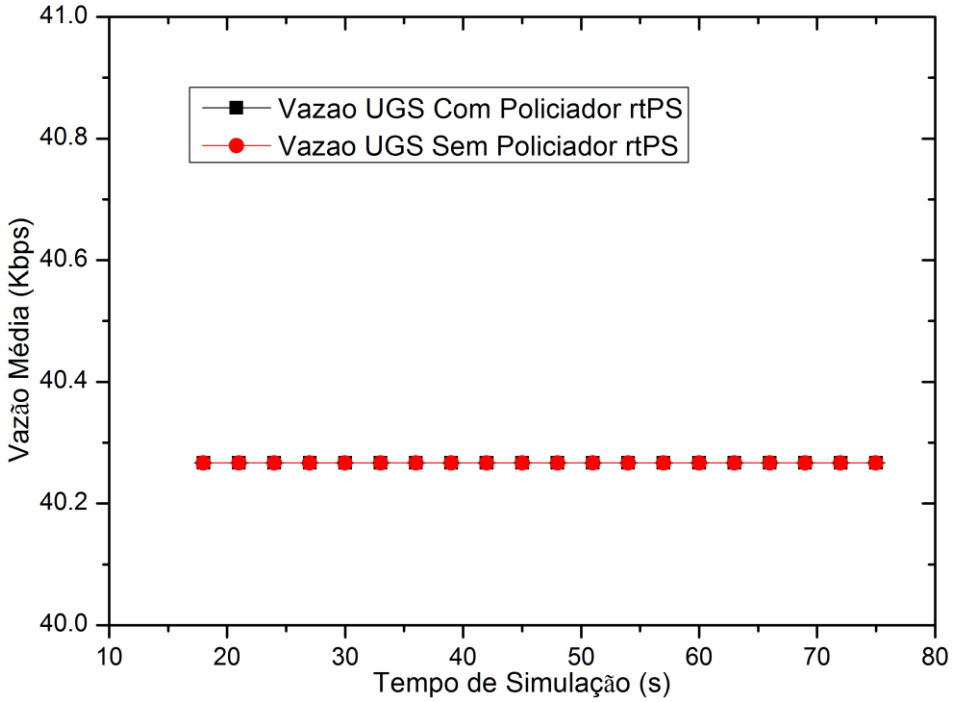

Figura 5.8: Vazão média em função do tempo de simulação.

O objetivo do experimento com resultados apresentados na Figura 5.9 é analisar a taxa média de descarte de pacotes em função da carga de tráfego aplicada à rede pelas conexões UGS. A carga de tráfego gerada por cada estação é de 16 Kbps e a taxa de geração de *tokens* é de 160 *tokens*/s. O *bucket* possui um tamanho de 160 *tokens*. Estão sendo utilizadas 15 conexões UGS, sendo que a primeira conexão é estabelecida na rede 15s após o início da simulação e as outras em intervalos regulares de 1s. Os valores atribuídos aos parâmetros neste experimento são similares àqueles utilizados por [48] alterando apenas o número de conexões.

Pode-se observar através da Figura 5.9 que a taxa média de descarte de pacotes para a classe UGS é aproximadamente 0%. Isso se deve a quantidade de *tokens*

armazenados no *bucket*, o que permite que mais pacotes de dados sejam transmitidos através do escalonador.

