RODRIGO FILEV MAIA

UMA ARQUITETURA DE CONTROLE DE QUALIDADE DE SERVIÇO APLICADA A REDES HETEROGÊNEAS E SERVIÇOS CONVERGENTES

São Paulo

2010

RODRIGO FILEV MAIA

UMA ARQUITETURA DE CONTROLE DE QUALIDADE DE SERVIÇO APLICADA A REDES HETEROGÊNEAS E SERVIÇOS CONVERGENTES

Tese apresentada à Escola Politécnica da Universidade de São Paulo como requisito para obtenção do título de Doutor em Engenharia Elétrica.

São Paulo

2010

RODRIGO FILEV MAIA

UMA ARQUITETURA DE CONTROLE DE QUALIDADE DE SERVIÇO APLICADA A REDES HETEROGÊNEAS E SERVIÇOS CONVERGENTES

Tese apresentada à Escola Politécnica da Universidade de São Paulo como requisito para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração:

Engenharia da Computação e Sistemas Digitais

Orientador: Professor Titular Moacyr Martucci Junior

São Paulo

2010

FICHA CATALOGRÁFICA

Maia, Rodrigo Filev
Uma arquitetura de controle de qualidade de serviço aplicada
a redes heterogêneas e serviços convergentes / R.F. Maia. -- São Paulo, 2010.
157 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Serviços (Qualidade) 2. Agentes inteligentes 3. Arquitetura de software 4. Multimídia interativa I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computa - cão e Sistemas Digitais II. t.

A minha fabulosa Esposa Denise, aos
maravilhosos Filhos Ana Luísa e Eduardo
e aos meus Pais Marco e Cida

AGRADECIMENTOS

Agradeço a Escola Politécnica por acolher este trabalho e ao Professor Titular Moacyr Martucci Jr. pelo tempo de orientação e pelas oportunidades de discussão que aprimoraram o trabalho apresentado e a pessoa que o fez.

Agradeço ao Departamento de Computação e Sistemas Digitais chefiado pelos Professores Titulares Antonio Marcos de Aguirra Massola e Selma Shin Shimizu Melnikoff pelo apoio tanto acadêmico quanto material que muito auxiliaram e contribuiram para esta tese.

Agradeço ao *Information Society Technologies* (IST) pelo apoio financeiro parcial a este trabalho através dos projetos de pesquisa IST-INSTINCT (IST-2004-507014) e IST-SAMBA (IST-2007-045403).

Aos doutores Célia e Rodrigo por me auxiliarem a manter-me "na linha" certa para atingir a conclusão deste trabalho e pelo apoio e conversas produtivas nos momentos que precisei. Agradeço a todos os professores do departamento PCS e aos professores do Centro Universitário da FEI pelas discussões a apoio durante os anos de pós-graduação.

Agradeço muito ao Eduardo Pydd por me auxiliar no desenvolvimento da aplicação desta tese e por solucionar as infinitas dúvidas sobre a linguagem de programação e desempenho de software.

Agradeço muitíssimo a minha família, Ana Luísa, Denise e ao "Neném" pelo apoio e amor incondicional e às vovós e ao vovô e titios pelos momentos que cuidaram de minha família com todo o amor para que eu pudesse finalizar esta empreitada.

RESUMO

Um dos objetivos das próximas gerações dos sistemas de comunicação é permitir que os usuários acessem e distribuam um ou mais serviços a qualquer hora, em qualquer lugar, independentemente do tipo de terminal (telefone convencional, telefone celular, assistentes pessoais digitais, notebooks, dentre outros) ou da tecnologia da rede de acesso utilizados. Esse cenário é denominado convergência de serviços utilizando-se redes heterogêneas, e em tal realidade, as arquiteturas de qualidade de serviço existentes em cada uma das tecnologias dos sistemas de comunicação não oferecem mecanismos de interoperabilidade e em diversos casos não há controle sob os fluxos de dados uma vez admitido na infraestrutura do sistema de comunicação, assim como questões de *handover* heterogêneo não são tratadas. A tese propõe uma arquitetura para controle de Qualidade de Serviço para um ambiente heterogêneo composto de *backbones* IP e redes de acesso de diversas tecnologias, sendo tal arquitetura composta de agentes autônomos e distribuídos nos equipamentos de um sistema de comunicação; assim como.controles baseados no comportamento de uma região de um sistema de comunicação e apoiados na teoria e princípios de sistemas complexos. Os agentes da arquitetura proposta utilizando o princípio de *preferential attachment* mostraram-se eficientes na determinação do caminho de melhor condição de qualidade de serviços. Os componentes da arquitetura proposta estão localizados em cada equipamento de comunicação, desde o dispositivo do usuário até o provedor de serviços. As medições realizadas pelos agentes e utilizando um algoritmo baseado no conceito de *preferential attachment* permitiram ao agente alterar o caminho de um fluxo de dados durante sua transmissão para outros caminhos que apresentaram condições mais adequadas de acordo com os parâmetros de QoS. A decisão é baseada no contrato de qualidade de serviço especificado entre usuário e provedor de serviço e, considerando sob controle todos os elementos envolvidos na comunicação; tem-se controle distribuído de qualidade de serviço fim a fim.

Palavras-chave: Qualidade de Serviço. Agentes. Sistemas Multiagentes. *Preferential Attachment*. Sistemas Complexos.

ABSTRACT

One of the targets of the next generation communication systems is to provide access to any service, to any user, anytime, anywhere, regardless the access network technology or type of user device (mobile phone, PDA, personal computer, and so on). This scenario is called convergence of services by heterogeneous networks, and in such scenario quality of service mechanisms presented in legacy communication systems do not provide mechanisms for interoperability between communication systems nor control data flows after control admission in the border of the communication systems. The heterogeneous handover is also not handled by such QoS architectures. This thesis proposes a QoS control architecture for an heterogeneous communication systems composed by IP backbones and several access networks for several kind of technologies. This architecture is composed by a multiagent system and has controls based on the local behavior of the communication system and supported by complex systems theory. The agent decision algorithm is based on preferential attachment concept and the experimentation results indicate that agents could identify a better path to handle a data flow according to QoS parameters. The agents decided to change the path used to transmit the flow data autonomously and according to quality of service contract between user and service provider. The measurements in the test based on preferential attachment algorithm was useful in order agent change flow data path during data flow transmission to other paths with better conditions according to QoS requisites. The agent decision is based on the parameter values defined between end user and service provider. Considering the control elements from proposed architecture it was achieved end-to-end distributed control.

Keywords: Quality of Service. Agents. Multiagent system. Preferential Attachment. Complex Systems.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

3GPP – *3rd Generation Partnership Project*

BB - *Bandwidth Broker*

DiffServ – *Differentiated Services*

EDGE – *Enhanced Data Rates for Global Evolution*

ETSI – *European Telecommunications Standards Institute*

FMC – *Fixed Mobile Convergence*

GPRS – *General Radio Packet Service*

GSC – Gerenciamento de Serviço do Consumidor

GSM – *Global System for Mobile Communication*

IMS – *IP Multimedia Subsystem*

IntServ – *Integrated Services*

IP – *Internet Protocol*

ITU-T - International *Telecommunication Union – Telecommunication*

MTBF – *Mean Time Between Fails*

MTTR – *Mean Time to Repair*

MTU - *Maximum Transfer Unit*

NGN – *Next Generation Network*

NGNM – *Next Generation Network Management*

ODP – *Open Distributed Processing*

PHB - *Per Hop Behavior* (DiffServ)

PSTN – Public *Switch Telephone Network*

QoS – *Quality of Service*

RSVP – *ReSerVation Protocol*

SLA – *Service Level Agreement*

SNMP –*Simple Network Management Protocol*

UMTS – *Universal Mobile Telecommunications Systems*

1 INTRODUÇÃO

Um dos pontos muito discutidos no âmbito das telecomunicações e sistemas de informação desde a década de 1990 refere-se à convergência dos sistemas de comunicação, que são considerados quaisquer sistemas capazes de receber um sinal elétrico (ou eletrônico) e transmiti-lo para outra localidade (Shannon, 2001). A convergência pode ser entendida, em parte, como a interconexão dos diversos sistemas de comunicação de tal forma que, diversos conteúdos possam ser transmitidos entre as diversas infraestruturas, desde o provedor de serviços até o usuário final. Esse movimento recebeu o nome de *Fixed-Mobile Convergence* (FMC) (Ciancetta, et.al, 1999) e preconizava a interconexão das redes de telefonia fixa e telefonia móvel. Contudo, atualmente a discussão é em torno da interconexão entre todos os sistemas de comunicação de tal forma a se ter acesso a qualquer tipo de serviço por qualquer sistema de comunicação. Naturalmente, as infraestruturas de telecomunicações, compostas pelos equipamentos das redes de telefonia e telefonia móvel, não foram concebidas para essa realidade, assim como a tecnologia base da Internet (protocolo IP) também não previa a convergência de conteúdos e a heterogeneidade. Embora haja argumentos para se considerar a Internet como de “natureza universal”, sob o ponto de vista de ser capaz de manipular diversos tipos de mídias (Knightson, Morita e Towel, 2005) e ser composta por diferentes tecnologias de redes de acesso, as infraestruturas que compõem a Internet (seus *backbones* e equipamentos de acesso) estão evoluindo para oferecer recursos para tratar todos os tipos de fluxos de dados adequadamente, como mecanismos de engenharia de tráfego e mecanismos para prover recursos com qualidade de serviço fim a fim.

Analisando o cenário histórico dos sistemas de comunicações dos últimos trinta anos, considerando a infraestrutura inicial da Internet (composta por uma rede de computadores e um *backbone*) e o sistema de telefonia fixa, tem-se que ambas apresentam diversas interfaces de comunicação (em particular o sistema de telefonia pública) como forma de prover acesso a diversos tipos de serviços. Esta afirmação torna-se mais contundente quando se analisa a expansão da Internet nas décadas de 1980 e 1990, cujo aproveitamento da

capilaridade do sistema de telefonia fixa pública (PSTN[1]) promoveu o acesso da população à “rede mundial de computadores”. Porém, uma característica presente neste cenário era a separação bastante clara dos serviços que cada um destes tipos de sistemas de comunicação provinham, uma vez que não havia serviços comuns até meados da década de 1990; época em que surgem, por exemplo, os primeiros serviços de voz sobre IP (VoIP) (Colcher, et.al. 2005).

A contínua evolução dos sistemas de comunicações, dos serviços ligados à computação e das tecnologias de geração de conteúdo levam à existência de serviços globais que poderão ser acessados por quaisquer redes de comunicação, em qualquer lugar, e com conteúdos de qualquer tipo, ou seja, heterogeneidade da rede e convergência dos serviços (Karlich, et.al., 2004), (ITU-T, 2004a), (ITU-T, 2004b). A ITU (2006) promove em sua especificação M-3060 sobre redes de nova geração (NGN) uma arquitetura que preconiza a integração horizontal dos serviços de rede, separando claramente aspectos de transmissão, controle e serviço para os ambientes heterogêneos; e a especificação TS-23-107 e TS 23-207, ambas da ETSI (2009a, 2009b) propõem e especificam o *IP Multimedia Subsystem* (IMS) como forma de integração e inter-operação de sistemas de comunicação e serviços. O IMS baseia-se nas propostas de NGN da ITU-T, claramente explicitado a interconexão e inter-operação de redes heterogêneas, assim como considera elementos de controle capazes de lidar com diversos sistemas heterogêneos.

As normas citadas tratam claramente da interconexão de sistemas de comunicação e mecanismos para troca de tráfegos, e também promovem a convergência de serviços, ou seja, um mesmo serviço ser prestado e entregue por diversas infraestruturas, cada qual com suas características particulares. As normas também indicam claramente a necessidade de serem especificados mecanismos de qualidade de serviço fim a fim. A arquitetura IMS especifica diversos mecanismos para manter a qualidade de serviço, e possui uma abordagem distribuída, além da especificação do IMS também não determinar que todos os elementos estejam em uma mesma infraestrutura ou em um

[1] PSTN – *Public Switch Telephone Network*

mesmo local, (Xu, et.al, 2007); (Magedanz, Gouveida, 2006). Logo, um sistema distribuído para controle de qualidade de serviço pode ser uma abordagem interessante, uma vez que devido às múltiplas tecnologias de redes de acesso o gerenciamento do serviço está migrando para as bordas da rede. (Calisti, Greenwood, 2007); e os sistemas multiagentes apresentam características que podem ser soluções adequadas ao cenário heterogêneo com serviços convergentes apresentado.

Ainda sobre prestação de serviço há a outra questão sobre qual tipo de dispositivo o usuário utilizará para a recepção do serviço. Atualmente, esses dispositivos não informam ao equipamento de borda do sistema de comunicação sobre o estado da qualidade do serviço que recebem da infraestrutura, nem tampouco as arquiteturas de qualidade de serviço atuais, notadamente as arquiteturas para redes IP, consideram a qualidade de serviço entregue ao dispositivo final. Os dispositivos finais para usuário final, independentemente da quantidade de redes de acesso disponíveis que esse dispositivo possa utilizar, esse é capaz apenas de se conectar, receber e enviar dados ou utilizar um determinado serviço apenas por uma das redes de acesso, sem possuir a capacidade de alternar entre redes de acordo com a qualidade de serviço prestada.

Segundo Serra (2007) é cada vez mais premente a necessidade de se ter qualidade de serviço, sendo essa considerada do ponto de vista do usuário final, ou seja, o contrato de qualidade de serviço deve levar em consideração a opinião do usuário e essa é transformada em valores de parâmetros de rede que devem ser controlados fim a fim. Logo, a qualidade deve ser controlada a partir do dispositivo do usuário final até o provedor de serviços. O dispositivo final do usuário deve ter capacidade de utilizar quaisquer redes de acesso para um mesmo serviço de acordo com a qualidade contratada pelo usuário final, o que pressupõe controle distribuído como proposto nesse trabalho.

Dado a quantidade de variáveis necessárias à definição de um serviço, como proposto por Serra (2007), assim como a dificuldade de se identificar as relações entre tais variáveis e entre essas variáveis em diferentes equipamentos, este trabalho se utiliza dos conceitos de sistemas complexos e de redes de escala livre para sustentar a argumentação da arquitetura

proposta. Redes de escala livre são aquelas que seguem uma distribuição denominada “Power Law”, cuja implicação é haver redes onde a maioria dos nós possui poucos *links* enquanto poucos nós possuem grande quantidade de conexões (Goh, Kahng, Kim, 2001), e dessa forma as políticas de QoS devem tratar as particularidades locais como forma de se atingir melhor controle da infraestrutura.

Para a utilização de tais conceitos na proposta de arquitetura o paradigma de sociedades multiagentes é propicio, dado as características de um agente de autonomia e comunicação, além dos comportamentos que podem emergir de uma sociedade multiagentes. Para tal é necessário elaborar uma ontologia[2] para os agentes, propor interfaces de comunicação entre os agentes e as tecnologias de QoS existentes em cada tipo de sistema de comunicação, e por fim munir os agentes de algoritmos que forneçam os subsídios para um agente atuar nos dispositivos e prover as políticas de QoS necessárias para os fluxos de dados em uma rede convergente e heterogênea. Uma sociedade multiagentes pode multiplicar os pontos de verificação e negociação de QoS, sem necessariamente causar necessariamente processamento em excesso do equipamento de borda, pois uma das características dos agentes é sua mobilidade, e, portanto, um agente é capaz de deslocar-se para locais com maior capacidade de processamento (embora essa tese não trate do tema de carga de processamento da arquitetura proposta). Ademais, problemas com a qualidade de serviço podem ocorrer em qualquer ponto da rede, e idealmente uma situação desse tipo poderia ser corrigida no local onde o QoS não está sendo satisfeito, sem depender dos equipamentos de borda da rede, ou mesmo dos equipamentos origem e destino do serviço.

[2] Ontologia é o estudo do ser, sendo através dela possível descrevê-lo para que seja então conhecido. Na medida em que a ontologia de um ser seja conhecida por outro torna-se possível ao primeiro entender o segundo e, portanto com ele se comunicar e trocar conhecimento. O eventual uso de diferentes ontologias para um mesmo ser permite sua descrição sob diversos enfoques, ou com diferentes roupagens. Neste caso consegue-se criar interfaces do ser descrito que sejam apropriadas para reconhecimento por interlocutores de diferentes espécies. (Maia, 2004).

1.1 OBJETIVO

O objetivo da tese é propor uma arquitetura de controle de qualidade de serviço para um ambiente heterogêneo composto de *backbones* IP e redes de acesso de diversas tecnologias. Os *backbones* IP são utilizados para transmitir diversos tipos de tráfego para diversas redes de acesso, cada qual com sua própria tecnologia. Os usuários finais estão conectados a uma ou mais redes de acesso, sendo que durante a prestação do serviço pode ocorrer mudança de caminho utilizado para a entrega dos tráfegos que compõem o serviço devido aos requisitos de qualidade estabelecidos entre o usuário final e o provedor de serviços.

A hipótese da tese é que uma arquitetura distribuída para controle de QoS possa responder às exigências oriundas dos contratos de qualidade de serviço de um usuário para um serviço dito convergente em um ambiente heterogêneo, controlando os tráfegos agrupados em classes de fluxos de dados. O agrupamento de fluxos de dados ocorre devido à decisão tomada pelos agentes segundo o princípio sob o qual um caminho melhor adaptado para uma determinada classe de fluxo de dados deve receber tal fluxo com maior probabilidade que os demais caminhos existentes. E a arquitetura sendo distribuída poderá reagir a eventos e mudanças das condições locais de um sistema de comunicação de tal forma a manter um caminho fim a fim controlado de acordo com os contratos de QoS.

Devido à complexidade e a quantidade de variáveis envolvidas na determinação do estado de um sistema de comunicação de forma global, e por não se ter a relação de como um requisito de controle dos fluxos de dados afeta o comportamento dos fluxos de dados e os demais requisitos em todas as conexões existentes em um sistema de comunicação, esse trabalho analisa localmente os efeitos causados pela alteração de um requisito e determina os caminhos que um determinado tipo de fluxo de dados deve percorrer de acordo com a qualidade exigida em contrato de SLA (ou outra forma equivalente). Todos os caminhos considerados pelo sistema distribuído devem ser obtidos via algoritmos de roteamento tradicionais ou caminhos pré-estabelecidos propostos por outras tecnologias, mas sem, contudo manter a restrição de se

ter apenas uma caminho ativo para um determinado destino; os elementos da arquitetura consideram todos os caminhos obtidos de forma a distribuir os fluxos de dados de maneira a atender todas as exigências de qualidade de serviço.

Tanto nas atuais redes de comunicação sem fio quanto nas redes com fio há certa capacidade alocada para transmissão de fluxos de dados, independentemente da tecnologia utilizada. Contudo, em redes sem fio pode ocorrer, dependendo da tecnologia de acesso, envio de dados de forma intermitente, ou seja, o sistema de transmissão do equipamento (em geral do usuário final) só é ativado quando há dados a transmitir. A arquitetura proposta nessa tese considera que a cada conexão feita por um dispositivo deve ser tratada de forma independente, não havendo correlação entre conexões feitas por um dispositivo para fins de controle de qualidade de serviço e conexões feitas para acesso a um serviço, uma vez que não será analisado neste trabalho conjunto de conexões que compõem um determinado serviço.

O conceito de arquitetura distribuída significa que não há uma única entidade do domínio administrativo que o gerencie e o controle por si só, mas sim diversas entidades autônomas cuja cooperação resulta em um efetivo controle da qualidade de serviço de todo o domínio administrativo. Este controle é exercido por uma sociedade multiagentes e classes de algoritmos para decisão dos agentes, os quais, para essa tese, interessam os algoritmos capazes de identificar o comportamento de tipos de fluxos de dados e como são tratados ou encaminhados. Uma arquitetura distribuída também é uma forma de preservar o legado, pois cada entidade da arquitetura pode possuir interfaces particulares apropriadas para cada sistema de QoS com o qual a arquitetura deva interagir; e sendo entidades independentes permitem tanto se ter diversas interfaces como permitem que as entidades possam tomar as ações apropriadas entre diversos domínios administrativos.

Essa tese também possui como hipótese que a qualidade de serviço é baseada em parâmetros oriundos dos contratos estabelecidos com o usuário final da aplicação na qual se deseja manter a qualidade de serviço. Portanto, a abordagem sobre qualidade de serviço nesse trabalho difere do que é geralmente feito, pois por se tratar de um ambiente heterogêneo os requisitos

de QoS podem diferir entre tecnologias, tanto em nome quanto em valores que podem assumir. Logo é necessário um conjunto de requisitos que possa ser traduzido para todas as tecnologias em questão (total ou parcialmente) e que ao mesmo tempo representem a qualidade fim a fim (Serra, 2007).

A arquitetura proposta será desenvolvida segundo o paradigma de sistemas multiagentes e ainda contará com as seguintes hipóteses:

- O conteúdo a ser transmitido através do *backbone* IP, embora seja destinado a diferentes redes de acesso, já possuem requisitos de QoS (valores) bem definidas e não faz parte desta tese defini-los;
- Os agentes de cada domínio possuem interfaces comuns (abertas) pelas quais a arquitetura proposta comunica-se e suas partes inter-operam;
- Cada agente também deve possuir uma interface com o sistema de comunicação que controla, sendo tal interface aderente aos requisitos tecnológicos do sistema de comunicação.

1.2 METODOLOGIA

Das diversas questões ainda em aberto no contexto das redes de nova geração, uma delas a necessidade de se ter mecanismos que possam inter-operar entre diversas tecnologias. Uma das facetas desse problema é como considerar os diversos equipamentos de comunicação e suas características locais que afetam a transmissão de dados, assim como estabelecer um padrão de comportamento dos mesmos, de tal forma a se ter condições de estabelecer políticas de qualidade de serviço.

Há ainda uma crescente necessidade de que as redes de comunicação, independentemente de tecnologia de transmissão ou forma de integração, transportem voz, dados e vídeo em velocidades cada vez maiores (Houéto, Pierre, 2005) e com maior confiabilidade, a qual pode ser interpretada com maior qualidade de serviço. Os sistemas atuais de qualidade de serviço são particulares de cada tecnologia de rede, e cada qual possui mecanismos específicos para o ambiente em que atua; e há diversos fatores que são

particulares de uma determinada infraestrutura e não são aplicáveis a outras. Quando se trata de QoS fim-a-fim o problema torna-se mais complexo uma vez que na maioria dos casos, as tecnologias de QoS não possuem interfaces entre si, ou seja, não trocam dados. Em contrapartida, além de ser complexo construir uma única arquitetura a qual trate de todos os aspectos de QoS, há uma grande dificuldade em substituir os diversos sistemas legados por novos.

Analisando as tecnologias de qualidade de serviço e engenharia de tráfego em ambientes IP identificou-se a característica estática de diversas soluções de determinação de caminhos, e em diversas soluções propostas como roteamento baseado em QoS, ou em determinação de caminhos dinâmicos via protocolo MPLS ou em soluções para redes 4G não se tem em consideração as diferenças entre os requisitos de fluxos de dados na determinação de caminhos (Lin, Qi, 2007), (Urushidani, Matsukata; 2007). A solução proposta por Martini et. al. (2008), por exemplo, classifica o tráfego de um túnel VPLS (*Virtual Private LAN Services*) ainda no modelo convencional do DiffServ, estratificando a rede em camadas e tratando todo o tráfego do túnel VPLS de uma única maneira.

Embora tecnologias como MPLS e VPLS, dentre outras permitam a segmentação de tráfego em um sistema de comunicação baseado na tecnologia IP de forma diferenciada em relação ao roteamento tradicional, as soluções analisadas não consideram a influência de tipos de tráfegos distintos podem causar uns aos outros, mesmo quando consideram alocação dinâmica de largura de banda em redes 4G ou 5G (todas baseadas em IP). (Gani, et.al. 2008), (Li, et.al. 2008). Da mesma forma, não é considerado a localização de determinadas entidades que possam causar efeitos particulares em um sistema de comunicação, quer seja por demandarem grandes recursos ou por terem seus serviços utilizados por diversas outras entidades distribuídas por diversas localidades de um domínio administrativo ou de diversos domínios administrativos.

