UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e Tecnologia

Programa de Pós-Graduação em Ciência da Computação

Arquitetura para controle de políticas de tarifação em redes WiMAX *mesh*

Erlon Rodrigues Cruz

São Carlos

Junho de 2009

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária da UFSCar

C957ap

Cruz, Erlon Rodrigues.
Arquitetura para controle de políticas de tarifação em redes WiMAX *mesh* / Erlon Rodrigues Cruz. -- São Carlos : UFSCar, 2009.
105 f.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2009.

1. Arquitetura de redes de computadores. 2. Sistemas de comunicação móvel. 3. WiMAX. 4. Tarifação. I. Título.

CDD: 004.65 (20ª)

Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Programa de Pós-Graduação em Ciência da Computação

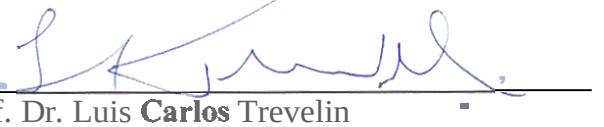
"Arquitetura para controle de políticas de tarifação em redes WiMax Mesh"

ERLON RODRIGUES CRUZ

Dissertação de **Mestrado** apresentada ao Programa de **Pós-Graduação** em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação

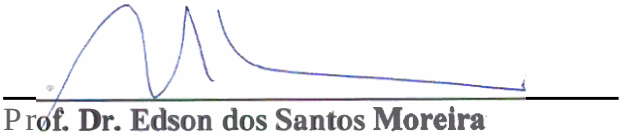
Membros da Banca:

Prof. Dr. Hélio **Crestana** Guardia
(Orientador - **DC/UFSCar)**



Prof. Dr. Luis **Carlos** Trevelin
(DC/UFSCar)

Prof. Dr. **Marcos Rogério** Salvador
(CPqD)



Pr**of. Dr. Edson dos Santos Moreira**
(ICMCNSP)

São Carlos
Junho12009

Agradecimentos

Ao grande Deus criador dos céus e da terra que me capacitou e possibilitou que eu chegasse nesta fase da minha vida acadêmica e profissional.

Aos meus pais que durante toda a sua vida não mediram esforços para me conceder a melhor educação ao seu alcance e durante toda minha jornada sempre estiveram do meu lado.

À minha família que desde o início da graduação até a fase final do mestrado tem me dado todo apoio necessário, seja ele financeiro, emocional ou espiritual.

Ao meu orientador, Hélio Crestana, que desde minha entrada na UFSCar é pra mim um grande exemplo como pessoa e como professor. Devido a ele desenvolvi grande parte do meu gosto e paixão pelo mundo das redes de computadores.

Aos meus colegas de turma que passaram comigo pelas duras trilhas e fizeram com que nosso laboratório se tornasse um ambiente amigável e familiar.

Aos demais que direta ou indiretamente contribuíram com a realização deste trabalho.

Resumo

Nos últimos anos, um grande esforço vem sendo empregado no estudo das redes *mesh* sem fio (WMNs). Como parte deste esforço, o padrão IEEE 802.16 *Wireless* MAN, especifica o modo de operação *mesh* para redes WiMAX, possibilitando que as WMNs estejam realmente disponíveis para uso. Diversos aspectos técnicos do funcionamento da camada física e de acesso ao meio têm sido investigados, porém, pouca atenção é dada à forma pela qual esta nova arquitetura irá tratar os aspectos de tarifação e negociação de serviços entre futuros provedores e usuários. Neste estudo, foram analisadas as atuais soluções para o problema em questão e é proposta uma nova arquitetura para tarifação, autenticação e gratificação de usuários para o padrão IEEE 802.16.

Abstract

In the last years, much effort has been applied to study Wireless Mesh Networks (WMNs). As part of this effort, the IEEE 802.16 Standard for Local and Metropolitan Area Networks specifies a mesh mode operation for WiMAX networks, opening possibilities for real mesh networks deployment. Several technical aspects of the physical and medium access layers of the standard have been studied, although, there is no definition on how this architecture will handle billing aspects and paid access. In this dissertation, the existing solutions for this question are analyzed and we propose a new architecture for billing users in IEEE 802.16 mesh networks.

Sumário

Glossário

Ad Hoc: Redes de computadores caracterizadas pela ausência de infra-estrutura fixa.

Backbone: Termo utilizado para especificar as interligações entre grandes redes de computadores.

Bridge: Dispositivo de rede que conecta redes com diferentes tecnologias na camada de enlace.

Broadcast: Transmissão multi-direcional de sinais. Em redes de computadores o termo é usado para descrever uma transmissão que é recebida por todos os nós de uma sub-rede.

Delay: Atraso que pode ocorrer entre o envio ou recebimento de dados durante a comunicação entre dois ou mais nós.

Downlink: Direção de comunicação da estação base (BS) para uma estação cliente (SS).

Gateway: Dispositivo de rede que opera como ponto de saída em sub-redes IP. Geralmente, todas as estações enviam seus tráfegos para o *gateway* e este os redireciona rumo a seus destinos.

Handover: Processo de transferência de uma chamada telefônica ou uma sessão de transmissão de dados de uma célula de cobertura para outra.

Host: Termo genérico para se referir a computadores ou estações de rede.

Hub: Repetidor de sinais utilizado para interconectar estações em uma sub-rede.

Jitter: Variação estatística do retardo na entrega de dados em uma rede, que, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados.

Label: Na tradução literal do inglês, *label* significa ‘rótulo’ ou ‘etiqueta’. Em nosso contexto utilizamos este termo para especificar pequenos rótulos que são adicionados aos datagramas.

Link: Em redes de computadores utiliza-se o termo *link* para indicar interligações entre *hosts*.

Mesh: Malha. Rede de computadores que se organizam em forma de malha.

Multi-hop: Termo usado para especificar quando a comunicação entre dois nós ocorre através de múltiplos nós intermediários que possuem a função de encaminhar a informação de um ponto a outro.

Switch: Comutador. Dispositivo de rede utilizado para encaminhar quadros entre estações de uma sub-rede**.**

Uplink: Direção de comunicação da estação cliente (SS) para uma estação base (BS).

Wireless: Sem Fio

Lista de Abreviaturas

Abrev.	Termo		Tradução
AAA	*Authentication, Authorization, Accounting*	-	Autenticação, Autorização e Contabilização
AK	*Authorization Key*	-	Chave de autorização
AP	*Access Point*	-	Ponto de acesso (sem fio)
ATM	*Asynchronous Transfer Mode*	-	Modo de Transferência assíncrono
BS	*Base Station*	-	Estação Base
CA	*Certificate Authority*	-	Autoridade Certificadora
CID	*Connection Identifier*	-	Identificador de Conexão
CPS	*Common Part Sublayer*	-	Subcamada Comum
CRC	*Cicling Redundancy Check*	-	Verificador de Redundância Cíclica
CS	*Convergence Sublayer*	-	Subcamada de Convergência
DBS	*Download Billing Session*	-	Sessão de Tarifação de *Download*
DCD	*Downlink Channel Descriptor*	-	Descritor de Canal de *Download*
DIUC	*Downlink Interval Usage Code*	-	Código de Intervalo de Uso de *Downlink*
DL-MAP	*Download Map*	-	Mapa de *Download*
DSL	*Digital Subscriber Line*	-	Linha Digital Subscritora
FDD	*Frequency Division Duplexing*	-	Duplexação por Divisão de Frequência
FEC	*Forward Error Correction*	-	Correção de Erro de Encaminhamento
GSM	*Global System for Mobile communications (originalmente de:*	-	Sistema Global Para Comunicações Móveis

	Groupe Spécial Mobile)		
ISM	*Industrial, Scientific and Medical*	-	Industrial, Científico e Médico
SKEY	*Session Key*		Chave de Sessão
LOS	*Line of Sight*	-	Linha de Visada
LSB	*Least Significant Bit*	-	Bit Menos Significativo
MAC	*Medium Access Control*	-	Camada de Acesso ao Meio
MIB	*Management Information Base*	-	Base de Informações de Gerenciamento
MSB	*Most Significant Bit*	-	Bit Mais Significativo
MTU	*Maximum Transmission Unit*	-	Unidade Máxima de Transmissão
NLOS	*Non Line of Sight*	-	Sem Linha de Visada
PDU	*Protocol Data Unit*	-	Unidade de Dados de Protocolo
PHY	*Physical Layer*	-	Camada Física
PKMv1	*Privacy Key Management version 1*		Protocolo de gerenciamento de chaves privadas versão 1
PMP	*Point-Multipoint*	-	Ponto-Multiponto
QoS	*Quality of Service*	-	Qualidade de Serviço
SA	*Security Associations*	-	Associações de Segurança
SAP	*Service Access Point*	-	Ponto de Acesso a Serviço
SNMP	*Simple Network Management Protocol*	-	Protocolo Simples de Gerência de Rede
SS	*Subscriber Station*	-	Estação Cliente
TDD	*Time Division Duplexing*	-	Duplexação por Divisão de Tempo
TDM	*Time Division Multiplexing*	-	Multiplexação por Divisão de Tempo
TEK	*Traffic Encription Key*	-	Chave de Criptografia de Tráfego
TDMA	*Time Division Multiple Access*	-	Acesso Múltiplo por Divisão de Tempo

UBS	*Upload Billing Session*	-	Sessão de Tarifação de *Upload*
UCD	*Uplink Channel Descriptor*	-	Descritor de Canal de *Upload*
UIUC	*Uplink Interval Usage Code*	-	Código de Uso de Intervalo de *Uplink*
UL-MAP	*Upload Map*	-	Mapa de *Upload*
UWB	*Ultra-wide-band*	-	Banda Ultra-larga
WISP	*Wireless Internet Service Provider*	-	Provedor de Serviços de Internet Sem Fio
WLAN	*Wireless Local Area Network*	-	Rede Local Sem Fio
WMAN	*Wireless Metropolitan Area Network*	-	Rede Metropolitana Sem Fio
WMN	*Wireless Mesh Network*	-	Redes sem Fio *Mesh*
WWAN	*Wireless Wide Area Network*	-	Rede Sem Fio de Largo Alcance

Lista de Figuras

Lista de Tabelas

1 Introdução

Redes *Mesh* Sem Fio (*Wireless Mesh Networks* - WMNs) são redes onde os nós possuem capacidade de auto-organização para comunicação, auto-formação e auto-reparo, organizando-se de maneira *ad hoc* e mantendo a conectividade da rede(AKYILDIZ et al, 2004). A principal característica que diferencia as WMNs das redes *ad hoc* convencionais é a sua composição e a divisão de funcionalidade entre dois tipos básicos de nós: *mesh clients* e *mesh routers*. Além da capacidade convencional de encaminhar pacotes, os *mesh routers* possuem funções adicionais para roteamento, não possuem restrições de energia e geralmente podem efetuar o papel de *gateway* interligando a rede *mesh* à Internet.

Para que as WMNs operem de forma apropriada, seus nós devem cooperar e encaminhar os pacotes de seus vizinhos aos destinos. Na maioria das vezes, este encaminhamento acarreta no consumo de recursos no nó, seja de energia, de processamento ou de largura de banda. Sabendo disto, a menos que haja alguma contrapartida, o encaminhamento de pacotes de vizinhos pode ser visto pelo proprietário de um nó como um desperdício de recursos. Deste modo, caso os usuários das WMNs não sejam de alguma maneira incentivados a re-encaminhar os pacotes em benefício dos outros nós da rede, eles provavelmente se comportarão de forma egoísta, impedindo que seu dispositivo seja utilizado pelos demais e, portanto, afetando diretamente o desempenho da rede(FANG et al, 2004).

Nos últimos anos, as WMNs têm atraído grande atenção tanto no meio acadêmico como na indústria e têm se mostrado como uma promissora tecnologia para acesso em banda larga sem fio. Uma das principais razões para esta popularidade repentina é a especificação de um modo de operação *mesh* para o padrão IEEE 802.16(IEEE 802.16, 2004), também conhecido como WiMAX. A adição do modo de operação *mesh* trouxe uma série de vantagens a essa tecnologia. Entre estas, pode-se citar a capacidade de transmissão sem linha de visada (NLOS), maior confiabilidade, segurança, vazão e disponibilidade(AKYILDIZ, 2004).

Diversos aspectos técnicos do funcionamento da camada física e da camada de acesso ao meio têm sido investigados nas WMNs, porém, pouca atenção é dada à forma pela qual esta nova tecnologia irá tratar os aspectos de tarifação e negociação de serviços entre futuros provedores e usuários. Tendo como foco esta situação, este trabalho propõe uma arquitetura que visa prover meios para possibilitar a tarifação dos usuários em domínios de

rede WiMAX *mesh*. A arquitetura de tarifação permite que diversas políticas de cobrança e recompensa sejam utilizadas e ajustadas de acordo com os interesses do provedor de serviços e de seus usuários. A arquitetura proposta também fornece mecanismos de incentivo aos usuários que colaboram com a rede redirecionando pacotes de seus vizinhos. Até o presente momento, não foi encontrado na literatura nenhum estudo propondo soluções que resolvam as questões referentes à tarifação de tráfego em redes WiMAX *mesh*.

O restante deste trabalho esta dividido da seguinte forma: no capítulo 2 é exibida uma visão geral sobre as redes sem fio de banda larga e suas principais tecnologias. No capítulo 3 é feito um estudo detalhado sobre o principais aspectos de segurança, arquitetura e funcionamento das redes *mesh*. No capítulo 4, apresentamos o padrão IEEE 802.16 explicando com detalhes seus modos de operação e seu funcionamento. Finalmente, no capítulo 5, introduzimos a arquitetura desenvolvida, discutimos os aspectos de segurança e desempenho relevantes e apresentamos os resultados obtidos através da construção da arquitetura em um ambiente simulado. Por fim, no capítulo 6 são apresentadas as considerações finais.

2 Redes Sem fio de Banda Larga

As redes de computadores, inicialmente estruturadas de forma cabeada, não eram capazes de possibilitar a comunicação entre dispositivos que não estivessem conectados fisicamente aos meios de transmissão. Ao prover mobilidade para comunicação em voz, as redes de telefonia celular revelaram um novo paradigma para comunicação, porém, elas não eram capazes de prover altas larguras de banda a diversos usuários simultaneamente. O propósito das tecnologias sem fio de banda-larga é prover aos dispositivos móveis comunicação sem fio com desempenho comparável às redes cabeadas.

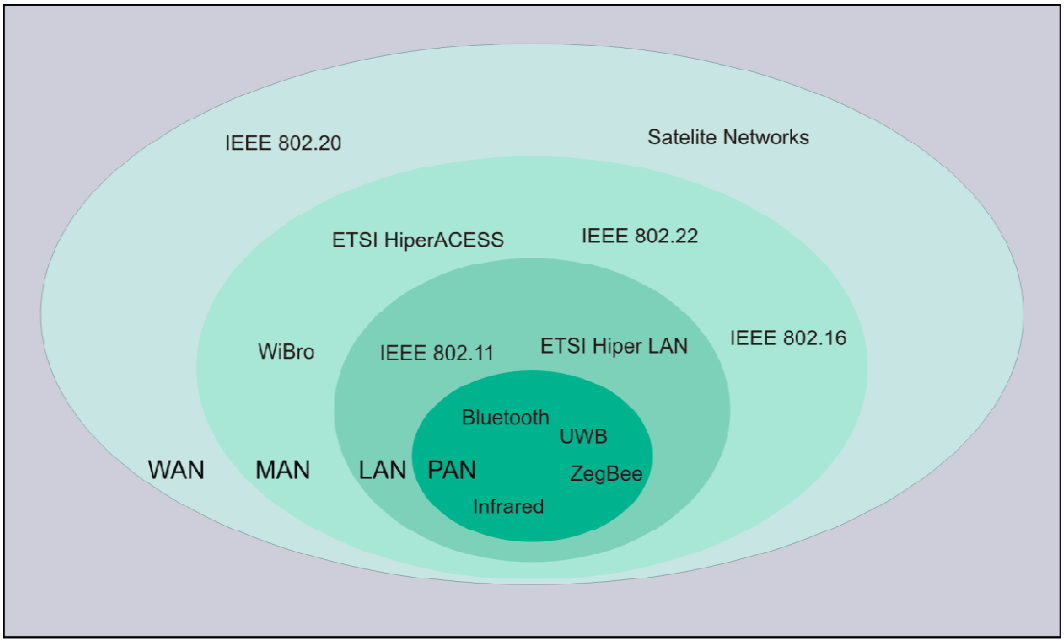


Figura 1: Área de cobertura dos diferentes tipos de rede

As tecnologias de rede sem fio podem ser categorizadas baseando-se em sua área de cobertura (**Figura 1**). As Redes Pessoais Sem Fio (*Wireless Personal Area Networks* - WPAN) são assim classificadas por possuírem curto alcance, geralmente alguns metros. As Redes Locais Sem Fio (*Wireless Local Area Networks* - WLANs) possuem raio de acesso em torno de algumas dezenas de metros, e são as mais utilizadas na maioria dos ambientes. As Redes Metropolitanas Sem Fio (*Wireless Metropolitan Area Networks* - WMANs) são projetadas para cobrir áreas maiores, geralmente todo o raio de uma cidade. As Redes Sem Fio de Largo Alcance (*Wireless Wide Area Networks* - WWANs) cobrem áreas maiores que uma cidade podendo se estender por centenas de quilômetros. Ao presente momento, para

algumas destas categorias vários padrões já foram homologados e para outras, estes padrões encontram-se em fase de desenvolvimento. Alguns destes padrões podem se encaixar em diversas categorias. Este capítulo resume cada uma das categorias de rede sem fio encontradas na literatura e os principais padrões e tecnologias relacionados a elas.

2.1. *Wireless* PAN

As redes pessoais sem fio (WPAN) são destinadas à conexão sem fio em curtas distâncias entre dispositivos. Apesar das redes pessoais serem utilizadas na maioria das vezes como um meio para interconectar dispositivos, (*e.g.*, fones de ouvido sem fio, controles-remoto, comunicação direta entre celulares, etc.), estas também podem ser estendidas de forma a conectar dispositivos à rede (BAATZ et al, 2000). Em geral, as tecnologias usadas em conexões WPAN possuem características em comum, como baixo consumo de energia dos dispositivos e curto alcance de comunicação.

Atualmente, essa categoria de redes sem fio pode ser representada pelas tecnologias *Bluetooth*, UWB, 802.15.4 e *Infrared*.

2.1.1. *Bluetooth*

O *Bluetooth*(BLUETOOTH, 2008) é uma especificação da indústria para um protocolo de redes pessoais. Este protocolo foi projetado para possibilitar envio de dados e voz entre dispositivos a curtas distâncias (entre 10m e 100m variando com a potência de transmissão e perfil de operação). Vários perfis de operação são especificados (*e.g.* perfil básico de impressão, perfil de acesso LAN, perfil de distribuição de vídeo, perfil de controle remoto, etc.) sendo cada um deles apropriado para determinadas aplicações. O *Bluetooth* opera na faixa ISM não licenciada de 2.4 GHz. A versão 1.2 do protocolo permite taxas de transmissão de até 1 Mbps enquanto a versão 2.0 pode atingir taxas de até 3 Mbps. Existe ainda uma versão 3.0 que está sendo desenvolvida pela WiMedia Alliance(IEEE 802.15.3, 2009) que permitirá taxas de transferência de até 480 Mbps.

2.1.2. UWB

O UWB, acrônimo em inglês de Banda Ultra-Larga refere-se a qualquer tecnologia de transmissão sem fio que utilize uma largura de banda de mais de 500 MHz(IEEE 802.15.3, 2009). O padrão IEEE 802.15.3 (IEEE 802.15.3, 2003) é uma especificação de uma tecnologia UWB. Este padrão opera na faixa de frequência não licenciada de 2.4GHz e foi projetado para atender os requisitos de aplicações de multimídia. Ele possibilita altas velocidades de transmissão que permitem transferências a taxas de dados de 11, 22, 33, 44 e 54 Mbps entre dispositivos a distâncias de até 70m. Outras características desta tecnologia são o suporte à qualidade de serviço e seu baixo consumo de energia. Além disto, o padrão pode prover conectividade *ad hoc* simples, que permite que os dispositivos automaticamente formem redes e troquem informações sem que seja necessária uma intervenção direta do usuário. O padrão provê também várias técnicas que podem ser utilizadas para aumentar a integração entre as redes 802.15.3 com outras redes sem fio.

2.1.3. IEEE 802.15.4

O padrão IEEE 802.15.4(IEEE 802.15.4, 2006) foi projetado para ser um padrão simples que possibilitasse comunicações com baixa taxa de dados e baixíssimo consumo de energia. Suas potenciais aplicações seriam em redes de sensores, brinquedos interativos, controle remoto e automação industrial. O padrão opera na faixa de 860MHz e também nas faixas de 2.4GHz possibilitando taxas de transferência que variam entre 20Kbps e 250Kbps em distâncias de alcance entre 10 e 100 metros de acordo com as taxas de transmissão.

Algumas outras especificações como o ZigBee(ZIGBEE, 2009), o WirelessHART(WHART, 2009) e o WiMi(WIMI, 2009) fornecem uma solução de rede completa especificando com mais detalhes a integração da camada MAC com os protocolos das camadas superiores. Estas especificações são baseadas no 802.15.4 e, portanto, mantém suas características referentes às camadas MAC e PHY.

2.1.4. *Infrared*

A padronização das redes *Infrared*(INFRARED, 2009) é gerenciada pela *Infrared Data Association*(IrDA). A IrDA é uma associação de companhias da indústria contendo mais de 150 membros. O padrão *Infrared* visa principalmente o baixo custo dos dispositivos e a transmissão de dados a curtas distâncias. O padrão opera no espectro infravermelho e possui taxas de transmissão de 115.200 bps na especificação 1.0 e taxas de até 4 Mbps na versão 1.1. Devido às características de sua faixa de operação e baixa potência de transmissão, o *Infrared* possui alcance médio de 4.5m e exige linha de visada.

2.2. *Wireless* LAN

As redes locais sem fio (WLAN) são destinadas para prover conexão entre dispositivos dentro do raio de algumas dezenas de metros. Devido a seu baixo custo de implementação, possibilidade de conexão rápida e ao aumento de usuários de dispositivos móveis, as WLANs passaram a ter um papel importante em escritórios, residências e ambientes empresariais.

O uso intensivo das tecnologias de transmissão sem fio trouxe à tona diversos problemas. O mais visível deles é a degradação de desempenho que se dá com o aumento de estações utilizando um canal de transmissão. Outros problemas relacionados à segurança e à provisão de Qualidade de Serviço (QoS) também são considerados nos diversos protocolos e tecnologias que utilizam transmissão sem fio e diversos métodos foram introduzidos para remediar estes problemas.

2.2.1. Família IEEE 802.11

Introduzido pela primeira vez em 1999, o padrão IEEE 802.11(IEEE 802.11, 1999) foi projetado de forma a prover conectividade sem fio em pequenos prédios, escritórios e redes locais, alcançando distâncias de até 100 m. Também conhecida como Wi-Fi, esta categoria de rede foi uma das grandes novidades tecnológicas nos últimos tempos e é até hoje a categoria de rede sem fio mais popularizada.

O padrão inicial operava na frequência de 2.4 GHz e previa taxas de transferência de até 2 Mbps. A especificação seguinte desta família, o IEEE 802.11b(IEEE 802.11b, 1999) utiliza o espectro de 2.4 GHz e aumentou a taxa de transferência nominal para

11 Mbps. Posteriormente, a introdução de dois novos padrões, o IEEE 802.11a (IEEE 802.11a, 1999) e o IEEE 802.11g(IEEE 802.11g, 2003), possibilitou taxas de transferência de até 54 Mbps. Para resolver problemas de segurança e inserir suporte a QoS, mecanismos adicionais foram inseridos e homologados os padrões IEEE 802.11i(IEEE 802.11i, 2003) e IEEE 802.11e (IEEE 802.11e, 2005). O próximo padrão da família, o IEEE 802.11n (IEEE 802.11n, 2009), poderá suportar taxas de transmissão de até 540Mbps. Ele insere diversas técnicas para aumento de desempenho e provisão de QoS.

2.2.2. Família ETSI HiperLAN

O padrão HiperLAN é um padrão europeu para acesso sem fio em redes locais. É uma alternativa ao IEEE 802.11 e foi definido pelo Instituto Europeu de Padrões de Telecomunicações (ETSI, 2009).

O padrão inicial, HiperLAN/1(ETSI HIPERLAN/1, 2002) foi desenvolvido em 1996. Ele opera no espectro de frequência de 5 GHz e suporta taxas de transferência de até 20 Mbps. O segundo padrão, HiperLAN/2(ETSI HIPERLAN/2, 2002), desenvolvido em 2000, suporta taxas de transferência de até 54 Mbps(ETSI HIPERLAN/2, 2002).

Apesar de o padrão HiperLAN haver sido desenvolvido com mais detalhes que o IEEE 802.11, especialmente por seu suporte a QoS e mobilidade, o HiperLAN não obteve sucesso no mercado e atualmente não há nenhum grupo ativo de desenvolvimento e aprimoramento do padrão como ocorre com o IEEE 802.11.

2.3. *Wireless* MAN

As redes metropolitanas sem fio (WMAN) são projetadas para cobrir áreas metropolitanas, podendo abranger cidades inteiras e até mesmo suas áreas rurais. Em sua configuração básica, as WMANs possuem dois tipos de dispositivos: a Estação Base (*Base Station* - BS) e Estação Cliente (*Fixed Subscriber*/*Subscriber Station* - SS). Este tipo de conectividade representa uma estrutura Ponto-Multiponto (PMP), como mostrado na **Figura 2**. As estações conectadas à rede podem ser veículos, estações fixas ou mesmo dispositivos móveis. As SSs que estiverem em uma distância além do raio de cobertura da BS podem se conectar através de antenas

direcionais, enquanto as estações e dispositivos dentro do alcance de transmissão da BS não necessitam ter visada direta(KURAN E TUGCU, 2007).

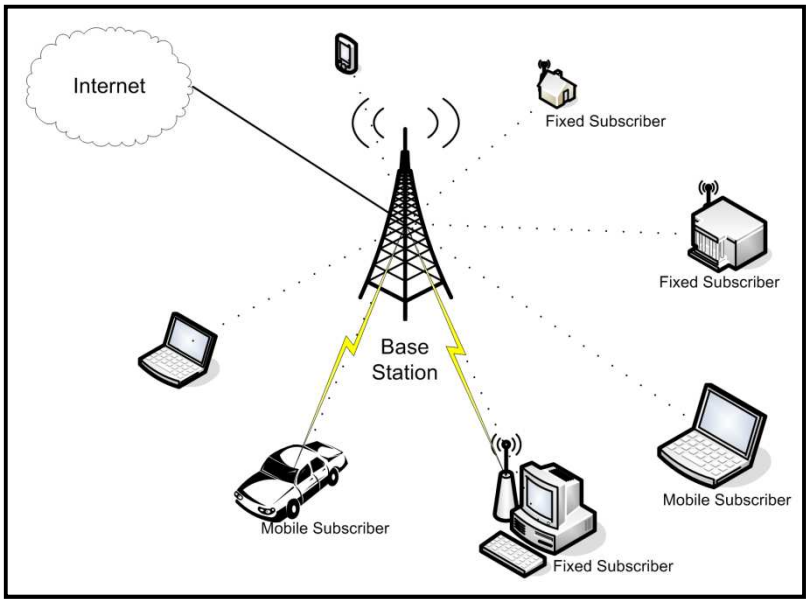


Figura 2: Configuração PMP de uma WMAN

Visando o aumento da interoperabilidade entre diversos produtos que provêm acesso sem fio às WMANs, companhias industriais criaram o WiMAX *Forum*. Através de cooperação entre estas diversas empresas, padrões como o IEEE 802.16 e HiperMAN vêm sendo desenvolvidos e diversas soluções para WMAN já estão disponíveis no mercado.