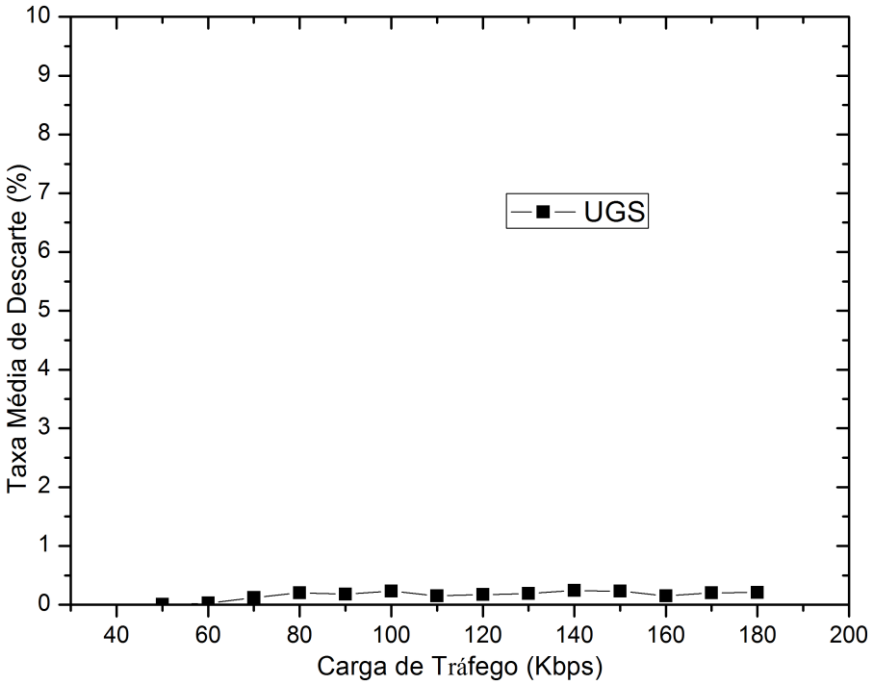

Figura 5.9: Taxa média de descartes em função da carga de tráfego.

5.6 - Conclusão

Neste capítulo foi avaliado, através de modelagem e simulação, o mecanismo de policiamento proposto no Capítulo 4. Em todos os experimentos analisados foram avaliadas a eficiência do mecanismo de policiamento em termos do tempo de simulação, vazão, atraso e descarte de pacotes e carga de tráfego, tanto para fluxos em tempo real quanto para fluxos em tempo não real.

Verifica-se através dos resultados obtidos que o mecanismo multi-policiador é eficiente e pode auxiliar de forma significativa no provimento de QoS para conexões de uma rede. Ademais, verificou-se que a utilização da fila de espera diminuiu o descarte de pacotes e aumentou a vazão média final para os fluxos não tempo real.

Capítulo 6

CONCLUSÕES GERAIS

Nos últimos anos as redes de comunicação sem fio vêm apresentando grandes avanços no fornecimento de serviços para os usuários finais, principalmente no provimento de Internet banda larga sem fio. Neste sentido, o padrão IEEE 802.16 surge como uma solução que possibilita benefícios e oportunidades aos usuários localizados em regiões de difícil acesso ou suburbanas. Diante deste cenário, esta dissertação apresenta as principais características presentes no padrão IEEE 802.16, visto que se trata de uma tecnologia BWA extremamente promissora permitindo a transmissão de dados sem fio a longas distâncias com QoS, sendo este um dos diferenciais em relação às tecnologias de redes sem fio convencional.

Atualmente, o padrão IEEE 802.16 surge como uma tecnologia promissora com custo relativamente baixo se comparado as redes de "última milha" cabeadas, e tem recebido uma atenção especial por parte da comunidade cientifica internacional como também das principais empresas de tecnologias espalhadas pelo mundo.

A principal característica do padrão IEEE 802.16 é o provimento de QoS, garantido através de mecanismos de escalonamento, CAC e policiamento de pacotes. Em virtude do padrão IEEE 802.16 deixar em aberto a oportunidade de implementação dos mecanismos citados anteriormente, surge uma ampla área de pesquisa e uma oportunidade para o desenvolvimento deste trabalho.