Em trabalhos como Griffin et. al. (2007) são consideradas formas de negociação de qualidade de serviço entre domínios administrativos, contudo não levam em consideração o tratamento das questões de qualidade de

serviço internamente ao domínio administrativo, assim como não considera a segmentação de tráfego baseado em suas características.

Já o modelo de sistemas complexos proposto por Barabási-Albert (1999) tem sido estudado para aplicações em qualidade de serviço como proposto por Yannuzzi et. al. (2006) onde se pode identificar a importância da distribuição de dados sobre engenharia de tráfego como forma melhor desempenho de uma solução de qualidade de serviço, assim como identificam a aderência do modelo de sistemas complexos (embora não originalmente aplicado às questões de qualidade de serviços em sistemas de comunicação).

Diversos trabalhos (Barabási, 2003), (Watts, 2003), (Barabási, 2009), (Park, Barabási, 2007) identificam que a distribuição de entidades[3] em uma rede qualquer guardam propriedades de relação, inclusive conteúdos em um sistema de comunicação. Como certamente o fluxo de dados tem relação com a distribuição de conteúdos, formulou-se a hipótese da tese de que o tratamento dos fluxos de dados podem seguir a relação de *preferential attachment* (também denomiado "*rich get richer*"), ou seja, se houver um provedor de serviços, por exemplo, que possua um determinado tipo de conteúdo, esse irá gerar certa quantidade de fluxos de dados de um determinado tipo. Quanto maior o sucesso desse provedor estima-se que maior será a quantidade de acessos aos seus conteúdos e, portanto maior a quantidade de fluxos de dados de um determinado tipo em uma região do sistema de comunicação onde tal provedor está. Tal provedor, assim como certa quantidade de usuários finais devem influenciar o comportamento dos fluxos de dados e essa influência pode ser percebida em todo o caminho fim a fim entre usuário final e provedor de serviços (Dezso, et.al, 2006) (Onnela, et. al. 2006).

Surge então a necessidade de se investigar o conceito "*rich get richer*" pode ser uma forma de tratamento e segmentação de fluxos de dados, ou seja, aquele equipamento que possui melhores condições de transmitir um

[3] Entidades são aqui entendidas como quaisquer elementos que possam se interligar em uma rede, sendo essa rede de qualquer tipo, inclusive uma rede que forme um sistema de comunicação.

determinado fluxo de dados terá a preferência de seus vizinhos para aquele determinado tipo de fluxo de dados para um determinado destino, em detrimento a outros tipos de fluxos de dados. Ainda deve ser considerado que em cada ponto de um sistema de comunicação há ingresso de novos fluxos de dados, o que sugere um tratamento particular em cada ponto da rede; trazendo o conceito de sistemas distribuídos, e em particular os sistemas multiagentes dado a característica de autonomia de um agente.

A hipótese da tese de se ter um sistema distribuído composto de uma sociedade multiagentes e tendo o mecanismo de decisão de cada agente o modelo Barabási-Albert (1999) é analisada através de uma estrutura composta por "roteadores virtuais" e um gerador de tráfego D-ITG (Botta, Dainotti, Pescapè; 2007) conforme ilustra a Figura 1.

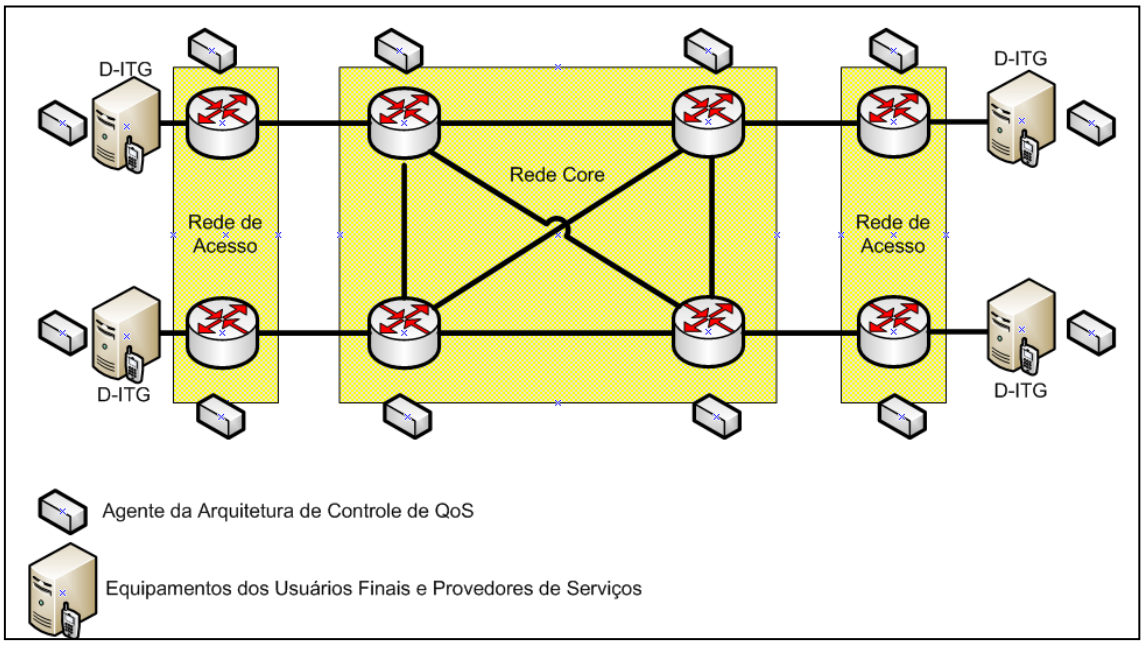

Figura 1 – Estrutura de verificação de hipótese da tese

Os testes realizados procuram identificar o comportamento da estrutura montada e se esta reage de forma similar um sistema de comunicação. O segundo tipo de testes procura delimitar como a estrutura de testes reage a anomalias via geração em algumas partes da estrutura de atrasos e perdas de pacotes segundo uma distribuição normal. E o terceiro tipo de teste utiliza os agentes da arquitetura proposta (localizados apenas no *backbone*) e o mecanismo de tomada de decisão para verificar as propriedades da arquitetura proposta.

A tese inicia com a discussão das questões de qualidade de serviço em redes heterogêneas operando com serviços convergentes de tal forma a estabelecer as bases para a proposta de uma arquitetura genérica e aberta de Controle de Qualidade de Serviço para tal cenário. Portanto, a elaboração da arquitetura necessita abordar os seguintes aspectos:

- visão de QoS local em cada equipamento da infraestrutura, considerando o dispositivo final do usuário e o equipamento provedor do serviço;
- identificação do tipo de fluxo de dados e de possíveis caminhos a serem percorridos, independentemente das tecnologias de transmissão de dados que compõem tal caminho;
- estimativa de comportamento de um equipamento e os caminhos para encaminhamento de fluxos de dados em relação aos tipos de fluxos de dados existentes na infraestrutura;
- Determinação do comportamento de um domínio administrativo em termos que possam ser analisados por equipamentos de comunicação, independente de sua tecnologia. É recomendado que a determinação do comportamento não seja composta por uma grande quantidade de estados, pois isso aumenta o tempo de processamento para dispositivos móveis como os encontrados atualmente;
- Planejamento de alocação e utilização dos recursos disponíveis para melhor aproveitar a infra-estrutura instalada, baseado em dados históricos.

Entende-se por domínio administrativo uma determinada porção de um sistema de comunicação sob o controle administrativo de uma única entidade, independentemente dos equipamentos que compõem o domínio administrativo.

Portanto, uma rede como a Internet é composta de diversos domínios administrativos, sendo que para a completa administração de uma infra-estrutura global de comunicação é necessário a comunicação entre diversos domínios administrativos.

A segunda discussão trata do comportamento de redes de comunicação de dados e da possibilidade de sistemas distribuídos serem adequados para o tratamento da questão de QoS. Para tal analisa-se os estudos de sistemas complexos propostos por Simon (1962) e por Barabási (2003), dentre outros, para estabelecer os fundamentos do comportamento de um sistema de comunicação como sendo de escala livre. Quando se trata de sistemas distribuídos compostos por agentes necessita-se de algoritmos para suporte a tomada de decisão para que um agente atinja seu objetivo[4]; e nesse trabalho é discutido uma classe de algoritmos capazes de lidar com o cenário proposto na tese e é feita uma comparação entre o modelo proposto na tese e tais algoritmos. O modelo de arquitetura de controle de qualidade de serviço proposto será construído e discutido em duas etapas. A primeira etapa será composta da análise de um agente em relação a um equipamento de rede, tendo como resultado a determinação das propriedades de um agente necessárias à manipulação e análise dos parâmetros e controle do sistema de qualidade de serviço do equipamento. A segunda etapa é composta da análise dos mecanismos de interação entre os agentes e discussão da representatividade desse mecanismo em relação ao comportamento emergente de uma rede de comunicação. Essa discussão será baseada em uma discussão estatística sobre o comportamento do tráfego de uma rede de comunicação, onde há a utilização de uma aplicação de simulação de redes de comunicação.

Como suporte à discussão da tese é pontuado no texto conceitos de sistemas distribuídos, redes de escala livre e arquiteturas propostas para as redes de nova geração. A revisão bibliográfica para a concepção da descrição funcional considera artigos científicos, normas técnicas da ITU-T, ETSI, 3GPP, assim como outras publicações consideradas relevantes.

[4] O objetivo de um agente nessa tese é controlar a qualidade de serviço dos fluxos que utilizem como parte do caminho o equipamento de rede gerenciado por ele.

1.3 JUSTIFICATIVA

Em se tratando de redes heterogêneas, há diversas iniciativas de se estabelecer arquiteturas de gerenciamento e controle de qualidade de serviço. Contudo, para se ter uma arquitetura de QoS fim a fim é necessário que todos os nós que compõem a estrutura de comunicação e que formam o caminho do fluxo de dados estejam comprometidos com o controle dos requisitos de qualidade demandados para determinado fluxo. Contudo, os mecanismos de controle dos atuais sistemas de comunicação não provêm tal garantia, tendo em consideração as redes que formam o *backbone.* Da mesma forma as redes de acesso não possuem mecanismos de controle de qualidade de serviço, tanto compostas por redes sem fio como redes com fio, embora possuam outras características de alocação de recursos e formas para se manter a qualidade de serviço, como por exemplo, definir em um canal de comunicação limite de atraso, probabilidade de queda de comunicação, dentre outros (Rao, Bojkovic, Milovanovic, 2006).

Marques et.al. (2002) coloca que as redes serão todas baseadas em IP, cada qual sob controle de um domínio administrativo. Sistemas recentes, como o UMTS possuem classificadores de tráfego, similares ao encontrados em redes IP (*DiffServ*), pois é uma forma de manipular na infra-estrutura diferentes tipos de tráfego, uma vez que essa técnica provê diferentes tipos de prioridades de manipulação de tráfego através de rótulos atribuídos aos tráfegos (Rao, Bojkovic, Milovanovic, 2006), (Gani et. al., 2008). Contudo, assim como o DiffServ em redes IP, não há um mecanismo para controle dos fluxos que reaja às intermitências de operação a não ser àqueles que executam descarte de pacotes (independente do critério de gerenciamento de fila adotado).

Hillebrand et.al. (2004) afirmam que as redes sem fio serão todas IP para se tornarem compatíveis com as redes de nova geração. Logo, os esquemas de qualidade de serviço deverão também operar sob a plataforma IP para troca de dados de controle. As arquiteturas atuais de QoS não possuem a abrangência necessária para o cenário de redes heterogêneas segundo Rejeb, et. al. (2007). As razões apontadas para as arquiteturas de qualidade de

serviço atuais não serem adequadas para o cenário em questão são o fato das arquiteturas não serem dinâmicas, e quando o são, que seus controles (protocolo RSVP) demandam demasiados recursos para reserva e gerenciamento de um caminho com qualidade de serviço garantida. (Chimento, 1998)

Particularmente, em relação ao RSVP, a questão pauta-se em que tal protocolo mantém uma grande quantidade de estados em cada equipamento de rede para garantia de recursos de um determinado fluxo de dados, resultando em problemas de gerenciamento dos estados que controlam um determinado fluxo de dados. Os caminhos com qualidade de serviço, mesmo com reserva de recursos estabelecida no momento da conexão e desfeitos quando o fluxo de dados termina, são, em geral, estáticos em relação à alocação de recursos, ou seja, uma vez alocado a quantidade de recursos é imutável durante a duração daquele tráfego (Chimento, 1998).

As futuras arquiteturas de qualidade de serviço também necessitarão de mecanismos que facilitem o *handover* entre diferentes plataformas. Uma das possíveis formas de executar *handover* e manter a qualidade do serviço é conhecida como pré-reserva de recursos em diferentes redes, potencialmente naquelas onde um dispositivo móvel poderia se conectar. (Bless, et.al, 2007). Hillebrand et.al. (2004) propõem uma estrutura para sinalização entre domínios administrativos e que seja feita por equipamentos centralizados através de um protocolo específico. Esses equipamentos centralizados são similares ao *Bandwidth Broker* da arquitetura *DiffServ*. Maia et.al. (2005) propõem uma arquitetura para QoS baseado em equipamentos centralizados em cada domínio administrativo; contudo a arquitetura possui limitações para estabelecimento do comportamento da rede para tomada de decisão de QoS. Rejeb, et. al. (2007) propõem outra arquitetura centralizada de qualidade de serviço e similar ao proposto por Bless, et. al. (2004). Contudo essas arquiteturas ainda possuem limitações de tempo de resposta pelo fato de estarem distantes do local de falha de QoS, sendo que o próprio tráfego de controle de QoS pode ser comprometido pelos efeitos do evento que se pretende controlar. Outra limitação do sistema centralizado é não poder determinar com precisão o estado real da rede (estado global) e, portanto,

podem ocorrer falhas de negociação por não se considerar características locais do tráfego.

De forma geral, pode-se dizer que as arquiteturas de qualidade de serviço em redes IP *IntServ* e *DiffServ* preocupam-se mais com as características estáticas da qualidade de serviço do que com as características dinâmicas (ver item 2.1); e se pode apontar como uma das razões da ênfase nas características estáticas a não determinação das arquiteturas atuais de QoS do comportamento de cada nó de um sistema de comunicação.

Quando se trata da inter-operação de redes heterogêneas fazendo com que essas trabalhem de forma transparente, do ponto de vista do usuário se faz necessários mecanismos de controle e gerenciamento de recursos os quais, independentemente do caminho a ser utilizado para a transmissão de dados (por um ou mais domínios administrativos ou por redes de tecnologias distintas), possam gerenciar o caminho fim a fim a ser utilizado por um fluxo de dados. A norma da ITU-T M.3060 (2006) propõe mecanismos de gerenciamento de rede denominados (NGNM); contudo não determina se esses mecanismos são centralizados ou distribuídos. O mesmo ocorre com as definições do IP Multimedia Subsystem (IMS) estabelecidas como uma arquitetura para inter-operação de redes heterogêneas e serviços convergentes. Segundo Ward, et. al. (2006): “... IMS permite a convergência de redes através de arquiteturas de aplicações agnósticas independentes da tecnologia da rede de acesso...”. Koukoulidis e Sham (2006) afirmam que a arquitetura IMS provê valor agregado às redes GPRS, EDGE e UMTS através da possibilidade dessas trabalharem com serviços IP. Os mesmos autores enfatizam a necessidade de se ter qualidade de serviço assegurada através de diferentes tecnologias de rede, inclusive para usuários com dispositivos móveis.

Embora a arquitetura IMS defina um plano de controle para o gerenciamento dos recursos dos sistemas de comunicação que compõem a rede heterogênea, as normas ETSI não identificam uma solução centralizada ou distribuída, e também não são discutidos mecanismos para gerenciamento de *handover* e alocação de recursos. (ETSI, 2009c). A arquitetura de controle e gerenciamento de qualidade de serviços definido para o IMS determina que os

mecanismos devam prover garantias de qualidade fim a fim para quatro classes de tráfego, as quais abrangem desde tráfego convencional (ou *best effort*) até tráfego multimídia com requisitos de qualidade elevados (ETSI, 2009a).

Tendo em consideração todo o caminho percorrido por um fluxo de dados, o terminal do usuário deve ser considerado com um dos elementos da rede. Hillebrand et. al. (2004) sugere que cada tecnologia de rede que compõe uma infraestrutura possui melhores condições de manipular um determinado tipo de tráfego, e então, seria interessante para um terminal com múltiplos serviços trabalhar com diversas redes simultaneamente, sendo que seus mecanismos de controle deveriam utilizar para cada serviço, a rede mais apropriada. A arquitetura IMS não apresenta nenhuma restrição a esse tipo de operação; contudo, os mecanismos centralizados de controle e gerenciamento de qualidade de serviços apresentam uma limitação quando se considera o dispositivo final do usuário, pois embora tanto dispositivo quanto o sistema de comunicação possam determinar a localização de cada terminal em qualquer momento da comunicação (Anisetti, et.al., 2006), não é factível ter informação sobre todos os caminhos fim a fim para um provimento do serviço dados que as condições apresentadas por um caminho podem sofrer alterações em qualquer momento uma vez que o caminho é compartilhado em sistemas de comunicação baseados na tecnologia IP.

O cenário proposto em Hillebrand et. al. (2004) demanda velocidade para alocação de recursos entre o ponto inicial e final da comunicação, e para tal, pode-se ter algoritmos de preempção para alocação de tais recursos, cuja finalidade é reduzir o tempo de resposta para operações de *handover* vertical (Bless, et. al., 2007), (Ahmad, Kamruzzaman, 2007).

Para se ter preempção é necessário conhecer o comportamento da rede e as suas formas de organização. Barabási (2003) oferece um paradigma denominado teoria dos sistemas complexos, no qual as redes de comunicação de dados não possuem um comportamento aleatório, mas sim um comportamento denominado “escala livre”. Watts (2003) apresenta o conceito de “*rich get richer*” e descreve que em redes de escala livre há elementos que, por possuírem algum atributo (ou um conjunto desses), tornam-se elementos

com maior número de conexões, ou seja, alguém mais utilizado, acessado ou conhecido pelos demais integrantes de sua rede e também daquelas que estão conectadas ou possuem acesso a esse elemento de alguma forma.

Esse comportamento é identificado nas redes de comunicação de dados, independentemente de sua tecnologia. Por exemplo: as rotas em redes IP possuem alguns equipamentos em comum, geralmente pertencentes ao núcleo da rede que concentram grande quantidade de tráfego. E embora existam outros caminhos alternativos na rede, uma vez que ela é construída com conexões e caminhos redundantes, tais caminhos são subutilizados em detrimento de sobrecarga em alguns equipamentos. A análise do comportamento de redes através da visão de sistemas complexos permite, por exemplo, a análise de congestionamentos e de como o princípio "*rich get richer*" influencia o comportamento de uma infraestrutura (Zhao, et. al., 2005).

A teoria dos sistemas complexos argumenta que cada elemento contribui e determina parte do comportamento global. Logo, se os equipamentos que compõem um domínio administrativo forem capazes, de forma autônoma, de gerenciar e determinar, através de algoritmos de preempção, a utilização de seus recursos e sua possível alocação no tempo, estes podem determinar os melhores caminhos para um determinado fluxo de tráfego em certo instante de tempo. Tal comportamento autônomo é característica de um agente (Nwana, 1996). Além desse comportamento, um agente ainda pode ser móvel, o que traz maior flexibilidade e adaptabilidade para uma arquitetura de gerenciamento de um sistema de comunicação (Hagen, Breugst, Magedanz, 1998).

Há diversos trabalhos abordando a utilização de agentes para controle descentralizado de recursos, como o gerenciamento de rotas em uma rede IP (Papavassiliou, S.; et. al., 2002), ou para análise do comportamento de um terminal de usuário em uma rede NGN (Kim, et. al. 2006). Hadim e Mohamed (2006) identificam o paradigma de agentes como uma abordagem interessante para as questões de qualidade de serviço em redes de sensores sem fio.

Jia et. al. (2005) propõem uma arquitetura de qualidade de serviço composta por agentes, sendo que esses devem residir em diversos pontos da camada de controle de uma arquitetura IMS para realizar controle de admissão, configuração de um caminho com QoS fim a fim, dentre outras atribuições.

Contudo, o texto refere-se a uma abordagem de agentes já utilizada em redes IP, como os agentes SNMP. O texto não confere aos agentes nem inteligência nem autonomia para decisão sobre tratamento de um fluxo de dados.

Esta tese, propondo uma arquitetura de controle de qualidade de serviço composta por agentes aderentes ao paradigma de agentes e sociedades multiagentes, admite autonomia dos componentes da infra-estrutura para negociação e controle de caminhos fim a fim que possuam a qualidade de serviço requerida, independentemente de uma entidade centralizada executar ou determinar a configuração de tal caminho. A arquitetura proposta também considera que o dispositivo do usuário pertence à arquitetura de controle de QoS, sendo esse elemento ativo na determinação de caminhos e negociação dos parâmetros de qualidade de serviço.

A adaptabilidade, em parte oferecida pela autonomia, e a flexibilidade, oferecida pela mobilidade dos agentes, tendem a promover dinamicidade à arquitetura de QoS proposta e, aliada à monitoração que um agente pode executar, é possível elaborar ou se utilizar de algoritmos de tomada de decisão para que os agentes negociem contratos de serviços entre si para diversos pontos da infra-estrutura. Uma possibilidade é a utilização de caminhos que tenham como origem o equipamento do agente e destino o provedor de serviços, e que os caminhos sejam determinados seguindo uma abordagem "*rich get richer*" ou *"preferential attachment"*. Nesse contexto, se o agente detecta que há demanda por uma determinada classe de serviço, esse pode previamente estimar se caminhos com certas características de qualidade de serviço atendem à demanda e, portanto, quando receber uma determinada requisição de um dispositivo final (usuário), o agente já terá um caminho determinado e saberá, devido à sua monitoração, se poderá ou não aceitar determinada requisição.

A contribuição desta tese com o estudo de arquiteturas para controle da qualidade de serviço está em sua abordagem distribuída e com capacidade de adaptar-se às mudanças de características e volume de fluxos de dados de acordo com o paradigma de sistemas complexos. Por ser baseada em uma análise local em um determinado nó do sistema de comunicação, a tomada de decisão de um agente da arquitetura independe de dados recebidos de outros

agentes, uma vez que os efeitos das falhas e outros eventos refletem-se no nó analisado. E por fim a arquitetura apresenta componentes que possuem como função a negociação de requisitos de USLA (Serra, 2007) entre domínios administrativos.

2 ASPECTOS DE QUALIDADE DE SERVIÇO EM SISTEMAS DE COMUNICAÇÃO

Em termos gerais há duas formas de se abordar a qualidade de serviço: uma delas é o super dimensionamento de recursos e a outra é prover a quantidade de recursos adequada a um determinado tráfego e monitorar o uso para verificar a acuidade do uso dos recursos (Amidst, 1999). Embora a abordagem atual nos sistemas de comunicação de dados seja, em diversos casos, o super dimensionamento, dado a quantidade de recursos disponíveis, principalmente no *backbone*, essa não é uma solução sustentável em longo prazo. Uma das razões é a quantidade crescente de usuários e o crescente aumento das requisições de serviços interativos e multimídia, pois tais tipos de serviços necessitam que os recursos estejam disponíveis, dentro de limites mínimos e máximos, fato que não ocorre em uma rede de dados trabalhando no modelo *best effort*. Além disso, o super dimensionamento considera, em geral, a infraestrutura como um todo e não garante que um determinado trecho da infraestrutura possua recursos para um determinado serviço.

Embora existam diversas abordagens sobre o que significa qualidade de serviço (Fergunson, 1998), há pelo menos duas abordagens para defini-la: a abordagem qualitativa cuja definição aborda requisitos não funcionais de sistema e que afeta a percepção do usuário; e a abordagem quantitativa, comumente relacionada aos mecanismos de controle de qualidade de serviço.