2.3.1. Família IEEE 802.16

O padrão IEEE 802.16 foi desenvolvido com base em duas tecnologias: *Multichannel Multipoint Distribuition System* (MMDS) e *Local Multipoint Distribuition System* (LMDS). Estas tecnologias foram desenvolvidas por algumas companhias telefônicas com o intuito de prover uma alternativa ao acesso de banda larga DSL em áreas metropolitanas. O MMDS opera em faixas de 2.1GHz e 2.5-2.7 GHz com células de aproximadamente 50 km e taxas de transmissão variando entre 0.5 e 30MBps(CLEARY, 1997). Devido a sua facilidade de implementação comparada com o DSL, a tecnologia MMDS recebeu bastante atenção, porém, sua a largura de banda estava longe do ideal principalmente em células de 50 km. Assim, um novo tipo de serviço denominado LMDS foi desenvolvido para atuar em frequências

superiores e prover maior largura de banda(TANENBAUM, 2003). Operando em espectros de 28-31 GHz e 40.5-42.25 GHz, o LMDS possui células altamente setorizadas e alcance de até 5 km. A falta de padronização na implementação do LMDS trouxe muitos problemas de interoperabilidade entre aparelhos de diferentes fabricantes. Assim, para estabelecer um padrão para o LMDS, o IEEE criou o grupo de tarefa 802.16 que, em 2002, homologou a primeira versão do IEEE 802.16(TANENBAUM, 2003).

A versão inicial do padrão IEEE 802.16, também referido como WiMAX, somente provê conectividade PMP para estações com linha de visada (LOS) e frequências de operação de 10-66GHz. Os problemas de conectividade em LOS em ambientes urbanos forçaram o desenvolvimento de outras camadas físicas (PHY) que possibilitassem comunicações NLOS. Assim, estes ajustes foram introduzidos no IEEE 802.16a, que possui camada física NLOS operando nas faixas de bandas entre 2 e 11 GHZ e também especifica a operação do padrão no modo *mesh*. Após diversos ajustes, tanto na camada PHY como na camada MAC, foi homologado o padrão IEEE 802.16-2004(IEEE 802.16, 2004). No **Capítulo 4** o padrão IEEE 802.16 será abordado com mais detalhes e seu funcionamento tanto no modo PMP como modo *mesh*, será explanado detalhadamente.

2.3.2. ETSI HiperACCESS

O padrão HiperACCESS(ETSI HiperACCESS OVW, 2002), (ETSI HiperACCESS DEF, 2002), (ETSI HiperACCESS REQ, 1998), foi homologado em 2002 pelo ETSI. Ele é voltado para empresas de pequeno e médio porte e foi projetado para prover acesso de banda larga a estações com linha de visada e também operar como *backbone* em redes de telefonia celular. Entre suas principais características podemos citar:

- Faixas de frequências entre 11 e 43.5 GHz;
- Topologia PMP com um AP no centro e terminais de acesso (AT) como nós;
- Camada de enlace orientada à conexão com suporte refinado de QoS;
- Suporte FDD e TDD;
- Possui uma variedade de modulações para a camada PHY para diferentes condições nos *links*;
- Possui uma camada de convergência para otimizar a integração com protocolos como IP, ATM e Ethernet.

2.3.3. WiBro (*Wireless Broadband*)

Uma das mais recentes tecnologias desenvolvidas para prover acesso aos usuários estacionários e móveis em WMANs é o WiBro (HONG, 2004), (YOON, 2004). Seu desenvolvimento começou em 2003 na Coréia do Sul e terminou em 2004. Sua segunda fase, feita em colaboração com o IEEE 802.16e foi concluída em 2005.

A tecnologia WiBro é bastante parecida com o IEEE 802.16, incluindo todas as suas partes obrigatórias, porém o WiBro foi projetado desde o começo com usuários móveis em mente. Da mesma forma que o IEEE 802.16, o WiBro opera em faixas de frequências de 2.3 GHz a 2.4 GHz com canais de 9 MHz, baseando-se no OFDMA com diferentes esquemas de modulação (*e.g*. QPSK, QAM-16 e QAM-64). Contudo, o WiBro só permite duplexação por tempo (TDD). Uma típica célula WiBro possui raio de 1 Km, largura de banda de 18 Mbps para *download* e 6 Mbps para *upload*, porém estas taxas foram aumentadas na segunda versão do padrão. Na camada MAC, as principais diferenças entre o WiBro e o IEEE 802.16 é que ao visar mobilidade desde o início do projeto, a primeira versão do WiBro já incluía mecanismos de *handover* e seus mecanismos de QoS não incluem taxa de bits constante. A segunda versão do WiBro é considerada interoperável com dispositivos WiMAX.

2.3.4. IEEE 802.22

O padrão IEEE 802.22(IEEE 802.22 WG,2009) é um padrão ainda em desenvolvimento que pretende prover acesso de banda larga a áreas rurais que não possuam acesso a outras tecnologias. Para alcançar distâncias tão grandes, o padrão é utiliza espectros inutilizados das faixas UHF e VHF, entre 54 e 862 MHz. Para descobrir quais frequências estariam livres para uso, – essas frequências costumam variam muito de um país para outro – o padrão pretende utilizar uma forma centralizada para descoberta destes canais. Dependendo da faixa de frequência utilizada e da distância das estações, que pode chegar até 40 Km, o padrão promete prover taxas de transmissão de até 18 Mbps.

2.4. *Wireless* WAN

As tecnologias de acesso WWAN consistem geralmente de redes direcionadas a cobrir completa ou parcialmente áreas continentais, podendo ser utilizadas como *backbone* entre WMANs isoladas. Além desta cobertura continental, algumas tecnologias voltadas para WWAN (*e.g*. IEEE 802.20) buscam dar suporte a estações móveis em alta velocidade.

2.4.1. IEEE 802.20

Pensando em trazer suporte à mobilidade à primeira versão do padrão IEEE 802.16, alguns especialistas optaram por desenvolver um padrão específico para tal propósito. Assim, um novo grupo de tarefa foi designado pelo IEEE para desenvolver um padrão voltado para mobilidade: o IEEE 802.20(IEEE 802.20, 2009).

Uma vez que o principal objetivo do IEEE 802.20 é possibilitar mobilidade a dispositivos veiculares com velocidade até 250 km/h, sua largura de banda é considerada muito menor que a especificada em padrões como o IEEE 802.16 e IEEE 802.11 e o tamanho das células gira em torno de 15 km(ZOU et al, 2004).

A conclusão do IEEE 802.20 foi prevista para o final de 2004, porém, por possuir praticamente os mesmos propósitos do IEEE 802.16e que se encontra mais maduro e mais completo, seu desenvolvimento foi suspenso.

3 Redes *Mesh*

As Redes *Mesh* Sem Fio ou *Wireless Mesh Networks* (WMN) vêm sendo objeto de pesquisas por serem vistas como a próxima geração das redes *Wireless*. As WMNs são redes dinamicamente auto-organizáveis e auto-configuráveis, cujos nós, dispostos em uma topologia em malha, compõem uma rede *ad hoc*(AKYILDIZ, 2004). Porém, ao contrário das redes *ad hoc* tradicionais, as redes *mesh* possuem menor mobilidade e uma infra-estrutura que possibilita que os nós acessem a Internet.

Os nós componentes da rede *mesh* podem ser de dois tipos: clientes *mesh* e roteadores *mesh,* que contêm funções adicionais de roteamento para suportar redes *mesh*. Além disto, podem servir como *gateways* ou *bridges*, *wireless* ou cabeadas para implementar integração com redes de outros enlaces, como WiMAX ou Ethernet. Roteadores *mesh* possuem mínima mobilidade e formam o *backbone* para os clientes *mesh*. Estes também podem trabalhar como roteadores, desde que possuam os protocolos necessários para tanto. Dentre os diversos benefícios encontrados nas redes *mesh* podemos citar: baixo custo inicial, facilidade de manutenção, robustez, confiabilidade, maior extensão dos serviços, etc.(AKYILDIZ, 2004).

3.1. Redes *Mesh* x Redes *Ad Hoc*

Wireless Mesh Networks (WMNs) são casos específicos de redes *ad hoc*. As redes *ad hoc* são formadas por dispositivos de rede que pretendem se comunicar, mas não possuem infra-estrutura fixa disponível ou organização pré-determinada de *links*(RAMANATHAN et al, 2002). Nas redes *ad hoc*, cada nó é responsável pela descoberta dinâmica de quais são os outros nós com os quais pode comunicar diretamente, ou seja, quais são seus vizinhos (formando uma rede *multi-hop*). Devido à mobilidade e à potencial entrada e saída dinâmica de alguns nós, a topologia da rede pode ser alterada e essas constantes mudanças podem gerar múltiplas rotas entre dois nós. Quanto maior o número de participantes de uma rede *ad hoc*, mais complexa será a comunicação. Assim, redes *ad hoc* são projetadas para serem usadas em situações em que a infra-estrutura não está disponível ou não é confiável, ou ainda em

situações de emergência. Dentre as principais aplicações das redes *ad hoc* podemos citar: computação móvel em áreas remotas, emprego militar, comunicações táticas, busca e salvamento em situações de desastre, redes temporárias em salas de reuniões e em aeroportos(ACHARYA et al, 2003). No caso das WMNs, assume-se que os roteadores *mesh* são fixos (ou possuem pouca mobilidade) formando uma infra-estrutura fixa. Os clientes são móveis ou fixos e utilizam a infra-estrutura formada pelos roteadores mesh para se comunicar com *host* fora daquela rede.

3.2. Fatores Críticos de Desempenho

Ao considerarmos qualquer sistema projetado para redes *mesh*, devemos considerar alguns fatores críticos que influenciam diretamente no seu desempenho. Estes fatores são sumarizados como segue(AKYILDIZ, 2004):

Técnicas de transmissão: Devido à grande quantidade de nós transmitindo no mesmo espectro de transmissão, o desempenho das redes mesh tende a degradar-se devido à interferência. Para aumentar o desempenho da comunicação de dispositivos sem fio, diversas técnicas, como o uso de transmissores de rádio re-configuráveis, frequenciômetros cognitivos e até mesmo técnicas de software devem ser consideradas. Todos estes avanços na camada de transmissão requerem sofisticados mecanismos nas camadas superiores (*e.g.* MAC, rede, etc.) e, portanto, os atuais protocolos MAC e de roteamento precisariam ser re-projetados utilizando uma abordagem multicamada.

Escalabilidade: Em uma rede *multi-hop* problemas com escalabilidade são constantes, *i.e.*, quando o tamanho da rede aumenta, seu desempenho reduz-se significativamente. Os protocolos usuais utilizados no roteamento podem não ser capazes de achar uma rota confiável, os protocolos de transporte podem derrubar conexões e protocolos MAC podem reduzir significativamente a vazão. Devido à organização *ad hoc* das redes *mesh*, esquemas de acesso ao meio centralizados, tais como TDMA e CDMA, são de difícil implementação. Quando consideramos uma rede *multi-hop*, esquemas de acesso ao meio com CSMA/CA são mais favoráveis, porém este possui baixa eficiência no reaproveitamento do meio de transmissão. Assim, para melhorar a escalabilidade das WMNs, protocolos híbridos

com CSMA/CA e TDMA, ou CDMA, podem oferecer uma solução interessante e são um desafiador campo para pesquisa.

QoS e banda-larga: Diferentemente das redes *ad hoc*, a maioria das aplicações das WMNs utilizam serviços de banda-larga com altos requerimentos de QoS. Assim, além de garantir baixo atraso de transmissão fim-a-fim, outras métricas de desempenho, tais como *jitter*, vazão por nó e taxa de perda de pacotes, devem ser consideradas por estes protocolos de comunicação.

Compatibilidade e interoperabilidade: Uma característica desejada nas WMNs é que estas suportem tanto clientes *mesh* como clientes tradicionais de diversas tecnologias. Assim, para possibilitar essa interoperabilidade, certos roteadores *mesh* devem ter a capacidade de interagir com outras tecnologias de transmissão.

Facilidade de uso: Os protocolos em uma WMN devem ser projetados para que a rede seja o mais autônoma possível, em questões de gerenciamento de energia, auto-organização, controle dinâmico de topologia, controle robusto de falhas de *links* e rápidos mecanismos de autenticação e subscrição de usuários.

Limitação de recursos: Normalmente, os clientes *mesh* possuem recursos limitados, tanto em aspectos de largura de banda, quanto à bateria ou poder de processamento. Desta forma, torna-se inviável implementar procedimentos criptográficos complexos ou protocolos de configuração que exijam muita sinalização.

3.3. Segurança em WMN

Devidos às características das WMNs elas são bem mais vulneráveis a ataques que as tradicionais redes cabeadas. Desenvolver uma arquitetura *mesh* à prova de falhas é uma tarefa desafiadora. Os mecanismos de segurança podem ser implementados em diferentes camadas da pilha de protocolos. As atuais soluções de segurança podem ser eficientes contra ataques em uma determinada camada mas ainda faltam mecanismos para prevenir ataques que explorem falhas na pilha de protocolos como um todo. As seguintes questões são as principais dificuldades a serem superadas quando se deseja prover segurança nas WMNs(ZHANG et al, 2009):

Canal de transmissão compartilhado: Nas redes cabeadas, existe uma linha de transmissão dedicada entre os nós correspondentes; porém, em redes sem fio, a transmissão é

por natureza compartilhada com todos os nós dentro do raio de transmissão. Portanto, caso um atacante esteja no raio de transmissão ele será capaz de ouvir todas as comunicações enviadas entre nós correspondentes.

Associação autorizada: Nas WMNs os roteadores *mesh* formam uma topologia fixa que permite aos clientes *mesh* a qualquer tempo entrar ou sair da rede. Se não houver mecanismos apropriados para autenticação dos nós, um intruso pode facilmente entrar na rede e então disparar ataques.

Compartilhamento de informações: O tráfego transmitido em uma WMN pode ser encaminhado através de múltiplos nós até que chegue a seu destino. Mesmo que todos os nós que encaminharam tenham sido devidamente autenticados, caso não haja mecanismos robustos de criptografia de tráfego, estes nós terão acesso a todas as informações trocadas entre os correspondentes.

Limitações de recursos: Geralmente, os clientes *mesh* possuem baixo poder computacional. Desta forma, o uso de procedimentos criptográficos complexos pode reduzir seriamente a viabilidade dos mecanismos de segurança.

3.4. Padrões de redes *mesh* em desenvolvimento

Além das complicações inerentes às funcionalidades oferecidas pelas redes *mesh*, a falta de padrões na indústria para esta tecnologia prejudica sua ampla utilização. Alguns grupos de tarefa do IEEE estão encarregados de projetar as devidas adaptações para que protocolos tais como o IEEE 802.11, 802.16, e 802.15.4, possam suportar o modo de operação *mesh*. Atualmente, somente os protocolos IEEE 802.16 e IEEE 802.15.4 possuem especificações para operação em *mesh* concluídas.

3.4.1. IEEE 802.11

Para criar uma extensão do padrão IEEE 802.11 que pudesse operar no modo *mesh*, o IEEE criou o grupo de tarefa 802.11s(IEEE 802.11s, 2009). O grupo de tarefa 802.11s é responsável por definir a camada PHY e MAC para redes *mesh* de forma que estas estendam a cobertura das tradicionais redes 802.11.

As redes Wi-Fi *mesh* poderão funcionar em dois modos de operação: modo infra-estruturado e modo cliente *meshing*. No primeiro, os APs são interconectados através de *links* sem fio e descobrem dinamicamente a topologia da rede, configurando automaticamente sua tabela de rota. Os clientes conectados a estes APs não necessitam possuir suporte ao protocolo *mesh*. Assim, os *links* entre os APs formam uma infra-estrutura para transmissão sem fio diminuindo os custos necessários para aumentar a cobertura das redes sem fio. O outro modo de operação, *i.e.*, cliente *meshing*, é um conjunto independente de serviços básicos (IBSS) operando na camada 3 do padrão OSI/ISO. Neste modo, todos os nós da rede se organizam de maneira *ad hoc* e não é feita distinção entre os clientes e os APs. Para maximizar os benefícios da rede *mesh*, ambos os modos de operação poderão funcionar transparentemente em uma mesma rede.

3.4.2. IEEE 802.15

Criado com o objetivo de possibilitar redes pessoais (PAN) de banda larga, o padrão IEEE 802.15.3.a é baseado na camada PHY MultiBand OFDM Alliance (MBOA) e utiliza banda ultra larga (UWB) para atingir taxas de transmissão de até 480Mbps(IEEE 802.15 TG, 2008). Uma nova camada MAC proposta pelo MBOA, adiciona ao IEEE 802.15.3 forte suporte à conectividade *mesh* e mobilidade. Esta camada MAC usa a estrutura *piconet* combinada com um gerenciamento descentralizado de recursos para permitir reserva de *slots* de tempo e prover um acesso ao meio no estilo TDMA.

Além da proposta anteriormente apresentada, o IEEE criou o grupo de tarefa 802.15.5 para padronizar mecanismos nas camadas PHY e MAC que possibilitem conectividade *mesh* em PANs(IEEE 802.15.5 TG, 2008).

3.4.3. IEEE 802.16

Enquanto os padrões IEEE 802.15 e IEEE 802.11 oferecem conexão dentro de algumas dezenas de metros, o IEEE 802.16 foi delineado para permitir a comunicação entre usuários dentro de um raio de quilômetros. Em sua especificação inicial, o IEEE 802.16 define a operação para frequências entre 10 e 66 GHz em comunicação com linha de visada. A

extensão IEEE 802.16a amplia esta cobertura de transmissão para frequências de 2 a 11 GHz, possibilitando assim comunicação NLOS. Nesta extensão também foram acrescentadas especificações para possibilitar que as estações se conectem de forma não estruturada, *i.e.*, modo *mesh*(BARRY et al, 2005).

Apesar de possuir diversas limitações (*e.g.* baixa escalabilidade, falta de suporte à QoS, etc.), o IEEE 802.16 *mesh* é a primeira especificação aberta de um protocolo que possibilita comunicação *mesh*. Assim, espera-se que ele seja um início promissor para a comunicação *multi-hop* sem fio. No capítulo subsequente, é abordado o funcionamento detalhado de todo o padrão IEEE 802.16 com ênfase em seu modo de operação *mesh*.

4 O Padrão 802.16 (WiMAX)

O WiMAX (*Worldwide Interoperability for Microwave Access*/Interoperabilidade Mundial para Acesso de Micro-Ondas), é um sistema de comunicação sem fio emergente projetado para prover acesso de banda larga com ampla cobertura(VAUGHAN-NICHOLS, 2004). Nos últimos anos, o grupo de trabalho do IEEE 802.16 vem desenvolvendo uma série de padrões para esta tecnologia. O primeiro destes, homologado em 2001, provê suporte para comunicações na faixa de frequências entre 10 e 66 GHz (IEEE DRAFT STANDART 802.16/D4, 2001). Em 2003, o IEEE 802.16a introduziu uma especificação adicional do padrão para operação nas frequências entre 2 e 11 GHz (IEEE DRAFT STANDART 802.16a, 2001). Recentemente aprovado, o padrão IEEE 802.16-2004 consolidou esforços de grupos de trabalhos anteriores, como IEEE Std 802.16™, IEEE Std 802.16a™ e IEEE Std 802.16c, reunindo diversas de suas vantagens e possibilitando comunicação sem fio de banda larga. O padrão define a camada física (PHY) para sistemas operando em um espectro de banda que pode variar de 2 a 66 GHz, a camada de acesso ao meio (MAC) e subcamadas de convergência (*Convergence Sublayer* - CS) para transporte de datagramas IP, ATM e Ethernet.

4.1. Modelo de referência

Para que fosse possível prover suporte a um extenso número de usuários com diferentes demandas de tráfego (*e.g.* voz, dados, vídeo, etc.), a arquitetura do novo padrão necessitaria ser flexível, eficiente e robusta, possibilitando que cada usuário possuísse diferentes níveis de QoS e diferenciação de serviços. Desta forma, o modelo de referência adotado (**Figura 3**) divide a camada MAC em três subcamadas.

A subcamada de convergência realiza a interação da camada MAC com as camadas superiores. Ela é responsável por processar, classificar, e mapear as PDUs das camadas superiores em diferentes classes de serviço. O padrão define dois mapas de convergência de serviços:

- Serviço de encapsulamento de células ATM;

- Serviço de encapsulamento de pacotes, definido para mapear serviços de pacotes como o IPv4, IPv6, entre outros.

A subcamada comum (*Common Part Sublayer* - CPS) executa as funcionalidades de acesso ao sistema como alocação de banda, estabelecimento e manutenção das conexões.

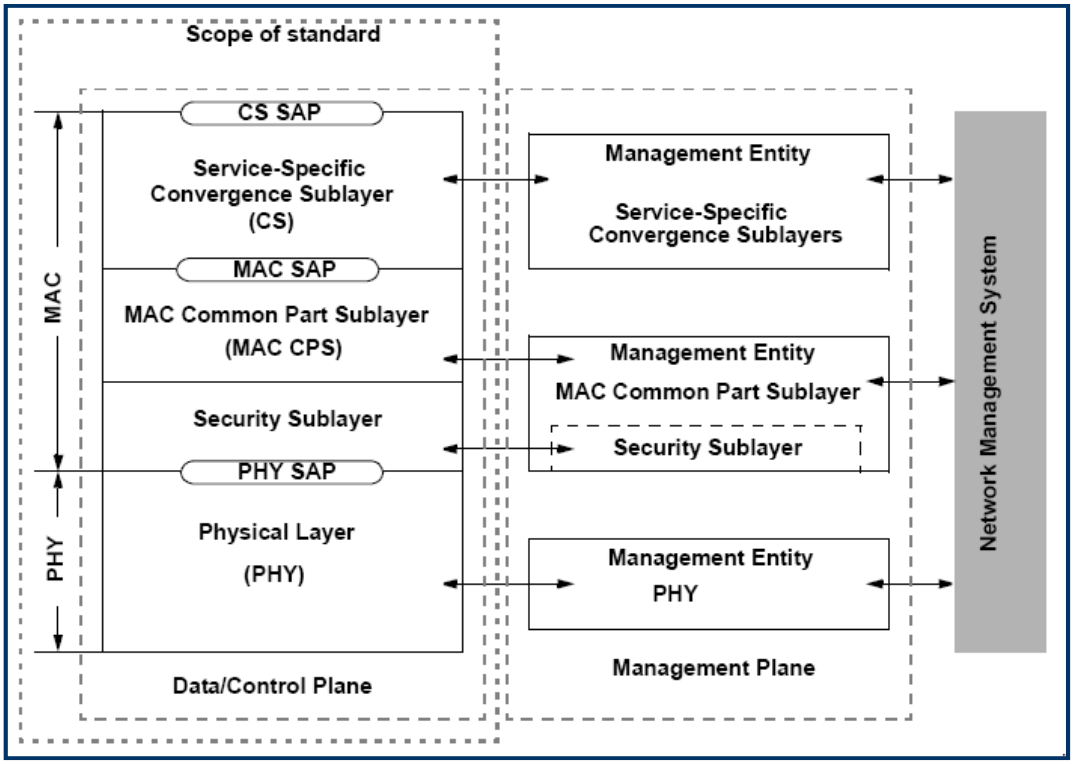


Figura 3: Modelo de referência IEEE 802.16(IEEE 802.16, 2004**)**

A terceira subcamada é a camada de segurança. A camada de segurança é responsável pela comunicação segura entre as estações efetuando os processos de autenticação, troca de chaves e criptografia.

4.2. Camada Física (PHY)

A primeira versão da camada PHY do padrão IEEE 802.16 foi especificada para operar em faixas de frequência de 10 a 66 GHz. Devido às propriedades das ondas nesta faixa de frequência, os pontos de comunicação devem possuir visada direta com a estação base e a taxa de transferência pode atingir velocidades de até 120 Mbits/s em canais de 25-28 MHz. A

versão IEEE 802.16-2004 adiciona a especificação de operação da camada física em faixas de frequência abaixo de 11GHz e quatro novos esquemas de modulação. A **Tabela 1** traz um resumo dos esquemas de modulação suportados pelo padrão.

Modulação	Frequências de Operação	Duplexação
*Wireless*MAN-SC™	10-66GHz	TDD/FDD
*Wireless*MAN-SCa™	Faixas licenciadas abaixo de 11GHz	TDD/FDD
*Wireless*MAN-OFDM™	Faixas licenciadas abaixo de 11GHz	TDD/FDD
*Wireless*MAN-OFDMA	Faixas licenciadas abaixo de 11GHz	TDD/FDD
*Wireless*HUMAN™	Faixas não licenciadas abaixo de 11GHz	TDD

Tabela 1: Tipos de modulação suportados no IEEE 802.16(IEEE 802.16, 2004)

4.3. Camada MAC

Uma das principais características da tecnologia IEEE 802.16 é o controle de acesso ao meio (MAC) orientado a conexão. Assim, todos os fluxos de dados são classificados em conexões e cada um destes possui um nível diferente de QoS. As conexões são unidirecionais e são identificadas por um identificador de 16 bits (CID). Conexões na direção da BS para a SS (*downlink*) podem ser *unicast* ou *multicast* enquanto conexões na direção da SS para a BS (*uplink*) são obrigatoriamente *unicast*.

Durante a inicialização de uma SS, três conexões específicas são estabelecidas em ambas as direções. Uma conexão básica, usada para transmissão de mensagens curtas de tempo-real, uma conexão primária de gerenciamento, usada para trocar mensagens e parâmetros de conexão mais tolerantes a atraso, e uma conexão secundária de gerenciamento, usada para trocar dados de configuração das camadas superiores. O formato do quadro da camada MAC (MAC PDU), é mostrado na **Figura 4**.

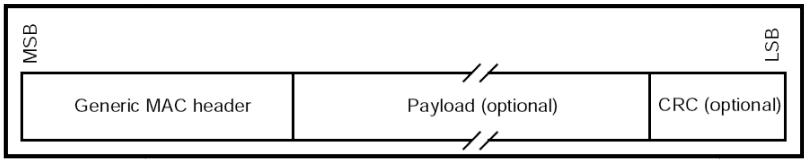


Figura 4: Formato do PDU da camada MAC do IEEE 802.16(IEEE 802.16, 2004)

A PDU MAC possui tamanho variável e dois tipos de cabeçalho são definidos: cabeçalho genérico, e cabeçalho de requisição de banda. Estes cabeçalhos são mostrados na **Figura 5** e **Figura 6**.

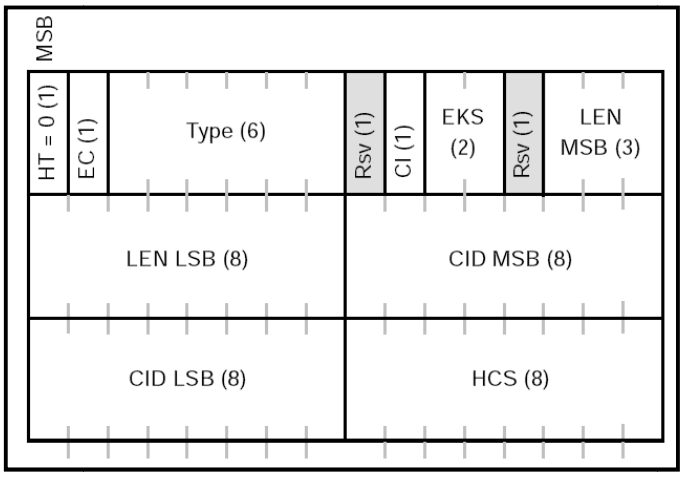


Figura 5: Cabeçalho MAC genérico do IEEE 802.16(IEEE 802.16, 2004)

Os campos do cabeçalho MAC genérico do IEEE 802.16 são definidos na

Tabela 2.