O objetivo principal desta dissertação foi apresentar um mecanismo de provisão de QoS, que realiza o policiamento de dados, para o padrão IEEE 802.16. Diante disso, para o desenvolvimento desta dissertação foi necessário, inicialmente, apresentar todas as características básicas do padrão bem como todos os mecanismos utilizados na provisão de QoS. Foi apresentada a especificação e as principais características do padrão IEEE 802.16, bem como uma breve comparação do *WiMAX* com outras tecnologias existentes. Foi detalhada a evolução do padrão desde o IEEE 802.16a até o padrão IEEE 802.16m. Foram apresentados os modos de operação utilizados e o modelo de referência do padrão IEEE 802.16, bem como as principais características das subcamadas pertencentes à camada MAC e os detalhes da camada física.

Aspectos relativos aos mecanismos necessários para o provimento de QoS no padrão IEEE 802.16 foram descritos. Além disso, as principais características dos mecanismos de provisão de QoS no padrão IEEE 802.16 e as definições básicas de escalonamento e CAC foram apresentadas. Em seguida as principais técnicas utilizadas no policiamento de tráfego na literatura foram citadas.

Com base no levantamento bibliográfico realizado foi apresentada a proposta de pesquisa desenvolvida nesta dissertação, que consiste num mecanismo de policiamento de tráfego de dados no sentido *uplink* para prover QoS para as aplicações não tempo real. O mecanismo de policiamento proposto utiliza a técnica *token bucket* devido ao fato deste permitir e detectar possível violação de parâmetros negociados no contrato de tráfego. Além disso, o mecanismo proposto é multi-policiador e atende a cada uma das classes de serviços UGS, rtPS, nrtPS e BE, com o diferencial de utilização de uma fila de espera para o tratamento do tráfego nrtPS e BE.

Por meio de modelagem e simulação avaliou-se a eficiência do mecanismo de policiamento proposto para classes em não tempo real. De acordo com os resultados obtidos foi verificado, para as classes nrtPS e BE, uma melhora significativa na taxa média de descarte. Verificou-se que o tamanho do *bucket* e a taxa de geração de *tokens* influenciam de forma significativa na taxa de descarte para as classes não tempo real. Outro fato importante verificado foi que a utilização da fila de espera diminui significativamente o descarte de pacotes para o tráfego não tempo real.

Não obstante os resultados obtidos mostrarem vantagens do mecanismo de policiamento proposto, alguns pontos que podem melhorar o desempenho do mecanismo não foram tratados nesta dissertação. Dentre eles, sugere-se a inserção de uma segunda fila de espera no mecanismo de policiamento de forma que pacotes de tráfego BE e nrtPS possam ser armazenados em filas distintas. A inserção desta fila irá permitir um tratamento diferenciado aos tráfegos de dados que forem armazenados nas filas de espera.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S. Ahson and M. Ilyas. *WiMAX Aplication*. Boca Raton: CRC Press, 2008.

[2] A. Belghith and L. Nuaymi, *Design and Implementation of a QoS-included WiMAX Module for NS-2 Simulator. Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications*; pp. 28, 2008.

[3] L. Mokdad, J. Ben-Othman, and M. Cheikh, *Improving QoS for BE Traffics in WiMAX Networks. Computer Systems and Applications (AICCSA), IEEE/ACS International Conference on*; pp. 1-5, 2010.

[4] S. Ghazal, J. Ben-Othman, and J.P. Claude, *Traffic Management Based on Token Bucket Mechanism for WiMAX Networks*. Cluster Computer, 2011.

[5] IEEE 802.16-2001, *IEEE Standard for Local Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Systems. tech. rep., IEEE Computer Society*, 2001.

[6] C. Cicconetti, L. Lenzini, and E. Mingozzi, *Quality of Service Support in IEEE 802.16 Networks, University of Pisa Carl Eklund, Nokia Research Center*, 2006.

[7] S. Ahmadi, *An Overview of Next-Generation Mobile WiMAX Technology*. Santa Clara: Intel Corporation, 2009.

[8] Y. Zhang; H. Chen, *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Network, Auerbach Publications*, 2008.

[9] C. So-In, R. Jain, A. Tamini, *Scheduling in IEEE 802.16e Mobile WiMAX Networks: Key Issues and a Survey*, E.U.A: IEEE, 2009.