Fergunson (1998),Gozdecki, Jajszczyk, Stankiewicz (2003) e Carneiro, et.al. (2006) definiram que uma arquitetura de QoS deveria controlar os seguintes parâmetros de uma rede:

- Atraso: tempo gasto para um pacote ser enviado da origem até ser processado no destino, considerando: (i) atraso de processamento: decodificação e tratamento do cabeçalho do pacote de dados; (ii) atraso de fila; (iii) atraso de transmissão: tempo de processamento para “retirar os bits do meio e processá-los”; (iv) atraso de propagação: tempo de propagação de sinal no meio (Odom, Cavanaugh, 2004).

- Variação de atraso: diferença entre o atraso experimentado por uma porção de dado[5] e pela porção de dado subseqüente.
- Porcentagem de perda de bits: porcentagem de dados que não atingem o destino ou são corrompidos durante a transmissão.
- Volume ou vazão da rede: quantidade de dados que atravessam uma determinada de rede por unidade de tempo.

Chalmers (1998) e Serra (2007) ainda acrescentam parâmetros qualitativos como relevantes para se definir a qualidade de serviço, como confiabilidade, criticidade, qualidade percebida e custo. Confiabilidade implica em considerar tempos entre falhas e reparos, dentre outros. Criticidade está relacionado com a importância do tráfego, cuja importância deve de alguma forma ser representada no contrato de qualidade de serviço (posteriormente discutido neste trabalho). Qualidade percebida é o julgamento qualitativo do resultado da transmissão do conteúdo em termos de mídia e quaisquer outros aspectos relacionados com o serviço em questão.

Freire e Soares (2002) oferecem uma visão quantitativa de qualidade de serviço, na qual basta se alocar banda e demais recursos em diferentes infra-estruturas para os diferentes tipos de clientes dado um ambiente heterogêneo. Essa definição de QoS destaca a atual heterogeneidade dos ambientes e traz uma severa implicação, pois cada infraestrutura possui mecanismos próprios de gerenciamento e controle de qualidade de serviço, sendo que esses podem operar com tecnologias distintas, ou ainda, mesmo que com tecnologias similares, esses não são capazes de trocar dados e não consideram o efeito que um domínio administrativo exerce em outro.

Essa tese considera como qualidade de serviço os aspectos propostos por Fergunson (1998) e Chalmers (1998) e centrados no usuário final do serviço, ou seja, considerando qualidade de serviço fim a fim como proposto

[5] A expressão “porção de dados” é entendida como uma certa quantidade de bits a serem transmitidos sob um mesmo cabeçalho de protocolo (para controle).

em Serra (2007) [6]. Os parâmetros a serem utilizados no modelo proposto nesta tese devem considerar também que um determinado fluxo de dados terá seus parâmetros de qualidade entendidos por todas as infra-estruturas às quais irá passar independentemente da tecnologia de transmissão da rede (heterogeneidade), e deverá considerar serviços interativos.

Essas considerações sobre a qualidade de serviço deverão constar do contrato de qualidade de serviço (USLA) estabelecido entre o provedor do serviço e o usuário final, tanto no que tange os aspectos estáticos quanto os aspectos dinâmicos de QoS como mostrado a seguir.

2.1 ASPECTOS ESTÁTICOS E DINÂMICOS DA QUALIDADE DE SERVIÇOS

Um sistema de controle de qualidade de serviços possui dois aspectos: o estático são os requisitos que se mantêm imutáveis durante o serviço, enquanto o aspecto dinâmico trata das mudanças que podem ocorrer no ambiente e dos mecanismos necessários à manutenção dos requisitos do SLA estabelecido para um determinado fluxo de dados (Chalmers, 1999), (Wang, et. al., 2000), (Wang, 2001).

2.1.1 Aspectos Estáticos de Qualidade de Serviço

Os principais aspectos estáticos da qualidade de serviço envolvem a especificação, a negociação, o controle de admissão e reserva de recursos (se houver). A especificação do contrato de QoS trata da criação de um acordo entre o provedor de serviços e o usuário final e é baseado na especificação de requisitos de rede (Chalmers, 1998), (Aurrecoechea, 1998). Contudo, nesta tese será utilizada a abordagem proposta por Karam (2006) e Serra (2007) na qual os valores de requisitos para a utilização de um serviço são resultado das

[6] Contudo, para as provas de conceito desse trabalho não são consideradas opniões de usuário para estabelecimento de controle, sendo esse baseado em SLAs. A arquitetura, em sua forma geral, considera que a opinião do usuário pode ser refletida em contratos de SLA como proposta em Serra (2007).

características do serviço a ser prestado e a percepção do usuário que utiliza tal serviço em relação à qualidade. A percepção do usuário é que determina o intervalo de valores que um determinado requisito pode ter para que na opinião do usuário o serviço tenha qualidade.

Dado um contrato de QoS, os mecanismos para interação entre provedor do serviço e usuário final devem ter como parâmetros de controle a especificação do contrato; sendo tais controles definidos como admissão e controle de recursos alocados para esses fluxos de dados, dentre outros. O controle de admissão é composto de mecanismos que permitem ou não um determinado fluxo de dados ser transmitido através de um domínio administrativo. Segundo Marques et. al. (2002) há diversas formas de executar um controle de admissão, sendo as formas centralizadas em equipamentos dedicados, como um *Bandwidth Broker* (BB) são as mais utilizadas. Contudo, também pode haver controles distribuídos e baseados em agentes, como proposto Jia et. al. (2005).

A reserva de recursos é segundo Chalmers (1998) uma extensão do controle de admissão, pois uma vez um fluxo aceito no domínio administrativo, os recursos necessários deverão ser alocados de certa reserva de recursos existente no domínio administrativo. Essa alocação de recursos pode ser executada no final do processo de negociação como propõem o *Integrated Services* (IntServ) ou ainda pode ser pré-definida como ocorre com o *Differentiated Services* (DiffServ), ambos em redes IP. (Farrel, 2005). As redes de telefonia utilizam o processo de reserva de circuitos quando da admissão da chamada telefônica em uma rede, sendo essa alocação válida e pré-definida em todos os domínios administrativos que interconectam a origem e o destino da comunicação. É de se destacar que em sistemas de telefonia um canal já possui certos recursos reservados e que oscilações nas quantidades de recursos alocados em tais redes de acesso são em geral provenientes de alterações físicas do ambiente de operação ou falha da rede, tendo ações do usuário como fator não preponderante de tais oscilações.

2.1.2 Aspectos Dinâmicos de QoS

Os aspectos dinâmicos do gerenciamento de qualidade de serviços envolvem a monitoração, manutenção, renegociação e "*policing*" dos fluxos de dados já estabelecidos em um domínio administrativo (Penna, Wandersen, 2006).

A monitoração é composta por mecanismos que medem a situação da infra-estrutura. Os resultados de uma medição podem ser enviados para pontos específicos de coleta de dados (estações de gerenciamento).

Policing está relacionado a sistemas que garantam que todos os elementos de um dado domínio administrativo respeitem o contrato a que estão submetidos. (Cisco, 2003)

A manutenção está relacionada a mecanismos que tomam ações em um determinado domínio administrativo para sustentar o contrato enquanto ocorrem variações nas condições de recursos da infraestrutura de um sistema de comunicação. Quando o contrato não pode ser respeitado por uma intermitência ou falha da infraestrutura de comunicação, então os mecanismos de renegociação devem estabelecer uma forma de se seguir o contrato de qualidade de serviço. Nessa renegociação pode ser estabelecida uma qualidade de serviço inferior a utilizada antes da falha ou intermitência, desde que o contrato possua essa condição. Como proposto por Bhargava, et. al. (20005) há diversas formas de se fazer acompanhamento e controle de parâmetros, inclusive renegociação de valores de parâmetros da infraestrutura que atendam aos requisitos do serviço.

Deora et.al. (2003) destaca que um modelo de QoS deve ser acompanhado em pelo menos três visões (todas dinâmicas):

- qualidade como funcionalidade: as funcionalidades providas pelo serviço e como essas afetam o usuário;
- qualidade como conformidade: o serviço é prestado de acordo com as especificações (de contrato);
- qualidade como reputação: qualidade percebida pelo usuário, ou seja, durante o tempo de prestação do serviço a qualidade é

mantida; duração essa que deve ser considerada como a somatória de todos os intervalos de tempo em que o serviço foi prestado.

Nesta tese é estendido o conceito de qualidade como reputação, podendo ser entendida adicionalmente como a percepção entre entidades quaisquer de que o prestador de serviço está cumprindo os requisitos estabelecidos ao longo do tempo de duração do serviço, e pela da quantidade de vezes que o serviço é prestado. Em vez de apenas o usuário pode-se ter um equipamento pertencente à infraestrutura de um sistema de comunicação que contabiliza a forma como um serviço é prestado. Essa contabilização pode ser entendida como a percepção do equipamento de um determinado serviço prestado.

2.2 ARQUITETURAS DE QUALIDADE DE SERVIÇO

Os diversos sistemas de comunicação existentes possuem pelo menos uma arquitetura de QoS, sendo que tal arquitetura reflete as características da infraestrutura que compõe o sistema de comunicação. Contudo, quando se trata da inter-operação de arquiteturas de QoS distintos é necessário promover uma visão comum de como tais arquiteturas de qualidade de serviço em diversos domínios administrativos podem trabalhar com diversos tipos de parâmetros. Essa visão se faz necessária para que todas as arquiteturas possuam um entendimento comum entre os parâmetros e possam executar os mecanismos de controle de qualidade de serviço de acordo com os parâmetros estabelecidos. Diversos mecanismos desse tipo são propostos em diversas normas, como o *Policy Decision Function* na especificação da 3GPP ou o *Resource and Admission Control Subsystem* proposto pela ETSI TISPAN (ETSI, 2009a), (ETSI, 2009b), (ETSI, 2006), (ETSI, 2005).

Nos itens subseqüentes são destacadas algumas características das arquiteturas de QoS em sistemas de comunicação baseados na tecnologia IP, identificando os pontos chave de tais arquiteturas e os pontos que podem ser entendidos como comuns para todas as arquiteturas, independentemente da tecnologia da rede. A discussão de arquiteturas de qualidade de serviço são os aplicados às infraestruturas que utilizam o protocolo IP a tendência é que todas as redes sejam IP segundo a ETSI (2009c).

2.2.1 Arquiteturas de Qualidade de Serviço em redes IP

Tendo em consideração duas abordagens de arquiteturas de qualidade de serviço para redes IP (*DiffServ* e *IntServ*) ambos possuem controle de admissão para conexões. Entretanto, o tempo de resposta para criar um caminho com QoS em ambos os métodos pode não ser apropriado para "conexões de trânsito", ou seja, conexões as quais o caminho que utiliza torna-se indisponível ou insuficiente para manter os requisitos de QoS necessários. Segundo Kim e Sebuktekin (2002) e o tempo de resposta para o IntServ é de aproximadamente 185ms para estabelecer um caminho em uma rede IP com demandas próximas às medidas em redes ditas em produção, e como esse tempo é gasto antes de iniciar-se a transmissão, apenas tráfegos multimídia com transmissão "ao vivo" sofreria com o *setup* inicial. Contudo, o caminho estabelecido em geral mantém os requisitos de QoS durante todo o tempo de transmissão. A questão envolvendo o IntServ está na complexidade de se utilizar e manter um grande número de estados para cada fluxo transmitido. Adicionalmente, o IntServ é restrito a um domínio administrativo, uma vez que são necessários mecanismos para gerenciamento de admissão entre diversos domínios administrativos (Gozdecki, Jajszczyk, Stankiewicz; 2003), (Trimintzios, et.al. 2001).

Já os mecanismos da arquitetura DiffServ comportam-se dividindo os recursos de uma infraestrutura entre diversas categorias de tráfego, cada qual identificada por um código (*DiffServ Codepoint*). É importante destacar que a identificação por fluxo em uma arquitetura DiffServ é apenas mantida nas bordas da rede (Mykoniati, et. al., 2003). O tratamento dos fluxos de dados em cada equipamento pertencente ao domínio DiffServ é determinado pelo *Per Hop Behaviour* (PHB) (Gozdecki, Jajszczyk, Stankiewicz; 2003). No *DiffServ* um tráfego é admitido se há recursos detectados pelo controle de admissão; contudo, a decisão de um sistema de controle de admissão não considera possibilidade de falhas em toda a infraestrutura, e, portanto, falhas internas podem acontecer e os recursos não estarem disponível em todos os caminhos possíveis da infraestrutura, e a arquitetura não provê formas de detecção desses caminhos possíveis em caso de falha. A arquitetura *DiffServ* ainda

conta com um sistema de controle denominado *Bandwidth Broker* (BB) e sua função é gerar políticas de acesso para os roteadores de borda aceitarem ou não um novo tráfego (Nichols, Jacobson, Zhang, 1999). Mesmo havendo um BB centralizado para cada domínio administrativo, há problemas de escala quando se trata de redes maiores (Mykoniati, et. al., 2003).

Outra tecnologia de rede IP atualmente bastante utilizada, denominada MPLS utiliza rótulos para tráfegos pré-determinados, principalmente considerando que tais rótulos determinam caminhos dentro de uma rede que originalmente não estão presentes nas tabelas de roteamento dos equipamentos (Trimintzios, et.al. 2001). Tais caminhos podem ser incorporados ao roteamento de uma rede IP e podem ser considerados caminhos preparados para determinados fluxos de dados (engenharia de tráfego). Embora o MPLS possa ser utilizado para organização de tráfego vinculado aos valores presentes na classificação de tráfego da arquitetura *DiffServ* (RFC 3302, Muezerie, 2005), e por conseqüência ser considerado como mecanismo de QoS, o MPLS não provê em si mecanismos para garantia de qualidade de serviço, além de não considerar o dispositivo do usuário em sua arquitetura.

Todos os métodos descritos não consideram características dinâmicas do tráfego, ou seja, não consideram o comportamento dinâmico das conexões e de suas inter-relações, assim como não consideram as características do serviço e sua localização, sendo que trabalhos que analisam o comportamento de sistemas de comunicação identificam que a localização e tipo de serviço influenciam o comportamento da rede (considerando desempenho e perfil de tráfego) (Barabási, 2007). Há trabalhos Sebuktekin, et.al. (2008) e Tommasi, Modenlini e Trico (2006) que propõem a união de técnicas e particularmente o uso do protocolo RSVP (*Resource Reservation Protocol*) para prover dinamicidade a estruturas de Qualidade de Serviço e para arquiteturas de qualidade de serviço que possam atuar entre diferentes domínios administrativos.

2.2.2 Arquiteturas de Qualidade de Serviço em redes sem fio

Segundo a norma ETSI 23.107 (ETSI, 2009a) as redes sem fio 3G/UMTS foram especificadas para oferecer serviços com níveis de qualidade apropriados, tendo como princípio as qualidade de serviço fim a fim, conforme explicitado na Figura 2. Na arquitetura UMTS um serviço de transporte define as características de qualidade de serviço entre os pontos finais da comunicação. E o serviço fim a fim pode ser visto como a composição de diversos serviços oferecidos entre cada uma das redes que compõem o sistema de rede utilizado (Vasconcelos, 2002).

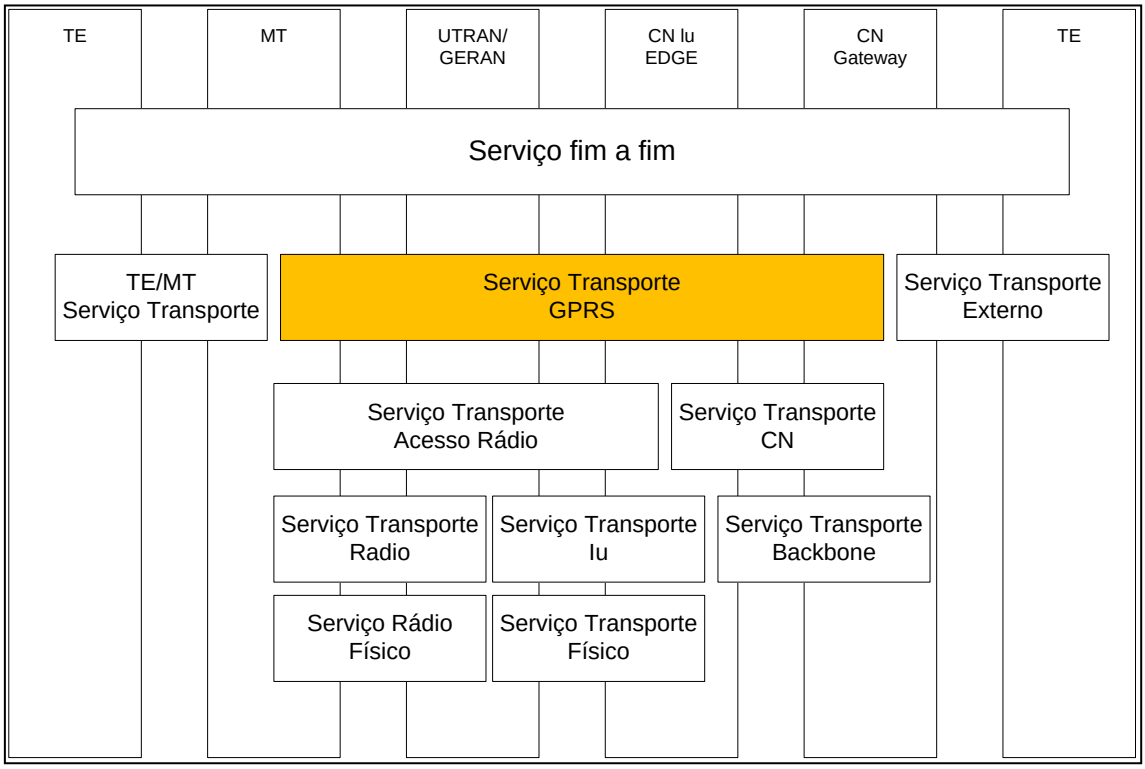

Figura 2 – Estrutura de Qualidade de Serviço proposta pelo 3GPP (ETSI, 2009b)

Embora não seja claramente separado na Figura 2, há duas camadas no sistema de transporte do UMTS as quais possuem funções de QoS. Na camada de controle há quatro serviços sendo:

- Gerente de serviços: responsável pelo estabelecimento, modificação e manutenção dos serviços dos quais é responsável, além de prover recursos para as funções da camada do usuário;

- Função de tradução: exercida entre os serviços internos do sistema de transporte UMTS e os protocolos das redes externas que possuem interface com a rede UMTS. A principal função é a tradução de atributos entre protocolos, incluindo os atributos de QoS;
- Controle de admissão e de capacidade: serviço que mantém dados sobre todos os recursos existentes na rede UMTS e sobre a quantidade desses recursos que estão alocados pelo sistema de transporte UMTS. Também é capaz de reservar recursos para serviços se esses forem alocados por um serviço de transporte UMTS;
- Controle de subscrição: utilizado para verificação se um determinado serviço de transporte possui privilégios de requisitar um serviço da infraestrutura UMTS com a qualidade de serviço especificada.

A camada do usuário tem como função manter a sinalização operacional e controlar o tráfego do usuário dentro de certos limites definidos pelos parâmetros de qualidade de serviço. As funções descritas a seguir devem prover com garantias os recursos alocados de acordo com a política de QoS (ETSI 2009a):

- Função de mapeamento: serviço de marcação que registra em cada unidade de dados a ser transmitida os padrões de QoS que o serviço de transporte deve utilizar;
- Função de classificação: atribui às unidades de dados do terminal móvel ao serviço de transporte adequado (quando o terminal possui mais de um serviço de transporte com o *Mobile Termination*[7] (MT));

[7] Mobile Termination (MT): ponto da rede UMTS onde o terminal do usuário conecta-se. O MT pode oferecer diversos serviços ao terminal do usuário, cada qual com um determinado serviço de transporte ativado.

- Gerente de recursos: distribui de acordo com os requisitos de qualidade de serviço os recursos entre os recursos;
- Condicionador de tráfego: mantém a conformidade entre os recursos definidos, via QoS, de um determinado serviço e os pacotes de dados utilizados pelo mesmo. Um pacote de dados que não conforme ou é descartado ou marcado como não conforme, e terá a preferência de descarte em caso de congestionamento;

Comparando-se as funções do plano do usuário e do plano de controle com o modelo DiffServ nota-se diversas similaridades e mecanismos que possuem comportamentos próximos àqueles encontrados na arquitetura IP, embora não seja necessariamente tráfego IP a ser enviado pela rede 3G/UMTS. Contudo a norma TS 23.207 recomende que o backbone da rede UTMS possa utilizar quaisquer tecnologias de transmissão e enlace, a camada três da rede de núcleo deve ser IP. (ETSI, 2009b) (Evangelista, Guardieiro, 2007).

Um ponto que se deve destacar da arquitetura de QoS proposta pela 3GPP é a participação do dispositivo do usuário final no controle de qualidade de serviço, pois o dispositivo do usuário final pode exercer a função de *DiffServ Edge Function*, ou seja, o dispositivo pode aplicar determinados comportamentos (PHB) aos pacotes de suas aplicações. Contudo, essa função não é obrigatória e depende de como o equipamento de borda da rede 3G/UMTS atua em relação à QoS. O dispositivo do usuário também pode atuar com sinalização RSVP dependendo novamente do cenário do equipamento de borda da rede 3G/UMTS. (ETSI, 2009b).

Embora este texto apresente apenas características de redes 3G/UMTS e de como a rede 3G/UMTS está relacionada com a tecnologia IP, os conceitos apresentados podem ser estendidos a outras tecnologias de redes sem fio como apresentado e proposto por Qiang; Romdhani e Turletti, 2004, Li, et.al. (2008), Tsigkas e Pavlidou (2008), Hafajee e Chan (2005).

2.2.2.1 Classes de tráfego e parâmetros de QoS em redes 3G/UMTS

Todo o tráfego que pode ser utilizado em redes 3G/UMTS ou em redes sem fio de um modo geral deve ser classificado em quatro categorias de tráfego (Chuah, Zhang, 2005), (ETSI, 2009a):

- Conversação: para conversações de tempo real que requerem baixo atraso fim a fim;
- *Streaming*: tráfego multimídia que deve ser entregue de modo contínuo e, geralmente, é assimétrico;
- Interativo: tráfego gerado por aplicações que em geral tem um ser humano ou outro equipamento efetuando requisições para um equipamento remoto, como aplicações de *m-commerce*, consulta a banco de dados e navegação na Internet, dentre outros.
- Classes *background*: aplicações que executam transferência de dados como troca de arquivos, mensagens tipo SMS ou MMS.

As classes de tráfego propostas para redes 3G/UMTS podem ser relacionadas com as categorias da arquitetura DiffServ conforme a tabela abaixo (Saad, El-Ghandour, Jehan; 2008), demonstrando a proximidade existente entre a arquitetura DiffServ e a arquitetura UMTS[8]:

Classes Qos UMTS	Classes DiffServ	Motivo
Conversação	EF	tráfego que requer baixo atraso e baixa variação de atraso
Streaming	AF/Classe 4	tráfego que requer baixa variação de atraso
Interativo	AF/Classe 3	trárego requer baixo atraso, mas pode ser superior ao atraso máximo da classe de Conversação
Background	AF/Classe 2, 3, ou *best effort*	não há requisitos para o tráfego, exceto confiabilidade

Tabela 1 – Relação entre Classes DiffServ e classes UMTS (Saad, El-Ghandour, Jehan; 2008)

Chuah e Zhang (2005) agrupam os diversos parâmetros de qualidade de serviço de redes 3G/UMTS em três categorias:

[8] Tal proximidade foi explorada em termos de simulação na estrutura montada para a prova de conceito desta tese, utilizando os códigos DSCP para classificação de tráfego.

- Atributos de atraso: atraso de transferência;
- Atributos de banda: máxima taxa de bits, taxa de bits garantida;
- Atributos de confiabilidade: ordenação de dados na entrega do tráfego, manipulação da prioridade de tráfego, dentre outros.

Na categorização não são levados em consideração parâmetros relacionados a descarte de dados, uma vez que para tráfegos conversacionais ou mesmo de *streaming* podem não ser considerados uma vez que não podem ser retransmitidos ou é desejável que não sejam. Isso pode estar relacionado com uma característica do dispositivo do usuário que pode apenas transmitir dados em *slots* de tempo determinados, e uma vez que tenha mais tráfego para ser transmitido do que é possível alocar no *slot* de tempo, tal tráfego é descartado já no dispositivo do usuário; e, portanto, não sendo considerado pela rede 3G/UMTS.