Nome	Tam. (bits)	Descrição
CI	1	Indicador de CRC
CID	16	Identificador de conexão
EC	1	Controle de encriptação
EKS	2	Tipo de chave de encriptação
HCS	8	Soma de verificação de cabeçalho
HT	1	Tipo de cabeçalho (0 no caso de MAC genérico)
LEN	11	Tamanho total da PDU
Type	6	Indica sub-cabeçalhos e dados adicionais contidos na carga útil da PDU

Tabela 2: Campos do cabeçalho MAC genérico do IEEE 802.16(IEEE 802.16, 2004)

O quadro MAC de requisição de banda consiste em um quadro sem carga útil contendo um cabeçalho MAC de requisição de banda.

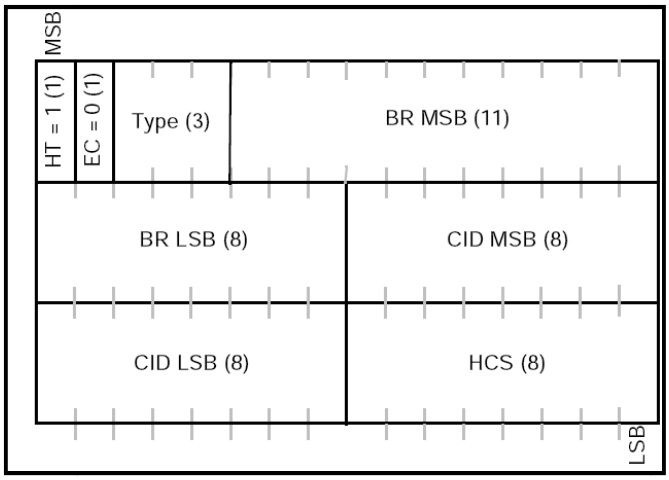


Figura 6: Cabeçalho MAC de requisição de banda do IEEE 802.16(IEEE 802.16, 2004)

Os campos do cabeçalho MAC de requisição de banda são definidos na **Tabela 3**.

Nome	Tam. (bits)	Descrição
BR	19	Quantidade de banda (em bytes) requisitada pela SS
CID	16	Identificador da conexão
EC	1	Não utilizado (sempre 0)
HCS	8	Soma de verificação
HT	1	Tipo de cabeçalho (1)
Type	3	Tipo de requisição de banda

Tabela 3: Campos do cabeçalho MAC de requisição de banda do IEEE 802.16(IEEE 802.16, 2004)

Na camada de acesso ao meio (MAC) do IEEE 802.16 são definidos dois modos de operação: ponto-multiponto (PMP) e modo *mesh*. No primeiro modo, os nós (SSs) são posicionados em torno de uma estação base transmissora (BSs) e se organizam em forma de células. Todas as estações devem estar dentro do raio de transmissão da BS e toda a comunicação entre os nós deve passar obrigatoriamente pela BS. No modo *mesh*, as SSs podem re-encaminhar pacotes de outras SSs que não possuem acesso direto à BS e, portando, nem todos os nós necessitam estar dentro do raio de transmissão da BS.

Nos tópicos que se seguem é dada uma visão detalhada do funcionamento do WiMAX em seus dois modos de operação: PMP e modo *mesh*.

4.3.1. Modo Ponto-Multiponto

No modo PMP o padrão IEEE 802.16 opera através de uma estação base (BS) central que usa uma antena para transmitir para todas as estações clientes (SS) dentro de seu raio de alcance. A BS pode também dividir seu raio de cobertura, através de antenas setorizadas, e transmitir para cada setor em um canal de frequência. Todas as estações dentro de um canal de frequência recebem a mesma transmissão. Considerando o raio de transmissão da BS, a BS é o único transmissor no sentido *downlink* e seu escalonador coordena as transmissões. As SSs escutam o canal de transmissão e, ao receberem um quadro de dados, verificam se o identificador de conexão daquele quadro pertence a alguma de suas conexões e somente o aceitam se este houver sido endereçado a ela.

4.3.1.1. Estrutura do canal de transmissão

O canal de transmissão no IEEE 802.16 PMP é dividido em duas partes: *downlink* (transmissão da BS para a SS) e *uplink* (transmissão da SS para a BS). Estes canais podem ser multiplexados via TDD ou FDD. As transmissões no canal de *downlink* são feitas de modo TDM, com uso de preâmbulos de re-sincronização. O canal de *uplink* funciona no modo TDMA. Em ambos os canais, *uplink* e *downlink*, é usado o esquema de modulação adaptativa que permite a alteração do mecanismo de modulação de acordo com a qualidade do sinal de transmissão ou recepção.

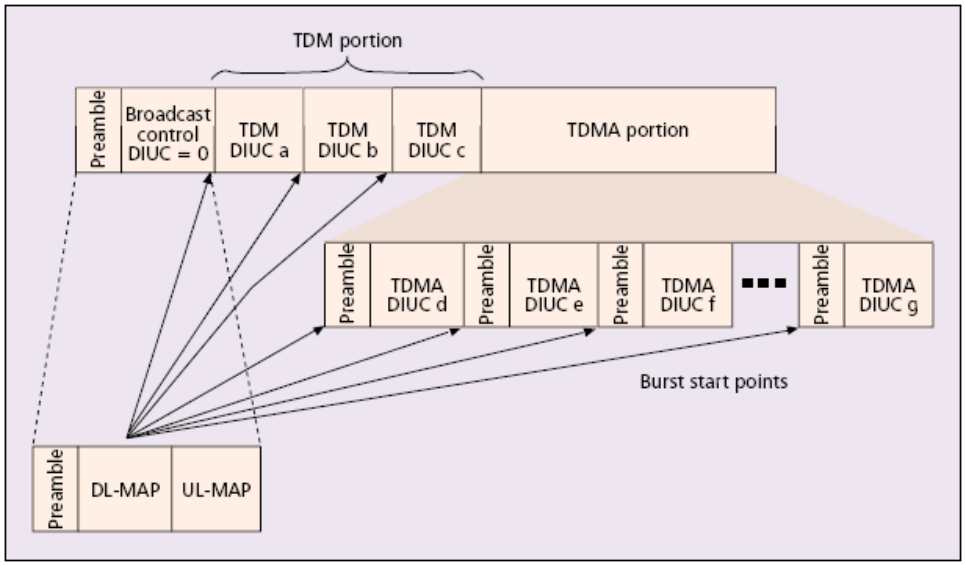


Figura 7: Quadro de transmissão FDD (EKLUND et al, 2000)

Cada quadro da camada PHY (**Figura 7**) inicia-se com um preâmbulo de sincronização. Este preâmbulo é seguido por uma porção de controle que contém o mapa de *download* (DL-MAP) e o mapa de *upload* (UL-MAP). O DL-MAP define a qual estação se destinam os dados transmitidos em cada *slot* do canal de *download*, o tempo de início de cada *slot*, e o Código de Intervalo de Uso de *Downlink* (DIUC), *i.e.*, o perfil de transmissão para cada SS. O UL-MAP define quais SSs devem transmitir nos determinados *slots*, o tempo de início de cada *slot* do canal de *upload*, e o Código de Intervalo de Uso de *Uplink* (UIUC), *i.e.*, o perfil de recepção para cada SS. A porção de controle é seguida pelas transmissões do canal de *downlink* que são efetuadas no esquema TDM. Após o término do período de *downlink*, ocorre um espaço de transição e inicia-se o *uplink* onde as SSs disputam o canal em um esquema TDMA. O modo FDD utiliza duas faixas de frequência distintas para *download* e *upload* enquanto o modo TDD utiliza a mesma faixa de frequência, dividindo-a em períodos de *download* e *upload*. O quadro de transmissão do IEEE 802.16 PMP é exibido na **Figura 7**.

4.3.1.2. Classes de Serviço

As estações clientes compartilham o *uplink* para a BS sob demanda. Dependendo da classe de serviço utilizada, a SS pode receber permissão contínua para transmitir ou deve requisitar à BS permissão para tal.

Dentro de cada setor de transmissão, os usuários conectados à BS estão sujeitos às restrições de serviço impostas pelo protocolo de transmissão que controla as disputas entre os usuários e, para cada um destes, modela os parâmetros de *delay* e QoS concedidos. Isto é possível devido às cinco diferentes classes de serviço oferecidas que são implementadas através de concessões de banda não solicitadas, *polling*, e procedimentos de contenção de disputa. As seguintes classes de serviço são oferecidas:

Unsolicited Grant Service - **UGS**: Projetado para dar suporte a fluxos de dados de tempo real onde o tráfego gerado possui taxa constante de transmissão, *e.g.*, conexões VoIP sem supressão de silêncio. As concessões a este serviço são concedidas periodicamente sem que haja requisição explícita.

Real-time Polling Service - **rtPS**: O rtPS também pode ser usado para aplicações com fluxos de tempo real, porém, com taxa de transmissão de dados variável, *e.g.*, vídeo MPEG. Diferentemente do UGS, para receber concessões para transmitir este serviço uma SS deve enviar requisições à BS.

Extended Real-time Pooling Service - **ertPS**: O rtPS estendido foi introduzido posteriormente, no padrão(IEEE 802.16, 2006), e é um serviço baseado no UGS e no rtPS para atender fluxos de tempo-real com pacotes de tamanho variável, *e.g.*, VoIP com supressão de silêncio. Para o serviço ertPS, assim como no UGS, uma quantidade de recursos é concedida sem que haja necessidade de *pooling*. Contudo, no ertPS esta quantidade pode ser alterada mediante requisições enviadas pela SS.

Non-real-time Polling Service - **nrtPS**: O nrtPS é voltado para aplicações tolerantes a maiores atrasos na entrega de pacotes, *e.g.*, FTP. Neste tipo de conexão sob demanda as SS devem enviar pedidos de concessão para a BS.

Best Effort Service - **BE**: O serviço BE é direcionado a aplicações que não possuem nenhum requerimento rígido de QoS, *e.g.*, HTTP, e-mail. Para este serviço devem ser feitas requisições de banda sob demanda e estas possuem menor prioridade em relação aos outros tipos de requisição de serviço.

Dois tipos de concessão de banda são oferecidos pelo padrão: Concessão Baseada em Conexão (*Grants per Connection* - GPC) e Concessão Baseada em Estação (*Grants per Subscriber Station* - GPSS). Na Concessão Baseada em Conexão a largura de banda é explicitamente garantida para cada conexão, de acordo com o seu tipo de fluxo, que requisita sua própria oportunidade de transmissão. Na Concessão Baseada em Estação a

estação cliente requisita oportunidades de transmissão para todos os serviços que ela mantém. Esta estação é responsável por alocar concessões de transmissão para os diferentes tipos de serviços mantidos por ela.

4.3.2. Modo *mesh*

O segundo modo de operação do WiMAX é o modo *mesh*. A principal diferença entre o modo PMP e o modo *mesh*, é que no modo PMP todo tráfego deve enviado através BS enquanto no modo *mesh*, este pode ser roteado através de outras SSs ou ocorrer diretamente entre duas SSs. A **Figura 8** mostra uma configuração típica deste tipo de rede.

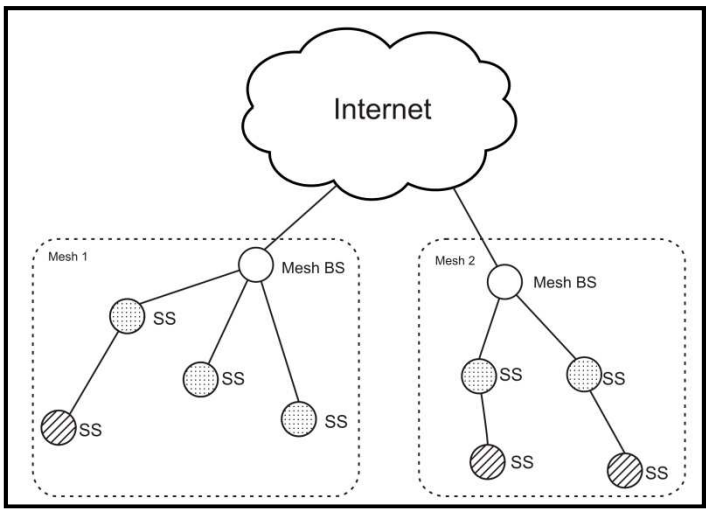


Figura 8: Configuração típica das redes 802.16 mesh

Dentro da rede *mesh* o *host* que conecta a rede com a Internet é denominado *Mesh* BS e todas as outras estações são chamadas *mesh* SS. *Uplink* e *downlink* são considerados como: tráfego em direção à *mesh* BS e tráfego da *mesh* BS para as SSs. Outro importante conceito a ser lembrado ao estudarmos o modo *mesh* do IEEE 802.16 é a definição de “vizinhança” e “vizinhança estendida”.

Como exibido na **Figura 9**, os vizinhos de um nó são aqueles nós que possuem *link* direto para ele e sua vizinhança estendida e composta pelos vizinhos de seus vizinhos.

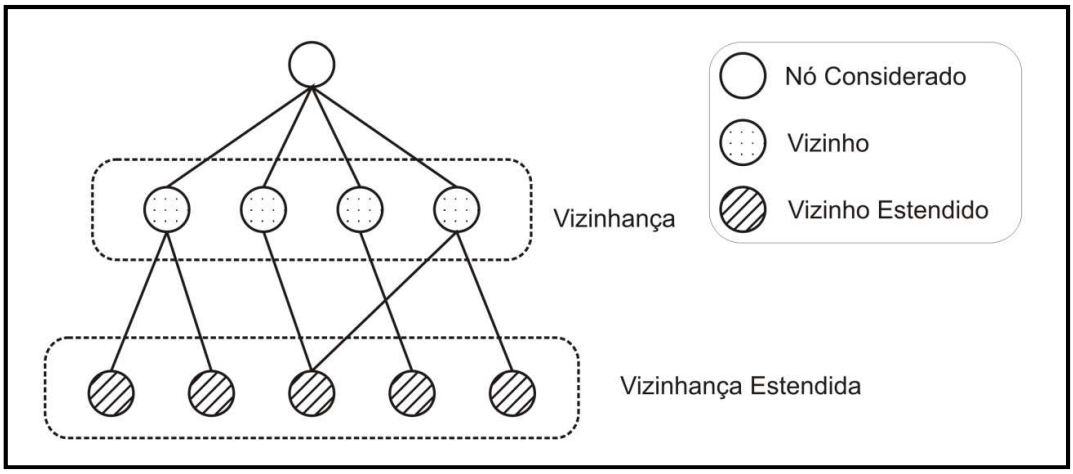


Figura 9: Vizinhança e vizinhança estendida e um nó

4.3.2.1. Estrutura do canal de transmissão

No 802.16 *mesh* o canal de transmissão (**Figura 10**) é dividido em sub-quadros de dados e controle. Durante os quadros de controle, as estações coordenam quais nós poderão transmitir no próximo quadro de dados. Estes quadros de controle fornecem também informações para que novos nós possam se juntar à rede e informam quais *links* na rede se encontram ativos. Nos sub-quadros de dados, as estações que previamente foram escalonadas podem transmitir seus dados de forma livre de colisão.

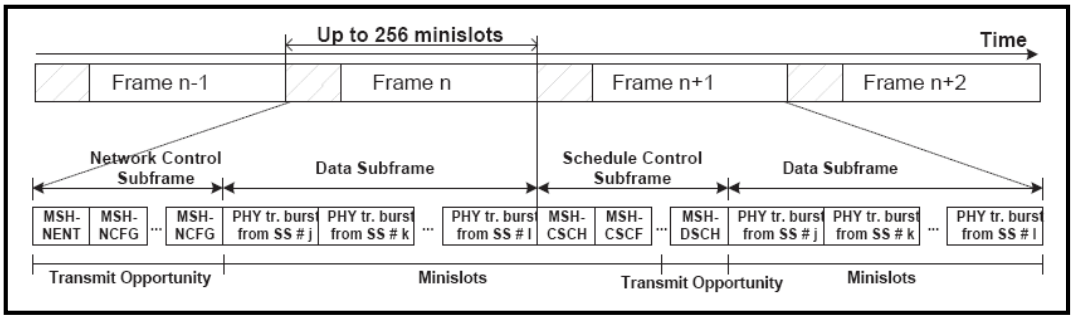


Figura 10: Estrutura do canal de transmissão do IEEE 802.16 *mesh*(FANCHUN, 2007)

O escalonamento, *i.e.*, controle sobre quais estações transmitem nos determinados sub-quadros, pode ser feito de forma centralizada ou distribuída. No escalonamento centralizado, a BS coordena as transmissões garantindo que não haja colisões.

Todos os nós dentro de uma determinada quantidade de saltos[1] enviam requisições de transmissão à *mesh* BS e esta deve definir a alocação de recursos para cada *link* da rede, comunicando às SSs seus agendamentos de transmissão. Já no escalonamento distribuído, as SSs devem coordenar um escalonamento entre si de forma que possam transmitir sem que haja colisões. Em ambos os modos de escalonamento, todas as transmissões de um nó devem ser agendadas com seus vizinhos e vizinhos estendidos e nem mesmo a *mesh* BS, pode transmitir sem antes haver agendado sua transmissão com sua vizinhança e vizinhança estendida.

O escalonamento e a configuração de rede são feitos através de 5 tipos de mensagens definidas pelo padrão. Estas mensagens são exibidas na **Tabela** 4.

Mensagem	Função
MSH-NENT	Esta mensagem carrega os parâmetros necessários para uma estação iniciar o processo de entrada na rede. Um nova estação deve informar seus dados nesta mensagem e caso não possua *link* direto com a BS, deve escolher uma das estações vizinhas como *sponsor*. Este processo de entrada na rede é descrito detalhadamente na **Seção 4.3.2.2**.
MSH-NCFG	Esta mensagem contém informações sobre os vizinhos de um nó, potência de transmissão, distância da estação à BS, etc. Todos os nós da rede devem transmitir esta mensagem com seus parâmetros e retransmitir a todos os vizinhos as mensagens que receber.
MSH-CSCF	Esta mensagem é utilizada no modo de escalonamento centralizado. É enviada por *broadcast* para informar todos os nós sobre a quantidade de estações na rede e o número de canais disponíveis para transmissão.
MSH-CSCH	Mensagem enviada pelas SSs para requisitar oportunidades de transmissão. E enviada pela BS para conceder oportunidades de transmissão. Quando enviadas pela BS, estas mensagens devem ser propagadas por toda a rede informando o escalonamento do próximo quadro de transmissão.
MSH-DSCH	Mensagem utilizada para configuração do escalonamento distribuído. No escalonamento distribuído, as estações se auto-coordenam para agendar as transmissões do próximo quadro.

Tabela 4: Mensagens de escalonamento e configuração de rede do WiMAX *mesh*

[1] Considera-se cada salto (*hop*) como um *link* entre dois nós, assim, dois nós que possuem *link* direto estão a um salto de distância.

4.3.2.2. Formato dos quadros do modo *mesh*

No modo de operação *mesh* o cabeçalho genérico (**Figura 5**) deve ser seguido pelo sub-cabeçalho *mesh*. O cabeçalho *mesh* consiste em somente um campo que é o Identificador de Conexão (CID). Desta forma, os quadros transmitidos no modo *mesh* possuem a estrutura exibida na **Figura 11**.

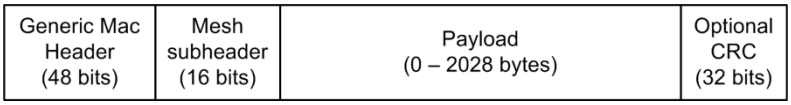


Figura 11: Quadros transmitidos no modo *mesh*

O conteúdo carregado no quadro é indicado pelo próprio CID. Se a conexão for uma conexão de gerenciamento, a mensagem contida no quadro será uma mensagem de gerenciamento. Caso contrário, trata-se de um quadro de dados.

4.3.2.3. Processo de entrada na rede

O procedimento de entrada de rede é especificado através dos canais lógicos (**Figura 12**) que uma estação candidata deve acessar durante o processo de entrada.

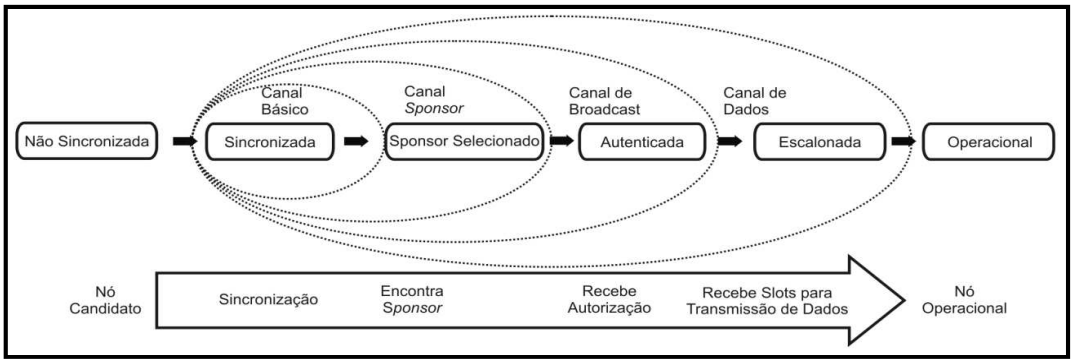


Figura 12: Estados do procedimento de entrada na rede 802.16 *mesh*(DJUKIC AND VALAEE, 2006)

Inicialmente, um nó que deseja entrar na rede (nó candidato) escuta o meio físico buscando os preâmbulos de sincronização dos sinais transmitidos pelas *mesh* SS ou pela *mesh* BS. Uma vez sincronizado, o nó candidato escuta por pacotes de configuração de rede e caso

não possua um *link* direto com a BS, escolhe uma das estações vizinhas para ser seu *sponsor*. O papel do *sponsor* é intermediar a comunicação entre o nó candidato e o restante da rede, alocando parte do seu canal de dados para as mensagens enviadas pelo nó candidato. O nó candidato transmite então uma mensagem ao potencial *sponsor* indicando que deseja entrar na rede. Uma vez aceito pelo *sponsor*, o nó candidato envia através dele mensagens de autenticação à BS (O processo de autenticação é explanado com mais detalhes na seção 4.3.2.4 deste capítulo). Após a autenticação, o nó candidato fecha o canal de *sponsor* e passa a utilizar o canal de broadcast para transmitir outras mensagens de configuração da rede, obtém um endereço IP através de mensagens DHCP, e está apto para requisitar oportunidades de transmissão. O procedimento de entrada resumido no parágrafo acima é dividido em 8 etapas:

1. **Sincronização inicial com a rede:** Após a inicialização ou perda de sinal, o nó deve ouvir o canal de transmissão e esperar por mensagens do tipo MSH-NCFG. Ao receber esta mensagem, o nó obtém uma espécie de tempo de rede contida no campo '**Timestamp**' da mensagem. Caso não receba nenhuma mensagem, o nó deve continuamente alternar entre as faixas de frequências disponíveis até que encontre uma rede válida. Após a sincronização da camada PHY, a camada MAC deve tentar descobrir os parâmetros de rede e ao mesmo tempo ir construindo a lista de vizinhos.
2. **Obtenção de parâmetro de rede:** Após receber um determinado número de mensagens MSH-NCFG, a estação deve construir a lista de vizinhos e atribuir a cada um desses *links* um identificador de 8 bits. Através destas mensagens o nó candidato extrai também a potência de transmissão utilizada pelos vizinhos, a quantidade de BSs disponíveis, e o mapa com o escalonamento que indica para cada estação quando estas podem transmitir.
3. **Abertura de canal *sponsor*:** Uma vez construída a lista de vizinhos, o nó candidato deve escolher um dos vizinhos e enviar uma mensagem **MSH-NENT:NetEntryRequest** para o vizinho escolhido como *sponsor*. O *sponsor* por sua vez pode aceitar ou recusar o pedido. Caso aceite, responde com uma mensagem **MSH-NENT:NetEntryRequest** e está apto para encaminhar as mensagens de autenticação e registro do novo nó. A partir daquele momento, as mensagens que o nó candidato deseja enviar à BS são recebidas pelo *sponsor*, encapsuladas em datagramas UDP e enviadas à BS. As mensagens de resposta da BS para o candidato são enviadas para seu *sponsor* que desencapsula o datagrama UDP e entrega MAC ao candidato.
4. **Autorização:** O processo de autorização utiliza um protocolo de gerenciamento de chaves PKMv1 especificado pelo padrão e é descrito com detalhes na seção 4.3.2.4.

5. **Registro:** Na etapa de registro é atribuído ao nó candidato um identificador de 16 bits (**Node ID**). Após a etapa de autorização, todas as estações na sub-rede são identificadas com um Node ID único atribuído pela BS.
6. **Conectividade IP:** Neste ponto a estação deve utilizar o protocolo DHCP (DHCP, 2009) para obter um endereço IP e quaisquer outros parâmetros necessários para se obter conectividade IP.
7. **Sincronização de relógio:** O nó estabelece a data e hora através do Protocolo de Tempo definido pela RFC-868(TIME PROTOCOL, 1983).
8. **Transmissão de parâmetros operacionais:** Para configurar outros parâmetros de transmissão como tamanho de PDUs, fluxos de serviço e parâmetros de QoS, o novo nó deve enviar uma mensagem DSA-REQ para a BS requisitando a descrição destes parâmetros.

4.3.2.4. Autenticação

Para poder acessar a rede, um nó deve estar autenticado junto ao operador de rede. O padrão IEEE 802.16-2004 estabelece um protocolo de gerenciamento de chaves (PKMv1) para ser utilizado durante a autenticação. Este protocolo define o processo de troca de Chaves de Autorização (AK) e Chaves de Criptografia de Tráfego(TEK).

Cada estação possui um certificado X.509(X509, 2002) concedido por seu fabricante. Este certificado contém a chave pública do nó e seu endereço MAC. Antes de enviar a mensagem requisitando autenticação, o nó envia ao servidor de autenticação uma mensagem contendo o certificado do seu fabricante. O servidor de autenticação pode desta forma verificar as credenciais do fabricante junto à uma autoridade certificadora (CA) e garantir a autenticidade do nó. A **Figura 13** mostra o processo de autenticação de um nó.

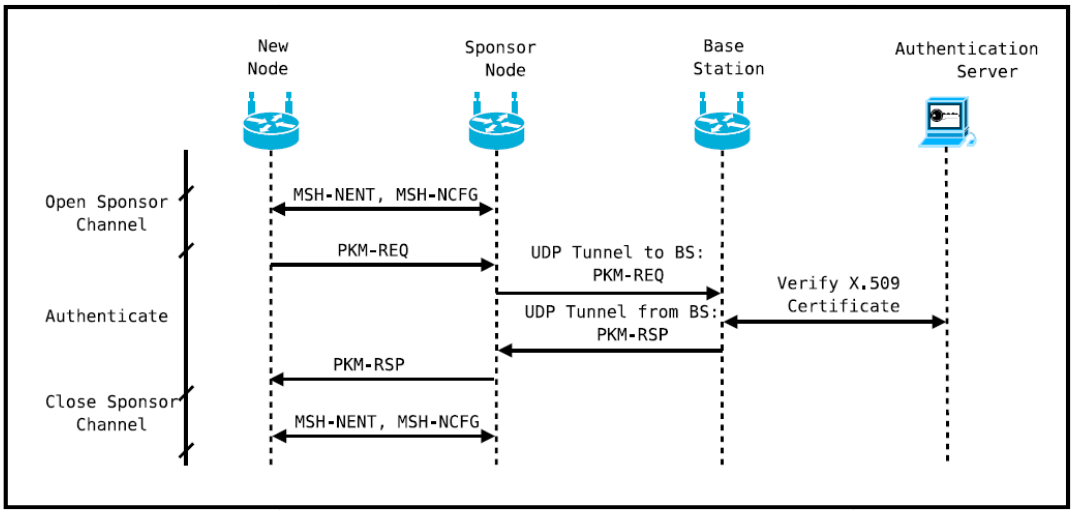


Figura 13: Processo de Autencicação de um nó da rede *mesh*(DJUKIC AND VALAEE, 2006)

Após encontrar um *sponsor*, o nó candidato envia ao servidor de autenticação uma mensagem (PKM-REQ: *Auth Request*) requisitando entrada na rede. A mensagem de requisição carrega o certificado do nó. Após a verificação da autenticidade do certificado, o servidor de autenticação retorna uma mensagem contendo uma AK e uma lista de Associações de Segurança (SA), ambas cifradas com a chave pública do nó candidato. As SAs são utilizadas para gerenciar informações de criptografia entre o nó requisitante e seus vizinhos e assim como as AKs e TEKs, possuem tempo de vida limitado, devendo ser periodicamente renovadas.