[10] *WiMAX FORUM*, Disponível em: <http://www.wimaxforum.org>. Acesso em Abril de 2012.

[11] J. F. Borin, *Mecanismos para Provisão de Qualidade de Serviço em Redes IEEE 802.16***.** Tese de Doutorado, Unicamp, 2010.

[12] J. F. Borin, *Provisão de Qualidade de Serviço em Redes IEEE 802.11*. Dissertação de Mestrado, UNICAMP, 2004.

[13] C. L Soares, *Proposta de um Algoritmo de Controle de Admissão de Conexões Baseado em Threshold para as Redes IEEE 802.16*. Dissertação de Mestrado, UFU, 2009.

[14] A. Bacioccola, C. Cicconetti and C. Eklund, L. Lenzini, Z. LI and E. Mingozzi, IEEE 802.16: *History, Status and Future Trends***.** *Computer Communications*, vol. 33, no. 2, pp. 113-123, Nov. 2009.

[15] R. Prasad and F. J. Velez, *WiMAX Networks: Techno-Economic Vision and Challenges.* Berlim: Springer, 2010.

[16] C. A. Rodrigues, *Escalonamento de Tráfego em Redes WiMAX no Modo PMP*. Dissertação de Mestrado, UNB, 2009.

[17] C. Eklund, R. B. Marks, *IEEE Standard 802.16: A Technical Overview of the WirelessMan™ Air Interface for Broadband Wireless Access*. *IEEE Communications Magazine,* v. 40, no. 6, pp. 98-107, 2002.

[18] IEEE 802.16-2004, *IEEE Standard for Local and Metropolitan Area Networks – Part16: Air Interface for Fixed Broadband Wireless Access Systems*. tech. rep., *IEEE Computer Society*, October, 2004

[19] S. Naves, R. Chan and A. M. Alberti, *Wimax-IEEE 802.16: Principais Tecnologias, Cenários e Estudo de Caso.* Santa Rita do Sapucaí, 2006.

[20] I. C. Msadaa, D. Câmara and F. Filali, *Scheduling and CAC in IEEE 802.16 Fixed BWNs: A Comprehensive Survey and Taxonomy*. *IEEE Communications Surveys Tutorials*, v. 12, no. 4, pp. 459-487, 2010.

[21] IEEE 802.16-2005, *IEEE Standard for local and metropolitan area networks – Part16: air interface for fixed Broadband Wireless access systems*. tech. rep., *IEEE Computer Society*, February, 2005.

[22] Y. A. Sekercioglu, M. Ivanovich and A. Yegin, *A Survey of MAC Based QoS Implementation for WiMAX Networks*. *Computer Networks*, vol.53, no. 14 pp. 2517-2536, 2009.

[23] IEEE 802.16-2005, *Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in licensed Band*, tech. rep *IEEE Computer Society*. pp. 1-822, 2006.

[24] A. Ghosh, D. R. Wolter, J. G. Andrews and R. Chen. *Broadband Wireless Access with WiMAX 802.16: Current Performance Benchmarks and Future Potencial. IEEE Communications Magazine*, vol. 43, n. 2. pp. 129-136, 2005.

[25] M. S. Kuran, T. Tugcu, *A Survey on Emerging Broadband Wireless Access Technologies. Computer Networks*, vol. 51, no. 11, pp. 3013-3046, 2007.

[26] Cisco home Page, *Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting.* Disponível em: <http://www.cisco.com>. Acesso em Abril 2012.

[27] M. Ma, *Current Technology Developments of WiMAX Systems***.** Singapura: Springer, 2009.

[28] K. Wongthavarawat, A. Ganz, *Packet Scheduling for QoS Support in IEEE 802.16 Broadband Wireless Access Systems*, *International Journal of Communication Systems*, vol. 16, pp.81-96, n. 1, February, 2003.