Ainda segundo Chuah e Zhang (2005) os requisitos para diversos tipos de tráfegos em redes 3G/UMTS podem ser agrupados conforme a Tabela 2:

Tolerante a erros	Conversação Voz e Vídeo	Mensagens de voz	Streaming Áudio e Vídeo	Fax
Intolerante a erros	Telnet, jogos interativos	e-commerce, WWW, navegação web	FTP, downloads	notificação de email
	Conversação (atraso << 1sec.)	**Interativo (atraso aprox. 1sec.)**	**Streaming (atraso < 10sec.)**	**Background (atraso > 10 sec.)**

Tabela 2 – Requisitos qualitativos de QoS (Chuah, Zhang, 2005 adaptado)

A norma TS 23.107 considera os valores da Tabela 3 para os diversos parâmetros de rede para as diversas classes de tráfego.

Classe de Tráfego	Classe Conversação	Classe Streaming	Classe Interativa	Classe Background
Máxima taxa Transferência (kbps)	< 2048	< 2048	< 2048	< 2048
Maximo SDU	< =1500	< =1500	< =1500	< =1500
Taxa de Transferência (ms)	100 (máximo)	250 (máximo)	----------	----------
Taxa Garantida (kbps)	< 2048	< 2048	----------	----------

Tabela 3 – Parâmetros característicos em relação às classes de tráfego UMTS (ETSI, 2009a, adaptado)

Uma análise conjunta da Tabela 2, Tabela 3 e Tabela 4 indica os valores dos parâmetros de rede necessários para a prestação de um determinado conjunto de serviços. Logo, uma arquitetura de qualidade de serviço deve prever mecanismos que possam executar o controle fim a fim e manter os valores em faixas adequadas de acordo com os valores anteriormente explicitados.

Embora diversos parâmetros das tabelas apresentadas tenham sido elaboradas para o âmbito de redes 3G/UMTS há alguns parâmetros que são comuns a toda e qualquer sistema de comunicação, como o atraso, banda e taxa de transferência. Dessa forma, pode-se também considerar os valores característicos propostos por Chuah e Zhang (2005) conforme a tabela a seguir.

Meio	Aplicação	Grau de simetria	Taxa de transmissão	Parâmetros de Performance		
				Atraso fim a fim	Variação de Atraso	Perda de Informação
Áudio	Conversação de voz	two-way	4-25kbps	< 150ms	< 1ms	< 3%
Vídeo	Video fone	two-way	32-384 kbps	< 150ms		< 3%
Dados	tráfego de controle	two-way	< 28,8 kbps	< 250ms	N/A	Zero
Dados	Jogos interativos	two-way	< 1kbps	< 250ms	N/A	Zero
Dados	Telnet	two-way (simétrico)	< 1kbps	< 250 ms	N/A	Zero

Tabela 4 – Requisitos de QoS para redes UMTS (Chuah, Zhang, 2005 adaptado)

2.3 ASPECTOS DO CONTRATO DE QUALIDADE DE SERVIÇO CENTRADO NO USUÁRIO (USLA)

Embora o modelo predominante nos sistemas de comunicação baseados na tecnologia IP seja o de melhor esforço (*best effort*), há um claro movimento para que essas mesmas redes possam trabalhar com diferentes níveis de QoS, pois entre diversos motivos, os provedores de serviço necessitam de acordos de QoS para entregar conteúdos multimídia e serviços interativos ou não, como sistemas de comunicação por voz e vídeo sob demanda, dentre outros. Segundo Serra (2007) pode se considerar um próximo passo preparar e habilitar os clientes a influenciar o comportamento e as configurações dos

serviços que são entregues, de forma a se cumprir as especificações do USLA. Esse novo passo é denominado nesse trabalho de Gerenciamento de Serviço do Usuário Final e sua meta é manter a qualidade do serviço sob a perspectiva do usuário final, sendo necessário ter-se qualidade de serviço fim a fim e bidirecional como define Verma (1999), onde QoS bidirecional é: "... definida entre pares de organizações para se ter um relacionamento simbiótico. Nesses casos cada organização tem duas funções simultaneamente: ela é provedora de seu próprio serviço e consumidora dos serviços da outra organização. O USLA constitui o fundamento legal para a entrega do serviço". Além do aspecto da qualidade fim-a-fim, deve ser considerado que caso o dispositivo do usuário detecte que o caminho entre ele e a rede de acesso não seja satisfatório, que esse possa alterar o caminho utilizado, independentemente da tecnologia de acesso utilizada, ou seja, o caminho pode ser provido por uma ou mais redes de acesso com tecnologias distintas, o que pressupõe mecanismos de *handover*. A arquitetura de QoS deve ser capaz de oferecer dados suficientes para se executar o handover de acordo com as necessidades de qualidade de serviço.

Ainda segundo Verma (1999), o SLA deve ser utilizado tanto pelo provedor quanto pelo usuário final, pois ao mesmo tempo em que o SLA pode ser utilizado para orientar a prestação do serviço, também pode ser utilizado pelo usuário final para verificar a efetividade da prestação do serviço. Portanto, os seguintes componentes são típicos de um SLA (Verna, 1999), (Serra, 2007):

- A descrição do serviço que será provido;
- O desempenho esperado do serviço (através da especificação dos requisitos de qualidade);
- Um procedimento detalhado para manipulação dos problemas que possam ocorrer com o serviço;
- As conseqüências caso um provedor de serviço não atenda o nível de serviço contratado;
- Uma descrição sob quais condições o USLA não se aplica.

2.4 QUALIDADE DE SERVIÇO EM NGN

Na norma ITU M3060/Y2401 (2006) a redes NGN são apresentadas como capazes de "... entregar novos serviços que estão disponíveis em qualquer

lugar, em qualquer momento, através de qualquer dispositivo, e utilizando qualquer mecanismo de acesso escolhido pelo usuário". Para tal cenário ser possível há a necessidade de se ter mecanismos que garantam qualidade para a entrega do serviço solicitado pelo usuário segundo seu contrato de serviço. Por serviço entende-se o conceito utilizado na indústria de telecomunicações, o qual define que serviço de telecomunicações é "... um conjunto de informações do usuário e de capacidades de transmissão provido por um grupo de usuários e por um sistema de telecomunicações (ANS T1.523-2001, Telecom Glossary 2000). Os conteúdos podem ser de áudio, vídeo e conteúdos multimídia, interativos ou não, pois a única exigência é que o provedor do serviço de telecomunicações tenha capacidade de transmitir e entregar a mensagem.

2.4.1 Requisitos e Arquitetura de QoS em Redes de Nova Geração

Segundo a ITU-T (2006) a gestão de uma NGN deve considerar a determinação das fronteiras entre diversos domínios administrativos e possuir mecanismos e pontos de referência para identificação dos processos que trabalham em diferentes domínios administrativos. A recomendação também explicita que uma NGN deve possuir mecanismos que permitam a dispersão geográfica dos aspectos de controle de um sistema de gestão, como forma de melhorar o serviço e a interação com o usuário final. O serviço é considerado fim-a-fim e os mecanismos presentes na NGN devem garantir a qualidade fim-a-fim, ou seja: "... assegurar a capacidade de gerenciar, durante o seu ciclo de vida completo, os recursos da NGN, tanto físico quanto lógico. Isso inclui recursos na rede básica, rede de acesso, componentes interconectados e os seus clientes e redes de terminais." (ITU-T, 2006)

A ITU-T também propõe um conjunto de requisitos para um sistema de gestão de NGN, tais como (ITU, 2006):

- permitir uma entidade (empresa ou indivíduo) adotar múltiplas funções em diferentes redes e oferecer capacidade de continuidade de um serviço em caso de eventos que prejudiquem a capacidade da rede em continuar atendendo os serviços;
- permitir monitoração pró-ativa;

- ter capacidade de alocação de recursos fim-a-fim integrados e ter capacidade de alocar dinamicamente recursos na rede sem intervenção de terceiros;
- manter independência de gerenciamento e controle de um domínio administrativo, tendo a habilidade de trocar informações de gerenciamento através das fronteiras entre eles.

Dentre as arquiteturas propostas para NGN há o IMS que segundo Ward (2006) "... o IMS permite a convergência das redes através de aplicações agnósticas independentes das redes de acesso"; e um dos principais objetivos do padrão é: promover serviços IP de valor agregado utilizando diversas tecnologias de redes de acesso, suportando diversas aplicações para um usuário móvel com qualidade de serviço garantida entre diferentes redes de acesso (Koukoulidis, Shah; 2006).

A arquitetura IMS é composta de três camadas: plano de aplicação, plano de controle e plano de usuário (Camarillo, Garcia-Marti´n, 2006). Na camada de controle, os componentes de uma arquitetura de controle de QoS devem lidar com um ambiente heterogêneo e deve ter um conjunto de funcionalidades na camada de controle especificado no padrão. Os conceitos presentes na camada de controle do IMS discutidos na tese são (ETSI, 2009c):

- *User Equipment* (UE): funcionalidades relacionadas ao dispositivo do usuário;
- *Call State Control Functions* (CSCF): funcionalidades relacionadas ao controle da sessão do usuário;
- *Home Subscriber Service* (HSS): controla o perfil do usuário;
- *Policy Decision Function* (PDF): relacionado com decisão sobre o tráfego de QoS;
- *Media Gateway* (MG): conversão de formatos e protocolos para que um determinado fluxo de dados seja utilizado em uma determinada de rede de transmissão.

O CSCF ainda pode ser dividido em diversos elementos *-CSCF como identificado na figura 3. O *Proxy*-CSCF (P-CSCF) é o ponto de contato entre o

terminal do usuário e a rede IMS e tem como função registrar o terminal, traduzir mensagens entre o terminal e a rede IMS, assim como pode prover funcionalidades de segurança. O elemento Policy Decision Function (PDF) atrelado ao P-CSCF tem importante papel nas recomendações para mecanismos de qualidade de serviço em redes IMS, pois é responsável pela alocação de recursos para um determinado serviço (Camarillo, Garcia-Marti´n, 2006).

O *Interrogation*-CSCF (I-CSCF) tem como principal função enviar as informações pertinentes dos usuário para o mecanismo de controle de serviço (geralmente o S-CSCF). O *Service*-CSCF (S-CSCF) essencialmente executa o controle do serviço, relacionando as informações do usuário presentes no *Home Subscriber System* (HSS) e controlando a seção do serviço (ETSI 2009a), (Camarillo, Garcia-Marti´n, 2006).

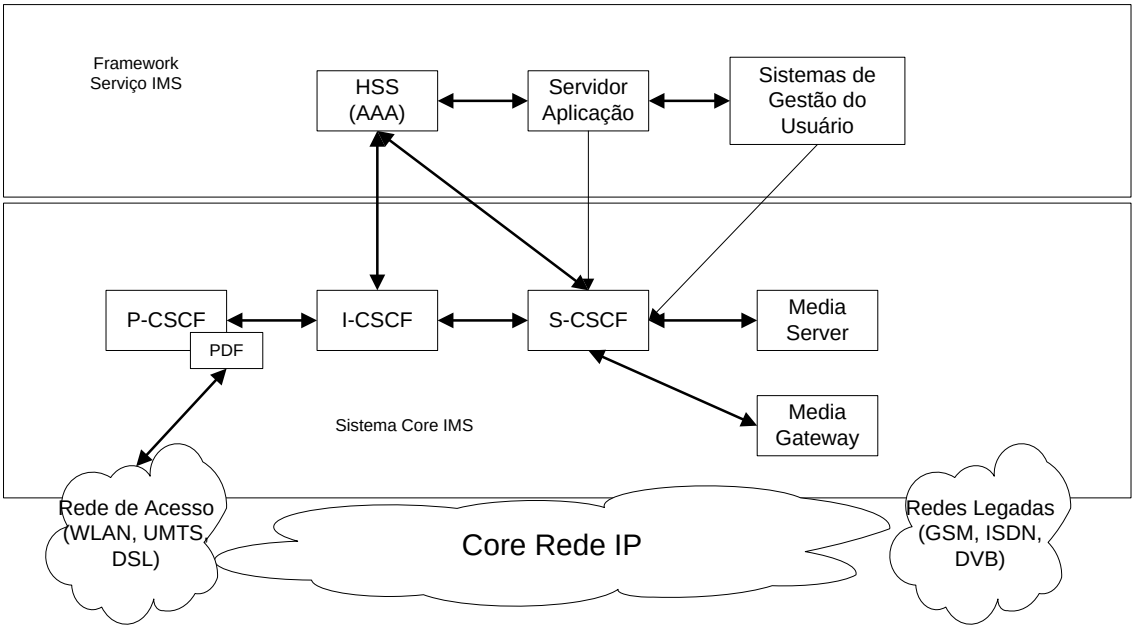

Figura 3 – Estrutura do IMS (Magedanz, Gouveia, 2006)

Todos os elementos CSCF são elementos de controle e são baseados em mensagens SIP. Também devem ser replicados na rede de tal forma a proverem recursos para atender a demanda de serviços, assim como devem guardar relação de independência, embora devam seguir uma política comum ao domínio administrativo a que pertencem. Contudo, diversos textos colocam

a arquitetura *DiffServ* como o deve prover qualidade de serviço no domínio administrativo através das informações oriundas dos elementos CSCF.

2.4.2 Qualidade de serviços entre domínios administrativos

Segundo Verdi, et. al. (2006) ainda não é trocado nenhum tipo de informação de qualidade de serviço e engenharia de tráfego entre domínios administrativos[9]. A necessidade em trocar tais informações está na prestação de um serviço com qualidade de serviço fim-a-fim como atualmente demandado por diversos tipos de organizações, assim como a necessidade de novas aplicações como *as Virtual Private LAN Services* apresentarem os mesmos requisitos de qualidade encontrados em redes corporativas (Martini, et.al, 2008).

Diversas propostas indicam que uma das formas de se trocar dados de qualidade de serviço e mesmo de engenharia de tráfego entre domínios administrativos é utilizar o protocolo de roteamento BGP, incluindo dados de QoS, em geral DSCP (indicando claramente a utilização da arquitetura DiffServ). (Griffin, et. al.; 2007). O uso do protocolo BGP mais informações de qualidade de serviço permitiriam manter os requisitos de qualidade de um tipo de serviço entre domínios, tendo como parâmetros de troca entre domínios administrativos os requisitos do serviço e como o serviço foi prestado nos domínios administrativos anteriores.

Kumar e Saraph (2006) propõem que além dos dados de qualidade de serviço sejam transmitidos pelo protocolo BGP, os rótulos MPLS também deveriam ser trocados como forma de se ter *Virtual Private Networks* estabelecidas entre domínios administrativos distintos. Mellouk, Zeadally e Mueller (2008) pontuam a importância dessa troca de informações entre domínios administrativos, mas alertam para o fato da heterogeneidade aumentar a complexidade dessa troca de informações devido às diferenças entre tecnologias de rede.

---

[9] Na terminologia de roteamento BGP esses domínios administrativos são denominados Sistemas Autônomos.

O ponto comum de todas as argumentações está na necessidade de se trocar dados de qualidade de serviços entre domínios administrativos, mas de tal forma a todos os sistemas de comunicação tenham entendimento comum dos parâmetros de qualidade aplicados às suas tecnologias.

2.5 COMPORTAMENTO DE TRÁFEGO EM SISTEMAS DE COMUNICAÇÃO BASEADOS NO PROTOCOLO IP

Um sistema de controle de qualidade de serviço deve possuir mecanismos que o tornem capaz de determinar o estado e as demandas dos fluxos de dados, e, portanto conhecer as características dos fluxos de dados como forma de classificá-los.

De acordo com Kim; et. al. (2008) ainda não há uma melhor forma de como classificar o tráfego de um sistema de comunicação, sendo que diversas técnicas podem ser adotadas em decorrência do tipo de análise a ser feita. Segundo Kim; Wim e Um (2005) a abordagem de análise baseada em características de fluxo de dados é uma abordagem mais interessante para qualidade de serviço por ser possível interpretar parâmetros que influenciam cada tipo de fluxo de dados; uma vez que a abordagem baseada em portas (TCP/UDP) e por *payload* tratam de aspectos relacionados com assinatura de tráfego como forma de identificar o tipo de aplicação e a distribuição de tráfego na rede (Kim; et.al, 2008). De acordo com Vishwanath e Vahdat (2006) uma das técnicas para estimar e considerar a capacidade de um canal de comunicação (ou *link*[10]) a taxa de transferência, atraso e perda de pacotes.

Portanto, a abordagem de análise de fluxos de dados deste trabalho é feita por fluxo e os *links* são analisados por taxa de transferência (apresentada pelo fluxo de dados), atraso e perda de pacotes.

[10] Neste trabalho o termo link será utilizado para representar um trecho de um caminho de comunicação entre duas entidades por ser o termo mais empregado na literatura referenciada.

2.5.1 Caracterização de tráfego e de rotas na Internet

De acordo com Sinha; Papadopoulos e Heidemann (2007) a maior parte do tráfego da Internet possui tamanho de pacote entre 40 e 1500 bytes (40% e 20% respectivamente); sendo o restante de tamanho de pacotes distribuído de acordo com a função distribuição de probabilidades da Figura 4.

Nas análises de Kim; Won e Hong (2006) a duração de distribuição de fluxos dados TCP na Internet tem como média de 57,32 segundos, enquanto tráfegos UDP apresentam duração média de 10,72 segundos. Contudo, o número de fluxos de tráfego UDP é 3,4 vezes maior do que o tráfego TCP. A maioria dos fluxos de dados TCP ou UDP apresenta fluxos menores do que 1000 bytes, por se tratarem em geral de aplicações como mensagens instantâneas e transferência de arquivos via *peer-to-peer*. Considerando fluxo de dados VoIP tem-se que o tamanho de um pacote pode variar entre 80 bytes e 480 bytes para o codec G.711 e pacotes de fluxo de dados vídeo (MPEG-1) tem tamanho entre 1025 bytes e 1518 bytes para 50% dos pacotes gerados por uma transmissão de vídeo (Calyam, Leem, 2005), (Toral; et.al.; 2008).

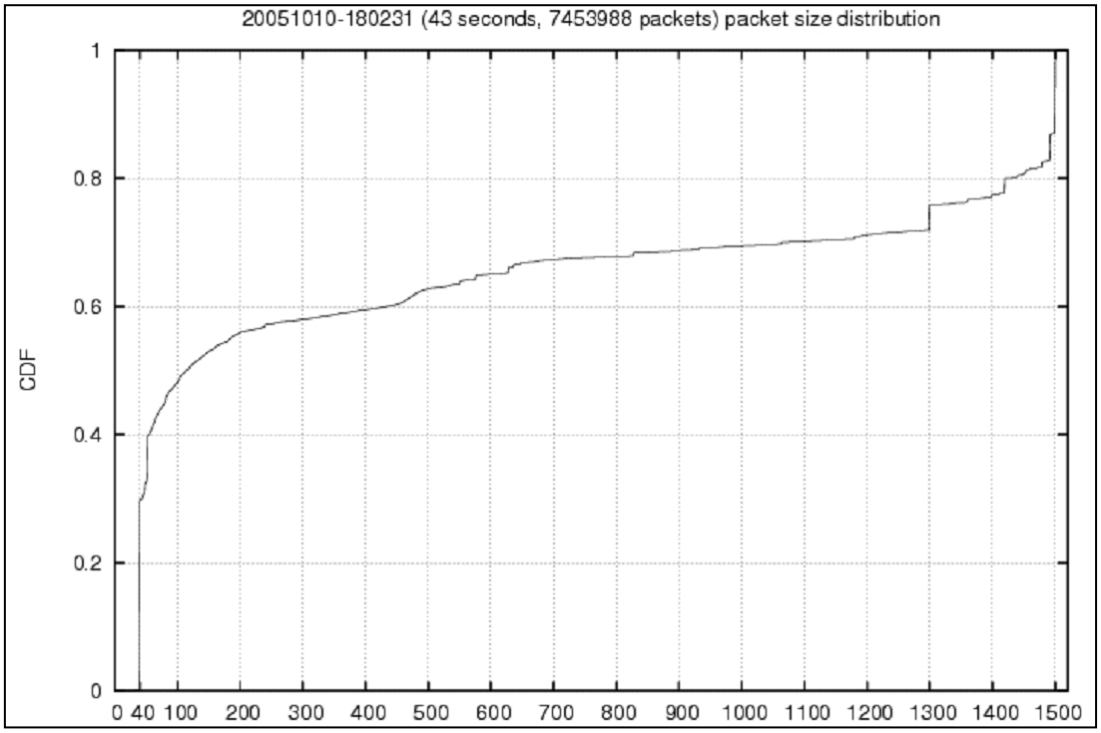

Figura 4 – Função distribuição de probabilidade de tamanho de pacotes na Internet (Sinha, Papadopoulos, Heidemann; 2007)

Sobre as rotas na Internet constatou-se que a maioria não é persistente, sendo que a maior parte dos caminhos são “*prevalence*”, ou seja, a rota (completa) é provavelmente conhecida. Essas rotas tem persistência desde alguns segundos até dias (Paxson, 2006). Logo, os caminhos na Internet podem sofrer mudanças sem que isso prejudique ou impossibilite a comunicação entre dois pontos finais.

3 ARQUITETURAS DISTRIBUÍDAS E SISTEMAS MULTIAGENTES

Apesar de diversos trabalhos ((Mellouk, Zeadally, Mueller; 2008), (Marques, Aguiar, Chaher, 2003), (Horlait, Rouhana, 2000), dentre outros) discutirem e proporem mecanismos de QoS fim a fim, a maioria não considera o dispositivo do usuário final como elemento ativo da arquitetura de controle de qualidade de serviço; e consideram que o caminho em que se pode controlar a qualidade está restrito até a rede de acesso, uma vez que o dispositivo do usuário final não tem condições de tratar qualidade, principalmente porque só possui um tipo de conexão. Neste tese admite-se um dispositivo do usuário final capaz de negociar requisitos serviços, e desta forma há elementos de controle de qualidade de serviço distribuídos em diversos pontos do sistema de comunicação, similar ao proposto nas especificações de redes IMS (ETSI, 2009b).

Uma abordagem distribuída de QoS deve considerar as seguintes características: (Bellavista, Corradi, Stefanelli, 2003), (Aurrecoechea, 1998), (AMIDST, 1999), (ETSI, 2009a), (Ward, et.al. 2006):

- monitoração do QoS: monitorar e gerenciar serviço de componentes de acordo com o contrato de SLA;
- localização: permitir decisões em tempo de execução baseadas na topologia de rede e os recursos envolvidos;
- adaptação ao domínio: conciliar a distribuição do serviço e as mudanças dinâmicas do ambiente;
- adaptação dos parâmetros: conciliar e traduzir os requisitos do usuário em parâmetros de QoS para cada tecnologia de rede;
- transparência: aplicações não consideram a complexidade nem do gerenciamento tampouco do controle de QoS;
- princípio da integração: QoS é uma relação entre duas ou mais aplicações (levando em consideração os requisitos do usuário). Para

isso, o QoS deve ser configurável, previsível e sustentável para satisfazer todas as camadas ao longo do caminho fim-a-fim;

- princípio da separação: os serviços são compostos por diversas partes relacionadas, onde algumas podem estar localizadas em diferentes camadas da comunicação infra-estrutura. Da mesma forma, o gerenciamento e controle de QoS e a transferência dos dados são mecanismos distintos e podem se valer de um *middleware* para sua integração.

Entende-se por middleware como uma camada de software projetada para auxiliar no gerenciamento da complexidade e da heterogeneidade características de sistemas distribuídos, oferecendo soluções para interoperabilidade, segurança, dentre outros (Issarny, Caporuscio, Georgantas, 2007). Logo, as abstrações de programação oferecidas pelo *middleware* podem prover transparência com respeito à distribuição em uma ou mais das seguintes dimensões: localização, concorrência, replicação, falha e mobilidade. Também é possível ver o *middleware* como um elemento de interoperabilidade entre sistemas heterogêneos no sentido de permitir que aplicações de negócio comuniquem-se de maneira transparente, independente de sua infra-estrutura computacional (interfaces, protocolos de comunicação, sistemas operacionais ou plataformas de hardware) (Maia, 2006).