A chave de autorização (AK) é uma chave de 20 bytes compartilhada entre o servidor de autenticação e a estação. Desta chave são derivadas outras chaves (e.g., Key Encripton Key) que são usadas ora para criptografia durante a troca de chaves secretas entre as estações ou autenticação de mensagens entre duas estações. Outros dois tipos duas chaves importantes no PKMv1 são a Chave Secreta do Operador e as Chaves de Criptografia de Transmissões (TEK). A primeira é uma chave secreta enviada pelo servidor de autenticação na resposta *Auth Reply*. Esta chave é conhecida por todos os nós autenticados junto ao operador. A segunda é a chave secreta compartilhada ente dois nós e é utilizada para cifrar as transmissões nos *links* estabelecidos entre eles.

4.3.2.5. Roteamento

O roteamento realizado pela camada de rede em redes 802.16 *mesh* está intrinsecamente relacionado com os estados dos *links* entre os nós, podendo haver alteração de rotas com a

entrada ou saída de nós. Esta característica requer um protocolo de *roteamento* multicamada, *i.e.*, o protocolo de roteamento na camada IP deve obter informações fornecidas pela camada MAC.

As transmissões entre estações de diferentes sub-redes ou entre uma SS e a Internet devem ocorrer através da *mesh* BS, enquanto dois nós da mesma sub-rede, eventualmente através de outros nós, podem se comunicar sem que o tráfego cruze a *mesh* BS.

Através de um *link* de *broadcast*, todos os nós operacionais enviam periodicamente mensagens de configuração de rede (MSH-NCFG). Estas mensagens de configuração além de carregarem parâmetros de transmissão do nó emissor contêm informações sobre o estado dos *links* daquele nó para com seus vizinhos, tornando-os conhecidos para todas as estações da sub-rede. Desta forma, é possível para cada nó saber toda a topologia da rede e, a partir desta aplicar um algoritmo de roteamento. O padrão em si não especifica nenhum algoritmo de roteamento, porém na literatura encontramos ótimos estudos propondo algoritmos e mecanismos de escalonamento para maximizar a vazão ((JIN et al, 2008) e (TAO et al, 2005)), diminuir a interferência causada pelas transmissões (WEI et al, 2005), e prover QoS (SHETIYA AND SHARMA, 2005) em redes WiMAX *mesh*.

4.3.3. Camada de convergência e conexões

Classificação de fluxos

Para clarear o funcionamento da subcamada de convergência do modo *mesh*, iremos primeiro explicar seu funcionamento detalhado no modo PMP. Considere o cenário exibido na **Figura 14**. Nesta sub-rede a BS possui 8 conexões MAC com as estações clientes. Cada conexão é unidirecional, *i.e.*, só enviam dados em um sentido: *downlink* ou *uplink*. Assim, para que as estações possam enviar e receber dados, é necessário que haja no mínimo duas conexões por estação. Uma estação pode possuir diversas conexões e cada um delas estar relacionada com um tipo de fluxo (e.g., HTTP, e-mail, VoIP, etc). Estas conexões podem ser criadas durante a etapa de inicialização da SS ou posteriormente sob demanda.

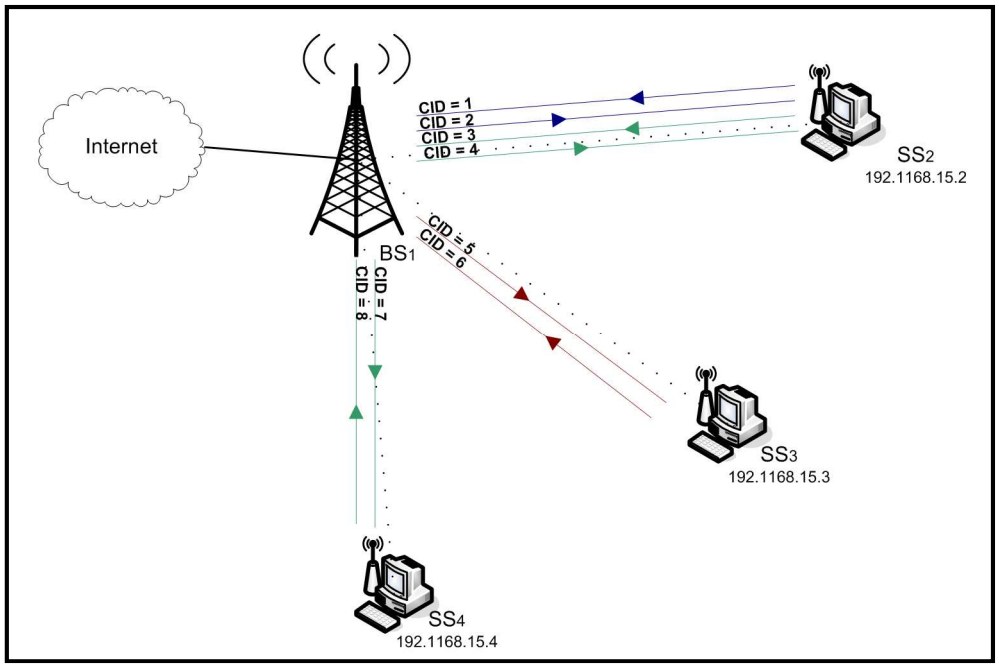


Figura 14: Ambiente PMP com conexões

No *downlink*, quando a BS receber um pacote[2] irá verificar seu cabeçalho IP e cabeçalho do protocolo (*e.g.*TCP, UDP, etc) carregado pelo pacote. Baseando-se por estes campos, a BS pode determinar em qual das suas conexões o pacote deve ser classificado. Cada uma das classes de serviço possui um *buffer* de envio. Com base nestes *buffers*, a BS irá gerar o mapa de *downlink*. Na **Figura 15** pode-se ver este processo de classificação e envio dos pacotes para o fluxo de *downlink*.

O padrão IEEE 802.16 não exige que as classes de serviço utilizadas no modo PMP sejam obrigatórias no modo *mesh*, tanto porque o modo *mesh* não possui conexões fim-a-fim. No modo *mesh*, em cada nó intermediário por onde o pacote for enviado o quadro MAC é desencapsulado, decifrado caso o *link* use algum tipo de criptografia, enviado para as camadas superiores, e caso deva ser redirecionado, o pacote deverá ser novamente mapeado em uma das conexões daquela estação. Esta forma de transmissão dificulta a garantia de QoS.

[2] O padrão 802.16 define a operação da sub-camada de convergência para 3 tipos de quadros: ATM, IP e Ethernet. Para reduzirmos o escopo do trabalho, nesta seção e também no restante do texto iremos considerar somente datagramas IP.

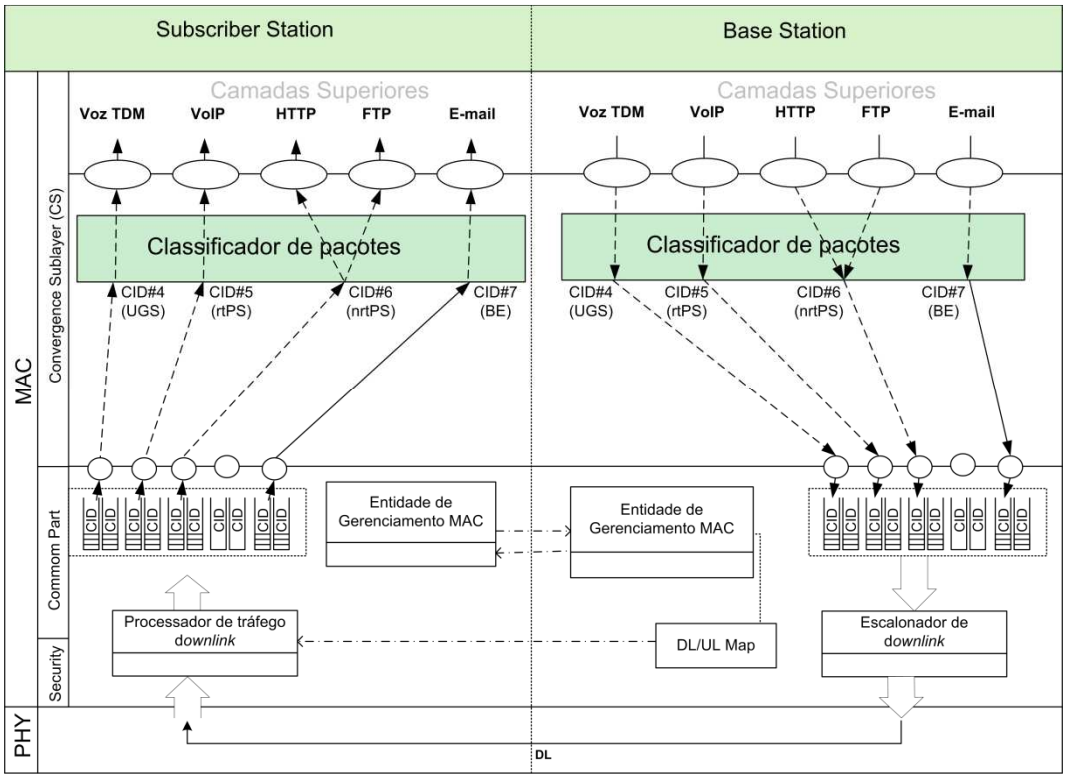


Figura 15: Processo de classificação e envio de datagramas do IEEE 802.16

O protocolo de roteamento *mesh* deve estar atrelado à camada MAC, pois é na subcamada de convergência que o pacote será classificado e enviado por um dos *links* ativos do nó. Portanto, o principal critério de classificação no modo *mesh* será o destino do pacote e não sua classe de serviço como no modo PMP.

Diversos detalhes do funcionamento da sub-camada de convergência não são definidos e ainda restam diversos problemas referentes à integração entre a MAC e os protocolos e serviços das camadas superiores (*e.g.*, ARP, DHCP, *broadcast*, etc). O IETF designou um grupo de trabalho para estudar e padronizar estas questões e maiores detalhes sobre o assunto podem ser encontrados no site (IPo802.16, 2009) do grupo.

5 Arquitetura de tarifação

A proposta deste trabalho é apresentar uma arquitetura escalável que possibilite gerenciar, autenticar, tarifar e também criar políticas de incentivo aos usuários em redes WiMAX *mesh*. Como parte desta arquitetura, apresentamos um novo protocolo de contabilização de pacotes que, além de permitir contabilizações precisas, oferece segurança contra fraudes e possíveis ataques. A implementação do protocolo de contabilização é feita através de uma modificação na subcamada de convergência do modelo de referência do padrão IEEE 802.16 e é validada através de um simulador de rede.

5.1. Relevância da proposta escolhida

As redes *mesh* sem fio (WMN) têm mostrado um grande potencial para tornarem-se um meio amplamente utilizado na computação ubíqua de alta velocidade (AKYILDIZ, 2004). Espera-se que assim como as redes de telefonia celular, em um futuro não muito distante existam diversos provedores de WMNs(ZHANG E FANG, 2007). Uma importante questão relacionada às redes *multi-hop* que tem sido pouco abordada na literatura trata-se da dependência de cooperação entre os nós para que haja um bom funcionamento da rede. Como estudado por Cagalj *et al* (CAGALJ et al, 2004), para economizar seus recursos, contudo, os nós de uma rede *mesh* podem se comportar de forma egoísta evitando encaminhar pacotes dos nós vizinhos. A proposta aqui apresentada oferece uma forma de minimizar este problema. Introduzimos um mecanismo que garante para os usuários uma tarifação justa e atrativa, e para os provedores de serviço uma forma de atrair mais usuários e estender sua área de cobertura.

5.2. Trabalhos Relacionados

Pouco tempo após sua criação, o crescimento da Internet fez com que esta deixasse de ter fins puramente militares e acadêmicos e passasse a ser utilizada para fins comercias. A comercialização dos serviços de acesso à Internet trouxe à tona a necessidade de mecanismos para contabilização e controle de acesso dos usuários destes serviços. Devido a isso, diversos mecanismos para tarifação e contabilização de tráfego têm sido propostos.

5.2.1. Tarifação em redes IP

Richard J. Edell *et al* (RICHARD et al, 1995), propõem um sistema de tarifação para contabilizar tráfego de conexões TCP. Apesar de considerar uma arquitetura de rede que não é tão comum atualmente (*e.g.* terminais utilizados para o acesso de diversos usuários simultâneos, recursos de rede extremamente escassos, etc.) e de seu sistema se limitar à contabilização de tráfego TCP, este sistema traz considerações importantes sobre problemas relacionados à escalabilidade e autenticação em sistemas de contabilização. Ibrahim *et al* (IBRAHIM et al, 2002) realizam um estudo das formas de tarifação praticadas por volta do ano de 2002 e propõe um mecanismo de tarifação baseado na quantidade de tráfego gerada pelos usuários. A principal idéia de seu trabalho consiste em interceptar as conexões que os usuários tentam estabelecer durante o acesso à rede. Quando há uma tentativa de abertura de uma nova conexão TCP com algum *host* da Internet, o estabelecimento da conexão é prorrogado até que o usuário seja autenticado e seja feita a verificação de que ele possui créditos para pagar pelo acesso. Se o usuário estiver apto para pagar, a conexão é estabelecida e seu tráfego será computado.

5.2.2. Tarifação em redes sem fio

A tarifação em redes possui características bastante distintas quando tratamos de redes de telefonia móvel e redes IP móveis. A principal diferença é a forma pela qual o usuário é tarifado. A forma tradicional na qual os usuários são tarifados em redes de telefonia móvel (geralmente pelo tempo de conexão), não é apropriada para tarifar tráfego de dados em redes IP e nestas duas tecnologias a contabilização do tráfego é feita de maneira diferente. Iremos considerar em nosso caso somente os mecanismos de tarifação em redes IP móveis.

O advento das redes sem fio e de cenários com mobilidade IP trouxe novos aspectos à questão de tarifação. Um destes aspectos é a suposição de que o operador de rede pode efetuar cobranças indevidas sobre os usuários. Nestas situações o operador deveria provar que as tarifações impostas são realmente devidas pelo usuário. Considerando tais cenários Zhou J. e Lam KY (ZHOU; LAM, 1998) e Chen HB e Hsueh SC(CHEN; HSUEH, 2003) propõem soluções para possibilitar tarifação irrefutável para usuários móveis. Desta forma, uma vez que um usuário tenha emitido um pagamento, o operador pode provar que este foi de fato emitido pelo usuário. Ambas as soluções combinam mecanismos de assinatura digital e cadeias *hash*. Cada emissão de pagamento consiste em um 'elo' da cadeia *hash* que deve ser assinado com a chave privada do usuário e emitido conforme este utiliza o serviço. Outro estudo similar a estes é o que foi realizado por Tewari H. e O'Mahony (TEWARI; O'MAHONY, 2003). Prevendo um futuro onde as redes de acesso seriam operadas por inúmeros ISPs independentes e os dispositivos poderiam trafegar livremente entre estes domínios, os autores apresentam um esquema também baseado em cadeias *hash* para permitir a contabilização de uso da rede, a rápida autenticação de datagramas[3] e a redução das mensagens de sinalização.

5.2.3. Tarifação em redes *multi-hop*

Um dos aspectos mais relevantes relacionados à tarifação em redes *multi-hop* refere-se à necessidade de cooperação entre as estações. Seria desejável para um provedor de acesso que se proponha a fornecer acesso *multi-hop* que este recompensasse as estações que cooperassem para o aumento da disponibilidade de vazão da rede.

Este problema é colocado em discussão por Salem *et al*(SALEM et al, 2003). Considerando um cenário onde um ISP mantenha *mesh* BSs como gateways de rede, os autores propõem um mecanismo para garantir recompensas para as estações que encaminharem pacotes dos vizinhos. Para tanto, o protocolo introduz a idéia de sessão de

[3] Neste texto, a expressão 'autenticação de datagramas' ou 'autenticação de pacotes' consiste no processo de verificação de integridade dos dados contidos no pacote e certificação da autenticidade do emissor. A verificação certifica que os dados que foram recebidos são os mesmos que os enviados pelo emissor. A certificação de autenticidade garante que um pacote contendo o endereço de origem de um emissor realmente tenha sido enviado por ele.

tarifação. Antes de transmitir, uma estação deve configurar uma sessão fim-a-fim, indicando as características do tráfego e a rota de transmissão. Configurada a sessão, todos os pacotes são transmitidos com um *label* anexado e enviados através daquela sessão, permitindo que os *mesh gateways* possam ter ciência e controle da quantidade de dados transmitidos e quais estações participaram da transmissão. Todo o tráfego enviado e recebido deve ser confirmado pela estação de destino de forma que o ISP saiba que esta de fato recebeu os pacotes a ela enviados. Uma vez confirmado este recebimento, todas as estações intermediárias são recompensadas. Ao final do trabalho, os autores discutem as diversas formas de ataque que poderiam ser levantadas dentro do cenário considerado e garantem que seu protocolo é seguro contra todas elas.

Considerando um cenário onde diversos ISPs fornecem acesso a seus usuários através de redes *mesh*, Y. Zhang e Y. Fang propõem o UPASS(ZHANG; FANG, 2007), um passe universal usado para identificação, tarifação e gratificação interdomínio dos usuários em WMNs. O sistema de tarifação UPASS é análogo aos atuais sistemas de cartão de crédito. Algumas autoridades certificadoras concederiam aos usuários um UPASS e fariam acordos com os ISPs de forma que estes não necessitassem estabelecer uma relação de confiança com os usuários que desejarem utilizar seus serviços. Através de um protocolo de micro-pagamento combinado com técnicas de assinatura digital e funções *hash* de uma via, o UPASS garante a incontestabilidade das cobranças realizadas pelos ISPs, assegurando que os usuários possam utilizar o serviço de diversos provedores, pagando-os e sendo recompensados pelo tráfego re-encaminhado sem que haja necessidade de se preocupar com a idoneidade dos provedores.

Apesar de fornecerem vários detalhes teóricos sobre seu funcionamento, nenhum destes trabalhos ((ZHANG; FANG, 2007), (SALEM et al, 2003)) fornece detalhes sobre quais tecnologias de transmissão sem fio são suportadas ou quais camadas do modelo ISO/OSI eles estariam alocados. Como será demonstrado no próximo capítulo, nossa arquitetura de tarifação fornece todos os detalhes para seu funcionamento na camada MAC do padrão IEEE 802.16.

5.3. Considerações, premissas gerais e requisitos de segurança

5.3.1. Arquitetura de rede

O cenário considerado para o desenvolvimento desta proposta consiste em um domínio de operação de um provedor de serviço de acesso sem fio (*Wireless Internet Service Provider* - WISP). Este cenário é exibido na **Figura 16**.

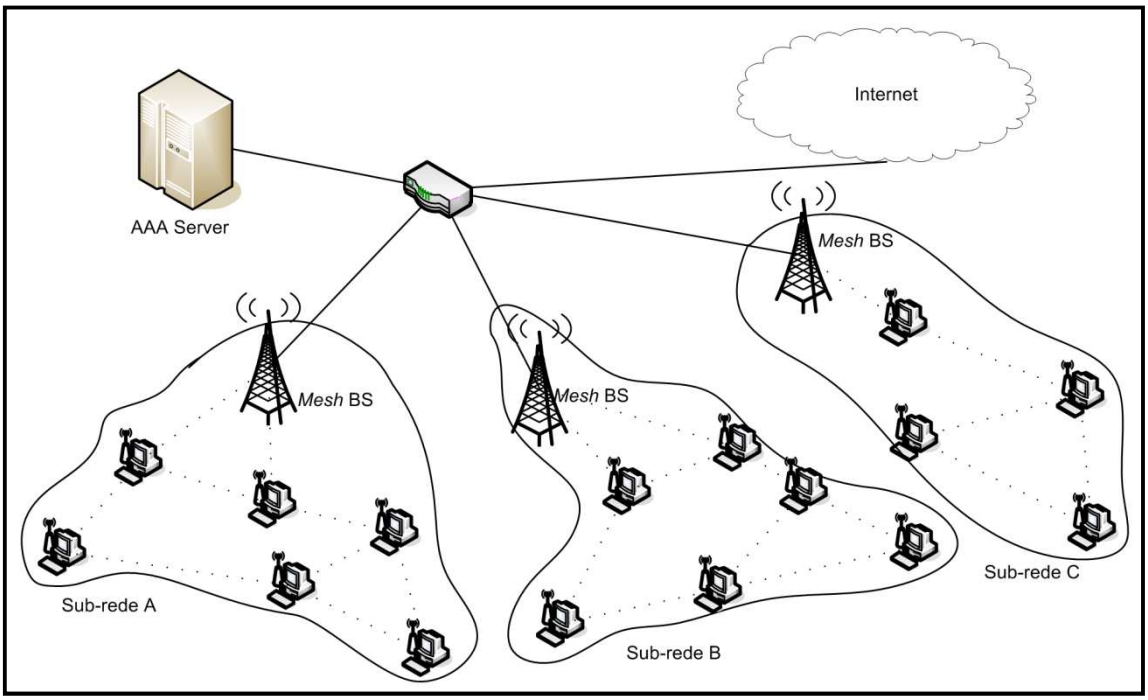


Figura 16:Cenário de operação e um WISP

Dentro da sub-rede, dois tipos de estações (dispositivos) são consideradas: estações base (*mesh* BS) e estações clientes *mesh* (*mesh* SS). As *mesh* BSs atuam como *gateways*, possibilitando que as estações clientes tenham acesso à Internet. As *mesh* SSs são estações fixas ou móveis pertencentes aos usuários. Estas estações, além de serem utilizadas por seus proprietários para acessar a rede, podem atuar como roteadores encaminhando pacotes de outros usuários.

Todo o tráfego das estações da sub-rede para a Internet, e no sentido inverso (da Internet para a sub-rede), deve obrigatoriamente passar pela *mesh* BS. Esta consideração não impede que as estações se comuniquem diretamente, porém, simplifica o processo de roteamento nos nós, pois haverá somente um *gateway* de acesso à Internet para cada sub-rede. As estações da sub-rede podem se conectar diretamente à *mesh* BS ou através *links multi-hop* com as SSs da rede.

Para obter acesso à rede, uma estação deve primeiramente estar autenticada. O processo de autenticação deve ocorrer conforme especificado pelo padrão IEEE 802.16(IEEE 802.16, 2004), onde é requerido que cada estação possua credenciais únicas e estabeleça associações de segurança com a *mesh* BS. Estas credenciais são associadas ao usuário quando este se afilia ao provedor ou durante uma fase de *login*, que pode ser requerido antes que este acesse a rede. Os dados de autenticação, autorização e contabilização do usuário são gerenciados por um servidor de autenticação (*Authentication*, *Authorization*, *Accounting* - AAA). Depois de verificado que o usuário está autorizado, a associação usuário/estação é feita. Portanto, no decorrer deste texto, quando nos referirmos à estação, estamos considerando que existe um usuário responsável pelo tráfego emitido e recebido por ela.

Assumimos também que os nós são estáticos ou possuem pouca mobilidade. Portanto, o conceito de mobilidade no cenário previsto limita-se a pequenas movimentações dentro da área de cobertura da sub-rede (micro-mobilidade).

De maneira geral, a topologia das redes *mesh* possui forma de árvore com raiz principal na *mesh* BS. Através do mecanismo de propagação de estado de *links* utilizado no padrão, todos nós da sub-rede possuem conhecimento da topologia. O IEEE 802.16 não especifica um protocolo de roteamento obrigatório, o que permite que qualquer uma das soluções existentes, tais como apresentado em (JIN et al, 2008), (TAO et al, 2005), (SHETIYA; SHARMA, 2005) possa ser utilizada.

O tráfego de dados da sub-rede é dividido em dois tipos: *downlink* e *uplink*. O tráfego de *downlink* corresponde às transmissões provenientes da Internet fluindo em direção às estações. Já o tráfego de *uplink* é proveniente das estações da sub-rede flui em direção à Internet. Para possibilitar que o WISP possa realizar a tarifação sobre os usuários, a *mesh* BS deve efetuar a contabilização dos pacotes transmitidos e recebidos, identificando, para cada fluxo de transmissão, as estações destinatárias e as intermediárias que encaminharam os pacotes de sua origem ao destino na sub-rede. Identificadas as estações participantes da transmissão, o destinatário é debitado e aos intermediários é concedida uma quantia de crédito apropriada. Os débitos e créditos dos usuários são registrados em bases de gerenciamento de informações (*Management Information Base* - MIB) e cada BS possui um agente SNMP. Através do SNMP, as informações sobre os créditos e débitos de cada usuário são mantidas atualizadas e sincronizadas entre as *mesh* BSs e o AAA *Server*.

Por motivos de simplificação, consideraremos o WISP como uma entidade confiável que sempre atua de forma justa, atribuindo corretamente os encargos aos usuários.

5.3.2. Requisitos da arquitetura

O mecanismo de tarifação foi delineado com as seguintes considerações em mente:

Procedimentos de criptografia com baixo custo computacional: os procedimentos de criptografia, relacionados com a autenticação de pacotes e contabilização de dados na rede de acesso devem encontrar um bom equilíbrio entre robustez e desempenho.

Economia dos recursos de armazenamento dos nós: o mecanismo de tarifação deve levar em conta que muitas SSs possuem limitações de armazenamento. Portanto, caso seja necessário armazenar qualquer informação sobre os datagramas encaminhados, este espaço para armazenamento deve ser o menor possível e também ser liberado o quanto antes. Caso também seja necessário armazenar muita informação na BS, a escalabilidade do sistema seria comprometida.

Redução da quantidade de mensagens de sinalização: cada nó em uma rede *mesh* possui uma antena *ommi*-direcional, o que faz com que este tipo de rede gere bastante ruído. Este ruído produz interferências que causam erros e forçam a retransmissão de pacotes (INTEL, 2004) e, portanto, a falta de controle sobre a quantidade de pacotes enviados pode degradar severamente o desempenho da rede (YI LI et al, 2007). Caso seja necessário para o mecanismo de tarifação adicionar qualquer procedimento que requeira a troca de mensagens de sinalização, estas mensagens devem ser reduzidas ao mínimo para que os recursos da rede sejam aproveitados ao máximo.

Contabilização confiável: a contagem de pacotes feita pela BS deve ser justa e precisa, evitando que o ISP deixe de recompensar os usuários cooperativos e mesmo deixe de receber por parte do serviço fornecido.

Compatibilidade com o padrão IEEE 802.16: uma vez que o mecanismo de contabilização é construído sobre um padrão de indústria, as alterações realizadas na camada MAC não devem afetar a compatibilidade dos dispositivos com o padrão.

5.3.3. Ameaças à segurança

Uma vez que os usuários das estações intermediárias são recompensados pelo tráfego encaminhado, encaminhar pacotes dos vizinhos torna-se algo racional. Entretanto, a distribuição destas recompensas pode aumentar as tentativas de ataques contra o sistema.

Considerando esta premissa, somente serão consideradas ameaças, ataques que visem a burlar o sistema e fazer com que um usuário receba mais créditos que o merecido. Nenhuma estação é obrigada a participar do encaminhamento de pacotes de terceiros[4], porém estas não podem reclamar os benefícios que receberiam caso colaborassem. Dentre as principais formas de ataque e tentativa de fraude no protocolo de tarifação pode-se citar(JAKOBSSON et al, 2003):

Rejeição de pacotes: uma estação pode descartar os pacotes que devia re-encaminhar e ainda assim reclamar os créditos pelos pacotes descartados.

Injeção de pacotes: um nó intermediário injeta pacotes a um determinado nó e reclama créditos, como se houvesse participado de um encaminhamento.

Enchimento de pacotes: uma estação intermediária pode colocar enchimentos no pacote e reclamar pelos *bytes* transmitidos.