[29] P. Dhrona, *A Performance Study of Uplink Scheduling Algorithms in Point to Multipoint WiMAX Networks*, Queens's University, Kingston, Canadá, 2007.

[30] E. C. Rosa, *Proposta de um Esquema para Provisão de QoS no Padrão IEEE 802.16.* Dissertação de Mestrado, UFU, Brasil, 2011.

[31] K. I. Park. *QoS in packet networks*, vol. 779, USA: Springer-Verlag, 2005.

[32] T. Tsai, C. Jiang and C. Wang, *CAC and Packet Scheduling Using Token Bucket for IEEE 802.16 Networks, Journal of Communication*, vol. 1, no. 2, pp. 30-37, May 2006.

[33] P. P. Tang and T. Y. C. Tai, *Network Traffic Characterization Using Token Bucket Model, INFOCOM'99. Proceeding. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*; vol. 1; pp. 51- 62; 1999.

[34] A. Ahmed, A. Shami, *A New Bandwidth Allocation for EPON-WiMAX Hybrid Access Networks. GLOBECOM, 2010 IEEE Global* Telecommunications Conference; pp. 1-6; 2010.

[35] Network Simulation 2 – NS-2. Disponível em: <http://www.isi.edu/nsnam/ns/>. Acesso em abril de 2012.

[36] C. V. N. Albuquerque, *Arquitetura de Implementação de Alto Desempenho para Sistema de Comunicação Multimídia*, Dissertação de Mestrado, UFRJ, 1995.

[37] J. Junior, J. Monteiro, *On the Efficiency of Policing Mechanisms for ATM Networks, IEEE* ITS'94, pp. 470-474, 1994.

[38] L. Dittman, S. Jacobsen, K. Moth, *Flow Enforcement Algoritms for ATM Networks, IEEE JSAC*, vol. 9, n.2, pp. 343-349, 1991.

[39] J. Temporim, *Redes Wireless IEEE 802.16 WiMAX, UEL*, Dissertação de Mestrado, UEL,2007.

[40] F. L. Figueiredo, L. C. P. Pereira, *Tecnologia WiMAX: Uma visão geral*, CPqD, vol. 4, PP. 7-26, 2008.

[41] G. Varghese, *Network Algorithmics: Um Interdisciplinary Approach to Designing Fast Networked Devices*. California: Elsevier, 2005

[42] H. Dewing, S. Potter, *Implementing QoS Solution in Enterprise network*, Disponível em: <http://www.tmcnet.com/it/0202/0202inim.htm>, Acesso em setembro 2012.

[43] European Telecommunications Standards Institute, *General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDN*, Technical Report ETR 003, ETSI, 1990.

[44] W. B. Silva, *Um Estudo Comparativo do Desempenho das Disciplinas de Escalonamento WRR e WF^{2}Q no Suporte à QoS em Ambientes de Redes de Acesso IEEE 802.16*. Dissertação de Mestrado, UFU, 2008.

[45] C. Cicconetti, A. Erta, L. Lenzini and E. Mingozzi, *Performance Evaluation of the IEEE 802.16 MAC for QoS Support*. *IEEE Transactions on Mobile Computing*, vol. 6, n. 1, pp.26-38, 2007.

[46] Nortel Networks. *Benefits of Quality of Service (QoS) in 3G Wireless Internet*. Disponível em: <http://www.nortelnetworks.com. Acesso em Agosto de 2012.

[47] A. Vogel, B. Kerherve, G. Bochmann, and J. Gecsei, *Distributed Multimedia and QoS: a Servey, Multimedia, IEEE*, vol. 2, n. 2, pp.10-19, 1995.

[48] S. Ghazal, J. Ben-Orthman, *Traffic Policing Based on Token Bucket Mechanism for WiMAX Networks. ICC, IEEE International Conference on* , pp. 1-6, 2010.

[49] S. Ayyorgun, W. Feng, *A Deterministic Characterization of Network Traffic for Average Performance Guarantees. In: 38th Annual Conference on Information Sciences and Systems (CISS'04),* Princeton, NJ, 2004.