Uma sociedade multiagentes pode ser interpretada como um *middleware*, e o uso de agentes como proposto por Fok; Roman e Lu (2009) e Lynch e Pesch (2009), bem como suas sociedades, possuem as características consideradas essenciais em um *middleware*. Porém, agentes e sociedades multiagentes apresentam propriedades que não são consideradas essenciais em um *middleware*, e que podem ser de grande valia para sistemas distribuídos.

Embora não haja total concordância em torno de uma única definição para o que seja um agente, há algumas definições de referência a muitos estudos bastante aceitas, como a proposta por Shohan (Bradshaw, 1997) ou por Russel e Norvig (2004) como agente sendo uma entidade de software que funciona de forma contínua e autônoma e vinculado a um determinado ambiente. Pode-se também abordar como Wooldridge e Jennings (1995) e Wooldridge (2002), que

define um agente como uma entidade encapsulada capaz de resolver problemas, ou como Laurel (1997): “um agente é uma personagem, encenada pelo computador, que age representando os interesses de um usuário no ambiente virtual”. Segundo Nwana (1996), “um agente refere-se a um componente de software ou hardware que é capaz de executar tarefas em nome do usuário”.

O ponto comum e importante de todas as definições é o fato de colocar um agente como uma entidade autônoma, sem a intervenção do ser humano ou outros sistemas, em todo ou na maior parte do tempo de operação. A autonomia, bem como outras características que um agente pode apresentar (como reatividade, continuidade e capacidade de inferência, dentre outros) podem ser atribuídas a um agente considerando o meio onde este se encontra, pois o ambiente pode ser definido como a estrutura onde o agente realiza suas ações e percebe (ou recebe) sinais enviados pelas entidades com as quais se relaciona ou que de alguma forma o influenciam.

Analisando-se diversas propostas de tipos de agentes, duas possíveis arquiteturas abstratas podem ser definidas:

- agentes puramente reativos: são aqueles que executam uma ação baseada exclusivamente na observação feita, sendo a decisão tomada com base apenas na mudança de estado do ambiente (no instante da observação), sem considerar a história;
- agentes baseados em estados internos: possuem uma máquina de estados, responsável por determinar as ações do agente no meio.

Os agentes com estados internos ainda podem ser divididos em agentes com percepção e agentes com percepção e modelos de mundo.

Há tarefas que um único agente não pode solucionar sozinho, pois não possui toda a habilidade e o conhecimento necessário ou lhe falta algum recurso, não importando qual arquitetura ou tipo de agente seja desenvolvido. Segundo Jennings e Wooldridge (1995) e Cucurull, et.al. (2009) o paradigma de desenvolvimento de agentes e sistemas multiagentes apresenta como características marcantes componentes auto-suficientes e com capacidade de interação entre componentes similares. Embora não haja a exigência de uma

comunicação através de interfaces pré-determinadas, o sistema deve contar com um mecanismo de negociação entre os agentes, tanto para realizar acordos de tarefas que devam ser realizadas quanto para informar e comunicar uma ação. Isto pressupõe alguma troca de mensagens e, portanto o estabelecimento de protocolos.

Os sistemas compostos de muitos agentes, ou sistemas multiagentes propiciam o surgimento de comportamentos globais não programados em nenhum dos agentes que fazem parte do sistema (Mařík, Lažanský; 2007). Contudo, a conseqüência do surgimento de comportamentos não programados estão na incerteza dos resultados que serão alcançados pelo conjunto de agentes (ou sociedade de agentes), dado que tal sociedade não possui um controle centralizado e, portanto o sistema opera conforme as evoluções individuais dos agentes. Isto acontece porque os agentes são autônomos e possuem interesses próprios, ou seja, seguem as ações que os levem a alcançar seus objetivos. Neste ponto temos que ou os agentes trabalham de forma cooperativa, ou seja, em conjunto para atingir objetivos próprios ou então trabalham individualmente, em busca apenas de seus interesses (Huhns, 1999), (Rezende, Prati; 2003).

3.1 COMPARAÇÃO ENTRE AGENTES E *MIDDLEWARE*

Quando se utiliza o termo *middleware*, independentemente de sua plataforma de desenvolvimento ou operação, espera-se encontrar algumas características, as quais serão confrontadas com o paradigma multiagentes. As características de *middleware* que serão discutidas são:

- facilidades de comunicação;
- identificação e localização (*naming*);
- persistência;
- transações distribuídas;
- segurança.

3.1.1 Facilidades de Comunicação

As facilidades de comunicação são essenciais a um *middleware*, e podem ser entendidas como um serviço que oferece o transporte de mensagens entre

duas entidades, sendo que a aplicação não necessita conhecer os detalhes de como esta comunicação é feita (Tanembaum, Steem, 2002). Da mesma forma, as facilidades de comunicação em uma sociedade multiagentes podem ser desenvolvidas de diversas formas. Porém, a infra-estrutura necessária para o estabelecimento dos agentes deve prover mecanismos reguladores de comunicação, protocolos para organização das mensagens, e padrões de linguagem necessários para o entendimento dos agentes.

Os mecanismos reguladores da comunicação podem ser síncronos ou assíncronos, tendo três aspectos para caracterizar plenamente a comunicação (Weiss, 1999), (Bentahar, 2005):

- a sintaxe: estruturação dos símbolos;
- a semântica: o significado dos símbolos;
- e a pragmática: a veracidade da informação.

Na comunicação entre agentes, também há dois tipos protocolos de comunicação necessários para o entendimento entre os agentes: coordenação e cooperação. (Huns, 1999). Os protocolos de coordenação são utilizados com o intuito de melhorar o desempenho da sociedade multiagentes, permitindo a melhor utilização dos recursos disponíveis no ambiente, e informando quais tarefas estão sendo executadas. Já os protocolos de cooperação são aqueles que permitem a distribuição de tarefas, bem como sua decomposição em unidades menores, requerendo assim soluções mais simples, as quais podem ser executadas por agentes menos sofisticados. Porém, o controle desta distribuição deve garantir que a decomposição não sobrecarregue os agentes, ou possa exaurir recursos críticos do ambiente de execução de um agente, uma vez que normalmente existem em quantidade limitada de recursos em se considerando dispositivos como PDAs e telefones celulares.

Embora a comunicação seja um importante aspecto de *middleware*, é necessário avaliar os mecanismos de interação entre uma aplicação e o sistema multiagentes (Mařík, Lažanský; 2007), (Bellifemine, et.al., 2008). Assim como um *middleware*, o sistema multiagentes necessita de uma interface com a aplicação, e como pode ocorrer em um *middleware*, a sociedade multiagentes não obriga que todas as entidades que a compõem utilizem a mesma interface de comunicação entre aplicação e agente, pois podem existir

agentes especializados em interagir com aplicações legadas e fazer a tradução e encaminhamento das solicitações para os demais agentes, como mostra a Figura 5. A figura explicita que um agente possui uma ou mais interfaces com os sistemas legados em que atua (legenda interfaces com legado na figura) e interfaces entre sistemas dos quais recebem e enviam dados (interface Sistema X e Y). E ainda há a interface com o sistema multiagentes (interface MAS) pela qual um agente participa da sociedade de agentes. Contudo, entre os agentes a interface e mecanismos de comunicação devem ser comuns.

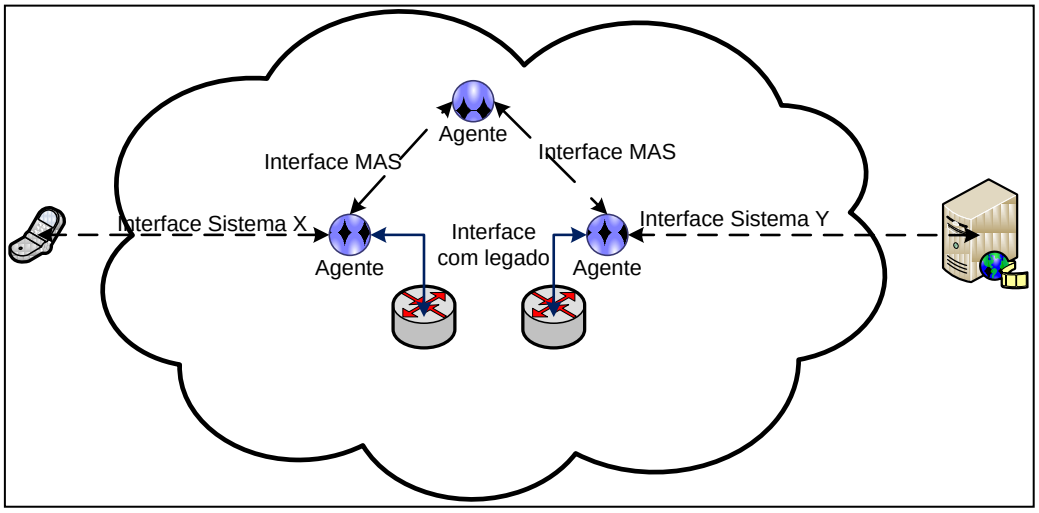

Figura 5 – Serviços em uma sociedade multiagentes

3.1.2 Identificação e Localização

O serviço de identificação e localização pode ser definido como a forma pela qual as entidades compartilham recursos e se localizam em um sistema distribuído. Em um middleware orientado a objetos há dois conceitos importantes que lidam com a questão de localização: *proxy* e *broker*.

O *proxy* pode ser entendido como um intermediário entre o cliente e o processo servidor (também denominado *servant*), o qual pode existir em ambas as extremidades de comunicação e possui como função básica a transparência de localização dos componentes de uma aplicação e qualquer outro detalhe de localização, comunicação e protocolo (Stal, 2002). Porém o *proxy* possui como uma de suas características a pouca flexibilidade de localização de processos servidores, uma vez que os endereços destes processos precisam ser escritos no *proxy*. Para remover tal limitação tem-se a idéia do *broker*.

O *broker*, também chamado de “serviço de registro” é um centralizador de serviços de localização, e sua função é permitir que tanto processos servidores quanto clientes possam localizar uns aos outros. Uma vez feita esta localização, a comunicação ocorre sem a intervenção do *broker* (Stal, 2002), (Endrei, et. al., 2004).

Em sociedades multiagentes existe a necessidade de comunicação, porém o paradigma não especifica mecanismos para que esta comunicação ocorra. Contudo, há diversas arquiteturas de sociedades multiagentes que oferecem as estruturas necessárias à comunicação de agentes. Atualmente existe um consórcio denominado FIPA (*Foundation for Intelligent Physical Agents*) cuja missão é desenvolver padrões para agentes tendo como foco a interoperabilidade. (FIPA, 2008a), (Greenwood, et.al., 2007). É importante frisar que a FIPA não define como devem ser desenvolvidos os mecanismos de localização e de mensagens de uma sociedade multiagentes, contudo, define três mecanismos que oferecem suporte ao ambiente dos agentes: *Service-root*, Diretório de agentes e Diretório de serviços.

Quando um agente é iniciado (ou criado), o agente notifica sua existência a um agente denominado *service-root*, que possuirá o localizador de serviços disponíveis no ambiente, e cuja responsabilidade é gerenciar o ciclo de vida do agente e auxiliará este a utilizar os recursos do meio.

O serviço “diretório de agentes” é o local onde os agentes, ao serem ativados, registram-se. Isto é feito pelo *service-root*. Os dados obrigatórios são o nome (*agent-name*), único em toda sociedade multiagentes, e pelo menos um localizador (*agent locator*), o qual possui o tipo de transporte e o endereço para atingir o agente. A estrutura do “diretório de agentes” ainda pode conter outros atributos, como a descrição dos serviços dos agentes e suas restrições, dentre outros (FIPA, 2008c).

Já o serviço de “diretório de serviços” possui como função fornecer os significados de cada serviço presente no ambiente de forma não ambígua e mantendo a coerência entre os agentes. Este serviço não substitui o anterior, mas o complementa, uma vez que suas descrições fazem com que agentes o consultem e acessem o “diretório de agentes” procurando por aqueles que possuem a especificação do serviço desejado. Cabe destacar que o diretório

de serviços é uma referência para os agentes e não se presta a prover serviço ao usuário final do contexto desta tese.

3.1.3 Persistência

Em um middleware, persistência significa prover facilidades de armazenamento, que podem ser desenvolvidas por serviços de diretórios, bancos de dados, ou outras tecnologias.

Um agente vale-se das mesmas ferramentas de um middleware para persistência de dados, ou seja, um agente, localizado em algum local provido de um sistema de armazenamento de dados pode armazenar determinadas informações para seu usuário, ou ainda um agente pode conversar com um sistema gerenciador de banco de dados para que este armazene os dados de uma transação qualquer.

Porém, um agente possui uma característica relevante que não é visto em geral em um middleware: a continuidade temporal de um agente. Isto significa que ele pode permanecer desativado por certo período, durante o qual mantém seus estados internos, e que ao ser reativado retomará como seu estado inicial o mesmo estado imediatamente anterior à desativação, ou seja, o agente reinicia seu processamento do ponto exato onde parou. Esta característica é importante, pois garante que o conhecimento adquirido pelo agente seja mantido e possa ser restabelecido quando este for reativado.

3.1.4 Transações Distribuídas e gerenciamento de recursos

Pode-se definir transações distribuídas como operações que ocorrem em diferentes locais de forma atômica, ou seja, ou todas as operações são executadas corretamente ou, se uma operação falhar, então todas as demais operações são desfeitas. (Tanembaum, 2002); (Vinoski, 2004). Diversas arquiteturas de *middleware* possuem essa característica, e segundo Emmerich (2000), há uma categoria denominada "*Transactional Middleware*" cuja principal característica é: "suporte a transações envolvendo componentes que rodam em servidores distribuídos".

As principais características para se ter capacidade de prover transações distribuídas são (Emmerich, 2000):

- Rede de comunicação: meio pelo qual os componentes se comunicam;
- Coordenação: cliente pode pedir serviços a terceiros de forma síncrona ou assíncrona e ter uma forma de estabelecer uma seqüência de operações para se obter o resultado esperado;
- Confiabilidade: garantir que ou toda a transação é feita ou nada é feito;
- Crescimento escalar: suporte à replicação e balanceamento de carga entre os participantes da transação;
- Heterogeneidade: componentes podem trabalhar sob diversas plataformas de software, sistemas operacionais ou hardware, sem prejuízo para a aplicação (de forma transparente).

Em sociedades multiagentes, todos estes conceitos e características estão presentes no que é denominado “mecanismo de cooperação”. Há pelo menos três modos de cooperação entre sistemas multiagentes: mercado, quadro de avisos e redes de contrato. (Weiss, 1999).

No mecanismo de cooperação conhecido como “mercado”, cada tarefa possui um preço, e cada agente pode ser classificado como:

- produtor: aquele que transforma um bem (“de capital” ou livres) [11] em outro bem diferente do bem original;
- consumidor: aquele que troca bens.

[11] Segundo Houaiss (2009) bens de capital são: ... ...“bens intermediários, que servem para a produção de outros, como matérias-primas, aço etc. e bens livres são “... passiveis de repartição ou separação sem que sua substância ou sua estrutura de altere sem perda de sua função original”.

O objetivo de cada agente é atingir seus objetivos com o maior lucro[12] nas operações. Cada um dos agentes oferta suas habilidades em um serviço de anúncios (como um serviço de diretório, por exemplo), e quando um agente solicita a realização de determinada tarefa, este deve “pagar o preço” estipulado. Esta é a forma que os agentes possuem para alcançar o objetivo. Entendem-se por preço um atributo ou atividade que um agente contratante de um serviço deve fornecer ao agente contratado para que esse último execute o serviço requerido (Jungir, Rumo, Teor, 2007), (Das, et. al.,2007).

Já no mecanismo de “quadro de avisos” (*blackboard*) os agentes publicam as tarefas demandadas para que todos possam consultá-las. Qualquer agente que provê algum serviço verifica o quadro à procura de alguma tarefa que possa realizar (compatível com suas habilidades e recursos). Achando-a, ele executa a tarefa e publica o resultado do trabalho no mesmo quadro. Este sistema prevê que um agente pode não conseguir realizar a demanda por completo, e neste caso sua contribuição é publicada e algum outro agente pode continuar o trabalho (Huhns, 1999).

Note que o mecanismo de quadro de avisos opera publicando necessidades, enquanto o de mercado trabalha oferecendo serviços a determinados preços. Pode-se colocar como vantagem do quadro de avisos a independência de especialidades dos agentes e a diversidade de técnicas de solução para um determinado pedido, uma vez que os agentes podem contribuir com parte da solução, ou mesmo gerar uma solução incremental. Necessariamente, ambos os mecanismos ou qualquer outro da categoria deve manter uma comunicação padrão entre os agentes, embora o sistema de quadro de avisos permita flexibilidade na representação das informações, ou seja, diversas ontologias, desde que o protocolo seja seguido e a ontologia publicada e utilizada pelos agentes.

Outro mecanismo que pode ser utilizado é a rede de contratos, onde o agente que possui uma tarefa a ser realizada é chamado gerente, enquanto aqueles que executam a tarefa são os contratados. O gerente deve anunciar o

[12] Lucro significa maior eficiência na realização das tarefas.

que deve ser feito, e cada contratado que possuir as condições de execução envia sua proposta. Cabe ao gerente analisá-las e associar um contrato a um determinado agente, que executará o serviço. Um agente pode ser gerente e um prestador de serviços simultaneamente, desde que de tarefas distintas, uma vez que não apresenta sentido um auto-contrato, pois este tipo de demanda é resolvida pelo próprio agente. Novamente, o agente deve sempre avaliar suas condições de realizar a proposta feita antes de oferecê-la (Weiss, 1999), (FIPA, 2008b).

Em todas essas arquiteturas, um pedido de tarefa pode não ser realizado, pois os agentes com as habilidades necessárias para a solução podem não estar disponíveis, ou já comprometidos com outras demandas. Pode ocorrer também, nos casos das redes de contrato, que os agentes estejam ainda esperando respostas de propostas que foram feitas e que sejam mais importantes e, portanto simplesmente não respondem, uma vez que se ambas as propostas forem aceitas, não haverá recursos suficientes para realizá-las. Nesta configuração da sociedade de agentes, pode-se dizer que não há recurso algum disponível e, embora esta situação de recursos exauridos (*starvation*) possa ser passageira, pode ocorrer o colapso da sociedade, uma vez que esta pode não ser capaz de realizar nenhuma outra tarefa. Uma forma de se resolver esta situação é existir um agente supervisor, cuja função é detectar *deadlocks* ou falta de recursos, além de buscar formas de solução para este tipo de situação. Como ele apenas deve atuar em situações que exigem solução de impasse apenas e não atua na prestação de serviço pelo agente, não se pode afirmar que ocorre centralização quando há um agente supervisor, mas sim que existe um serviço de supervisão (que mantém a autonomia dos agentes) no ambiente multiagentes.

3.2 QUALIDADE DE SERVIÇO SOB A PERSPECTIVA DE AGENTES

De acordo com Jamalipours (2005): "… o suporte de QoS fim a fim em redes heterogêneas e móveis com tráfegos IP e multimídia requer a colaboração eficiente entre diversas redes que estão envolvidas no caminho de comunicação fim a fim." Portanto, uma forma de se estabelecer esse caminho de QoS é haver um conjunto de controles distribuídos que negociem entre si

trechos do caminho que ofereçam garantias de cumprimento do QoS. Para levantamento e acompanhamento do caminho os agentes podem utilizar diversos modelos para calcular a disponibilidade de recursos e a previsibilidade dos mesmos. A abordagem multiagentes possui mecanismos de comunicação e negociação capazes de estabelecer caminhos em uma rede de dados e apresentar arquiteturas flexíveis para reagir em caso de falha ou mesmo adaptar-se às flutuações de rede (Chen, Cheng, Palen, 2009), sendo essa flexibilidade e robustez advêm da capacidade de cada agente em um sistema multiagentes tomar decisões baseados tanto em dados históricos quanto no estado da infraestrutura local quanto de apenas um nó; e ainda pode ter como objetivo a otimização dos recursos da rede (ou do nó) dependendo de seus objetivos, algoritmos de tomada de decisão e negociação (Adler, et.al., 2005). Isso significa que um agente é capaz de executar operações de engenharia de tráfego, manipulação e processamento de dados de tal forma a monitorar e controlar a qualidade de serviço (Chen, Cheng, Palen, 2009), (Tang, Jin, 2009), (Kone, 1998). Baschieri (2002) propõe o uso de agentes móveis e de sociedades multiagentes como *middleware* para aplicações de QoS que oferecem acesso ubíquo, ou seja, os agentes podem manipular conteúdos (ou fluxos) de qualquer origem de acordo com seus parâmetros, e monitorar as condições do caminho e prover correções se necessário. Manvi (2004) destaca outras características consideradas obrigatórias para um agente ser utilizado no ambiente de telecomunicações:

- autonomia;
- capacidade de tomar decisões;
- continuidade temporal;

É relevante destacar em Fok, et.al. (2009) que sociedades multiagentes provêm duas características importantes para arquiteturas de qualidade de serviços. A primeira característica é o crescimento escalar que pode ser alcançado por uma sociedade multiagentes, pois podem ser colocados outros agentes na rede enquanto ela cresce. A segunda característica é a tolerância a falhas, pois caso um equipamento de rede falhe, o agente pode se mover (independentemente) para outro nó de rede e continuar executando suas

tarefas, e caso o agente seja perdido, esse pode ser clonado e instalado em outro local da rede. O uso de agentes e sociedades multiagentes não substitui as tecnologias de QoS presentes em cada tipo de sistema de comunicação. A sociedade multiagentes pode ser utilizada para se ter uma visão comum de qualidade de serviço em toda a infra-estrutura heterogênea. Logo, uma sociedade multiagentes comporta-se como um *middleware* para as redes heterogêneas, de acordo com as funcionalidades e propriedades exigidas em um *middleware*. Para tal, é necessário que os agentes ofereçam uma interface para os sistemas de QoS (legados) e uma ontologia para prover um entendimento comum de parâmetros de QoS. No caso dessa tese, esse entendimento comum deve ser baseado em contratos de QoS denominados USLA. Logo, a sociedade multiagentes deve possuir as seguintes características:

- Agentes devem inter-operar com os componentes existentes nos sistemas legados ou com os novos sistemas que advirão;
- Agentes devem ser capazes de localizar os agentes mais próximos os quais ofereçam caminhos que atendam aos requisitos do contrato de QoS;
- Agentes devem ser capazes de negociar requisitos de QoS e construir caminhos que atendam aos requisitos do fluxo de dados a ser transmitido de tal forma a construir um caminho fim a fim;
- Alguns agentes devem gerenciar a sociedade multiagentes para evitar deadlocks e escassez de recursos e resolver tais tipos de questão quando essas forem detectadas;
- Agentes devem possuir mecanismos que controlem o cumprimento dos acordos de QoS estabelecidos entre os agentes.

A arquitetura multiagentes proposta nesta tese possui mecanismos para satisfazer as propriedades citadas e esses mecanismos devem prover controle de admissão com características similares ao proposto em Giri, et. al. (2009), onde o controle de admissão é distribuído e permita a decisão por se executar *handover* baseado em parâmetros de QoS.

4 UMA PROPOSTA DE ARQUITETURA MULTIAGENTES PARA CONTROLE DE QUALIDADE DE SERVIÇO EM REDES HETEROGÊNEAS

A arquitetura proposta tem como alicerces o paradigma de sociedades multiagentes e o paradigma de complexidade de redes proposto por Barabási e Albert (1999) (Dorogovtsev, Mendes e Samukhin, 2000), visto que a questão de qualidade de serviço possui a característica de ser distribuída e ter uma relação entre parâmetros e fluxos de dados ainda não claramente definida.