Re-encaminhamento cíclico: um ou mais nós intermediários podem conspirar de forma conjunta e enviar o mesmo pacotes em rotas cíclicas, de forma que pareça que estes enviaram maior número de pacotes do que realmente fizeram.

Ataque de repetição: Um dos nós intermediários pode salvar pacotes em buffer e posteriormente reenviá-los de forma a aumentar a quantidade de tráfego pela qual deveria ser recompensado.

Superfaturamento de rota: um usuário pode escolher a maior rota dentre as possíveis, fazendo com que o ISP tenha que recompensar mais estações do que seria necessário por aquele tráfego.

O mecanismo de contabilização proposto foi delineado de forma a suplantar as ameaças aqui expostas.

5.4. Protocolo de contabilização

[4] Esta obrigatoriedade se resume ao fato de que um usuário pode de alguma forma indisponibilizar sua estação para o encaminhamento de pacotes, seja com o desligamento da estação durante períodos em que não esteja utilizando, ou mesmo com mecanismo de *sofware* que descartem pacotes de vizinhos.

5.4.1. Notação

O protocolo de contabilização utiliza os seguintes termos quando se refere aos seus métodos criptográficos:

Código de verificação de mensagem (CVM): O código de verificação de mensagem é um código único gerado através de uma função *hash* de uma via. Esta função é denotada por:

$$f_h(x) = CVMx$$

A função $f_h(x)$ toma uma mensagem x qualquer e retorna um código de verificação ($CVMx$) de tamanho fixo que é associado univocamente à entrada x. Esta função é irreversível, *i.e.*, é impossível obter a mensagem x a partir de CVMx. No contexto deste trabalho, quando mencionarmos sobre o CVM de um pacote, estamos nos referindo ao CVM de sua carga útil.

Função de criptografia simétrica (*fc*): A função de criptografia simétrica é utilizada para enviar uma mensagem cifrada entre dois correspondentes. Seja m uma mensagem que será enviada entre um emissor E e seu receptor D. E e D compartilham uma chave secreta Ks. A função de criptografia simétrica é dada por:

$$fc(Ks,m) = M$$

Onde M é a mensagem cifrada que possui o mesmo tamanho de m. A função inversa de fc é:

$$fc^{-1}(Ks,M) = m$$

Cadeia de Cifras (CAD): Considere uma mensagem m que será enviada de um emissor E e será encaminhada por n receptores intermediários I_n (i=1,2,...n) até um destinatário D. Cada um dos receptores intermediários compartilha uma chave secreta Kn com o emissor. A cadeia de cifras desta transmissão é dada por:

$$CAD_{E\rightarrow D}(m) = f_c(K_n, f_c(K_3, f_c(K_2, f_c(K_1, m))))$$

A partir do emissor, cada receptor intermediário I_n criptografa a mensagem recebida e a envia para o receptor I_{n+1}. Assim, sucessivamente até que D receba a mensagem. Esta mensagem é a Cadeia de Cifras de *m*. A mensagem inicial *m* pode ser recuperada desde que se tenha o valor $CAD_{E\rightarrow D}$, a sequência dos nós que cifraram a mensagem, e as chaves secretas dos receptores intermediários. Conforme será esclarecido posteriormente, o valor $CAD_{E\rightarrow D}$ sempre é enviado por *D* ao emissor (pois este é o único que conhece todas as chaves secretas) e este aplica a função reversa (CAD^{-1}) para obter a mensagem *m*. A função CAD^{-1} função é dada por:

$$CAD^{-1}(CAD_{E\rightarrow D}) = f_c^{-1}(K_1, f_c^{-1}(K_2, f_c^{-1}(K_3, f_c^{-1}(K_n, CAD_{E\rightarrow D})))) = m$$

5.4.2. Contagem de pacotes

Para que seja possível mensurar as recompensas e cobranças que o operador deve aplicar, todos os pacotes que cruzarem a BS devem ser contados. É necessário também que o recebimento e a integridade dos pacotes enviados pela BS sejam confirmados pelos receptores, e que a BS garanta que os pacotes que recebeu das estações não foram modificados durante o caminho. Além disso, cada nó intermediário deve ser capaz de provar que encaminhou corretamente os pacotes dos vizinhos.

Modelo de contagem

Para facilitar o entendimento do mecanismo de contabilização e como este enfrenta os problemas de segurança expostos na seção **5.3.3**, considere os seguintes exemplos:

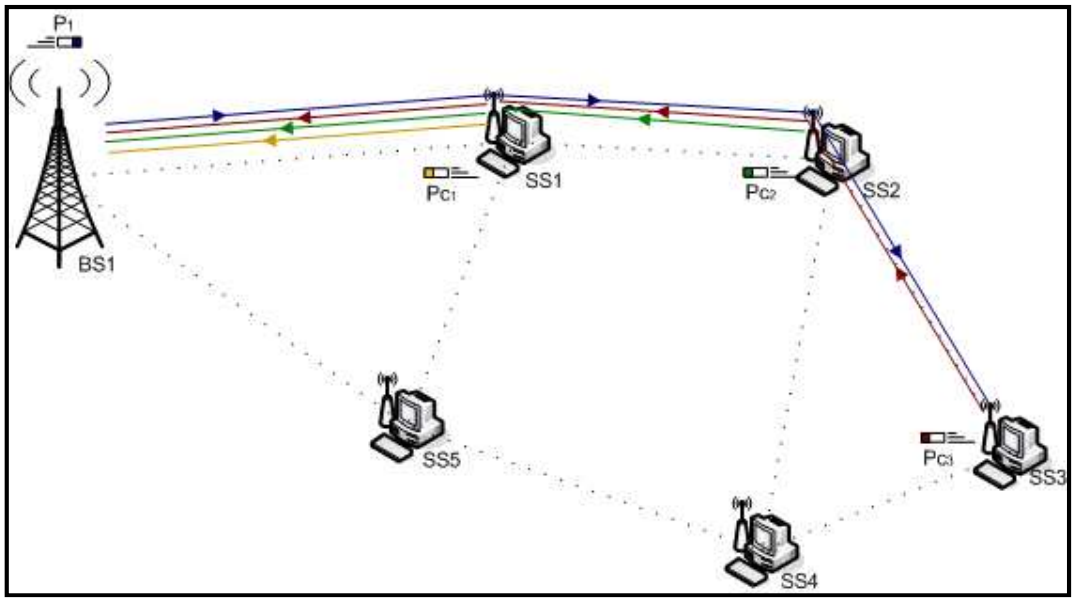


Figura 17: Contabilização de pacotes (*downlink*)

Downlink: A contabilização dos pacotes de *downlink* é feita quando um pacote direcionado a alguma estação da sub-rede cruza a *mesh* BS. Um típico cenário pode ser visualizado na **Figura 17** onde um pacote (*P1*) é enviado a *SS3*.

P1 é encaminhado por *SS1* e *SS2*. Para evitar que as estações intermediárias (neste caso *SS1* ou *SS2*) recebam créditos sem que *SS3* tenha recebido o pacote, *SS3* deve calcular o CVM de *P1* e enviá-lo em uma mensagem de confirmação cifrada (*Pc3*) a *BS1*. *BS1* que previamente fez o mesmo cálculo do CVM, pode assim conferir a integridade do pacote que foi recebido por *SS3*.

Como prova de que encaminharam os pacotes, as estações intermediárias *SS1* e *SS2* devem calcular o CVM de *P1* e enviá-los em uma mensagem de confirmação (*Pc1* e *Pc2* respectivamente) à *BS1*. Quando *BS1* receber os pacotes de confirmação das estações, compara os CVMs com o que previamente calculara e assim, *SS1* e *SS2* recebem os devidos créditos.

Uplink: A contabilização dos pacotes de *uplink* é feita quando um pacote direcionado à internet cruza a *mesh* BS. Um típico cenário pode ser visualizado na **Figura 18** onde um pacote (*P2*) é enviado por *SS3*. Novamente, *BS1* necessita saber que o pacote enviado por *SS3* não foi alterado pelas estações intermediárias. Portanto, após enviar *P2*, *SS3* deve enviar uma mensagem de confirmação cifrada (*Pc5*) contendo o CVM de *P2*. As estações intermediárias (*SS1* e *SS2*) que encaminharem *P2* devem então calcular os respectivos CVMs e enviá-los à *BS1* em pacotes de confirmação (*Pc3 e Pc4* respectivamente). Quando *BS1* receber

os pacotes de confirmação das estações poderá fazer as devidas atribuições de crédito e débitos.

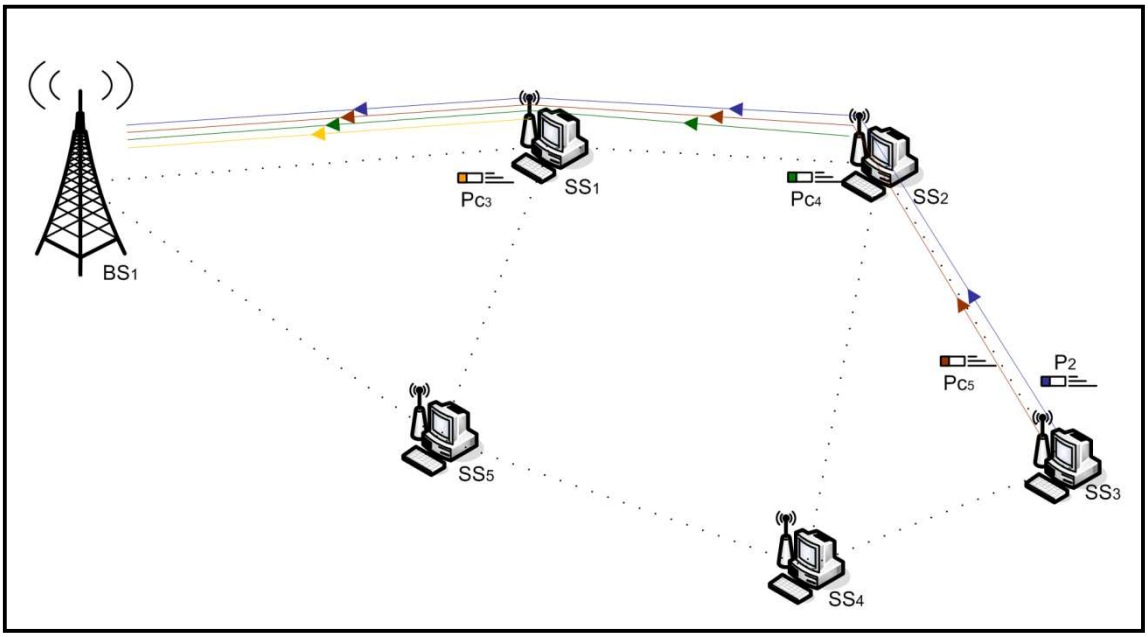


Figura 18: Contabilização de pacotes (*uplink*)

Sessões de tarifação

O mecanismo descrito acima é suficiente para garantir segurança contra as ameaças descritas na **Seção 5.3.3**, porém, a transmissão individual de pacotes de confirmação (*i.e.*, um pacote de confirmação para cada pacote transmitido/recebido) causaria um grande desperdício dos recursos da rede e comprometeria seriamente a escalabilidade da arquitetura. Para suplantar esta limitação, utilizamos o conceito de sessão de tarifação.

Uma sessão de tarifação pode ser vista como um canal estabelecido entre BS/SS, ou SS/BS, por onde trafega um fluxo de dados com determinadas características. Cada sessão possui um identificador único atribuído pela BS. Para identificar a sessão à qual pertencem, os pacotes recebem um *label* contendo o identificador de sua sessão. Este *label* contém também um identificador que permite que os pacotes de uma sessão sejam distinguidos dos demais. As mensagens de confirmação de uma sessão são enviadas em lotes. Ou seja, ao invés de enviar uma mensagem de confirmação para cada pacote que recebe, a estação agrupa as confirmações de vários pacotes e as envia à BS em um único pacote.

As sessões de tarifação são diferenciadas em sessões de *downlink* e *uplink* e podem ser classificadas de acordo com o fluxo de dados nelas transmitido. Apesar de não

serem limitadas a estas, as classes de sessões são as mesmas propostas para o modo PMP (*e.g.*, UGS, rtPS,etc). O uso de diversas classes de sessões permite que o operador de rede tarife ou recompense de forma diferenciada fluxos de dados que possuam maior prioridade. As sessões de tarifação são estabelecidas através de um protocolo que será especificado a seguir. Todas as mensagens usadas na sinalização entre SS e BS, e vice-versa, são enviadas cifradas com uma chave secreta (SKEY) e, portanto, somente os nós correspondentes podem acessar suas informações. O algoritmo proposto para ser utilizado na criptografia das mensagens de sessão é o AES(AES, 2001) com chaves de 128 bits. A SKEY é derivada da chave de autorização da estação (AK). Esta derivação é feita da seguinte forma:

SKEY = Truncate(SHA(PAD|AK), 128)

Onde,

PAD: O valor 0x55 repetido 64 vezes.

Truncate(*x*,*n*): Denota os primeiros *n* bits do valor *x*.

SHA(*y*,*z*): Denota o resultado da aplicação do algoritmo de *hash* SHA-1(SHS, 1995).

Sessão de tarifação de *downlink*

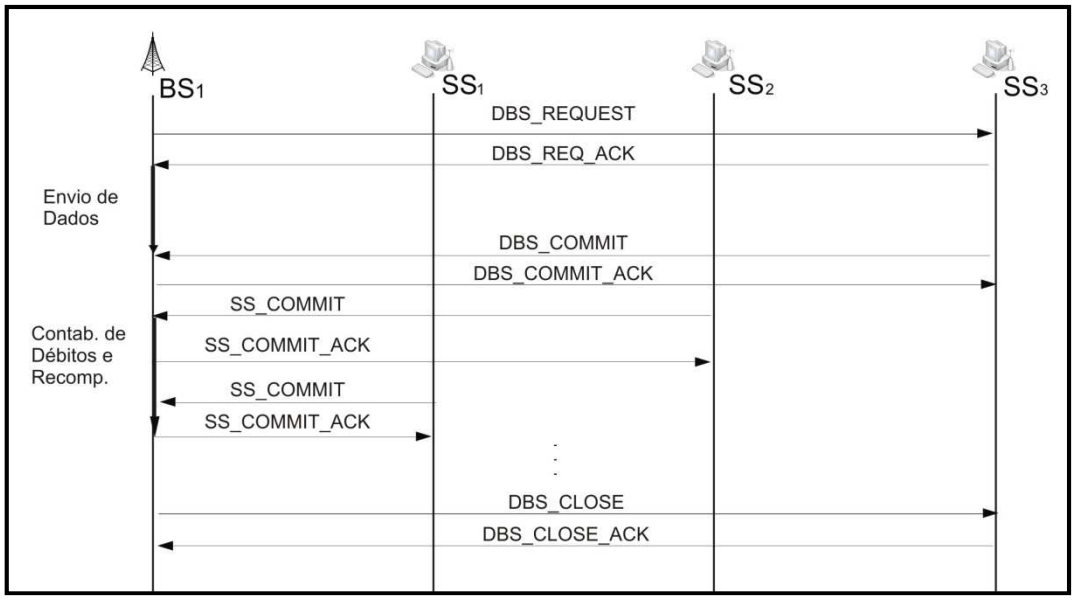


Figura 19: Processo de estabelecimento da sessão de *downlink*

O processo de estabelecimento das sessões de *downlink* é exibido na **Figura 19**. A sessão tarifação de *downlink* é iniciada quando um pacote direcionado a *SS3* chega a *BS1*. Antes de

retransmitir o pacote, a *mesh* BS envia uma mensagem (DBS_REQUEST) a *SS3* indicando que uma sessão de *downlink* será iniciada. A mensagem DBS_REQUEST contém o identificar de sessão que será usado nos *labels* da sessão e também indica a classe da sessão que será criada.

Após receber a confirmação (DBS_REQ_ACK) de *SS3*, a sessão é iniciada. A partir daquele momento, antes de enviar um pacote a *SS3*, *BS1* calcula o CVM do pacote e o armazena juntamente com o identificador do pacote no *buffer* daquela sessão para futuras verificações. Ao pacote é anexado um *label* que contém um número de sequência e um identificador da sessão a qual ele pertence. O pacote modificado é então encaminhado até *SS3*. *SS3* receberá o pacote, fará cálculo do CVM e armazenará este valor juntamente com o número de sequência do pacote no *buffer* daquela sessão. Conforme o número de CVMs do *buffer* for aumentando, *SS3* monta uma mensagem DBS_COMMIT e envia à *BS1*. Após receber o DBS_COMMIT, a BS compara os CVMs contidos na mensagem com os que calculara previamente e, desta forma, sabe quais pacotes enviados foram recebidos corretamente por *SS3*.

Antes de encaminharem o pacote, as estações intermediárias *SS1* e *SS2* devem fazer o cálculo do CVM e armazená-lo juntamente com o identificador contido no *label*. Posteriormente, esta confirmação é enviada à BS como prova de que encaminharam o pacote. As mensagens de confirmação enviadas pelas estações intermediárias são as SS_COMMITs. Conforme for recebendo mensagens das estações intermediárias, *BS1* compara os CVMs recebidos com os que armazenara previamente e assim efetua os devidos débitos e créditos às estações participantes da sessão.

Para obrigar que *SS3* envie as mensagens de confirmação *BS1* bloqueia o envio de pacotes para a estação caso não receba um DBS_COMMIT daquela estação dentro de um limite de tempo. Desta forma, se *SS3* não enviar as mensagens de confirmação deixará de receber pacotes. Caso *BS1* receba as mensagens SS_COMMIT antes da mensagem DBS_COMMIT, *BS1* descarta a mensagem SS_COMMIT não enviando a confirmação (SS_COMMIT_ACK) de que recebeu a mensagem. A estação intermediária irá retransmitir sua mensagem com *backoff* exponencial até que *BS1* receba o pacote de confirmação de *SS3* e confirme o recebimento, ou um limite de tentativas seja atingido.

Sessão de tarifação de *uplink*

O processo de estabelecimento das sessões de *uplink* é exibido na **Figura 20**. A sessão de tarifação de *uplink* ocorre de forma semelhante às sessões de *downlink*. Antes de começar a transmitir, *SS3* envia uma mensagem (UBS_REQUEST) à BS indicando o início da sessão. *BS1* envia uma confirmação (UBS_REQ_ACK) contendo um identificador para aquela sessão. *SS3* deve confirmar o recebimento do identificador (UBS_REQ_ACK_ACK) e então a sessão de *uplink* é iniciada. Durante o envio dos pacotes da sessão, *SS3* deve para cada pacote transmitido, calcular o CVM, anexar um *label* no pacote indicando seu número de sequência e o identificador da sessão. Os CVMs calculados devem ser agrupados em lotes e enviados posteriormente à *mesh* BS em mensagens UBS_COMMIT. *BS1* por sua vez, deve calcular os CVMs dos pacotes que receber de *SS3* e mantê-los uma tabela para que possa verificar posteriormente com os CVMs recebidos nas mensagens UBS_COMMIT. Semelhantemente às sessões de *downlink*, as estações intermediárias também devem fazer o cálculo do CVM enviar à BS em mensagens SS_COMMIT de forma que possam ser recompensadas.

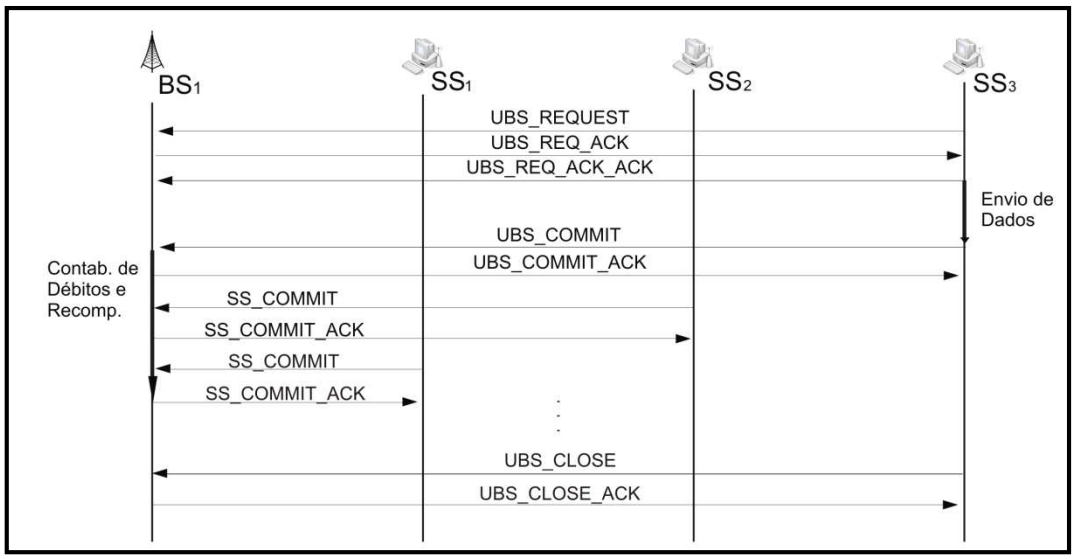


Figura 20: Processo de estabelecimento da sessão de *uplink*

Duração das sessões

Uma sessão estabelecida entre duas estações deve durar enquanto houver transmissão de dados na sessão. Caso não haja tráfego naquela sessão durante um limite de tempo estabelecido, a mesma deve ser finalizada. Este limite é negociado durante o estabelecimento da sessão e pode variar de acordo com o tempo de latência entre a SS e a BS.

Pacotes de confirmação

Os CVMs calculados pelas estações são armazenados temporariamente e em seguida são envidados à BS. Todas as estações possuem um tempo limite para enviar os lotes de confirmação. As estações destinatárias que não enviarem os lotes dentro deste limite terão seu tráfego cortado e as estações intermediárias não receberão créditos pelos pacotes encaminhados. Os lotes de confirmação devem ser montados conforme a especificação da **Tabela** 8 da **Seção 5.4.4**. O número máximo de entradas que um lote pode carregar é limitado pelo tamanho da MTU dos datagramas IP. Para uma MTU de 1500 *bytes* esse valor corresponde a 73 CVMs.

5.4.3. Mecanismo de tarifação

O mecanismo de tarifação proposto deve ser implementado na subcamada de convergência do modelo de referência do padrão IEEE 802.16. De acordo com o padrão, a subcamada de convergência deve efetuar a classificação das PDUs da camada superior, encapsulando cada fluxo de dados em uma determinada conexão. Com o mecanismo de tarifação, além de classificar as PDUs em conexões MAC, a subcamada de convergência deve classificar e agrupar os fluxos de dados em sessões de tarifação. Ela deve também gerenciar a criação de sessões, verificar a autenticidade das mensagens de confirmação e contabilizar o tráfego das estações da sub-rede. A arquitetura da subcamada de convergência com suporte a tarifação é exibida na **Figura 21**. A camada de tarifação é dividida em três principais componentes lógicos:

Classificador de tarifação: O Classificador de Tarifação classifica os pacotes recebidos em sessões. Esta classificação é feita com base nos cabeçalhos dos pacotes (*e.g.*, IP, TCP, UDP, etc.). De acordo com os parâmetros contidos nestes cabeçalhos o classificador verifica em qual sessão o pacote será classificado. Uma vez feita esta verificação, o classificador adiciona ao pacote um *label* contendo o identificador da sessão escolhida. Caso não exista nenhuma sessão já criada, o Gerenciador de Sessões é acionado para estabelecer uma nova sessão e o pacote será enviado após o estabelecimento da nova sessão. O Classificador de Tarifação também é responsável por retirar os *labels* das PDUs enviadas pelas camadas inferiores e entregá-las às camadas superiores.

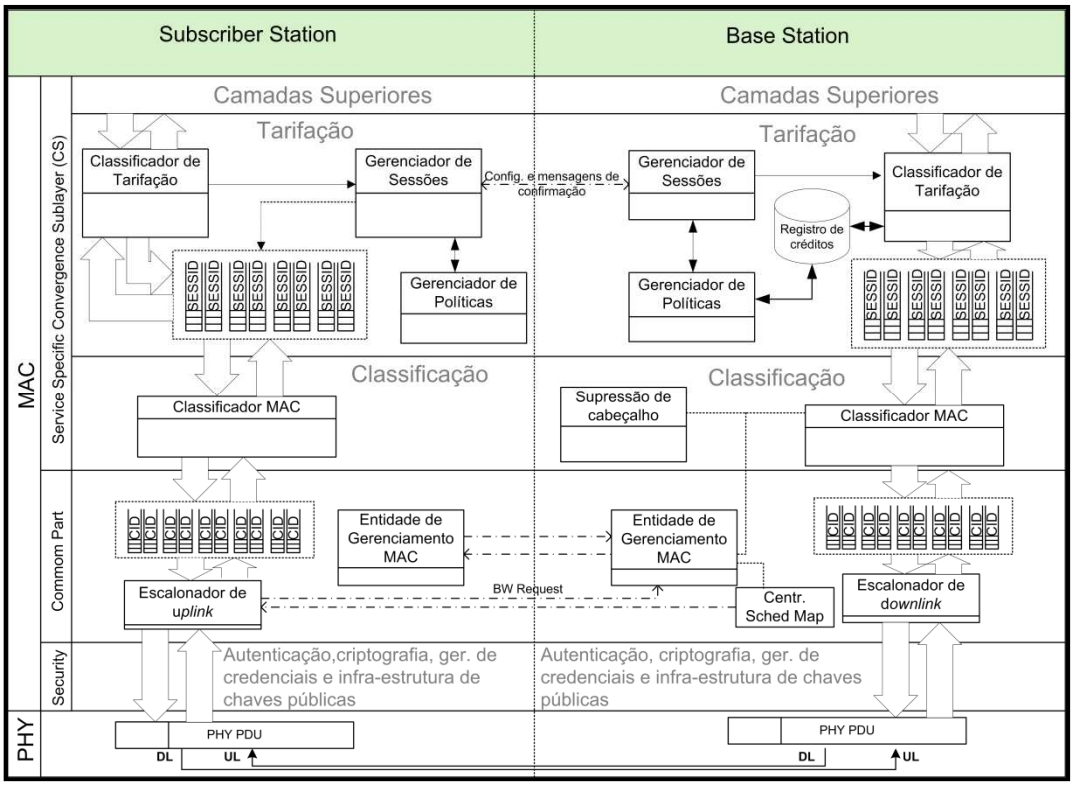


Figura 21: Arquitetura da camada de tarifação

Gerenciador de sessões: O gerenciador de sessões é responsável por enviar, autenticar e verificar as mensagens de sessão da estação. Ele é responsável também pelo processo de criação das sessões. Cada sessão possui um identificador único em toda a sub-rede. Este identificador é atribuído pelo gerenciador de sessões da BS.

Gerenciador de políticas: A criação de sessões deve obedecer a certas políticas que podem ser configuradas pela BS e em cada estação. Por exemplo, a BS pode fazer com que um fluxo de tempo real (rtPS) seja enviado dentro de uma sessão específica e assim possa ser diferenciado pelas SSs que encaminharem estes pacotes. Através do gerenciador de políticas é possível que haja interação entre um protocolo de roteamento que provê QoS e a camada de convergência. Como um exemplo prático de uma configuração deste tipo, o ISP poderia conceder recompensas maiores para sessões que exigissem maior QoS.

5.4.4. Protocolo de comunicação e formato de mensagens

Label

Ao receber um datagrama da camada IP, de acordo com os critérios definidos no Gerenciador de Políticas, um *label* deve ser inserido no pacote. O *label* (**Figura 22**) possui 64 bits e contém os campos exibidos na **Tabela 5**.

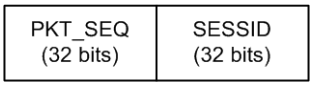


Figura 22: Label de tarifação

Nome	***Tam.(bits)***	***Descrição***
PKT_SEQ	32	Número de sequência do pacote
SESSID	32	Sessão em que o pacote foi classificado.