[50] S. Shenker, J. Wroclawski, *General Characterization Parameters for Integrated Service Network Elements*, RFC 2215, IETF, 1997.

[51] N. U. Ahmed, Q. Wang, L. O. Barbosa, *System Approach to Modeling the Token Bucket Algorithm in Computer Network*. Math Probl. Eng. 8, pp. 265-279, 2002.

[52] Safavi, A. Shames, A. Zamani, N. M, *A New Adaptive and Intelligent Traffic Shaper for High Speed Networks, International Journal of Information Sciences and Technology*, 2007.

[53] 3GPP, *QoS Concept and Architecture*, TS 23.107 v5.5.0, http://www.3gpp.org, 2002-2006.

[54] J. F. Borin, N. L. S. Fonseca, *Um Módulo Para Simulação em Redes WiMAX no Simulador NS-2, SBC*, pp. 180, Unicamp. 2008.

[55] S. Ghazal, Y. H. Aoul, J. B. Orthman, F. N. Abdesselam, *Applying a Self-configuring Admission Control Algorithm in a new QoS Architecture for IEEE 802.16 Networks, ISCC*, 2008.

[56] S. Ghazal, L. Mokdad, J. B. Orthman, *A Real Time Adaptive Scheduling Scheme For Multi-Service Flows in WiMAX Networks, IEEE Globecom*, 2008.

[57] E. Rathgeb, *Modeling and Performance Comparision of Policing Mechanisms for ATM Networks, IEEE JSAC*, vol. 9, n. 3, pp. 325-334, 1991.

[58] A. Berger, *Performance Analysis of a Rate Control Throttle Where Token and Jobs Queue, IEEE INFOCOM*, pp. 30-38, 1990.

[59] M. Faerman, C. V. Albuquerque, O. C. Duarte, *Janela Móvel Particionada: Proposta de Um Novo Mecanismo de Policiamento de Tráfego, Relatório Técnico do Grupo de Teleinformática da COPPE/UFRJ*, 1995.

[60] J. B. Orthman, L. Mokdad, *Improving QoS for UGS, rtPS, nrtPS, BE in WiMAX Networks, IEEE, ICCIT*, 2011, pp. 23-27, 2011.

[61] S. Y. Tang, P. Muller, H. R. Sharif, *WiMAX Security and Quality of Service: An End-to-End Perspective*, John Wiley, 2010.

Trabalhos Aceitos/ Publicados Pelo Autor

[62] H. B. Moraes e P. R. Guardieiro, *Um Estudo Comparativo de Propostas de Algoritmos de Escalonamento Para o Padrão IEEE 802.16, IX Conferência de Estudos em Engenharia Elétrica (IX CEEL)*, Uberlândia, Brasil, Maio 2011.

[63] H. B. Moraes and P. R. Guardieiro, *Traffic Policing Mechanism Based on the Token Bucket Method for WiMAX Networks. High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (ICESS), The 14th IEEE International Conference on High*

Performance Computing and Communications (HPCC – 2012), pp. 885-890, Liverpool - UK, 2012.

[64] H. B. Moraes and P. R. Guardieiro, *Traffic Policing Mechanism Based on the Token Bucket Method for WiMAX Networks. International Conference on Eletronics, Comunication and Computer Science (ICECCS 2012),* Nanning - China, 2012.

[65] H. B. Moraes and P. R. Guardieiro, *A Proposal Traffic Policing Mechanism Based on the Token Bucket Method for WiMAX Networks. 11th International Conference on Wireless Networks (ICWN),* Las Vegas - USA, 2012.

[66] H. B. Moraes and P. R. Guardieiro, *A Proposal Traffic Policing Mechanism Based on the Token Bucket Method for WiMAX Networks. 2nd International Conference on Wireless Communications and Mobile Computing (WCMC),* Palma de Mallorca-Espanha, 2012.