As atuais arquiteturas de qualidade de serviço podem ser aplicadas na maioria dos elementos de transmissão de dados de um sistema de comunicação; contudo esses elementos não atuam de forma autônoma por não determinarem ações de correção ou recuperação da qualidade de uma determinada classe de fluxo de dados e nem por poderem se adaptar às características dos fluxos de dados. Os esquemas de filas em interfaces utilizados em diversos equipamentos de comunicação seguem algoritmos que não consideram o perfil de tráfego e nem as condições locais do equipamento; em geral seguem um esquema de distribuição entre filas e priorização de tráfego padrão independentemente da localização e função dos equipamentos do sistema de comunicação (Odom, Cavanaugh, 2004). O paradigma multiagentes traz a autonomia e a capacidade de decisão para um elemento de um sistema de comunicação, além de propor mecanismos de negociação e comunicação entre elementos baseados nesse paradigma, o que permite a inter-operação entre elementos do ponto de vista de controle e de comum entendimento entre as decisões e solicitações geradas pelos agentes via definição de ontologias.

Embora existam diversos modelos para representação de redes complexas e redes livre de escalas, o modelo proposto por Barabási – Albert (Barabási, Albert, 1999) apresenta diversas características aderentes aos atuais sistemas de comunicação em relação à distribuição de conteúdos e distribuição de tráfego (Kurant, Thiran, 2006), (Meloni, et. al., 2008). Como os estudos de Xia, et. al. (2005); Barabási (2007) e Wang, et. al. (2006) indicam que tanto usuários possuem comportamentos que podem ser estimados quanto os provedores de

serviços também possuem uma demanda que pode ser estimada, ambos via uma distribuição *heavy tail*. Estima-se que o tráfego gerado e que deve ter qualidade controlada é reflexo desses comportamentos que podem ser estimados, com um agravante: não se tem em princípio a relação de como os parâmetros de um sistema de comunicação variam de acordo com os tipos de fluxos de dados e de suas quantidades. O modelo proposto por Barabási e Albert permite uma interpretação dos efeitos gerados pela interação dos fluxos de dados em um sistema de comunicação, como um mecanismo de recompensa e punição. Logo, aquele elemento que oferece melhor condição para um determinado tipo de fluxo de dados deverá ter preferência para transmissão em relação a outro elemento, desde que ambos possuam um caminho entre a origem e o destino do fluxo de dados. Esse conceito é denominado *rich get richer* ou *preferential attachment* (Barabási, Albert; 1999) (Barabási, 2003).

A contribuição da tese está em utilizar a abordagem multiagentes associado ao conceito de *preferential attachment* para que um elemento de um sistema de comunicação possa determinar qual deve ser o tratamento a ser despedido a um determinado tipo de fluxo de dados em um determinado momento de operação de tal forma a manipular a transmissão do fluxo de dados pelo canal mais apropriado e disponível. A arquitetura proposta também é adequada a um ambiente heterogêneo porque considera que dois elementos quaisquer possuem autonomia entre si, além de ter sua comunicação regida por uma ontologia; logo a comunicação entre domínios administrativos é considerada na arquitetura e para isso a ontologia deve definir o que deve ser trocado de informação de serviços e como os fluxos de dados a serem transmitidos podem percorrer o domínio administrativo. A arquitetura também considera o dispositivo do usuário final ativo na negociação e na decisão do tratamento do fluxo de dados a ser transmitido; podendo o agente do usuário optar por utilizar diferentes redes de acesso para diferentes tipos de tráfego de acordo com as condições oferecidas pelos provedores de acesso localizados na posição do usuário (novamente a aplicação do conceito *rich get richer* ou *preferential attachment*). O mesmo vale para os fluxos de dados entre sistemas autônomos, considerando que um sistema autônomo é uma coleção de um ou

mais domínios administrativos que compartilham a administração. Logo, os domínios administrativos, embora sejam independentes, compartilham um conjunto de regras. Esta idéia é similar ao que ocorre na segmentação de domínios de roteamento IP em um sistema autônomo de uma operadora de telecomunicações.

4.1 REQUISITOS DA ARQUITETURA DE CONTROLE DE QOS

Para se ter controle e tratamento dos fluxos de dados e manter interoperabilidade entre domínios administrativos é importante se ter uma forma de hierarquia de agentes para promover uma visão comum tanto do domínio administrativo ao qual o elemento controlado faz parte, quanto do conjunto de domínios administrativos que formam um sistema autônomo.

A arquitetura de controle de qualidade de serviço proposta considera o dispositivo do usuário final como um elemento ativo e integrante do controle de QoS. Portanto, o dispositivo final do usuário mede parâmetros da infraestrutura de comunicação constantemente e verifica se o contrato USLA está sendo respeitado. Caso não esteja, esse agente pode alterar a rede de acesso que esteja sendo utilizada, desde que o contrato de USLA preveja tal situação. É importante destacar que a infraestrutura não precisa ter registrado de antemão como é o contrato do dispositivo final do usuário, uma vez que ele é que controla o cumprimento do contrato, enquanto os demais agentes da infraestrutura trabalham em prol da política de QoS do domínio administrativo, executando ações de controle para que tal política seja respeitada.

Segundo Aurrecoechea (1998), uma arquitetura de controle de QoS deve apresentar os seguintes requisitos:

- Agendamento: agente deve ser capaz de gerenciar o agendamento de fluxos de dados;
- "*shapping*": o agente deve possuir técnicas de manipulação de fluxos de dados para regular a transmissão entre agentes;
- Monitoração (*policing*): agentes devem verificar se o contrato de QoS está sendo respeitado;

- Controle: agentes devem atuar em caso de alguma diferença ser detectada entre o acordo estabelecido e o executado;
- Sincronismo: mecanismos de controle de interações em fluxos multimídia, como ocorrem em canais de retorno.

Na arquitetura proposta os seguintes requisitos estão presentes:

- Tradução de QoS (ou mapeamento de QoS): agentes devem traduzir diferentes representações de QoS entre sistemas e tecnologias de QoS distintas;
- Controle de admissão: agentes deve verificar se os recursos requeridos por uma transmissão podem ser alocados e controlados;
- Monitoração de QoS: agentes devem verificar as condições de operação de qualquer classe de fluxo de dados que atravesse o equipamento monitorado;
- Manutenção e recuperação de QoS: se um agente detectar que os requisitos de QoS para uma classe de fluxos de dados não está sendo respeitados ou por alguma razão o caminho selecionado não possui recursos necessários durante a transmissão da classe de fluxo de dados, o agente deve agir de forma a encontrar outro caminho ou corrigir o caminho atual para que o fluxo continue a ser transmitido.

A arquitetura proposta deve possuir um mecanismo onde os agentes presentes no domínio administrativo no qual o fluxo de dados do usuário está sendo transportado possam informar as condições de QoS e anunciar suas capacidades, segundo o princípio do mecanismo de mercado. No domínio do problema da tese não é feita negociação propriamente dita, pois os agentes que representam uma determinada rede de acesso informam dados que servem de subsídios para o agente do dispositivo do usuário decidir qual rede de acesso utilizar. Portanto, no momento do acordo os agentes envolvidos devem ser agentes vizinhos, ou seja, entre agentes cujos equipamentos

possuam conexão direta uns com os outros em termos de roteamento[13], considerando como uma extremidade de comunicação o terminal do usuário.

Para a arquitetura ser efetiva é necessário que todos os agentes (provedor de serviço, operador de rede e do usuário) sigam conjuntos de regras de QoS que embora possam ser distintas, devem ter como mesmo princípio atender os requisitos de QoS em seu domínio de atuação. O provedor de serviços deve possuir um conjunto de regras que devem ser aplicadas em seu domínio administrativo para se estabelecer acordos de QoS. O agente responsável por essa atividade tem como função determinar qual política deve ser aplicada para cada tipo de fluxo de dados (requisitos do provedor de serviços).

O componente de QoS do terminal do usuário deve estabelecer verificações de QoS para qualquer fluxo de dados (de qualquer serviço), independentemente da localização do dispositivo e redes de acesso disponíveis. Logo, para ser efetivo em qualquer ponto das redes de acesso deve ter um mecanismo para verificar se é possível aceitar ou não uma nova conexão (para um novo fluxo de dados) respeitando os requisitos de QoS do novo fluxo e de todos os demais fluxos que já estejam em transmissão[14]. Logo, a arquitetura proposta possui diversos pontos de admissão e deve possuir algum mecanismo para determinar se há ou não um caminho disponível, sem se utilizar de uma arquitetura centralizada.

Para ser possível a admissão proposta os agentes necessitam de um método para estimar a probabilidade de que um caminho seja apropriado para manipular o fluxo de dados durante o tempo de transmissão (se esse for conhecido). Essa abordagem tende a ser apropriada para cada nó de rede

---

[13] Considera-se nesta tese que os elementos de comutação não representam pontos de gerenciamento e controle de QoS, pois não há condições de serem gerenciados em uma prova de conceito da arquitetura.

[14] Não se considere nesse trabalho a possibilidade de se ter fluxos agendados e reservas de recursos previamente à transmissão de um fluxo de dados. Embora a arquitetura dessa tese não apresente restrições a esse tipo de estratégia de transmissão, tal situação não faz parte do escopo discutido nesse trabalho.

controlar seus próprios recursos e alocá-los de acordo com suas premissas. O método proposto utiliza-se do histórico de tráfego, caracterizado por uma medida de sucesso ou de fracasso na transmissão de um tipo de fluxo de dados, para determinar comportamentos característicos de fluxos de dados através de conceitos oriundos dos sistemas complexos e, baseado nessa premissa, nos dados de recursos alocados o agente de um determinado nó verificará se há determinado conjunto de recursos para um novo fluxo de dados.

Segundo Robert (2001) a abordagem estatística para predição de comportamento de uma rede é possível, especialmente em se considerando que um *backbone* modelado como uma distribuição de Poisson para a carga da rede. Embora Paxson e Floyd (1995) atestem discrepâncias em modelagem de tráfego por Poisson, para o cenário proposto esta forma de modelagem é válida dada a característica de tráfego que se encontra em redes core, como analisado em Feldman, et. al. (1998) e Baratak, et. al. (2002). Contudo, a modelagem do tráfego será feita através de uma distribuiçao normal e serão utilizados mecanismos de *preferential attachment* como proposto por Barabási (2003) e Watts (2003), e Barabási (2007).

A abordagem proposta é similar às propostas de roteamento QoS em termos de agregação de rotas, pois a arquitetura proposta classifica os fluxos de dados através de um conjunto de parâmetros de QoS e pode também utilizar como parâmetro o destino a ser alcançado. A arquitetura proposta utilizando uma sociedade multiagentes como forma de controlar o ambiente distribuído, bem como tornar a decisão distribuída, é uma abordagem relevante, pois (Manvi, Venkataram, 2004), (Rubinstein, Duarte, Pujolle; 2000):

- Agentes são capazes de gerenciar sistemas legados uma vez que são capaz de ter uma interface de comunicação apropriada com cada tipo de equipamento e tecnologia;
- Agentes proporcionam menor quantidade de troca de mensagens de controle em relação a um sistema centralizado e reduz o tempo de resposta de um sistema de controle (Rubinstein, Duarte, Pujolle; 2000);

- Decisão distribuída pode acelerar a tomada de decisão e evitar um ponto central de falha. Entretanto, um sistema distribuído necessita de um sistema de controle que evite a falha (colapso) da sociedade multiagentes. (Manvi; Venkataram, 2004).

Uma questão importante para a arquitetura é qual algoritmo deve ser utilizado para prover a tomada de decisão dos agentes. Tal algoritmo deve prover respostas suficientemente rápidas tanto para indicar se o equipamento controlado deve ou não aceitar conexões quanto para determinar uma mudança nos tráfegos controlados quando necessário.

4.2 COMPONENTES DA ARQUITETURA PROPOSTA

A arquitetura proposta é composta por diversos tipos de agentes localizados em equipamentos de acesso e equipamentos de trânsito (componentes do núcleo da rede), assim como os equipamentos dos usuários finais e dos provedores de serviços. A sociedade multiagentes como arquitetura de controle de QoS é composta de diversos tipos de agentes que pode ser classificados como Agentes de QoS (*QoS Agents* – QA) e agentes de Coordenação (*Coordination Agents* – CA).

Um dos conceitos da arquitetura é que uma visão centralizada é improvável de ser alcançada devido à complexidade da rede; entretanto, é possível se ter uma abordagem estatística como forma de definir o comportamento de um equipamento. Se cada equipamento é capaz de controlar as condições de transmissão para que estejam de acordo com os contratos de QoS, desta forma otimizando seus recursos então é possível de se obter um caminho com QoS fim a fim, uma vez que em todos os trechos o contrato de QoS é respeitado. Entende-se que a hierarquia de agentes tem como requisito funcional que em cada trecho de um caminho possa ser configurado valores de parâmetros de QoS a serem respeitados, sendo que a relação destes parâmetros de todos os trechos de um caminho representem o contrato de QoS fim a fim estabelecido entre provedor de serviço e usuário final. Uma das possíveis formas de geração dos contratos para cada trecho é se utilizar dos dados históricos, havendo diversas abordagem como

mecanismos compostos de redes neurais e algoritmos fuzzy (Zhani, Elbiaze, Kamoun, 2010).

O conceito é similar com roteamento QoS em termos de agregação de tráfego, contudo difere no tratamento estatístico para a manipulação do tráfego e conexões de trânsito.

A sociedade multiagentes, em trabalhando como um *middleware* com serviços de QoS para infra-estruturas heterogêneas, deve ser capaz de ser utilizada com diversos tipos de algoritmos para negociação de caminhos e otimização de recursos, desde que tais algoritmos mantenham e contribuam com as seguintes características da arquitetura de forma a se construir o "QoS middleware" (Aurrecoechea, Campbell, Hauw, 1998), (Gao, Wu, Miki, 2004), Serra (2007):

- Conhecimento de QoS: monitorar e gerenciar componentes de serviços de acordo com os requisitos descritos no contrato de serviço (USLA);
- Conhecimento de localização: permitir a tomada de decisão (em tempo de execução) baseada na topologia da rede e nos recursos envolvidos;
- Adaptação para domínio: adaptar a distribuição dos serviços com as mudanças dinâmicas que ocorrem no ambiente;
- Adaptação de parâmetros: traduzir os requisitos do usuário em parâmetros de QoS para cada tecnologia de rede;
- Transparência: aplicações não devem considerar a complexidade do controle de QoS em sua operação;
- Princípio da integração: QoS é uma relação entre duas ou mais aplicações (levando em consideração os requisitos do usuário). Para tal, o QoS deve ser configurável, preditivo e ser mantido em todas as camadas (OSI) da infraestrutura para manter-se o QoS fim a fim;

- Princípio da separação: serviços são compostos de diversas partes relacionadas, onde tais partes podem estar localizadas em diferentes camadas da infraestrutura de comunicação.

Em cada nó da infraestrutura há um agente de controle da arquitetura de QoS (middleware distribuído), cuja função é manter o histórico do tráfego e determinar se para um novo fluxo de dados que começa a ser transmitido pelo equipamento controlado pelo agente pode ser aceito ou não. Barabási (2003) e (2007) e Watts (2003) propõem que qualquer sistema de comunicação apresenta comportamento derivado da interação dos dispositivos e das características do tráfego. O aspecto chave de tal abordagem é a capacidade da arquitetura de controle de QoS basear-se em tais aspectos de comportamento que possam influenciar o USLA tanto na rede de acesso quanto no núcleo da rede, independentemente das tecnologias de transmissão.

É possível que os equipamentos legados não tenham recursos suficientes para hospedarem um agente como proposto pela arquitetura, e portanto, os agentes necessitam de algum local onde possam executar os mecanismos de controle segundo o princípio do mecanismo de mercado a ser empregado na sociedade multiagentes. Esse local é denominado “mercado virtual” e pode ser qualquer equipamento com capacidade de processamento suficiente para receber os agentes. Nesse local os agentes poderão enviar para os equipamentos sob seu controle, assim como para outros agentes informações sobre o estado dos fluxos de dados controlados. Além disso, os agentes tem de ser móveis para serem capazes de ir até o “mercado virtual”.

O sistema de controle de QoS deve possuir agentes para o equipamento do usuário, para o provedor de serviços e para os equipamentos que compõem a infraestrutura do sistema de comunicação, assim como estabelecer a comunicação entre diversos domínios administrativos. A sessão seguinte descreve os agentes que apresentam as os requisitos descritos para os componentes da arquitetura de controle de QoS.

4.2.1 Agentes da Arquitetura de Controle de QoS proposta

O operador do sistema de comunicação e o operador de serviços devem ter cada um conjunto de políticas próprias que devem ser aplicadas para se estabelecer acordos de QoS em seus domínios administrativos. O componente da arquitetura de QoS no dispositivo do usuário deve estabelecer negociações de QoS para cada conexão, sendo que tal processo deve ocorrer independentemente da localização do usuário (considerando usuários móveis) e a tecnologia de acesso disponível. Para tal cenário qualquer local da rede de acesso deve estar pronto para determinar se é possível ou não aceitar uma nova conexão respeitando os parâmetros estabelecidos na USLA.

A arquitetura de controle de QoS proposta é composta pelos seguintes agentes:

- Agente do Usuário (*User Agent* - UA): responsável por negociar e verificar os requisitos de QoS de cada fluxo de dados do usuário;
- Agente de Borda (*Edge Agent* - EA): responsável por negociar os parâmetros de QoS entre o UA e o Resource Management Agent (RMA), funcionando como um controle de admissão;
- Agente de Política (*Policy Agent* - PA): responsável por informar e verificar se as políticas de QoS do operador da infraestrutura estão sendo respeitadas pelos agentes;
- Agente de Gerenciamento de Recursos (*Resource and Management Agent* - RMA): responsável por determinar a disponibilidade de recursos em um intervalo de tempo e controlar se o equipamento possui recursos para transmitir um determinado fluxo de dados;
- Agente de Serviço (*Service Agent* - SA): responsável por negociar os parâmetros de QoS para cada serviço do provedor de serviços que representa;

- Agente de Controle e Supervisão (*Supervision and Control Agent* – SCA): responsável por monitorar e resolver questões de conflito na sociedade multiagentes.

A organização hierárquica dos agentes é apresentada na Figura 6. Embora exista uma hierarquia também há autonomia dos agentes, ou seja, cada agente decide as ações a serem tomadas segundo suas regras internas; contudo, a monitoração de outros agentes é necessária caso determinadas situações de conflito surjam, como por exemplo, uma falta de recursos por motivos de falha de algum agente ou por problemas de comunicação entre dispositivos controlados.

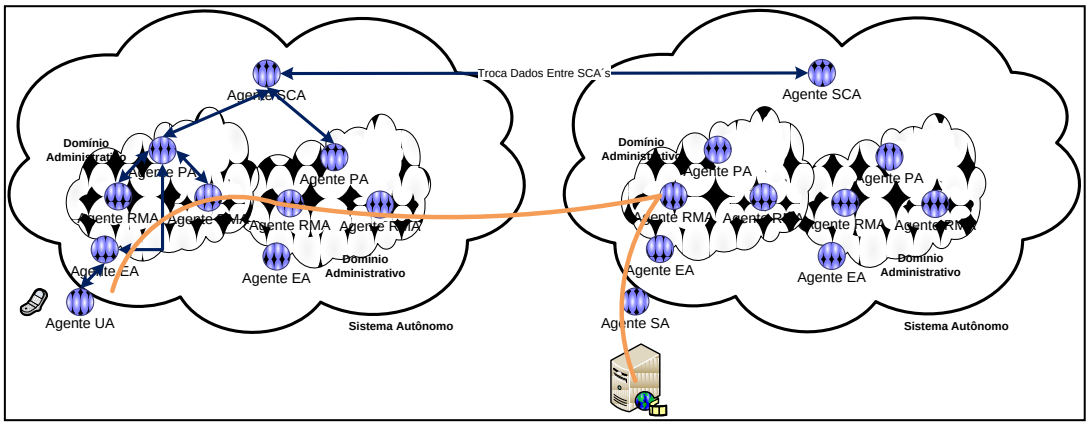

Figura 6 – Hierarquia dos agentes

4.2.2 Modelagem dos Agentes de QoS

Os itens a seguir descrevem os comportamentos e processos os quais representam os agentes da arquitetura.

4.2.2.1 Agente UA e Agente SA

O UA tem como função primária negociar os caminhos para qualquer tipo de fluxo de dados requisitado pelo usuário através de um serviço. Isto significa que o agente deve escolher o melhor caminho pela melhor rede de acesso disponível para um determinada classe de fluxo de dados, e também deve monitorar o estado da conexão para verificar se o USLA está sendo mantido e tomar ações caso isso não ocorra.

O agente do provedor de serviços (SA – *Service Agent*) é bastante similar ao UA, com a diferença que ele recebe requisições de serviço em vez de fazê-las. Com tais requisições é sua função estabelecer conexões com redes de acesso a entrega do serviço solicitado. Portanto, seus estados e processos são os mesmos que compõem o agente UA.

Os comportamentos que o agente UA e SA possuem são:

- Monitoração de Serviço: agente verifica continuamente o estado de todas as conexões ativas no dispositivo do usuário/provedor de serviços;
- Pedido de Oferta: agente envia uma requisição para todas as redes de acesso disponíveis para contratar o melhor serviço que atenda aos requisitos da USLA;
- Renegociação: se o agente detecta alguma degradação no serviço, ele reinicia a renegociação com todas as redes disponíveis para manter o USLA e prover o serviço sem interrupções.
- Serviço Finalizado: o agente indica para o agente EA que o serviço foi finalizado com sucesso;
- Falha Serviço: o agente indica para o agente EA que o serviço foi finalizado por não atendimento de USLA.

Os processos (transições do diagrama) do agente UA são:

- Verificação de Acesso: o agente verifica periodicamente todas as redes disponíveis e questiona sobre a capacidade das classes de fluxos de dados;
- Requisição de proposta para USLA: agente envia para todas as redes disponíveis uma especificação de USLA para a negociação de um novo fluxo de dados;
- Análise de proposta USLA: agente recebe propostas de serviços e escolhe a que melhor se adéqüe ao USLA requisitado;
- Serviço Estabelecido (aceitação de proposta USLA): agente informa a um EA que aceitou a proposta enviada;

- Monitoração de USLA (*Pooling*): agente monitora as conexões ativas e verifica se o USLA está sendo respeitado;
- Requisição de renegociação USLA: agente renegocia o USLA com todos os EA que não estão provendo serviço que está comprometido;
- Falha USLA: agente recebe as propostas de serviço e escolhe a que melhor atenda a USLA e mantenha a entrega do serviço;
- Serviço Estabelecido (aceitação de renegociação de USLA): agente informa ao EA vencedor que aceitou sua proposta e inicia a conexão;
- Serviço Indisponível: agente envia um aviso de finalização de serviços para o EA (que gerencia o fluxo de dados) e indica a razão pela qual o acordo foi revogado;
- Finalização Serviço: agente envia um aviso de finalização do serviço cuja execução foi bem sucedida.