Tabela 5: Campos do *label* de tarifação

O *label* deve ser adicionado após o sub-cabeçalho *mesh* no quadro MAC do padrão 802.16, conforme indicado na **Figura 23**.

Figura 23: Quadro MAC do 802.16 após inserção do *label* de tarifação

Mensagens de configuração de sessão

As mensagens de configuração de sessão (**Tabela** 7) são utilizadas para realizar o estabelecimento, o fechamento e o envio de mensagens de confirmação (*commits*) entre a BS e as estações. Elas possuem um cabeçalho de tamanho fixo que é seguido de uma carga útil de tamanho variável. Semelhante à forma na qual o padrão especifica o encapsulamento e tunelamento das mensagens iniciais durante o procedimento de entrada de rede, as mensagens de configuração são encapsuladas em datagramas UDP e possuem o formato ilustrado na **Figura 24**.

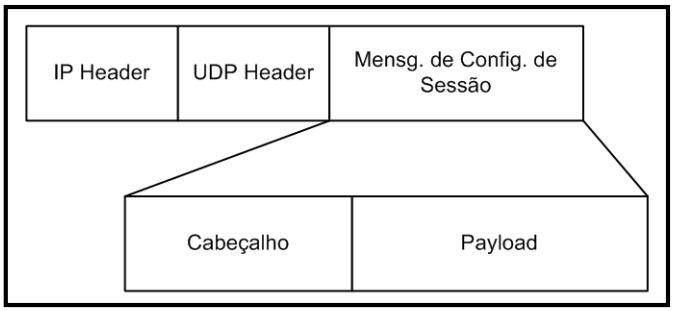


Figura 24: Encapsulamento das mensagens de configuração

O cabeçalho possui tamanho fixo. Seu formato é ilustrado na **Figura 25** e a descrição de cada um de seus campos é dada na **Tabela** 6.

MSG_TYPE (5)	MSG_SIZE (11)	SESSID MSB (16)
SESSID MSB (16)		SRC_NODEID (16)
MSG_CRC MSB(16)		MSG_CRC LSB(16)

Figura 25: Cabeçalho das mensagens de configuração

Nome	*Tam.(bits)*	*Descrição*
MSG_TYPE	5	Código indicando o tipo de mensagem contida na mensagem.
MSG_SIZE	11	Tamanho da mensagem de configuração (Conf. Session Header + Config. Payload).
SESSID	32	Identificador da sessão.
SRC_NODEID	16	Identificador (Node ID) do nó emissor da mensagem.
MSG_CRC	32	Soma de verificação da mensagem.

Tabela 6: Campos do cabeçalho da mensagem de configuração

A carga útil (*payload*) das mensagens possui tamanho variável e campos variam de acordo com o tipo da mensagem. O conjunto de mensagens definidas para o processo de configuração de sessões é dado na **Tabela** 7.

Tipo	*Nome*	*Descrição*
0	DBS_REQUEST	Mensagem de criação de sessão de *downlink*. Enviada pela BS quando possui um novo fluxo de transmissão destinado à SS.
1	DBS_REQ_ACK	Confirmação de recebimento.

2	DBS_COMMIT	Mensagem de confirmação de encaminhamento de pacotes de *downlink*. Deve conter os CVMs dos pacotes recebidos pelas SSs
3	DBS_COMMIT_ACK	Confirmação de recebimento
4	DBS_CLOSE	Mensagem de fechamento de sessão de *downlink*. Enviada pela BS quando esta decide finalizar uma sessão.
5	DBS_CLOSE_ACK	Confirmação de recebimento.
6	UBS_REQUEST	Mensagem de criação de sessão de *uplink*. Enviada pela SS quando esta possui um novo fluxo de transmissão destinado à Internet.
7	UBS_REQ_ACK	Confirmação de recebimento. Enviada pela BS. Deve conter o identificador para a sessão requisitada.
8	UBS_ REQ_ACKACK	Confirmação de recebimento da mensagem #7
9	UBS_COMMIT	Mensagem de confirmação de encaminhamento de pacotes de *uplink*. Deve conter os CVMs dos pacotes enviados pelas SSs.
10	UBS_COMMIT_ACK	Confirmação de recebimento
11	UBS_CLOSE	Mensagem de fechamento de sessão de *uplink*. Enviada pela SS quando esta decide finalizar uma sessão.
12	UBS_CLOSE_ACK	Confirmação de recebimento
	SS_COMMIT	Mensagem enviada pelas estações intermediárias para provar que encaminharam pacotes.
13	SS_COMMIT_ACK	Confirmação de recebimento enviada pela BS.
14-31	reservado	

Tabela 7: Mensagens de configuração de sessão

Os campos das mensagens de configuração são especificados na **Tabela** 8.

Tipo	***Nome***	***Campos***
0	DBS_REQUEST	**REQ_ID** (16 bits): Id gerado pela BS para tornar possível a diferenciação entre requisições enviadas simultaneamente. **SESS_TYPE** (8 bits): Tipo de dados que será trafegado na sessão.
1	DBS_REQ_ACK	**REQ_ID** (16 bits): Id gerado pela BS para tornar possível a diferenciação entre requisições enviadas simultaneamente.
2	DBS_COMMIT	**COMMIT_ID** (16 bits): Identificador do lote de confirmação utilizado para identificar lotes de uma mesma sessão. **NUM_PKTS** (32 bits): Número de pacotes confirmado no lote. for (i=0;i< NUM_PKTS;i++){ **PKT_SEQ** (32 bits): Sequência do pacote contida no *label* inserido pela BS.

		PKT_HASH (128 bits): CVM do pacote. O algoritmo utilizado para calcular o CVM é o MD5 com *digest* de 128 bits. }
3	DBS_COMMIT_ACK	**COMMIT_ID** (16 bits): Identificador recebido na requisição. **NUM_PKTS** (32 bits): Núm. de pacotes contabilizados.
4	DBS_CLOSE	**REQ_ID** (16 bits): Id gerado pela BS para tornar possível a diferenciação entre requisições enviadas simultaneamente.
5	DBS_CLOSE_ACK	**REQ_ID (16 bits):** Req_id recebido
6	UBS_REQUEST	**REQ_ID** (16 bits): Id gerado por cada SS para tornar possível a diferenciação entre requisições enviadas simultaneamente. **SESS_TYPE** (8 bits): Tipo de dados que será trafegado na sessão.
7	UBS_REQ_ACK	**REQ_ID (16 bits):** Req_id recebido
8	UBS_REQ_ACKACK	**REQ_ID (16 bits):** Req_id recebido

9	UBS_COMMIT	**COMMIT_ID** (16 bits): Identificador do lote de confirmação utilizado para identificar lotes de uma mesma sessão.
		NUM_PKTS (32 bits): Número de pacotes confirmado no lote.
		for (i=0;i< NUM_PKTS;i++){
		PKT_SEQ (32 bits): Sequência do pacote contida no *label* inserido pela BS.
		PKT_HASH (128 bits): CVM do pacote. O algoritmo utilizado para calcular o CVM é o MD5 com *digest* de 128 bits.
		}

10	UBS_COMMIT_ACK	**COMMIT_ID** (16 bits): COMMIT_ID recebido na mensagem de *commit* **NUM_PKTS** (32 bits): Núm. de pacotes contabilizados.
11	UBS_CLOSE	**REQ_ID** (16 bits): Id gerado pela BS para tornar possível a diferenciação entre requisições enviadas simultaneamente. **SESSID** (32 bits): Identificador da sessão que será fechada.
12	UBS_CLOSE_ACK	**REQ_ID** (16 bits): REQ_ID recebido na mensagem de *commit*.

	SS_COMMIT	**COMMIT_ID** (16 bits): Identificador do lote de confirmação utilizado para identificar lotes de uma mesma sessão.
		NUM_PKTS (32 bits): Número de pacotes confirmado no lote.
		for (i=0;i< NUM_PKTS;i++){
		PKT_SEQ (32 bits): Sequência do pacote contida no *label* inserido pela BS.
		PKT_HASH (128 bits): CVM do pacote. O algoritmo utilizado para calcular o CVM é o MD5 com *digest* de 128 bits.
		}

13	UBS_CONF_RECV	**COMMIT_ID** (16 bits): Identificador gerado por cada sessão para identificar entre as diversas mensagens de confirmação

		enviadas. **NUM_PKTS** (32 bits): Núm. de pacotes contabilizados.

Tabela 8: Campos presentes nas mensagens de confirmação

5.4.5. Integração e compatibilidade de dispositivos

O protocolo de tarifação é projetado para operar em um domínio de rede onde todos os dispositivos sejam compatíveis com o IEEE 802.16 *mesh* com suporte à tarifação. Todavia, em um ambiente realístico com dispositivos manufaturados por diversos fabricantes, esta premissa pode não ser passível de ser alcançada e, mesmo se no futuro o padrão especificar uma camada de tarifação como parte do padrão, haveria o problema da integração dos sistemas legados. A adição da camada de tarifação não altera a compatibilidade dos dispositivos caso estes estejam operando no modo normal (*i.e.*, sem suporte à tarifação). Apesar de nosso estudo não cuidar de todos os aspectos destes problemas de compatibilidade, daremos aqui algumas possíveis soluções para a resolução deste problema. Para entender o funcionamento da Arquitetura de Tarifação em redes homogêneas considere o cenário heterogêneo exibido na **Figura 26** (as estações incompatíveis estão destacadas das demais). Este cenário não impediria a tarifação, mas comprometeria a distribuição de recompensa aos nós intermediários que fossem incompatíveis, uma vez que para tal eles precisam provar que encaminharam os pacotes. A atribuição de créditos para estações que estivessem encaminhando tráfego entre a BS e uma estação incompatível também não seria possível pois, para isto, ambas as estações correspondentes devem possuir suporte à tarifação.

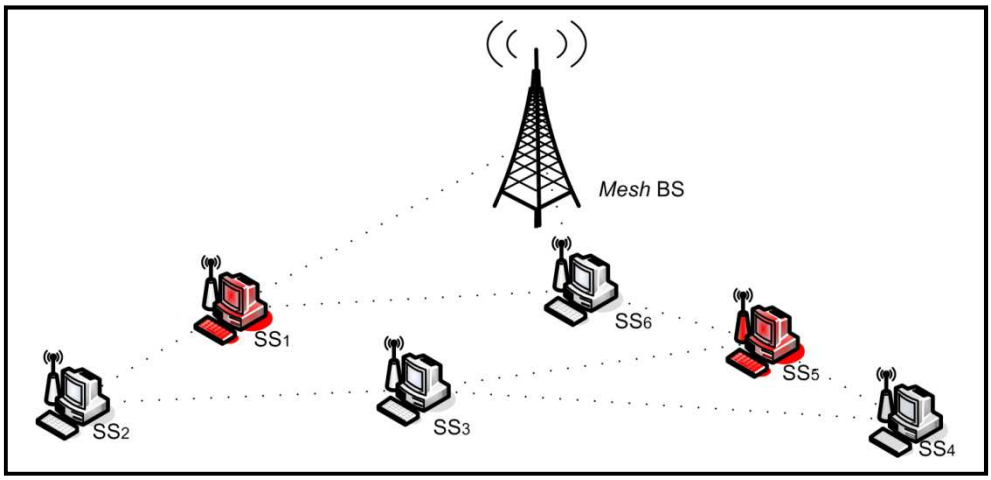


Figura 26: Rede WiMAX com dispositivos sem suporte à tarifação

Neste cenário podemos considerar as situações:

Estação incompatível com link direto (1 hop): Caso a estação cliente que não possua suporte à tarifação esteja ligada à BS através de um *link* direto (e.g *SS1*), as transmissões ocorrem normalmente e a estação é tarifada somente por seu tráfego, pois, para este caso, tanto no *downlink* como no *uplink*, não será necessário que haja qualquer tipo de prova das estações intermediárias.

Estação incompatível a mais de 1 hop da BS: Considere a estação *SS5*. Devido à incompatibilidade da estação, ela não estaria apta para estabelecer sessões de tarifação ou mesmo remover os *label* de tarifação inseridos. Caso haja tráfego para, ou proveniente desta estação, este tráfego deve ser encaminhado pelas estações intermediárias como se fosse tráfego normal. Neste caso, as estações intermediárias que o fizerem não receberão recompensa.

Transmissões através das estações incompatíveis: Suponha que a estação *SS4* deseje enviar dados no canal de *uplink* e a estação *SS5* faça parte da rota. *SS4* deve realizar o processo normal de estabelecimento de sessão. Uma vez que a camada de convergência utiliza os parâmetros dos protocolos (*e.g.*TCP port, IP dest, IP proto, etc.) das camadas superiores, a simples inclusão do *label* causaria erros nas estações incompatíveis. Uma solução para possibilitar o envio de pacotes com *label* sem que houvesse erros nas estações incompatíveis, seria enviá-los por tunelamento da mesma forma que as mensagens de autenticação são enviadas pelas estações ingressantes na rede (**Seção 4.3.2.3**). Assim, caso houvesse alguma estação incompatível na rede, as estações com suporte à tarifação deveriam ser informadas e então poderiam tratar estes pacotes e, ao invés de simplesmente encaminhá-los, efetuariam também o cálculo dos CVMs. O formato das mensagens de tunelamento definidos pelo padrão são exibidos na **Figura 27**.

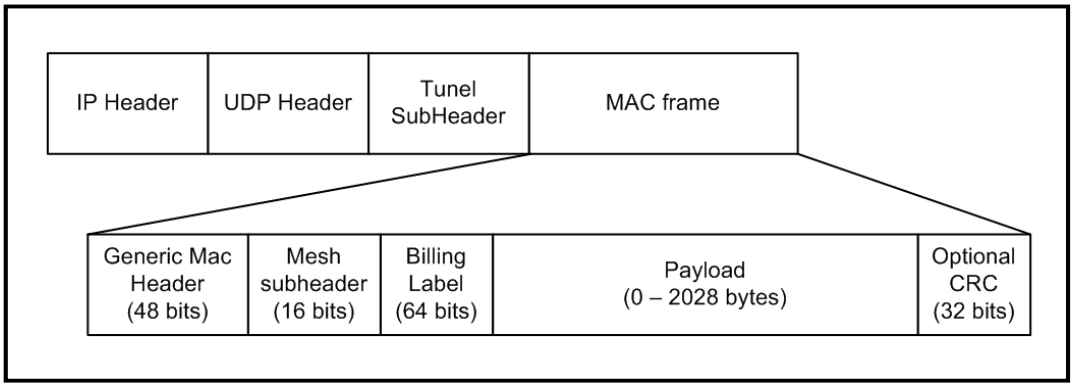


Figura 27: Posicionamento do *label* em redes heterogêneas

5.4.6. Formas de tarifação

Praticamente todos os serviços de acesso à Internet são tarifados de alguma forma. Neste estudo consideramos três esquemas de tarifação para redes *mesh*. Em todos eles, o provedor é responsável por tarifar os serviços aos usuários e recompensar os colaboradores.

Tarifação Baseada em Tempo de Tráfego - No serviço com tarifação baseada em tempo de tráfego, a tarifação ocorre de forma similar à dos serviços de telefonia celular. O usuário paga uma tarifa α *u-monet* (unidades monetárias) para cada unidade de tempo que acessa a rede (*e.g.* R$ 0,06/seg) e recebe β *u-monet* para cada unidade de tempo que gasta encaminhando tráfego dos nós vizinhos. Este serviço se aplica principalmente para fluxo de dados de taxa não variável (*e.g.* UGS).

Tarifação Baseada em Volume de Tráfego - No serviço com tarifação baseada em volume de tráfego, as taxas pagas pelo usuário se referem à quantidade de dados transmitida. O usuário paga uma tarifa digamos γ *u-monet* para cada unidade de tráfego transmitida e recebida (*e.g.* R$ 0,08/MB), recebendo ε *u-monet* para cada unidade de tráfego encaminhada aos vizinhos.

Tarifação Baseada em QoS - Finalmente, no serviço com tarifação baseada em QoS, é concedida ao usuário uma determinada largura de banda, digamos δ MBits e o pagamento pelo serviço é efetuado em intervalos regulares (*e.g.* mensalmente). Uma possível forma de recompensar usuários cadastrados nesta classe de serviço, seria aumentar sua vazão contratada. Ao final de cada um desses intervalos, a largura de banda do usuário poderia ser acrescida de $\tau.\mu$ Mbits, onde τ é uma constante e μ a vazão média do tráfego de terceiros re-encaminhados pelo usuário durante o intervalo em questão. Este tipo de tarifação é a preferida e é a mais utilizada entre usuários que contratam serviços de acesso à Internet(IBRAHIM et al, 2002).

A política de gratificação considera que os usuários devem receber seus bônus de acordo com o esquema de tarifação contratado. Ou seja, as estações que possuírem serviço por fluxo, recebem pela quantidade de fluxo transmitida, as por tempo, pela quantidade de tempo que gastou encaminhando o tráfego de outrem, e as baseadas em QoS recebem uma

quantidade adicional de largura de banda, de acordo com a largura de banda que esta liberou para o tráfego de re-encaminhamento.

Outro importante fator que será ponderado refere-se a quem atribuir os encargos da gratificação dos usuários intermediários. No mecanismo proposto por Zhang e Fang (ZHANG; FANG, 2007), os créditos utilizados pelo provedor para recompensar as estações intermediárias são descontados do próprio usuário, fazendo com que quanto mais *hops* ele esteja da BS, maiores sejam suas taxas de acesso. Na proposta aqui apresentada o ISP é encarregado de fazer a gratificação aos usuários intermediários, visto que estes podem se sentir desencorajados a utilizar o serviço caso o ISP possua taxas variáveis. Assim, independente da distância que esteja do ISP, o usuário sempre pagará a mesma tarifa de acesso.

5.5. Análise de segurança, viabilidade e sobrecargas

5.5.1. Proteção contra ameaças

O protocolo de contabilização resiste às ameaças apresentadas na **Seção 5.3.3** da seguinte maneira:

Proteção contra rejeição de pacotes: No *downlink*, caso uma estação intermediária descarte um pacote, ela não receberá nenhum crédito, visto que o pacote não chegará à estação destino e esta não enviará a confirmação de que recebeu o pacote. A BS somente efetuará a contabilização após receber a confirmação da estação destinatária. No *uplink* isto ocorre de forma semelhante. Desta forma, o descarte de um pacote implica na não contabilização do mesmo.

Proteção contra injeção de pacotes: Se uma estação forjar pacotes e enviá-los, não poderá reclamar créditos por estes, visto que, no *downlink* a BS calcula previamente o *hash* de todos os pacotes que passaram por ela e, no *uplink*, este *hash* é cifrado e enviado separadamente pela estação emissora.

Proteção contra alteração de pacotes: No *downlink*, se alguma estação intermediária alterar ou inserir dados nos pacotes, os códigos de confirmação dos mesmos quando calculados pelo receptor não coincidirão com os que foram calculados pela BS, logo a

contagem daquele pacote desconsiderada. No *uplink*, os *hashs* recebidos pela BS também garantem que nenhuma estação intermediária modifique os pacotes. Isto impede que as estações alterem o conteúdo dos pacotes sem que a BS perceba que houve alteração.

Proteção contra encaminhamento cíclico: Por mais que os pacotes sejam encaminhados em ciclos dentro da sub-rede, eles só serão tarifados e creditados uma vez para cada estação em que passou. Quando recebe um pacote de *commit* de uma estação intermediária, a BS irá creditá-la somente uma vez pelos pacotes referidos no *commit*. Caso receba da mesma estação um *commit* que se refira aos mesmos pacotes, a BS irá desconsiderá-lo.

Proteção contra ataque de repetição: De forma semelhante à proteção contra o encaminhamento cíclico, uma vez que a estação resgate os créditos de um pacote a BS não efetuará nenhuma atribuição posterior caso receba outro *commit* referindo ao mesmo pacote. Desta forma, é impossível que ocorra mais de um resgate por pacote.

Proteção contra superfaturamento de rota: Os usuários da sub-rede podem escolher uma rota maior que a rota ótima para o envio de um pacote. Se fizerem isto, todas as estações que encaminharem o pacote estarão aptas a receber créditos. Esta possibilidade não chega a ser uma fraude, pois, muitos protocolos de roteamento para redes *mesh* fornecem mais de uma rota para um mesmo destino. Se isto ocorrer, o ISP será prejudicado, pois, sempre terá que recompensar um grande número de estações quando poderia recompensar apenas algumas. Para evitar tal situação, utilizamos uma política que limita o valor da recompensa de acordo com a rota mínima para uma estação. Por exemplo, se a menor rota existente possuir 3 nós intermediários e a recompensa por cada byte transmitido for, digamos, β unidades monetárias/Kb, teremos como recompensa máxima 3β por Kb. Caso a rota de envio utilizada possua mais que 3 *hops*, a recompensa máxima será dividida igualmente entre os nós que fizeram o encaminhamento. Como o protocolo de roteamento é comum para todas as estações, espera-se que todas elas tenham condições de saber qual é a rota ótima. Caso a rota ótima não seja escolhida, todas as estações da rota receberam um valor menor de recompensa.

5.5.2. Problemas de segurança no mecanismo de sessões

Apesar de o protocolo apresentado resolver as ameaças de segurança expostos na **Seção 5.3.3**, algumas outras ameaças poderiam ser adicionadas pelo próprio protocolo de tarifação. São elas:

Negação de confirmação: A estação destino pode se negar a enviar os pacotes contendo CVMs de confirmação, tentando evitar que a BS debite pelo fluxo de dados que recebeu.

Forjamento de sessão: Uma estação intermediária pode tentar abrir uma sessão se passando por uma estação de destino que não tenha requisitado aquela sessão. A estação intermediária pode tentar fazer isto forjando mensagens de configuração de sessão e fazendo se passar pela estação destino. Após aberta a sessão, a estação intermediária pode disparar tráfego de algum *host* externo à sub-rede em direção à estação destino, ou mesmo enviar pacotes forjados como se a estação destino os estivesse enviando.

Forjamento de CVMs: Quando uma estação final enviar um pacote de confirmação com os CVMs dos pacotes recebidos por uma rota diferente da dos pacotes de dados, um usuário na estação intermediária pode copiar os CVMs e enviar um pacote de confirmação à BS alegando haver encaminhado aqueles pacotes.

Proteção contra negação de confirmação: Para que a estação destino seja obrigada a enviar as mensagens de confirmação, a BS determina uma quantidade limite de tráfego, digamos α *bytes*, que a estação destino tem direito de receber. Ultrapassada a quantidade α, a BS deixa de transmitir os pacotes para aquela estação até que receba uma mensagem de confirmação pelos pacotes posteriormente enviados. Caso a estação não tenha conseguido enviar as mensagens de confirmação por falhas de transmissão ou perda de *link*, esta deve armazenar os pacotes de confirmação e reenviá-los quando o link for restaurado.

Proteção contra forjamento de sessão: Uma vez que todas as estações da sub-rede possuem credenciais únicas, a estação que estiver entrando na rede deve enviar suas credenciais ao servidor de autenticação. Estas credenciais são enviadas cifradas com a chave pública da BS, evitando que as estações intermediárias possam verificar seu conteúdo. Somente no caso de haver ocorrido o comprometimento das chaves privadas da estação (fato que dificultaria bastante a identificação de quais estações estariam comprometidas) seria possível a uma estação personificar-se como outra e forjar sessões. Este fato, entretanto, foge ao escopo deste trabalho.

Proteção contra forjamento de CVMs: Para evitar que as mensagens de confirmação sejam copiadas por outras estações, estas mensagens são enviadas em pacotes cifrados com a chave secreta da estação.

5.5.3. Mecanismos alternativos

Além do protocolo apresentado (**Seção 5.4**) para contabilização de pacotes, outras soluções e variações foram analisadas. Nesta seção apresentaremos brevemente estas alternativas e mostraremos suas vantagens e desvantagens justificando o porquê de adotarmos a atual solução.

Cadeia de assinaturas

No mecanismo de cadeia de assinaturas, o *label* de cada pacote contém seu CVM. Conforme as estações fizerem o encaminhamento do pacote, elas devem aplicar uma função de criptografia f_C sobre o CVM, de forma que ao chegar ao destino, o *label* do pacote contenha a cadeia de cifras $CAD_{E \to D}$ dos nós daquela rota. No tráfego de *downlink*, a estação destino deve enviar a $CAD_{E \to D}$ à BS em uma mensagem de confirmação. No *uplink* a $CAD_{E \to D}$ estará contida no próprio *label* do pacote.

Esta solução possui a vantagem de reduzir o tráfego de mensagens de confirmação, pois, durante o *downlink*, somente a estação para qual o tráfego é destinado necessita enviar pacotes de confirmação e, durante o *uplink*, não é necessário o envio de pacotes de confirmação uma vez que as confirmações se encontram no próprio *label*.

Apesar de mais eficiente em termos de uso da rede, esta alternativa peca no quesito segurança e, devido à sua forma de funcionamento, não oferece proteção contra ataques de repetição (descrito na **Seção 5.3.3**). Outro ponto fraco nesta alternativa é o fato de que se qualquer uma das estações que participarem da $CAD_{E \to D}$ por algum motivo errar a assinatura, toda a cadeia estará perdida e nenhuma das estações inclusas na $CAD_{E \to D}$ será recompensada.

Sessões estáticas

O estudo realizado por Salem *et al* (SALEM et al, 2003), já mencionado na seção de trabalhos relacionados (**Cap. 5.2)**, utiliza um modelo de contabilização semelhante ao que propomos neste trabalho. O tráfego é dividido em *downlink* e *uplink* e antes de realizar as transmissões, é necessário o estabelecimento de sessões. A principal diferença é que, naquele caso, o mecanismo de sessões está atrelado ao protocolo de roteamento. Na proposta de Salem *et al*, as sessões são estabelecidas com base na rota. Ou seja, todos os nós da rota de transmissão da origem para o destino devem ser notificados da abertura da sessão e devem permitir que esta seja criada. Uma vez estabelecida a sessão, todo o tráfego será roteado através dela. As estações intermediárias não precisam enviar confirmações. Somente a estação destino envia um pacote com o lote de confirmações e todas as estações intermediárias da sessão são recompensadas.

O lado positivo desta solução é que a quantidade de pacotes com mensagens de confirmação é reduzida, pois as estações intermediárias não precisam enviar *commits* provando que participaram da transmissão. Porém, a quantidade de sinalização necessária para o estabelecimento das sessões é maior, uma vez que cada nó deve ser avisado durante a fase de estabelecimento de sessões. Outro ponto negativo desta solução é que em ambientes onde os nós possuam muita mobilidade, o processo de estabelecimento de sessões deverá ocorrer constantemente. Como veremos nas seções a seguir, este processo é a principal causa da perda de desempenho relacionada à adição de um mecanismo de tarifação em uma rede.

Apesar do protocolo que adotamos possuir um pequeno acréscimo na quantidade de mensagens de confirmação que devem ser trocadas em SS e BS, ele torna possível a diferenciação dos diversos tipos de fluxos de dados especificados no padrão IEEE 802.16. Além disso, ele trata satisfatoriamente dos problemas de segurança eliminando a possibilidade de fraudes. Seria interessante se pudéssemos comparar o desempenho da nossa solução com a de Salem *et al*, porém estes autores não apresentam resultados práticos, limitando-se ao escopo teórico de seu protocolo.

Lotes de confirmação

Chamamos de lotes de confirmação as mensagens enviadas com os CVMs. Em nosso protocolo, estes CVMs são adicionados sequencialmente em um pacote. Um problema desta abordagem é a limitação no número máximo de CVMs que pode ser carregado em um datagrama IP. Esta limitação faz com que para cada N pacotes de dados enviados, um lote de confirmação deva ser enviado. Em uma rede onde as estações correspondentes e estações

intermediárias devem enviar confirmações, isto pode ser um limitante à escalabilidade do sistema.

Uma alternativa interessante é o agrupamento dos CVMs. Este agrupamento pode ser feito basicamente de duas formas. Na primeira delas, ao invés de calcular os CVM de cada pacote individualmente, os pacotes seriam agrupados e o cálculo do CVM seria realizado para aquele grupo de pacotes. Outra opção seria calcular os CVMs de *n* pacotes individualmente e mesclá-los em um só CVM. Esta segunda alternativa é descrita com detalhes por Salem *et al*(SALEM et al, 2003). Uma das desvantagens desta alternativa é que o processo para verificar os lotes demanda bastante gasto computacional, o que também traria uma limitação na escalabilidade do sistema.

A única forma de encontrarmos a melhor combinação entre estas alternativas seria a implementação de todos estes métodos e verificação detalhada de cada solução. Esta possibilidade, no entanto, foge ao escopo de nosso trabalho. A alternativa que adotamos pode não ser a alternativa ótima, porém como será demonstrado na seção seguinte, não deixa de ser uma solução viável.

5.6. Metodologia e resultados

5.6.1. Detalhes da implementação

O mecanismo de tarifação aqui proposto foi implementado no simulador NCTUns(NCTUNS, 2009) e testes foram efetuados de forma que pudéssemos analisar as sobrecargas adicionadas. Para tanto, em todos os cenários e testes propostos, foi feita um comparação de desempenho da rede operando com e sem o mecanismo de tarifação.

5.6.1.1. Descrição do simulador

Para facilitar o entendimento das rotinas de testes, daremos uma breve descrição do funcionamento do simulador. O NCTUns é um simulador de eventos discretos[5]. Explicando em linhas gerais, ele é composto por uma fila de eventos, um escalonador e um gerenciador de módulos. Sua arquitetura é modular, permitindo que praticamente qualquer protocolo de rede possa ser simulado. Cada um de seus módulos ou conjunto de módulos simula um protocolo. Estes módulos podem ser agrupados em forma de pilha e assim representar um *host*, *switch*, *hub*, ou qualquer dispositivo de rede. A **Figura 28** traz um exemplo de uma topologia simples representada no simulador. Nesta topologia, duas estações estão conectadas através de um *switch*. Quando o *Host 1* envia um pacote para o *Host 2*, um novo evento é gerado e o pacote é encapsulado neste evento. A simulação possui um tempo simulado onde cada evento é gerado e processado de acordo com o instante (*timestamp*) em que ocorreu. O processamento deste evento consiste no envio do mesmo através da pilha de módulos do nó. O evento é transmitido módulo a módulo e cada um desses módulos manipula o pacote da forma apropriada. Ao chegar ao módulo 'interface' do *Host 2*, o pacote é desencapsulado e entregue à camada de aplicação.

Para coletar os resultados da simulação, o NCTUns oferece diversas rotinas de *log* prontas. Essas rotinas variam de acordo com o módulo utilizado. Através das rotinas de *log* do módulo 802.3, por exemplo, é possível registrar a vazão da rede, taxa de colisão de quadros e também diversos outros parâmetros. Além destes resultados, também é possível coletar dados com as aplicações que são executadas em cada nó. A aplicação utilizada no exemplo da **Figura 28**, o *ping*, retorna a latência entre o Host 1 e Host 2.

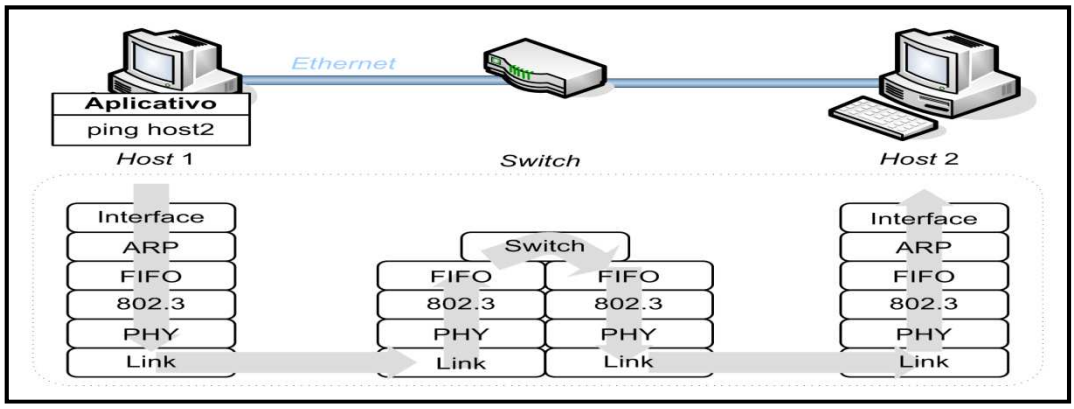


Figura 28: Mecanismo modular do simulador NCTUns

[5] Em um simulador de eventos discretos, os eventos (e.g recebimento ou envio de um pacote, queda de um link de rede, etc.) que ocorrem no sistema são representados como uma sequência de eventos ordenada pelo tempo em que elas ocorreram. O simulador possui um relógio virtual que marca o tempo de simulação. Assim, cada evento é processado de acordo com o tempo virtual que foi gerado.

5.6.1.2. Implementação da camada de tarifação

Para representar a camada de tarifação dois módulos foram implementados: BSConvSublayer e SSConvSublayer. O NCTUns fornece uma API para manipulação de eventos, temporizadores e pacotes. Através desta API, os componentes da camada de tarifação (**Figura 21**) foram modelados em classes na linguagem C++. O **Apêndice B** traz um diagrama de classes resumido das estruturas de dados dos módulos de tarifação e a descrição da execução de uma transmissão de pacotes. Devido à falta de espaço, alguns detalhes das classes foram suprimidos.

Após a implementação dos módulos de tarifação, estes foram adicionados à pilha de protocolo dos nós simulados. A **Figura 29** exibe um cenário onde os nós simulados possuem o módulo de tarifação.

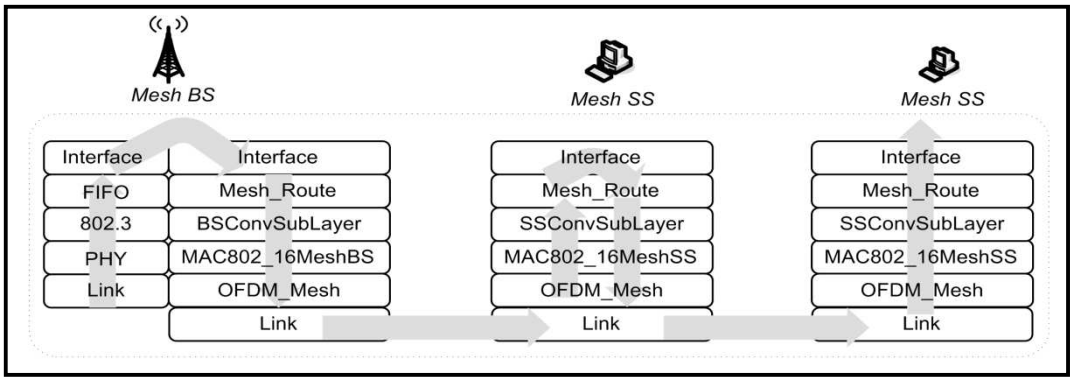


Figura 29: Pilha de módulos dos nós com suporte à tarifação

O **Apêndice A** traz com detalhes o processo de instalação, configuração, e execução dos testes do módulo de tarifação no simulador NCTUns.

5.6.1.3. Fluxo de teste

A precisão das contabilizações realizadas pela BS está entre os principais requisitos para a validação do mecanismo de tarifação. Para verificar esta precisão, as contabilizações de tráfego realizadas na BS foram comparadas aos valores exatos da quantidade de tráfego gerada pelo gerador de tráfego. O gerador de tráfego utilizado foi o Iperf (IPERF, 2009)

Primeiramente, o Iperf foi executado entre dois *hosts* reais. Em um destes *hosts*, o analisador de rede Wireshark(WIRESHARK, 2009) foi utilizado para capturar os pacotes e contar a quantidade exata de *bytes* transmitidos. O valor contado pelo analisador foi de 2097176 *bytes*. Após esta verificação, foi montado um cenário simulado semelhante ao da **Figura 30** e um tráfego TCP de 2097176 *bytes* foi enviado do No1 para SS3 e de SS3 para No1. As contabilizações efetuadas pelo módulo de tarifação da BS foram as seguintes:

BS:

```
user_ssid = 0
sInfo.active_dl_sessions = 1
sInfo.active_ul_sessions = 1
sInfo.bytes_forwarded = 0
sInfo.bytes_received = 2188324
sInfo.bytes_sent = 2162436
```

SS1:

```
user_ssid = 1
sInfo.active_dl_sessions = 0
sInfo.active_ul_sessions = 0
sInfo.bytes_forwarded = 4350760
sInfo.bytes_received = 0
sInfo.bytes_sent = 0
```

SS2:

```
user_ssid = 2
sInfo.active_dl_sessions = 0
sInfo.active_ul_sessions = 0
sInfo.bytes_forwarded = 4350760
sInfo.bytes_received = 0
sInfo.bytes_sent = 0
```

SS3:

```
user_ssid = 3
sInfo.active_dl_sessions = 1
sInfo.active_ul_sessions = 1
sInfo.bytes_forwarded = 0
sInfo.bytes_received = 2162436
sInfo.bytes_sent = 2188324
```

A quantidade total de *bytes* (4350760) encaminhados pelas estações intermediárias que foi registrada pela BS corresponde a um valor (4194352) 3,7% maior do que a que foi enviada pelo analisador de tráfego. Esta diferença deve-se ao fato de o módulo de tarifação contabilizar os pacotes de sinalização como SYN, ACK, etc., enviados pelo protocolo TCP.

5.6.1.4. Cenários de teste

Os testes de desempenho foram executados em 6 cenários diferentes, cada um possuindo um determinado número de nós intermediários, como exibido na **Figura 30**. A distância entre as estações é de aproximadamente 250m. Assim, para o cenário com 2 nós intermediários, temos uma distância de 750m entre a SS e BS. Todas as rotinas foram executadas em cenários com e sem camada de tarifação.

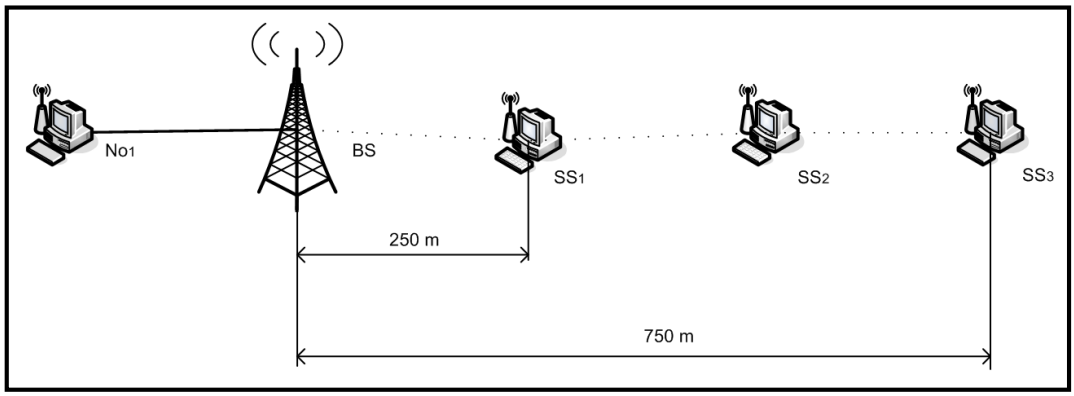


Figura 30: Detalhes dos cenários de simulação

5.6.2. Metodologia e resultados

Os testes foram efetuados de forma que pudéssemos analisar as sobrecargas adicionadas pela inserção do mecanismo de tarifação. Desta forma, em todos os cenários e testes propostos, foi feita uma comparação do desempenho do sistema com e sem o mecanismo de tarifação.

A primeira avaliação realizada foi o teste de vazão. A vazão da rede foi medida com a ferramenta Iperf. Diferente de outros simuladores, (e.g. NS-2) no NCTUns é possível executar aplicações reais dentro do ambiente simulado. Em cada um dos nós correspondentes

foi executado o Iperf e a vazão da rede foi coletada. O teste de vazão foi dividido em 3 rotinas de testes.

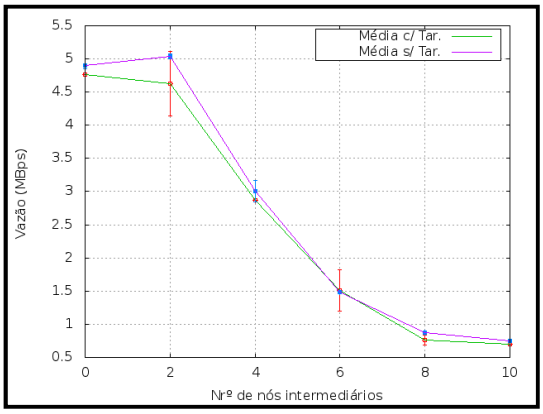


Figura 31: Vazão inicial *uplink*

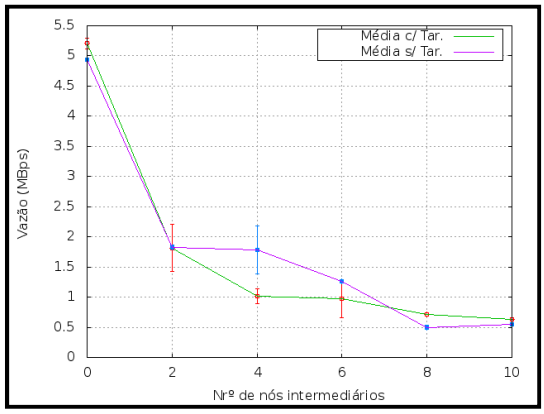


Figura 32: Vazão inicial *downlink*

A primeira rotina visou medir a vazão inicial, ou seja, a vazão do fluxo imediatamente após o estabelecimento das sessões. Para esta rotina foi utilizado um tempo simulado de 150s. Dentro deste tempo de simulação foi disparado um tráfego de 2MB tanto no sentido de *downlink* como *uplink*, coletando-se separadamente a vazão nos dois sentidos. Esta simulação foi executada 3 vezes consecutivas e as médias obtidas para cada cenário são exibidas nas **Figura 31** e **Figura 32**. As barras verticais dos gráficos correspondem ao desvio médio das medidas coletadas.

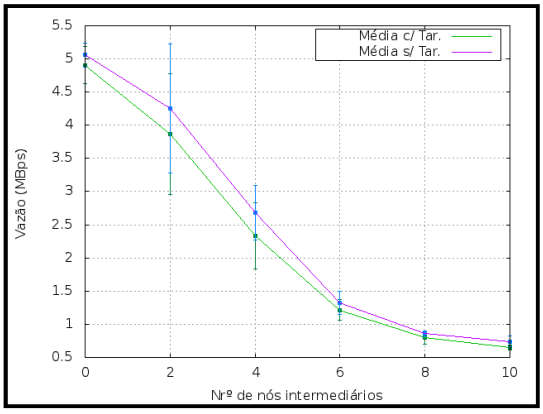


Figura 33: Vazão plena *uplink*

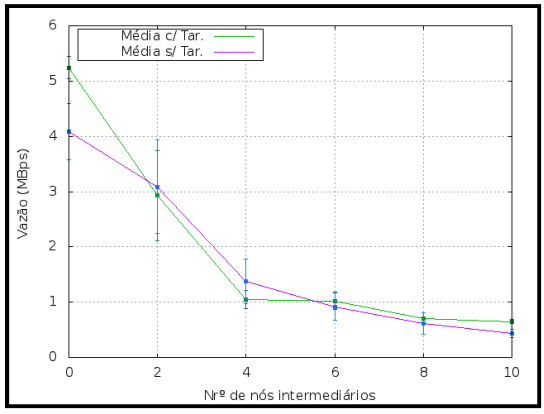


Figura 34: Vazão plena *downlink*

Na segunda rotina foi media a vazão plena, i.e., a vazão do fluxo após o estabelecimento das sessões. Nesta rotina foi utilizado um tempo simulado de 500s. Antes de disparar qualquer tráfego, foram enviados alguns pacotes de '*ping*' para que as sessões fossem estabelecidas. Após o estabelecimento das sessões de *downlink* e *uplink*, foram disparados por

5 vezes sucessivas um tráfego de 2MB, também nos dois sentidos. Cada um destes disparos ocorreu sem sobreposição de transmissão com fluxos anteriores e toda a simulação foi repetida 3 vezes. Os resultados das medidas são exibidos nas **Figura 33** e **Figura 34**, onde os pontos da linha principal do gráfico correspondem às médias dos resultados coletados.

Na terceira rotina, foi medida a vazão global do sistema, i.e., não foi feita nenhuma separação entre *downlink* e *uplink* e fluxo inicial e pleno. O tempo de simulação utilizado foi de 250s e neste período foram disparados 6 fluxos de 2MB, 3 no sentido de *downlink* e 3 no *uplink*. Esta simulação foi repetida 8 vezes e os resultados coletados são exibidos na **Figura 35**. A **Figura 36** trás uma comparação feita com base neste teste. Este gráfico dá ênfase à diferença da vazão global entre os cenários com e sem tarifação. Tomando como exemplo o último ponto (10, 26), temos para o ambiente contendo 10 nós intermediários a proporção (26%) na qual a vazão da rede sem suporte à tarifação sobrepuja a vazão da rede com suporte à tarifação.

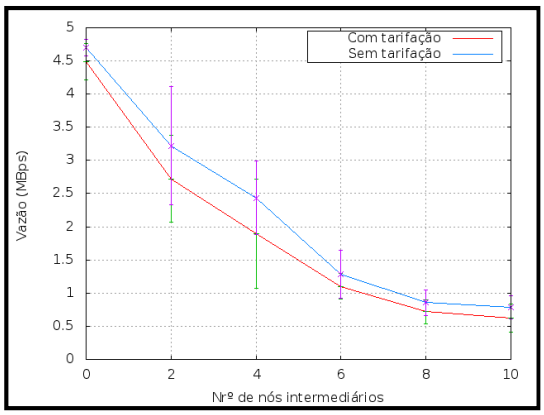


Figura 35: Vazão global média

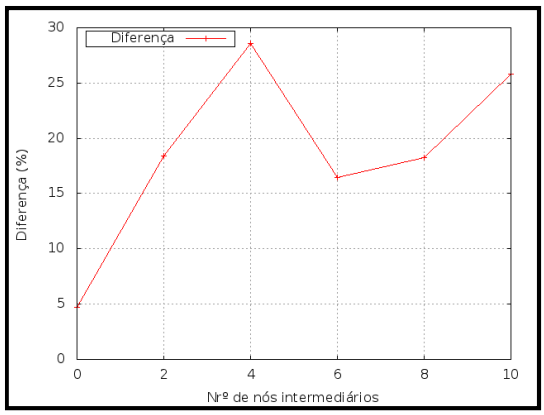


Figura 36: Diferença entre vazões dos sistemas com e sem tarifação

Conforme podemos notar nas **Figuras Figura 31** e **Figura 33**, os valores de vazão para o sistema com suporte à tarifação no *uplink* são ligeiramente menores que nos sistemas sem suporte à tarifação. Este comportamento era esperado uma vez que o mecanismo de tarifação adiciona *overheads* ao sistema. Para os resultados coletados no *downlink* (**Figuras Figura 32** e **Figura 34**) o sistema com tarifação apresenta valores menores em alguns cenários e em outros valores maiores ou iguais ao sistema com tarifação. Este comportamento pode ser explicado pelo algoritmo de geração de números aleatórios utilizado pelo simulador que gera uma margem de erro nas medidas coletadas e mostra que neste caso, a diferença entre os sistemas com e sem suporte à tarifação não são relevantes, pois levando em conta o

desvio padrão das medidas, os resultados ficam dentro da margem esperada. Para a vazão global média (**Figura 35**) também encontramos os resultados esperados e a vazão do sistema com tarifação é menor que a do sistema com tarifação. Como podemos visualizar na **Figura 36**, as diferenças entre as vazões globais dos sistemas com e sem tarifação variam entre 5% e 28%, apresentando uma média de 18%.

Medidas de Latência

A avaliação da latência foi realizada com a ferramenta 'ping' com pacotes de 64 *bytes*. Para obtermos uma medida mais precisa da latência, utilizamos um *script* que envia 50 pacotes de *ping* sucessivos e retorna somente a média dos tempos de resposta. A avaliação de latência também foi dividida em 3 rotinas.

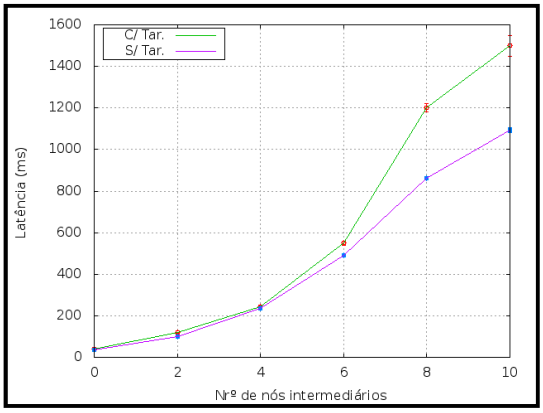


Figura 37: Latência inicial *uplink*

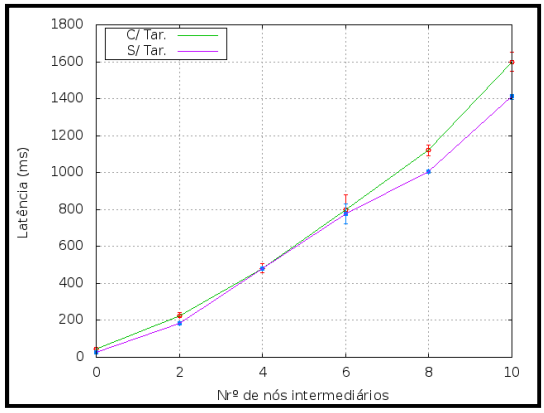


Figura 38: Latência inicial *downlink*

A primeira rotina mediu a latência inicial de *downlink* e *uplink*. Para esta rotina, o tempo de simulação utilizado foi de 100s para *downlink* e 100s para *uplink*. Neste período de simulação foi executado o *script* de *ping* que registrou a latência de envio de pacotes durante a fase inicial do estabelecimento de sessões. As simulações foram repetidas por 3 vezes e as médias obtidas são exibidas nas **Figura 37** e **Figura 38**.

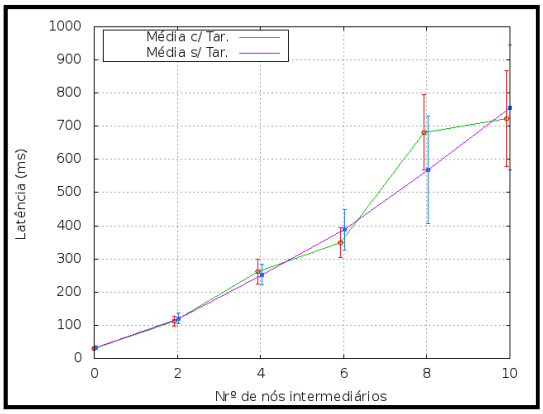


Figura 39: Latência plena *uplink*

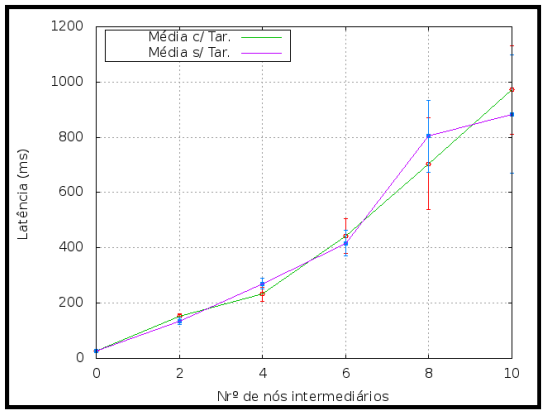


Figura 40: Latência plena *downlink*

A segunda rotina de avaliação da latência mediu a latência plena. Utilizamos um tempo simulado de 400s e dentro deste tempo, executamos o *script* de *ping* por 8 vezes para *downlink* e 8 vezes para *uplink*. Antes de iniciarem-se as medidas, foram disparados pacotes de *ping* para que o tempo de estabelecimento das sessões não fosse contabilizado. Esta simulação foi repetida por 3 vezes e as médias dos dados coletados são exibidas nas **Figura 39** e **Figura 40**.

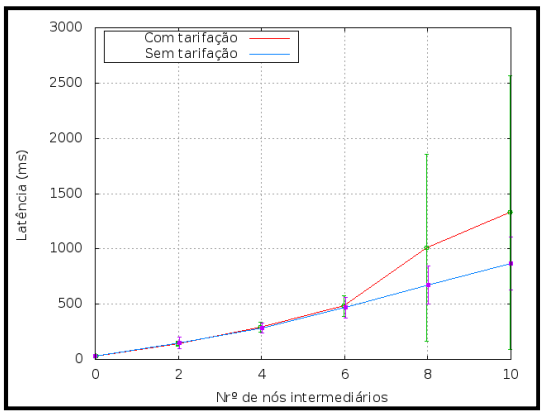


Figura 41: Latência global média

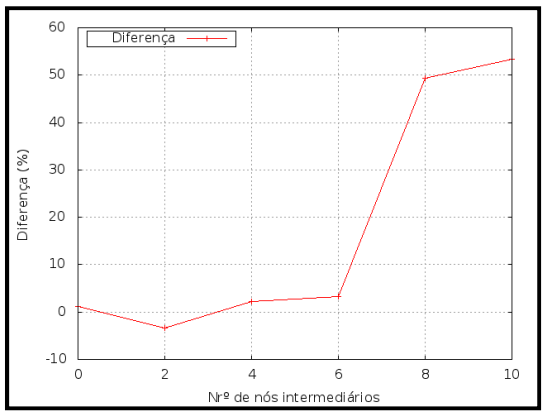


Figura 42: Diferença entre latência dos sistemas com e sem tarifação

Na terceira rotina, foi medida a latência global do sistema, i.e., não foi feita nenhuma separação entre *downlink* e *uplink* e fluxo inicial e pleno. O tempo de simulação utilizado foi de 600s e neste período, o *script* de *ping* foi executado 10 vezes para *downlink* e 10 vezes para *uplink*. Esta simulação foi repetida 3 vezes e os resultados coletados são exibidos na **Figura 41**. A **Figura 42** traz uma comparação feita com base neste teste. Este gráfico dá ênfase à diferença da latência global entre os cenários com e sem tarifação. Tomando como exemplo o ponto (6, 2), temos para o ambiente contendo 6 nós intermediários

a proporção (2%) na qual a latência da rede sem suporte à tarifação sobrepuja a latência da rede com suporte à tarifação.

Ao analisarmos os gráficos das **Figuras Figura 37** e **Figura 38**, podemos ver que a latência inicial nos sistemas com suporte à tarifação é ligeiramente maior, porém, esta diferença se acentua nos cenários com mais de 6 nós intermediários, e devido ao protocolo de estabelecimento de sessões, a latência inicial para o *uplink* é maior que a do *downlink*. Nas medidas de latência plena (**Figura 38 Figura 39**), podemos ver que a diferença entre latência nos sistemas com e sem suporte à tarifação é praticamente inexistente, o que mostra que uma vez estabelecida às sessões não há *overheads* na latência. O gráfico da **Figura 41** confirma os resultados das **Figuras 38** e **39** mostrando que os de latência são bem pequenos quando consideramos cenários com até 6 nós intermediários.

Medidas de fluxo de mensagens

Outra avaliação realizada foi a contabilização da carga de sinalização[6] enviada no sistema de tarifação. Para possibilitar que este parâmetro fosse medido, foi adicionado ao módulo de tarifação uma rotina para contabilizar todos os pacotes de dados enviados, pacotes de sinalização e confirmação e o tamanho destes pacotes. Os dados foram coletados durante a simulação da segunda rotina da avaliação de vazão. Nesta simulação foram enviados aproximadamente 18MB de dados entre o emissor e o correspondente. A **Figura 43** exibe o volume de dados transmitidos (linha superior) e o volume das mensagens de sinalização (linha inferior). O gráfico da **Figura 44** exibe a comparação da proporção de mensagens de sinalização em relação à quantidade de nós. Pode-se ver por estes resultados que a carga de mensagens de sinalização aumenta linearmente com o aumento de nós intermediários.