A relação entre processos e comportamentos é representada na Figura 7:

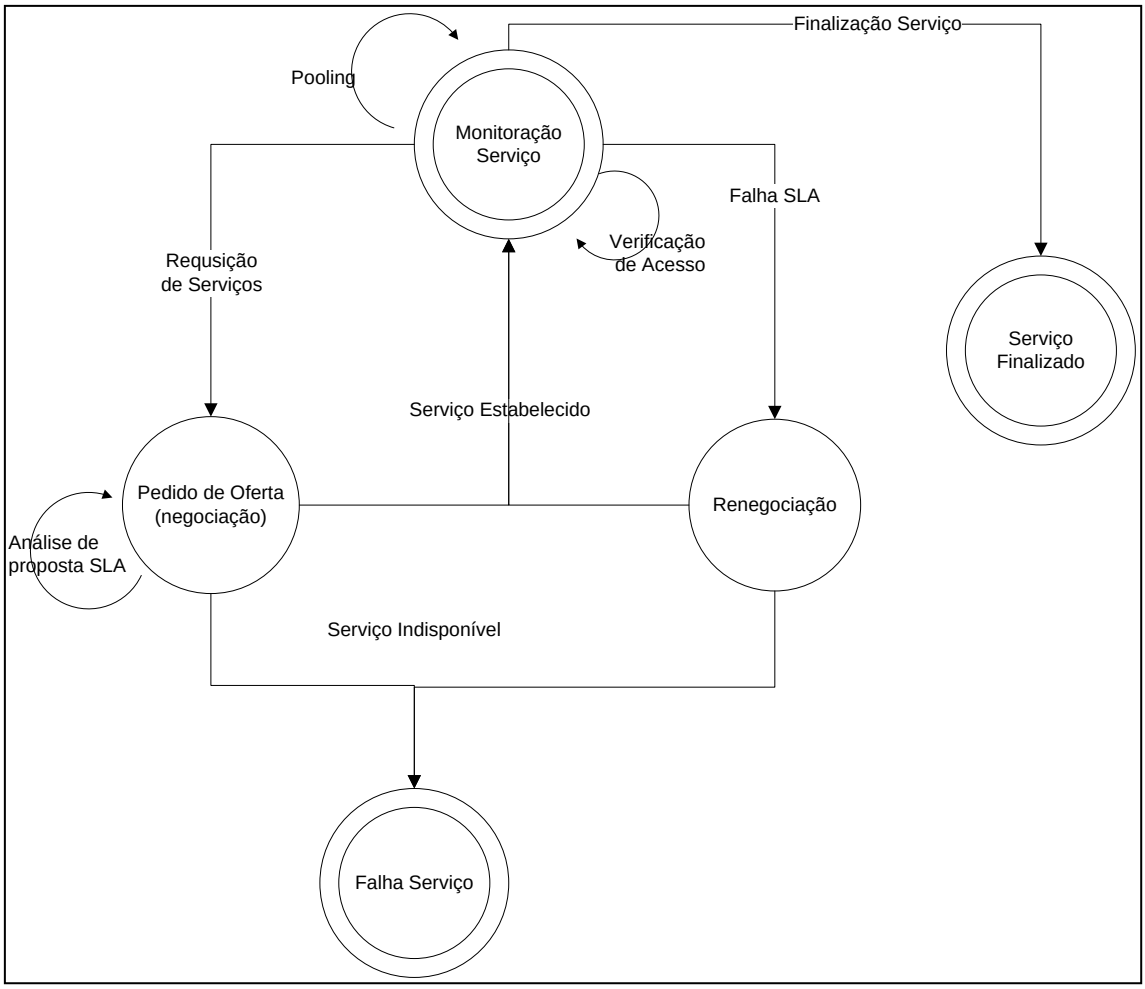

Figura 7 – Relação entre Comportamentos e Processos do agente UA e SA

4.2.2.2 Agente EA

O agente EA é um conjunto de agentes localizados nas bordas da infraestrutura de acesso e controla o acesso de um fluxo de dados em um sistema de comunicação. Seus comportamentos são:

- Atualizar Estado (domínio administrativo com PA): Agente comunica-se com SCA para obter dados atualizados sobre estado do sistema de comunicação.
- Aguardando Pedido de Serviço: agente espera por novas requisições de serviço (USLA);
- Monta Oferta de Serviço: agente monta uma oferta de serviços de acordo com os parâmetros da rede e do serviço requisitado;

- Aguarda Aceite ou Recusa de Oferta de Serviço: agente aguarda por resposta do agente UA ou SA (forma de não ofertar mais recursos do que a rede é capaz de oferecer).
- Atualizar Oferta de recursos do domínio administrativo: comportamento que periodicamente atualiza os dados de estado da rede vindos de SCA e atualiza dados de PA (no caso de um domínio administrativo);
- Informar estado da prestação de Serviços: ao receber requisição do agente UA ou SA o agente EA informa o estado da rede para o tipo de serviço requisitado.

Os processos do EA são:

- Ativar comportamento: agente ativa um comportamento (interno) para atualização do estado da rede.
- Pedido Serviço Recebido: agente ativa comportamento de montagem de uma oferta de serviço de acordo com o tipo de serviço requisitado;
- Envio de Oferta de Serviços: agente envia notificações para o UA ou SA com a oferta montada;
- Mensagem de Recursos vindos de PA: agente recebe mensagem de estado da rede do RMA para atualizar os parâmetros dos serviços do de seu domínio administrativo (origem e destino em um único domínio administrativo). Caso a origem e destino estejam em domínios distintos os dados virão de SCA e serão transmitidos pelo PA ao EA.
- Pedido de Estado de Serviço por UA ou SA: mensagem enviada por UA ou SA pedindo informe de valores de parâmetros de um tipo de serviço;
- Envio de Resposta ao UA ou SA: agente EA envia resposta ao pedido do UA ou SA com os dados dos parâmetros pedidos
- Resposta de Oferta de serviço recebida: o comportamento Aguarda Aceite ou Recusa de Oferta de Serviços informa ao comportamento

Aguardando Pedido de Serviço o estado da oferta e finaliza seu comportamento.

A relação entre processos e comportamentos está representada na Figura 8:

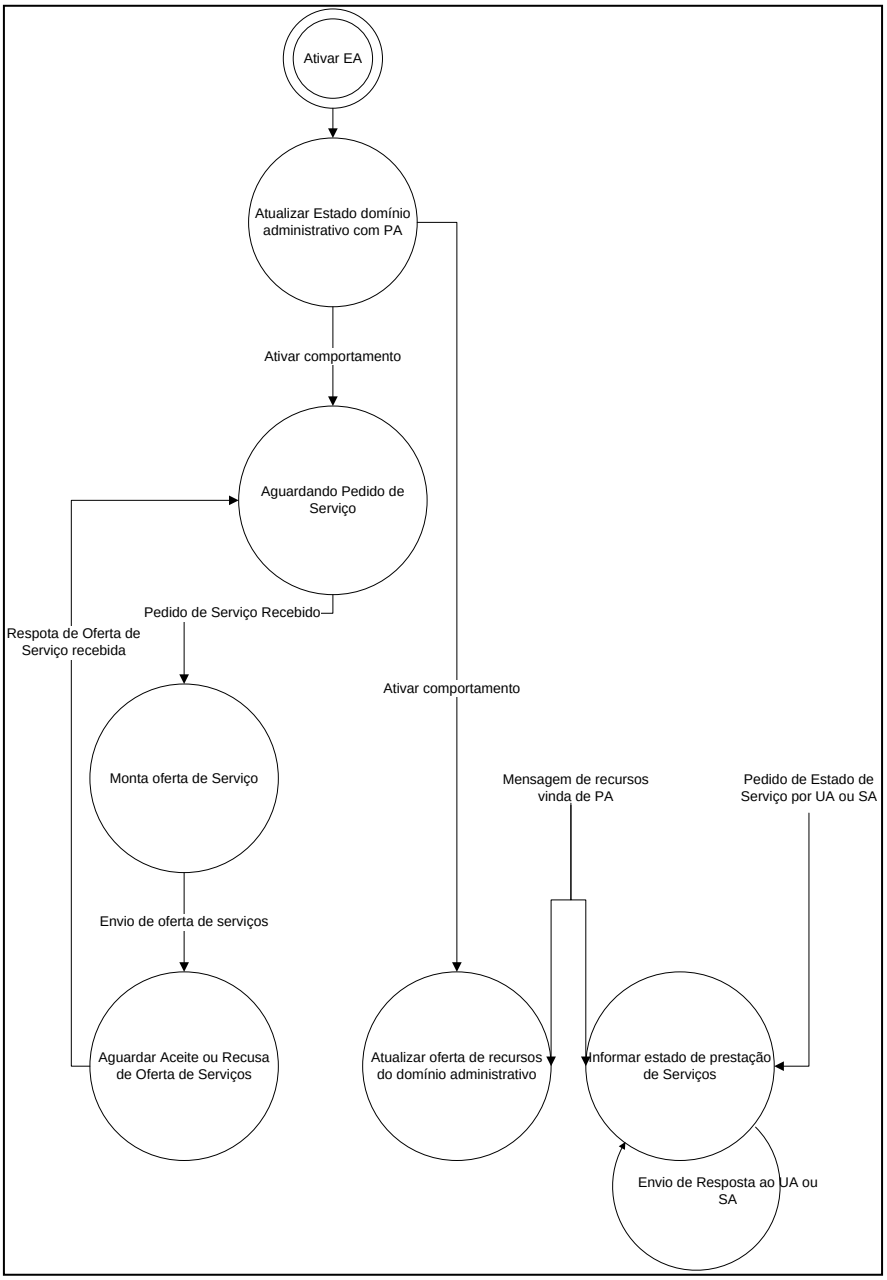

Figura 8 – Relação entre Comportamentos e Processos do agente EA

4.2.2.3 Agente RMA

O RMA é um agente presente em todo o equipamento controlado e cuja função é monitorar o estado do equipamento e construir um modelo de comportamento baseado nos parâmetros de rede. A monitoração deve garantir o cumprimento do acordo de USLA estabelecido para cada classe de fluxo de dados. Para tais atividades, o RMA possui os seguintes comportamentos:

- Ativação Agente: ativação do agente e de seus comportamentos. Neste estado o agente busca em PA os parâmetros que devem ser utilizados, e caso não tenham sido alterados ou a comunicação não se faça possível, então o agente utiliza seus valores armazenados;
- Monitoração e Análise de Fluxos: agente verifica continuamente o estado de todas as conexões ativas no dispositivo que gerencia;
- Alteração de caminho e tipo de fluxo de dados: se o agente detecta alguma degradação de uma classe de fluxo de dados, ele procura dentre os caminhos disponíveis aquele com maior preferência para manter o USLA e prover o serviço sem interrupções;
- Falha de Serviço: se o agente detecta alguma degradação mas não possui uma alternativa então uma mensagem é enviada ao agente PA de forma que esse possa tratar a falha adequadamente;
- Envio de Dados de P e Q para PA: o agente RMA informa periodicamente os valores de P e Q (ver item 4.3.1) de cada tipo de fluxo de dados para o agente PA como forma deste manter o controle do domínio administrativo (cálculo de SLM fim a fim no domínio administrativo);
- Alteração de valores de parâmetros de fluxos de dados: comportamento que após a análise do estado dos fluxos de dados nos caminhos utilizados determina um novo caminho para um determinado tipo de fluxo de dados;
- Mensagem Enviada: comportamento no qual uma mensagem de falha é enviada ao PA (de forma que esse possa tomar ações

pertinentes) e um registro foi criado como forma de documentação da falha.

Os processos (transições) do RMA são:

- Mensagem do PA: o agente RMA, ao receber uma mensagem do agente PA altera os limites dos parâmetros utilizados para determinar os novos valores de análise dos fluxos de dados;
- Parâmetros acima do limite estabelecido: se o agente detectar que há alguma degradação de um fluxo de dados, o processo de determinação de novo caminho é ativado;
- Caminho alterado com sucesso: mensagem que informa a um comportamento do agente que o fluxo foi encaminhado para um novo caminho que contém os valores de parâmetros adequados para o tipo de fluxo de dados;
- Falha na alteração do serviço: se o agente é incapaz de detectar um novo caminho com as condições adequadas, então é ativado o comportamento de tratamento de falhas (Falha de Serviço);
- Mensagem Enviada ao PA: mensagem que encerra o comportamento de Falha de Serviço indicando ao comportamento Monitoração que o PA foi avisado;
- Envio de Mensagem ao PA: mensagem que ativa o comportamento periódico de envio dos parâmetros de estado da rede ao PA;
- Envio de Falha ao PA: o agente RMA possui a confirmação que a mensagem foi enviada e que a falha foi registrada (ativando o comportamento Mensagem Enviada).

A relação entre processos e comportamentos está representada na Figura 9:

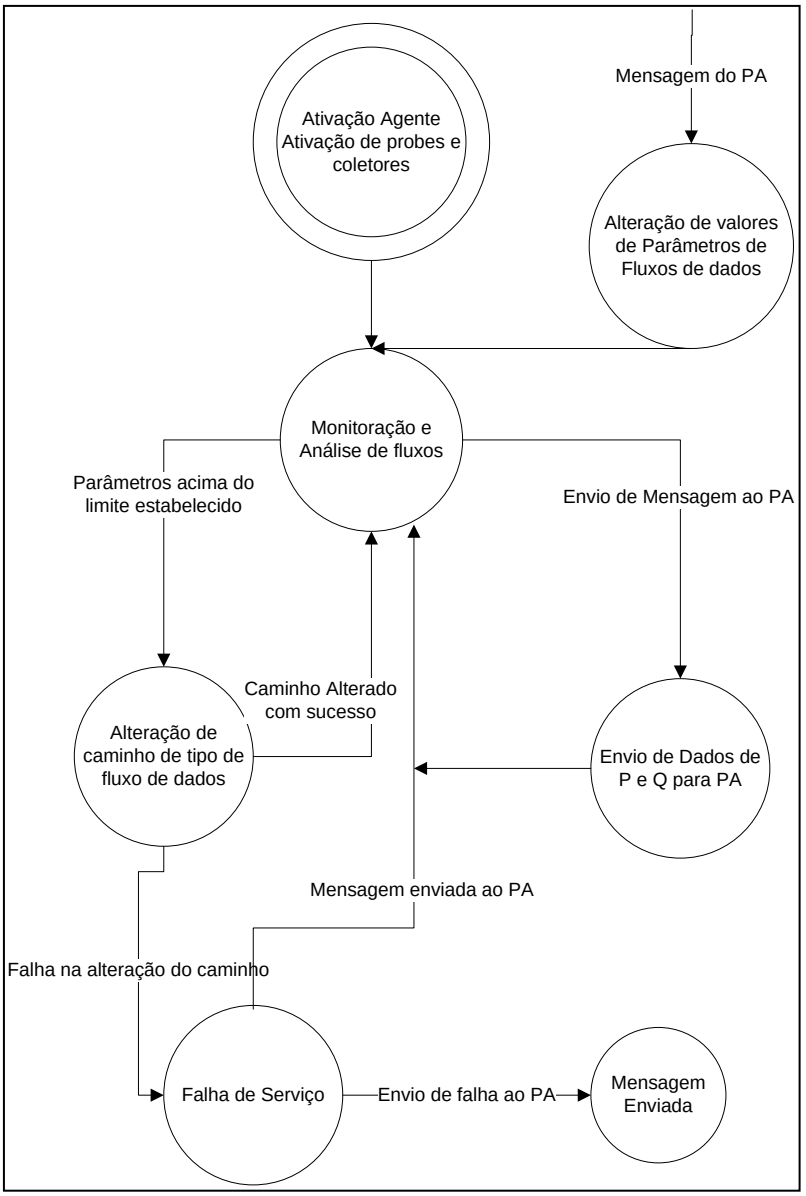

Figura 9 – Relação entre Estados e Processos do agente RMA

O caminho de QoS fim a fim é estabelecido quando as condições de transmissão do serviço são válidos em certo intervalo de tempo. O RMA pode alterar o caminho utilizado , ou seja, enviar o fluxo de dados para outro equipamento vizinho, em qualquer momento sem necessitar de notificar o UA requisitante do serviço detecte que o caminho utilizado não mais atende os requisitos do fluxo, quer porque o fluxo está sendo transmitido por mais tempo que o intervalo de tempo válido onde o RMA possuía recursos em tal caminho ou por qualquer eventualidade na rede que limite os recursos. A monitoração a ser executada é relacionada com o tipo de fluxo de dados identificado de forma

única no domínio administrativo, ou seja, não são analisados fluxos individualmente, pois se dois fluxos tem o mesmo identificador, significa que naquele domínio administrativo devem ser tratados da mesma maneira pois possuem o mesmo conjunto de requisitos. Dois fluxos podem, em princípio, serem tratados de formas distintas em dois domínios administrativos distintos, pois cada qual tratará cada fluxo de acordo com as políticas de qualidade de serviço do domínio administrativo.

O agente RMA ainda tem como seus agentes subordinados agentes denominados agentes RMALink, cuja função é monitorar as duas pontas que representam uma conexão e enviar os dados da monitoração para o agente RMA.

4.2.3 Hierarquia de agentes e coordenação

Embora os agentes de coordenação determinem as políticas que todos os agentes do domínio administrativo devem seguir, cada agente de QoS é autônomo para aplicar tais políticas. Logo, os agentes de coordenação devem estar em um nível superior da hierarquia para monitorar e determinar soluções para conflitos que possam ocorrer na sociedade multiagentes. Tais questões são tratadas como o problema de coordenação de agentes.

4.2.3.1 Coordenação de agentes

Um dos desafios em sistemas distribuídos é como controlar demandas crescentes por tarefas quando a distância dos nós tende a aumentar. Quanto mais complexa a tarefa, mais complexo é seu controle, principalmente tendo em consideração o potencial aumento do número de mensagens para obter tal controle. Nessa situação, a criação de grupos menores de agentes para controle pode ser uma abordagem interessante, desde que o desempenho obtido seja superior àquele obtido por sistemas únicos de controle (sem a divisão em grupos de agentes menores). (Jezic, Kusek, Sinkovic, 2006).

Das diversas abordagens propostas na literatura para coordenação de agentes ((Scerri, Vincent; Mailler, 2006), (Jezic, Kusek, Sinkovic, 2006), (Bonabeau, 1998)), a abordagem “estilo formiga” é apropriada para a

arquitetura proposta. Essa abordagem é baseada no comportamento apresentado por insetos para resolver problemas complexos como o de achar locais com alimento e descobrir um caminho de volta ao ninho. Tais sociedades são baseadas em algoritmos naturais de auto-organização, donde emergem comportamentos complexos, embora o comportamento de uma formiga (ou de um agente) seja simples e as regras de definição das ações também o sejam.

As formigas, de forma a determinar o caminho de volta até o ninho, utilizam uma substância natural para identificar os locais por onde passou entre a posição do alimento e o ninho. E assim fazem as demais formigas causando um reforço naquele caminho. As experimentações mostram que as formigas conseguem descobrir bons caminhos entre dois pontos (não necessariamente o melhor), e seu método cobre grandes regiões de interesse segundo uma premissa: achar locais onde há recursos para se alimentarem (Bonabeau, 1998),(Parunak, 1997). De certa forma a abordagem dos algoritmos de formigas (*ant algorithm*) guarda semelhança com o princípio de *preferential attachment* pois o caminho que se mostra com mais recursos é preferido pelas formigas, enquanto os caminhos que levam a menos recursos tem menor possibilidade de serem escolhidos por alguma formiga (Watts, 2003).

A abordagem das formigas também pode ser entendida como pequenos times que seguem um plano. Pequenos times possuem vantagens em relação a times grandes: trocam menores quantidades de mensagens e promovem o crescimento escalar. Algoritmos escaláveis são baseados em duas premissas (Scerri, Vincent; Mailler,2006):

- Uso de modelos probabilísticos e estados para informar gerentes;
- Criam algoritmos simples, robustos e eficientes para promover decisões rápidas.

A abordagem das formigas também apresenta desafios como a distribuição de informações entre os agentes e seus times e quais são os parâmetros de interação entre eles. O primeiro desafio é conseqüência do crescimento incremental (restrição de conhecimento devido à diminuição de troca de mensagens), e alguns mecanismos como o quadro de avisos ou estruturas hierárquicas não resolvem o problema do crescimento incremental

(Scerri, Vincent; Mailler,2006). O segundo desafio aparece devido a não linearidade dos parâmetros da infraestrutura. A falta de padrão pode resultar em dificuldades para a tomada de decisão em tempo de operação da infraestrutura usando a mesma política em diferentes pontos (tendo em consideração uma infra-estrutura heterogênea).

Na arquitetura proposta os agentes de um mesmo nível hierárquico não trocam dados entre si, apenas trocam dados entre as hierarquias superiores como forma de atingir maior escala no provimento dos serviços de QoS (ver item 4.3 para detalhamento), com exceção dos agentes PA que trocam dados entre seus pares.

4.2.4 Modelos dos agentes de coordenação

Os agentes de coordenação coordenam as ações dos times, aplicam regras vigentes para o domínio administrativo e resolvem falhas que possam ocorrer durante a operação dos agentes de QoS.

A arquitetura proposta possuiu dois agentes de coordenação os quais coordenam os planos dos times. Um plano são as regras que os agentes de um time utilizam para suporte à decisão e tais planos devem ser aderentes às políticas do domínio administrativo. O Agente de Política (*Policy Agent* –PA) monitora seu time e fornece as regras que os agentes devem seguir. Caso ocorra alguma falha o PA possui autoridade para determinar a ação que um agente deve tomar para resolver a falha. Contudo, o PA não possui autoridade para quebrar ou alterar a forma como o RMA manipula fluxos de dados que não estejam diretamente envolvidos com a falha.

O segundo agente de coordenação é denominado SCA e sua função é resolver conflitos entre times. É importante frisar que os agentes de QoS são autônomos e os agentes de coordenação não tomam todas as decisões relacionadas com a ação dos agentes; os agentes de coordenação influenciam apenas situações de falha na operação (como *deadlocks* e falta de recursos - *starvation*). O agente SCA tem função de sumarização de informações entre sistemas autônomos e como elemento de controle em caso de conflito entre agentes PA. Embora a prova de conceito não tenha abordado testes com o agente SCA é interessante que seus comportamentos sejam:

- Ativação PA: o agente é ativado e ativa os demais comportamentos do agente.
- Monitoração: agente verifica se os agentes RMA estão operando corretamente;
- Anúncio de regras: agente recebe novas regras do SCA e anuncia para os agentes sob sua responsabilidade. Regras são entendidas como conjunto de parâmetros para cada tipo de fluxo de dados a ser controlado;
- Solução de Conflitos entre RMA: se dois ou mais agentes não possuem recursos para o tratamento de um tipo de fluxo de dados e, portanto a operação de controle apresenta falha no nível hierárquico do RMA, o PA toma ações para minimização dos danos.

Os processos do PA são:

- Dados vindos de SCA: agente PA recebe um conjunto de regras que deve ser aplicado em seu domínio administrativo;
- Conflito detectado: processo que ativa o comportamento “Solução de Conflitos entre RMA”, informando os parâmetros do tipo de fluxo de dados e os agentes envolvidos;
- Solução de conflito enviada ao RMA: mensagem que indica finalização correta do comportamento “Solução de Conflitos”;
- Envio de Dados SCA: envio dos dados do domínio administrativo para o SCA (gerencia diversos domínios administrativos em um sistema autônomo);
- Pedido de propagação: agente envia mensagem para todos os RMA e EA de seu time para informar sobre novas regras que devem ser seguidas para atender às USLAs[15].

[15] Uma política de SLA é um conjunto de tipo de tráfego, origem, destino e requisitos que devem ser atendidos para a prestação de serviço segundo a perspectiva do usuário

- Propagação de valores de parâmetros: processo recursivo onde todos os agentes são notificados da necessidade de alteração de parâmetros dos tipos de fluxos de dados;
- Propagação executada: mensagem que indica que o comportamento terminou com execução completa;
- Receber P e Q: processo que periodicamente recebe os dados vindos dos agentes RMA do domínio administrativo controlado por PA;
- Informe Dados: processo que ativa o comportamento Envia Dados SCA e fornece todos os dados dos fluxos de dados a serem enviados ao SCA.