[6] O tráfego de sinalização corresponde a todas as mensagens (e.g., DBS_COMMIT, UBS_REQ, UBS_COMMIT, etc) geradas pelo protocolo de tarifação.

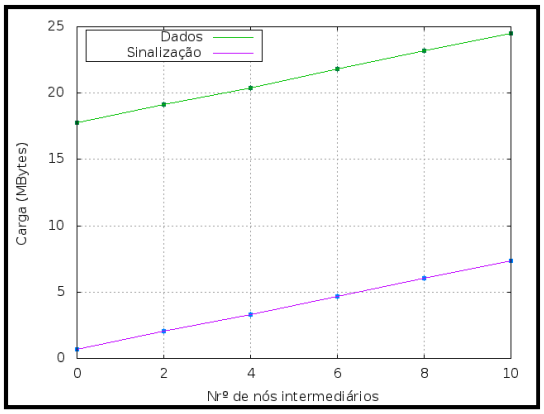


Figura 43: Pacotes de dados e sinalização enviados

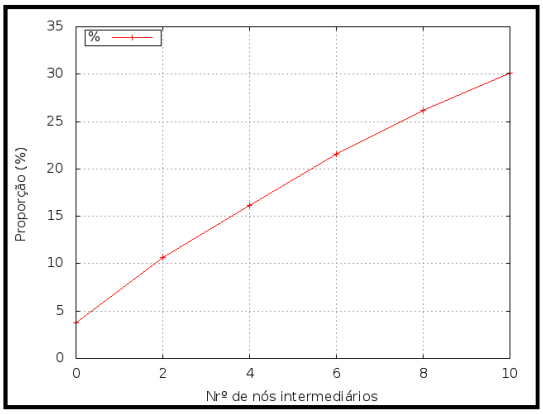


Figura 44: Proporção da carga de dados contra carga de sinalização

6 Conclusões e trabalhos futuros

Este trabalho apresenta uma arquitetura para tarifação em redes WiMAX *mesh*. Esta arquitetura provê um meio de motivar a cooperação em redes *multi-hop* através de recompensas. Para tanto esta arquitetura utiliza os mecanismos de segurança e autenticação especificados pelo padrão IEEE 802.16 e introduz um novo mecanismo para contabilização de pacotes.

Conforme podemos ver através das simulações apresentadas, o mecanismo de tarifação introduz *overheads* (em média 17,6 % para latência e 18 % para vazão), tanto na latência quanto na vazão da rede. Estes *overheads* já eram esperados uma vez que as modificações propostas para o padrão inserem rotinas de criptografia, mecanismos de negociação de sessões, e inserção e remoção de *labels* aos datagramas transmitidos.

Apesar de introduzir estes *overheads*, a arquitetura traz diversos benefícios tanto para o operador de rede quanto para os usuários. A arquitetura possibilita a contabilização em tempo real do tráfego da rede, ou seja, um usuário é tarifado ou recompensado imediatamente após provar que encaminhou determinado pacote ou conjunto de pacotes e desta forma, os CVMs utilizados como prova podem ser liberados economizando espaço de armazenamento. As contabilizações efetuadas pelo mecanismo se mostraram bastante precisas, apresentando um desvio de menos de 4% do valor real do tráfego emitido. Outra peculiaridade de nossa arquitetura é a possibilidade de atribuir diferentes políticas de recompensa para as sessões de tarifação. Em conjunto com um algoritmo de roteamento que ofereça QoS, esta alternativa poderia aumentar a eficácia dos serviços oferecidos, pois, o encaminhamento de pacotes enviados em sessões de maior prioridade (e.g., rtPS) poderia ser mais bem recompensado. Com o uso deste tipo de política as estações intermediárias estariam ainda mais motivadas a encaminhar aqueles pacotes.

Através do mecanismo de sessões de tarifação, podemos assegurar a robustez de nossa arquitetura contra diversos tipos de fraude e garantir que os requisitos de segurança levantados foram atendidos. Diferente de Salem *et al* (SALEM et al, 2003), nosso protocolo de sessões não está atrelado a nenhum algoritmo de roteamento e, portanto, garante maior modularidade à arquitetura.

Por estes e outros benefícios, podemos afirmar que a arquitetura de tarifação proposta é viável, principalmente se limitarmos seu escopo de aplicação ao cenário considerado para o estabelecimento da proposta.

Muitos aspectos ainda podem ser explorados em questões relativas à tarifação. Para trabalhos futuros seria interessante o estudo de meios para se reduzir os *overheads* causados pelo protocolo de sessões, mecanismos que possibilitem mobilidade das estações móveis entre redes de diversos ISPs não confiáveis, análise do consumo de energia nas estações intermediárias, etc. Outra linha de estudo que poderia ser derivada de nosso trabalho, é a implementação desta arquitetura em dispositivos reais, fato que não foi possível, pois até onde conhecemos, nenhum fabricante possui uma implementação da tecnologia WiMAX *mesh*.

7 Referências Bibliográficas

ACHARYA A. et al, *"High-performance architectures for IP-based multihop 802.11 networks"*, IEEE *Wireless* Communications 10 (5) (2003) 22–28.

AES, *"ADVANCED ENCRYPTION STANDARD (AES)"*, Federal Information Processing Standards, Nov. 2001.

AKYILDIZ I. F. et al, *"Wireless Mesh Networks: A Survey"*, Computer Networks (2004) 445–487.

BAATZ S. et al, *"Handoff Support for Mobility with IP over Bluetooth"*, Proceedings of the 25th Annual IEEE Conference on Local Computer Networks, page 143 – 200, Oct. 2000.

BARRY A. et al, *"Overview of Wi-Max IEEE 802.16a/e"*, in: 5th Annual Information Technology and Telecommunications 2005 (IT& T, '05) Cork, Ireland, 2005, pp. 779–784.

BLUETOOTH, *"The Bluetooth Technology Web Site"*, http://www.bluetooth.com disponível em Janeiro de 2008.

CAGALJ M. et al, *"On Cheating in CSMA/CA Ad Hoc Networks"* Technical report No. IC/2004/27, February 2004.

CHEN HB., HSUEH SC., *"Ligth-weigth Authentication and Billing in Mobile Communications"*, IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003.

CLEARY K., "Internet *via MMDS"*, IEEE International Broadcasting Convetion 1997 (IBC '97), Amsterdam, Holland, 1997.

DHCP, *"Dynamic Host Configuration Protocol"*, RFC2131.

DJUKIC P. AND VALAEE S. *"802.16 Mesh Networks"*, December 8, 2006.

EKLUND C. et al, *"IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access"*, IEEE Communications Magazine, June 2000

ETSI HiperACCESS ESP, Broadband Radio Access *Network*s (BRAN); *"HIPERACCESS PHY Protocol Specification"*, April 2002.

ETSI HiperACCESS OVW, Broadband Radio Access *Network*s (BRAN); *"HIPERACCESS System Overview"*, March 2002.

ETSI HiperACCESS REQ, Broadband Radio Access *Network*s (BRAN); *"Requirements and Architecture for Broadband Fixed Radio Access Networks (HIPERACCESS)"*, May 1998.

ETSI HIPERLAN/1, *"ETSI HiperLAN/1, Broadband Radio Access Networks (BRAN);*

'HIPERLAN Type 1' System Overview", February 2002.

ETSI HIPERLAN/2, *"ETSI HiperLAN/2, Broadband Radio Access Networks (BRAN); 'HIPERLAN Type 2'; System Overview"*, February 2002.

ETSI HiperLAN/2, Broadband Radio Access *Network*s (BRAN); *"HIPERLAN Type 2"*; System Overview, February 2002.

ETSI, *"European Telecommunications Standards Institute"*, http://www.etsi.org/ disponível em março de 2009.

FANCHUN et al, *"Routing and packet scheduling in WiMAX mesh networks"*, BROADNETS 2007.

FANG Y. et al, *"SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc" Network*s - WCNC 2004 / IEEE Communications Society.

HONG D., *"2.3 GHz Portable* Internet *(WiBro) for Wireless Broadband Access, ITU-APT Regional Seminar,"* www.
itu.int/ITU-R/study-groups/was/busan/Presentations/docs/itu-apt2004-presentation.pdf, 2004.

IBRAHIM H. A. et al, "*Billing System For Internet Service Provider (ISP)"* IEEE MELECON May 2002.

IEEE 802.11-1999, *"IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*, June 12, 1999.

IEEE 802.11a-1999, *"IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications High Speed Physical Layer in the 5 GHz Band"*, 1999.

IEEE 802.11b-1999, *"IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications High Speed Physical Layer Extension in the 2.4 GHz Band"*, September 16, 1999.

IEEE 802.11e-2005, *"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements"*, IEEE 802.11e-2005.

IEEE 802.11g-2003, *"IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz*

Band”, June 27, 2003.

IEEE 802.11i, *“Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”*, 2005(E) IEEE Std 802.11i-2003

IEEE 802.11n, *“Local and metropolitan area network--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 5: Enhancements for Higher Throughput”*, 2009

IEEE 802.11s, *“Status of Project IEEE 802.11s”*, http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm, disponível em abril de 2009.

IEEE 802.15 TG,*“IEEE 802.15 Standard Group Web Site”*, http://www.ieee802.org/15/>, disponível em Janeiro de 2008.

IEEE 802.15.3, *“Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)”*, IEEE 802.15.3-2003.

IEEE 802.15.4, *“Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”*, IEEE 802.15.4-2006.

IEEE 802.15.5, *“IEEE 802.15.5 WPAN Task Group”*, http://ieee802.org/15/pub/TG5.html, disponível em maio de 2008.

IEEE 802.16, *“IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems”*, Oct. 2004.

IEEE 802.20, *“IEEE 802.20 Mobile Broadband Wireless Access (MBWA)”, http://grouper.ieee.org/groups/802/20/*, disponível em 2009.

IEEE 802.22 WG, *“IEEE 802 LAN/MAN Standards Committee 802.22 WG on WRANs (Wireless Regional Area Networks)”*, http://www.ieee802.org/22/ disponível em março de 2009.

IEEE DRAFT STANDART 802.16/D4-2001, *“Local and Metropolitan Area Networks-Part 16: Standard Air Interface for Fixed Broadband Wireless Access”*, 2001.

IEEE DRAFT STANDART 802.16A, *“Local and Metropolitan Area Networks-Part 16: Standard Air Interface for Fixed Broadband Wireless Access Mesh Networking Extensions”*, 2003.

IEEE STANDARD 802.16-2004-16, *“Part 16: Air Interface for Fixed and Mobile*

Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1”, IEEE Std 802.16e, February 2006.

INFRARED, *“Infrared Data Assossiation”*, http://www.irda.org/ disponível em Janeiro de 2008.

INTEL, *“Understanding Wi-Fi and Wi-Max as Metro-Access Solutions”*, Intel Corporation, 2004.

IPERF, “*Iperf*” , http://www.noc.ucf.edu/Tools/Iperf/, disponível em março de 2009.

IPo802.16, “*IP over IEEE 802.16 Networks (16ng)*”, http://www.ietf.org/html.charters/16ng-charter.html disponível em abril de 2009.

JAKOBSSON M. et al, *"A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks"*. In Proceedings of Financial Cryptography, 2003.

JIN F. et al, A. Arora, J. Hwang, and H.-A. Choi, *“Routing and Packet Scheduling for Throughput Maximization in IEEE 802.16 Mesh Networks,”* submitted for publication, 2008.

KURAN M. S., TUGCU T., *“A survey on emerging broadband wireless access technologies”*, Comput. Netw. (2007).

MIWI,*“MiWi Wireless Networking Protocol Stack, describing the Microchip MiWi stack”*, http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1824&appnote=en520606, disponível em março de 2009.

NCTUNS, *“NCTUns Network Simulator and Emulator*”, http://nsl.csie.nctu.edu.tw/nctuns.html, disponível em ferevereiro de 2009.

RAMANATHAN et al, *“A Brief Overview of Ad Hoc Networks:*

Challenges and Directions”, IEEE Communications Magazine, Maio 2002.

RICHARD J. EDELL et al “*Billing Users and Pricing for TCP*”, IEEE Journal on Selected Areas in Communications, Vol. 13 No. 7 – Sep. 1995.

SALEM N. B. et al, *“A Charging and Rewarding Scheme for Packet Forwarding in Multihop Cellular Networks”*, MobiHoc’03, June 1–3, 2003, Annapolis, Maryland, USA.

SHETIYA H. AND SHARMA V., *“Algorithms for Routing and Centralized Scheduling to Provide QoS in IEEE 802.16 Mesh Networks”* in WMuNeP ’05: Proceedings of the 1st ACM workshop on Wireless Multimedia Networking and Performance Modeling, New York, NY, USA, 2005, pp. 140-149, ACM Press.

SHS, *“SECURE HASH STANDARD”*, Federal Information Processing Standards Publication, April 1995

TANENBAUM A. S., *"Redes de Computadores"*, Quata Edição, Prentice Hall, 2003.

TAO J. et al, *"Throughput Enhancement in WiMax Mesh Networks Using Concurrent Transmission,"* in International Conference on Wireless Communications, Networking and Mobile Computing, Sep 2005, pp. 871-874.

TEWARI H., O'MAHONY D., *"Real-Time Payments for Mobile IP"*, IEEE Magazine - February 2003.

TIME PROTOCOL, *"Time Protocol - 1983"*, RFC868.

VAUGHAN-NICHOLS S. J., *"Achieving Wireless Broadband with WiMAX" IEEE Comp.*, vol. 37, issue 6, June 2004, pp. 10–13.

WEI H. et al, *"Interference-Aware IEEE 802.16 WiMax Mesh Networks,"* in Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st, Vol. 5; 3102-3106.

WHART, *"HART Communication Protocol"*, http://www.hartcomm2.org/hart_protocol/wireless_hart/wireless_hart_main.html, disponível em março de 2009.

WIMAX BILLING, *"Arquivos fonte do projeto WiMAX Billing"*, http://www2.dc.ufscar.br/~erlon_cruz/files/wimax.tar.bz2

WIMEDIA,*"The WiMedia Alliance"* ,http://www.wimedia.org/, disponível em 03/2009

WIRESHARK, *"Wireshark Analisador de Tráfego"* , http://www.wireshark.org/, disponível em abril de 2009.

X509, *"Internet X.509 Public Key Infrastructure - 2002"*, RFC-3280.

YI LI et al, *"Effects of Interference on Wireless Mesh Networks: Pathologies and a Preliminary Solution"*, HotNets-VI Nov. 2007.

YOON S.Y., *"WiBro Technology"*, Samsung Electronics Co, Ltd. Technical Report Sep. www.itu.int/ITU-D/imt-2000/documents/Busan/Session3_Yoon.pdf, 2004.

ZHANG Y. E FANG Y., *"A secure authentication and billing architecture for wireless mesh networks"*. Wireless Networks (2007).

ZHANG Y. et al, *"Security in Wireless Mesh Networks"*, Auerbach Publications 2009.

ZHOU J., LAM KY, *"Undeniable Billing in Mobile Communications"*, Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking pg. 284-290 1998.

ZIGBEE, *"ZigBee Alliance Homepage"*, http://www.zigbee.org/ disponível em março de 2009.

ZOU F. et al, *"IEEE 802.20 based broadband digital network – the infrastructure for m-*

commerce on the train”, in: The 4th International Conference on Electronic Commerce (ICEB ’04), 2004, pp. 771–776.

Apêndice A – Instalação Ambiente de Testes

Passo 1 – Instalação do sistema operacional

A instalação do ambiente de testes se inicia com a instalação do sistema operacional onde o simulador será instalado. Parte do mecanismo do NCTUns depende de algumas modificações realizadas no *kernel* do Linux. Estas modificações, bem como o restante dos pacotes de instalação só possuem suporte para o sistema operacional Fedora Linux. A versão do simulador utilizada é a NCTUns 4.0. Seguindo as recomendações dos desenvolvedores, o sistema operacional que foi instalado é o Fedora 8.

Passo 2 – *Download* e instalação do simulador

O pacote de instalação do simulador deve ser baixado no site (NCTUNS) dos desenvolvedores. Seguindo as instruções contidas no tutorial contido no próprio pacote, o simulador deve ser compilado e o sistema cuidadosamente e configurado conforme as instruções.

Passo 3 – Adição do módulo WiMAX modificado

O módulo WiMAX modificado com suporte à tarifação bem como os cenários e as rotinas de teste podem ser encontrado no endereço (WIMAX BILLING). O primeiro passo após o download dos arquivos do projeto é a substituição da pasta ‘NCTUns-4.0/src/nctuns/module/wimax/’ pela pasta ‘wimax’ do projeto. A seguir as seguintes alterações devem ser feitas nos arquivos de código:

NCTUns-4.0/src/nctuns/nctuns.cc

```
92a93,94
>       REG_MODULE("myFIFO", myfifo);
>
182a185,187
>       REG_MODULE("BSBillingSublayer",BSConvergenceSublayer);
>       REG_MODULE("SSBillingSublayer",SSConvergenceSublayer);
>
```

NCTUns-4.0/src/nctuns/nctuns_api.h

```
< #define IPC          1
---
> #define IPC          0
```

NCTUns-4.0/src/nctuns/Makefile

```
142c142
<               -include autoconf.h
---
>               -include autoconf.h -I./module/wimax
220c220
< nctuns_flags  += -ltcl8.4 $(call cc-library,tcl8.4,$(srctree)/tcl)
---
> nctuns_flags  += -ltcl8.4 $(call cc-library,tcl8.4,$(srctree)/tcl) -lssl -lcrypto
```

Para compilar o simulador com suporte a tarifação comente a diretiva ‘BYPASS’ no arquivo ‘NCTUns-4.0/src/nctuns/module/wimax/debug_aux.h’ e execute os seguintes comandos:

```
$cd NCTUns-4.0/src/nctuns/
$make
$mv nctuns nctuns.billing
```

Após compilado o simulador com suporte à tarifação desabilite a camada de tarifação descomentando a diretiva ‘BYPASS’ do arquivo ‘debug_aux.h’. Repita o processo de compilação:

```
$cd NCTUns-4.0/src/nctuns/
$make
$mv nctuns nctuns.bypass
```

Passo 4 – Execução dos cenários

Os cenários de testes podem ser construídos na interface gráfica. Lembramos, portanto, que caso isso seja feito, a camada de tarifação deve ser instalada na interface gráfica de acordo com as instruções contidas no manual do desenvolvedor do pacote NCTUns. O leitor pode optar por executar alguns de nossos cenários que já se encontram configurados. Estes cenários se encontram no diretório ‘cenários’ da pasta do projeto. Os cenários estão organizados/nomeados da seguinte forma: *x*T*y* e *x*L*y*, onde *x* corresponde à quantidade de nós intermediários do cenário, *y* corresponde ao identificador do teste, e T e L ao tipo de teste que pode ser vazão ou latência respectivamente. As rotinas de execução destes cenários se encontram na pasta ‘tools’ do pacote do projeto.

Apêndice B – Diagramas de Classe do Módulo de Simulação

A **Figura 45** traz o diagrama de classes simplificado da implementação da camada de tarifação no simulador.

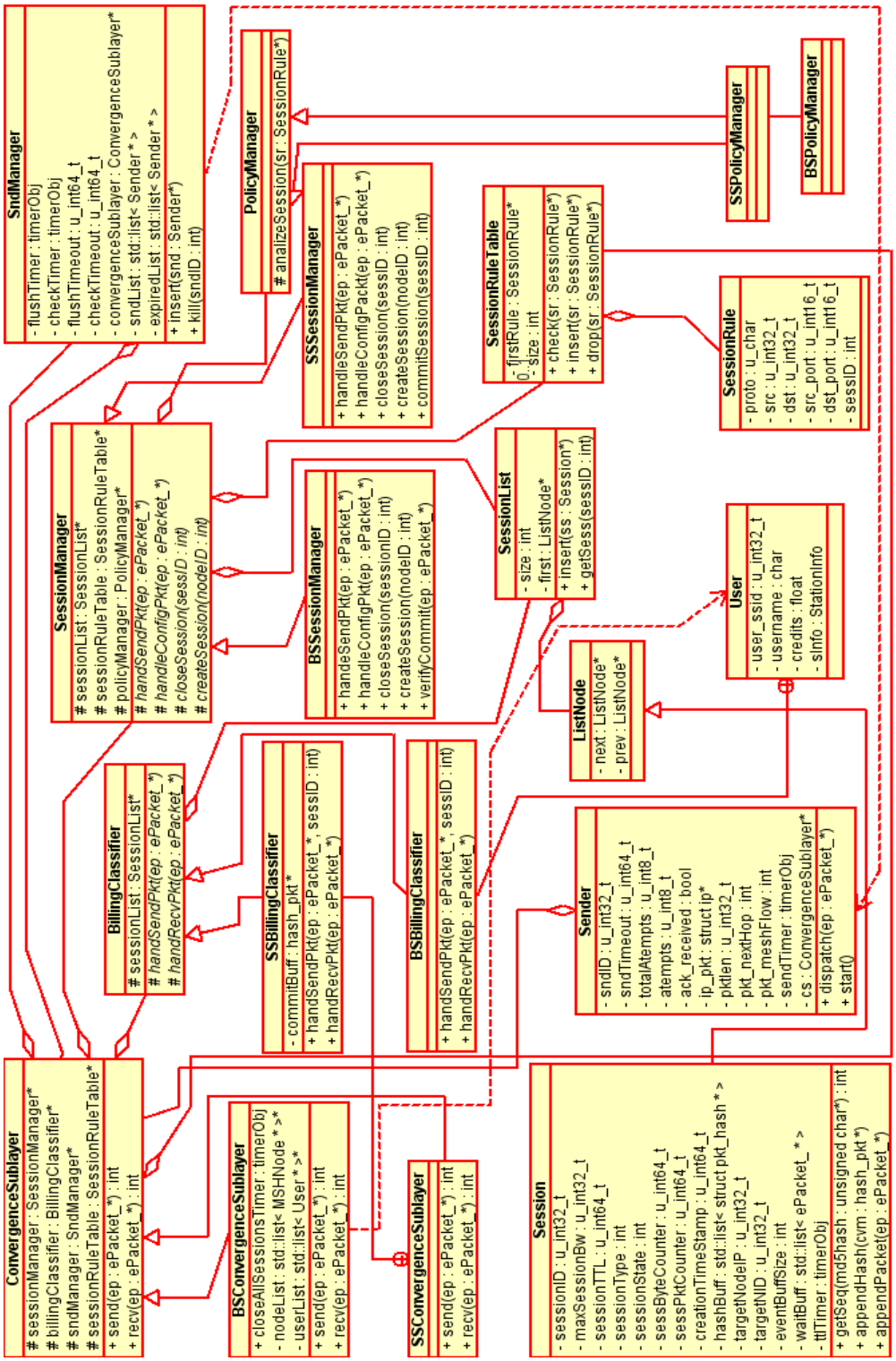


Figura 45: Diagrama de classe simplificado

A **Tabela 9** traz a legenda com os significados das relações entre as classes do diagrama.

	-	Agregação
	-	Associação direcional
	-	Composição
	-	Dependência
	-	Implementa (Generalização/Realização)
	-	Inclusão

Tabela 9: Legenda do Diagrama de classe

Sequência de execução

Descreveremos aqui um exemplo de execução de um cenário. Considere o cenário da **Figura 30** e um tráfego que corresponde a 100 pacotes ICMP (*ping*) enviados de No1 para SS3. A execução do módulo de tarifação se inicia quando um evento[7] é passado através do método *send()* da classe BSConvSublayer. O pacote é encaminhado para o método *handSendPkt()* da classe BSSessionManager. Esta função irá verificar se existe uma sessão com as mesmas regras que o pacote (nesta implementação utilizamos somente o endereço de destino como parâmetro). Como o pacote é o primeiro da série, uma nova sessão será criada. Ainda no método *handSendPkt()*, um objeto da classe Session é instanciado e uma mensagem UBS_REQUEST será enviada para SS3. O campo sessionState do objeto Session recém criado, recebe o valor SESS_NOT_READY indicando que ainda não foi recebido o ACK de SS3. Para enviar a mensagem UBS_REQUEST, a estação instancia um novo evento através da chamada *createEvent()* da API do NCTUns. Esta mensagem UBS_REQUEST é encapsulada no evento passada para o método *send()* da classe pai ConvSublayer. O método *send()* desta classe efetua funções de *log*, contando quantos pacotes e quais tipos são enviados

[7] Lembre-se que todos os pacotes são encapsulados em eventos. Portanto quando falarmos pacote ou evento nos referimos a mesma coisa.

e também faz a criptografia das mensagens de sessão enviadas. Todos os pacotes enviados pelas estações cruzam este método. Após cifrar a mensagem, o evento é enviado para o próximo módulo da pilha, neste caso o módulo MAC802_16meshBS. O evento será enviado por todos os módulos sequêncialmente (incluindo todos os módulos dos dois nós intermediários SS1 e SS2) até que chegue ao método *recv()* do módulo/classe SSConvSublayer do nó SS3. Este método irá decifrar a mensagem e enviá-la para o SSSessionManager através do método *handleConfigPkt()*. Todas os pacotes de configuração recebidos são encaminhados para este método que selecionará a ação a ser tomada de acordo com o tipo de mensagem recebida. Neste caso, como a mensagem que foi recebida é do tipo UBS_REQUEST, será instanciado um objeto Session e enviada uma mensagem de ACK para a BS. Quando a BS receber o ACK, mudará o estado da sessão para SESSION_ACTIVE e o método *handSendPkt()* que disparou todo este processo irá retornar o 'id' da sessão recém criada para a classe BSConvSublayer que irá inserir o 'id' na sessionList de seu SessionManager. Criada a sessão nos dois nós correspondentes (BS1 e SS3), o pacote é passado juntamente com o 'id' da sessão para o método *handSendPkt()* da classe BSBillingSublayer. Este método irá calcular o CVM dos dados do pacote através da função *md5sum()*. O *CVM* será armazenado na estrutura hashBuff do objeto de sessão instanciado na BS1. O armazenamento dos CVMs tanto na BS como nas SSs é feito em listas encadeadas da biblioteca padrão do C++. Este armazenamento não foi otimizado para simplificar a implementação. O *label* é então adicionado ao pacote e enviado adiante através da pilha de protocolos. Os nós intermediários que receberem este pacote irão tratá-los com os métodos *handRecvPkt()*. Neste método, é realizado o *CVM* do pacote, armazenado em uma lista tipo hashBuff e encaminhado pela pilha de protocolos. A classe SSConvSublayer da estação SS3 irá receber o pacote, calcular o *CVM* e armazená-lo no *buffer* hashBuff da sessão instanciada para aquele fluxo.

Para próximos 72 pacotes do fluxo de dados, as classes das estações irão efetuar um processo semelhante ao que foi descrito para o primeiro pacote, com exceção da criação da sessão que ocorre somente para o primeiro pacote da regra. A BS e as SS armazenarão os CVM no buffer do objeto sessão instanciado e as SSs intermediárias em um buffer do tipo hashBuff.

Quando o hashBuff atinge o a quantidade de 73 CVMs, SS3 irá montar uma mensagem DBS_COMMIT e enviar à BS. Os 28 CVMs restantes nas SSs serão enviados quando o temporizador ttlTimer do objeto sessão for zerado. As estações intermediárias irão fazer o mesmo, porém, a mensagem será do tipo SS_COMMIT. Este processo é executado

pela função *commitSession()* da classe SSSessionManager. Na BS, ao receber o pacote DBS_COMMIT, será feita uma comparação dos CVMs contidos na mensagem com os CVMs armazenados no objeto Session daquela sessão. Os CVMs que não coincidirem serão descartados da BS. Durante um período de tempo, a BS irá manter os CVMs no buffer. Neste período de tempo deve receber as mensagens SS_COMMIT enviadas pelas estações, conferir os CVMs contidos e atribuir os créditos e incrementar os contadores dos objetos User da BS.