A relação entre processos e comportamentos está representada na Figura 10:

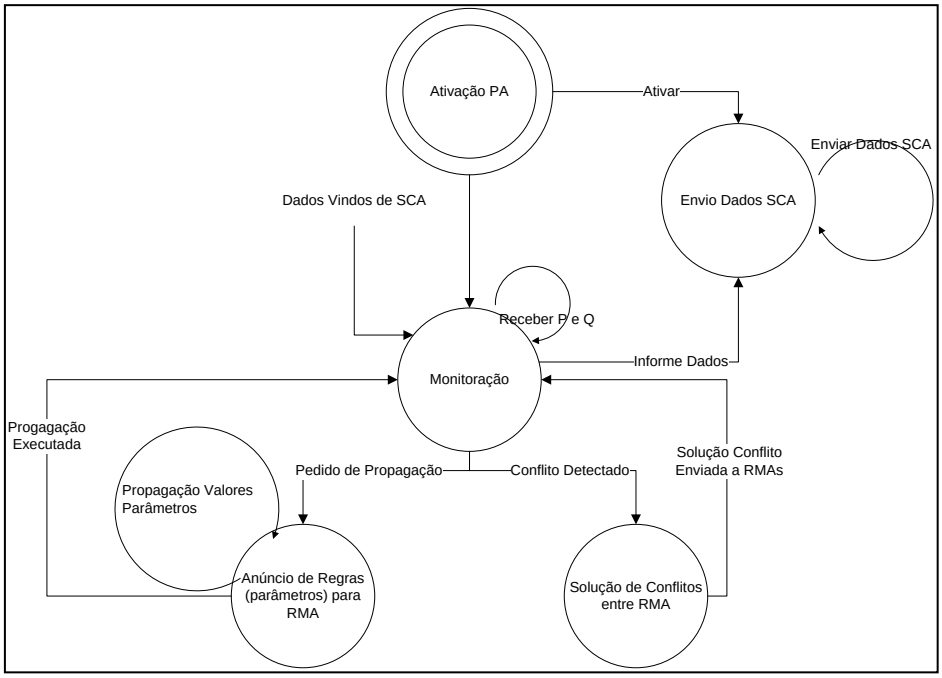

Figura 10 – Relação entre Comportamentos e Processos do agente PA

Os comportamentos do SCA são:

- Monitoração: o agente verifica o estado dos PA e determina se todos estão operando adequadamente;
- Solução de Conflito: caso um PA não responda a uma requisição ou dois PA entrem em conflito o agente SCA tem autonomia para enviar comandos para os agentes PA resolverem o conflito. Os comandos

são ações para ativar o desativar[16] um determinado agente (em princípio);

- Anúncio de regras: agente envia mensagem para todos os PA de seu sistema autônomo para informar sobre novas regras que devem ser seguidas para atender às USLAs;
- Dados inter-sistema autônomo o agente SCA troca dados com outros agentes SCA para montar o estado de cada tipo de fluxo de dados para cada destino de forma fim a fim;
- Falha em Conflito: comportamento onde o agente registra detalhadamente os motivos da falha para que essa seja informada a um administrador do sistema de controle de qualidade de serviços.

Os processos do SCA são:

- Propagação de regras: agente envia mensagem para todos os PAs do domínio administrativo contendo as políticas a serem seguidas;
- Detecção de conflitos: ações a serem enviadas para os PA como forma de restabelecer a operação de um domínio administrativo e dos agentes envolvidos na falha;
- Troca de Dados Inter-AS[17]: falha entre domínios administrativos; mensagem enviada aos operadores da infra-estrutura;
- Falha de anúncio: processo que ativa o comportamento de “Solução de Conflito” pois pelo menos um agente PA não foi notificado;
- Notificação administrador: notifica o administrador do sistema de controle que há uma situação que o sistema de controle de qualidade de serviço não possui condições de resolver de forma autônoma.

---

[16] Outros comandos podem ser elaborados para atuar em situações e casos específicos não cabendo a exploração das possibilidades neste texto.

[17] AS – Autonomous System (Sistema Autônomo) no contexto desta tese é um conjunto de domínios administrativos controlados por uma mesma entidade.

A relação entre processos e comportamentos está representada na Figura 11:

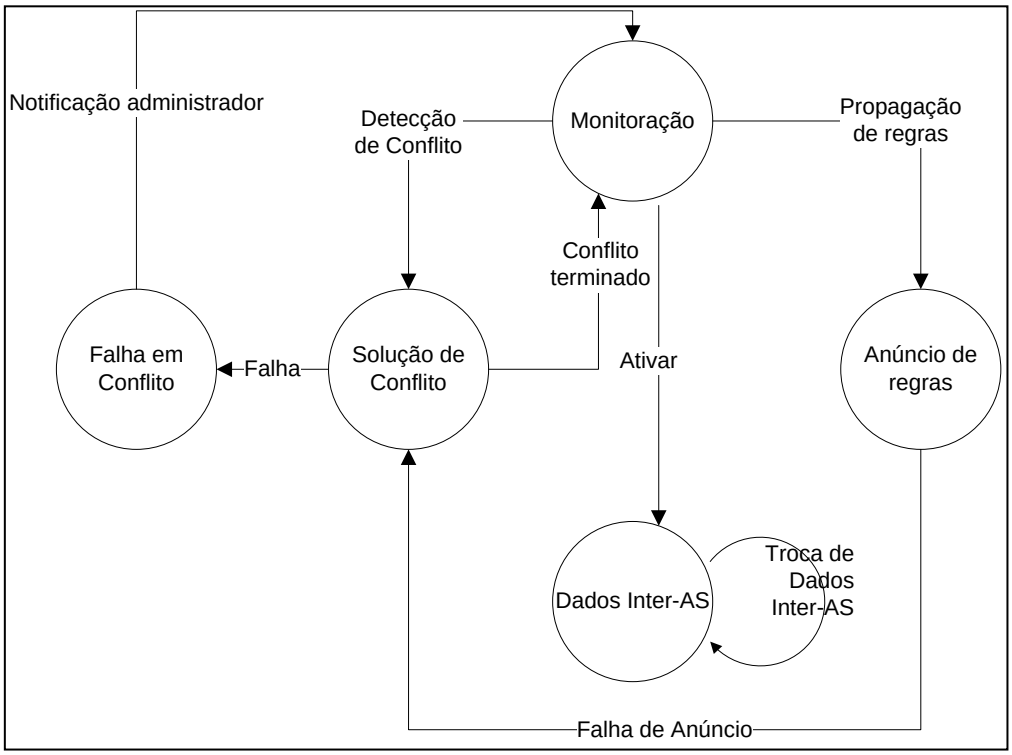

Figura 11 – Relação entre Comportamentos e Processos do agente SCA

4.3 MECANISMOS DA ARQUITETURA PROPOSTA

A arquitetura proposta nessa tese é composta por uma hierarquia de agentes cujo propósito é monitorar os estados dos fluxos de dados e reagir dinamicamente quando alterações no estado da rede possam vir a comprometer o contrato de qualidade de serviço de uma determinada classe de fluxos de dados.

Embora a arquitetura proposta seja composta de diversos componentes relacionados com sistemas multiagentes, a arquitetura não deve ser entendida como exclusiva em uma infraestrutura, devendo substituir o legado. A arquitetura proposta não pretende substituir os sistemas de QoS existentes, mas promove maior dinamicidade ao utilizar como base de decisão o comportamento da infraestrutura e os caminhos disponíveis entre origem e destino que não seja apenas a rota preferencial de uma tabela de roteamento e uma interface de comunicação com uma organização de fila particular. Além disso, a arquitetura proposta visa trazer uma visão local de qualidade de

serviço onde questões relacionadas à qualidade de serviço possam ser resolvidas no ponto onde ocorrem, de forma autônoma e respeitando as premissas da política de QoS do domínio administrativo a que pertence.

Considerando a organização dos sistemas de comunicação tem-se que:

- os usuários finais estão conectados a redes de acesso, cuja característica é prover capilaridade para acesso não ser utilizada como rede de trânsito de grandes volumes de dados a serem trocados entre outras duas redes de acesso.
- As redes de acesso (independente da tecnologia de transmissão de dados para o dispositivo final do usuário) estão interconectadas através de infraestruturas denominadas *backbones*, ou seja, infraestruturas cuja característica é prover recursos para troca de dados entre redes de acesso.

Os agente localizados nas redes de acesso enviam e configuram os parâmetros dos fluxos de dados nos elementos das redes de acesso. Esses agentes, por sua vez, recebem os valores dos parâmetros do contrato de uma hierarquia de agentes superior, os quais devem representar os diversos tipos de contratos a serem monitorados e controlados. O mesmo ocorre com os elementos do *backbone* e com os provedores de serviço.

Uma vez definido os valores dos parâmetros há a necessidade de se ter mecanismos de “admissão reverso” de fluxos de dados para cada elemento da infraestrutura, cujo propósito é garantir que um fluxo de dados não será enviado a um elemento de rede que não possui capacidade para manter os valores das variáveis que definem o *Service Level Management* (SLM) dentro dos valores esperados no USLA. O mecanismo de negociação é baseado nas equações propostas por Dorogovtsev, Mendes e Samukhin (2000) que expressam conexões preferenciais e pode ser descrito por dois parâmetros: sucesso na transmissão de um determinado tipo de fluxo de dados e fracasso na transmissão de um determinado tipo de fluxo de dados, denominados P e Q, respectivamente.

4.3.1 Mecanismo de decisão dos agentes de controle de QoS

O mecanismo proposto para que um agente decida sobre a qualidade de um determinado caminho é baseado no conceito de "*rich get richer*", ou seja, quanto melhor um determinado elemento de rede manipula um determinado tipo de fluxo de dados, maior a probabilidade dele receber uma nova requisição daquele tipo de fluxo de dados. O mecanismo de decisão para qual elemento da infraestrutura do sistema de comunicação determinado tráfego será enviado equivale a um controle de admissão, mas feito pelo ponto que enviará o fluxo de dados, pois este deverá optar por qual elemento oferece a melhor condição.

Segundo Barabási (2003) o efeito *rich get richer* ocorre em diversos processos naturais, assim como ocorre com os conteúdos da Internet e como a quantidade e localização das conexões de um sistema de comunicação aumentam. Esse efeito tem como uma de suas decorrências a possibilidade de estimar o surgimento de "hubs", ou seja, de pontos de alta concentração de um determinado serviço ou de um determinado comportamento em relação às demais partes do mesmo sistema, quer seja de comunicação ou de outra natureza. (Barabási, Albert, Jeong, 2000), (Egawa, Kiriha, Arutaki, 2007), (Oliveira, et. al. 2004).

Logo, essa tese utiliza como princípio que se um determinado elemento de rede está próximo a um serviço muito utilizado de um sistema de comunicação (ou seja, é um dos *gateways* do serviço) estima-se que tal equipamento tende a receber uma maior quantidade de um tipo de fluxo de dados em relação a outros tipos de fluxos e, portanto pode ser considerado um caminho preferencial para esse determinado tipo de fluxo de dados. E embora esse mesmo elemento possa ser caminho para estes outros serviços, se existirem outros possíveis caminhos determinados por outros elementos para os mesmos serviços pode acontecer de outros elementos serem caminhos preferenciais para outros tipos de fluxos de dados; ou seja, os elementos podem se tornar preferenciais por tipo de serviço de acordo com as condições do sistema de comunicação exigidas por esses serviços, de acordo com o conceito de *preferential attachment*.

Para ser possível a admissão proposta os agentes necessitam de um método estatístico para estimar a probabilidade de que um caminho seja apropriado para manipular o fluxo de dados durante o tempo de transmissão (se esse for conhecido).

Duas medidas são utilizadas para determinar *preferential attachment* no contexto da tese:

- P – probabilidade de um elemento ter sucesso ao enviar um determinado fluxo de dados, ou seja, qual é a preferência de um elemento para enviar determinada classe de fluxo de dados.
- Q – probabilidade de um elemento falhar na transmissão de um determinada classe de fluxo de dados.

Os valores de P e Q são calculados em uma base de tempo fixa (que pode variar em princípio de equipamento para equipamento) na qual o agente de controle:

- analisa todos os fluxos que foram transmitidos pelo equipamento controlado;
- classifica os tipos de fluxos de dados de acordo com um código, similar ao que é feito através do DSCP;
- verifica para quais fluxos as variáveis que definem a qualidade do serviço estão próximos ao limite de controle estabelecido (uma porcentagem do valor do parâmetro definido). De acordo com os valores atribuídos às variáveis os valores de P ou de Q são alterados.

Os fluxos que atingirem os valores limites das variáveis (ou de uma delas) será contabilizado como alta probabilidade de falha e serão utilizados para incrementar o valor de Q. Os demais fluxos serão utilizados para alterar o valor de P.

O valor de P baseado em Dorogovtsev; Mendes e Samukhin, 2000 é definido como:

$$P_t^a \quad = A + \frac{P_{t-1}^a + \; p_t^a}{\sum_x \; P_t^x}$$

onde:

- P_t^a - sucesso da entidade ‘a’
- A - valor de preferência pré-definido
- P_{t-1}^a - valor de sucesso do *preferential attachment* no instante t-1
- p_t^a – medida de serviços prestados com sucesso no instante t por ‘a’
- $\sum_x P_t^x$ – somatório da medida de sucesso de todas as classes de fluxos de dados transmitidas;

O valor de q é definido como:

$$Q_t^a = \frac{Q_{t-1}^a + q_t^a}{\sum_x Q_t^x}$$

onde:

- Q_t^a - falha da entidade ‘a’
- Q_{t-1}^a - valor de falha utilizado no *preferential attachment* no instante t-1
- q_t^a – medida de serviços prestados com falha no instante t por ‘a’
- $\sum_x Q_t^x$ – somatório da medida de falha de todas as classes de fluxos de dados transmitidas;

Não precisa que todos os agentes de um determinado tipo utilizem a mesma estratégia de cálculo, considerando os mesmos parâmetros, uma vez que dada a autonomia o agente pode decidir como deve se considerar um fluxo com falha ou com sucesso. Contudo o entendimento dos parâmetros deve ser o mesmo em todo domínio administrativo, caso contrario não se pode garantir que os fluxos sejam tratados de forma coerente.

Cada um dos *links* possui um valor de P e Q, calculado pelos agentes RMA aos quais aquele *link* inicia e termina e para um determinada classe de fluxo de dados e um destino. Desta forma o agente pode determinar qual *link* pode enviar que tipo de fluxo independentemente da direção que o fluxo de dados possua (solicitação ou resposta de serviço). Logo, um agente determina por si só qual é o *preferential attachment* com cada vizinho (peer).

Quando um agente não possui nenhum *link* com as condições necessárias, isso significa que o valor de P daquele agente diminuirá em relação àquela classe de fluxo de dados, enquanto o valor referente de Q aumentará. Embora não exista uma comunicação direta entre os agentes de controle para informar os valores de P e Q, esse dado é compartilhado pelo efeito que ele causa nas variáveis de controle de qualidade de serviços. O efeito de P e Q, de um determinado agente RMA é propagado através da hierarquia superior composta pelo agente PA, pois no momento que o agente RMA não oferecer condições de tráfego para um determinado tipo de fluxo e um determinado destino, os valores de P e Q sofrerão variação, e tais valores são periodicamente informados ao PA. Uma vez que todos os agentes RMA reportam-se ao seu respectivo PA, esse agente possui uma visão completa do estado de transmissão de todos os fluxos de dados da região do domínio administrativo da qual é responsável. A função do PA é então de informar os agente EA e os demais PA sobre as condições de tráfego e o agente EA torna o dado sobre o transporte de uma determinada classe de fluxo de dados para o agente UA, que pode determinar se continua ou não com a prestação do serviço via o agente EA escolhido.

A abordagem possui dois aspectos em relação ao controle. O primeiro é que falhas localizadas podem ser solucionadas sem a intervenção de um ponto central, ou seja, falhas localizadas podem ser dirimidas localmente sem causar mensagens ou demandar recursos externos ao elemento (mantendo a autonomia). O segundo ponto é relativo a como o dado é propagado. Logo, se um elemento falha e há caminho alternativo no domínio administrativo, essa reconfiguração também é local, e, portanto não causa impactos no comportamento do domínio visto de pontos externos, assim como não deve ser significativo em pontos não diretamente envolvidos com a falha no mesmo domínio administrativo. Portanto uma alteração de comportamento nos elementos de borda do sistema de comunicação só ocorrerá quando o domínio administrativo não comportar a quantidade de fluxos de dados requerida por uma razão que ocorra após o início do provimento do serviço, como uma falha ou conjunto de falhas que causem a indisponibilidade na entrega um certo conjunto (ou classes) de fluxos de dados para determinados destinos por todos

os caminho. Nesses casos o domínio administrativo como um todo sofrerá uma "punição" pois o valor de P e Q informados pelos agentes de borda do domínio administrativo para os usuários finais indicarão a inapropriação para o transporte de determinado fluxo de dados, ou seja, outros agentes de borda de outras redes de acesso podem ter "ofertas" mais interessantes para uma determinada classe de fluxo de dados e um destino (valor de P maior e Q menor).

4.3.2 Comunicação entre os agentes da arquitetura

Os agentes de controle presentes em cada elemento do sistema de comunicação não precisam trocar informações entre si para calcular suas variáveis de decisão, e isso não seria uma estratégia interessante, pois cada elemento de um sistema de comunicação sobre influências diversas dos elementos que estão conectados a ele de alguma forma (ou diretamente conectados ou elementos que enviam uma determinada classe de fluxo de dados que afeta de forma determinante[18] o elemento de rede). A comunicação existente ocorre entre os agentes de controle e os agente de coordenação (PA e SCA) e desses com os agentes de borda do sistema de comunicação, pois para que ocorra um entendimento comum sobre as capacidades de um domínio administrativo e haja uma negociação entre domínios administrativos os agentes de coordenação devem informar o estado de seu domínio administrativo ou de seu sistema autônomo.

A estratégia acima é necessária porque podem existir mais de um ponto de interconexão entre domínios administrativos, sendo que podem ocorrer

[18] Entende-se por afetar de forma determinante um tipo de fluxo de dados que quer pela quantidade quer pelos recursos demandados torna-se um dos fatores que alteram de forma significativa o comportamento do elemento do sistema de comunicação. Nessa tese não é discutido valores ou intervalos numéricos que definam a significância de um elemento sobre outro. Essa abordagem necessita de conceitos de lógica fuzzy os quais não fazem parte do contexto desse trabalho. Referências sobre esse assunto podem ser encontradas em (Wang, Lee, Ho, 2007).

entradas preferenciais de um domínio administrativo para alcançar-se um determinado destino, como ocorre hoje com o roteamento inter-AS (BGP) (Halabi, McPherson; 2000). Esse tipo de comunicação oferece subsídios para que ocorra um tratamento via roteamento entre domínios administrativos, de forma similar ao que ocorre entre os equipamentos de roteamento IGP em um domínio administrativo (como o agente reorganiza o tráfego em uma rede baseada no protocolo IP, por exemplo). Dessa forma a arquitetura proposta é capaz de inter-operar com os sistemas legados de roteamento para redes IPs e pode-se dizer que a arquitetura continuará compatível com as novas implementações e padrões de inter-operação de sistemas de comunicação (como discutido no item 4.4), pois diversos estudos indicam que todas as redes utilizarão como protocolo de inter-operação o IP (possivelmente IPv6) assim como sua estrutura de roteamento.

4.4 COMPARAÇÃO ENTRE A ARQUITETURA PROPOSTA E A ARQUITETURA IMS

A arquitetura IMS propõe uma serie de componentes, principalmente em sua camada de controle (ETSI, 2009a), (ETSI, 2009c), que são similares, em termos de funcionalidade com a arquitetura proposta. Os conceitos são:

- *Call State Control Function* (CSCF): funcionalidades relacionadas ao controle da sessão do usuário;
- *Home Subscriber Service* (HSS): controle o perfil do usuário;
- *Policy Decision Function* (PDF): relacionado com a decisões de tráfego de QoS.

O CSCF deve manipular protocolos utilizados para estabelecer caminhos de QoS e troca de parâmetros de QoS entre os equipamentos da rede e os elementos da arquitetura IMS . O CSCF é dividido nos seguintes componentes funcionais:

- *Proxy* CSCF (P-CSCF): primeiro ponto de contato entre a arquitetura IMS e o dispositivo do usuário. O P-CSCF envia dados de conexão para o terminal, função que é feita na arquitetura proposta pelo EA.

Contudo o EA envia dados do USLA estabelecido e não apenas da conexão;

- *Interrogating* CSCF (I-CSCF): contatar pontos entre o operador da rede (de um domínio administrativo) e o assinante do serviço, o qual atribui um S-CSCF e um parâmetro de utilização do serviço (CRD – *Charging and Resource Utilization*). Tais funções estão presentes no RMA e também no EA.
- *Serving* CSCF (S-CSCF): mantém o estado da sessão do serviço na infraestrutura. Essa função está presente no RMA, UA, EA e AS.

O S-CSCF utiliza o *Home Subscriber Service* (HSS) para prover um serviço de qualidade adequada ao usuário. O IMS não especifica se esse elemento é centralizado ou não, embora a abordagem distribuída seja sugerida. Na arquitetura proposta nesta tese não há impedimentos de haver um equipamento centralizador de perfil de usuário. Contudo, esse deve também ser distribuído para o dispositivo do usuário, pois tais dados são necessários para se optar por um determinado USLA de uma rede de acesso ("oferta"). A arquitetura proposta propõe que o perfil do usuário seja manipulado e armazenado pelo UA.

A arquitetura proposta pressupõe provedores de serviço com infra-estrutura para entrega de conteúdos interativos e multimídia. Certamente esses elementos possuem diversas características do I-CSCF pois é esse o elemento no IMS que armazena características do serviço, como por exemplo a qualidade a ser transmitida e que tipo de recursos são utilizados por determinado serviço. O provedor de serviço também necessita de alguns dados do HSS, pois este fica localizado na rede de origem do usuário (onde ele está cadastrado). Contudo, em se considerando diversas redes possíveis de serem utilizadas pelo usuário, é necessário os dados estarem distribuídos para determinar qual é a rede a ser utilizada pelo usuário. Logo, torna-se uma vantagem para a abordagem heterogênea ter o agente UA como provedor de tais informações.

Já as funções do S-CSCF também necessitam estar disponíveis para o provedor de serviço e para o operador da infra-estrutura de comunicação, mas

também necessitam estar no dispositivo do usuário, pois ele deve determinar mudanças na entrega dos serviços caso o USLA não seja mantido. A distribuição dos dados também é útil para a realização de operações de *handover* (embora tal discussão não faça parte do escopo dessa tese).

O IMS também possui o *Policy Decision Function* (PDF) cuja principal função está relacionada com a especificação de parâmetros de QoS. O PDF pode estar localizado na infraestrutura do sistema de comunicação e deve conter conjuntos de dados que especifiquem cada contrato de QoS. Quando o PDF recebe a especificação do serviço, a USLA e a identificação do usuário, ele deve prover os dados das configurações para os elementos da rede. Na arquitetura proposta essa especificação de configuração deveria ser enviada aos agentes (UA, EA, RMA e SA), que conhecendo os possíveis caminhos e suas capacidade de entregar tal conteúdo, determinam o caminho a ser utilizado, independentemente de consulta a um sistema central. As requisições iniciam-se no UA (que também é responsável por medir os parâmetros de QoS durante a execução do serviço e controlar o dispositivo) e termina no SA, localizado no provedor do serviço.

5 DESENVOLVIMENTO E RESULTADOS EXPERIMENTAIS DA ARQUITETURA DE CONTROLE DE QOS PROPOSTA

A realização de uma prova de conceito sobre o comportamento dos agentes é apresentada neste capítulo como forma de verificar se o conceito de *preferential attachment* pode resultar em um controle de qualidade de serviço efetivo, assim como identificar se o comportamento autônomo dos agentes permite se ter coerência nas decisões de qualidade de serviços. Para atingir as metas da prova de conceito foi construída uma aplicação composta de agentes RMA e uma infraestrutura IP montada através da criação de máquinas virtuais. As conexões entre essas máquinas foram feitas de forma a se construir uma rede dividida em três partes: uma rede de núcleo, redes de acesso e rede de dispositivos de usuários finais, como ilustrado na Figura 12.

Os resultados experimentais foram obtidos através da implementação de parte da arquitetura proposta em uma plataforma para programação de sociedades multiagentes denominada JADE (Bellifemine, Poggi, Rimassa, 2001), (Bellifemine, et.al, 2008) utilizando tecnologias e linguagem de programação Java como suporte à implementação do *software*. A implementação de uma rede de *backbone* e de redes de acesso realizou-se através da instalação de máquinas virtuais com sistema operacional LINUX personalizado para representar e se comportar como um equipamento de rede (roteador). O controle de geração de fluxo de dados com características particulares e as alterações do funcionamento da infraestrutura foram executadas através das aplicações *Distributed Internet Traffic Generator* (D-ITG) e NETEM (*Network Emulator*) respectivamente.

Todos os experimentos e cenários consideraram todos os elementos operando sob o protocolo IP, sendo que cada elemento pode ser configurado para representar um tipo de rede de acesso distinto, ou um tipo de comportamento de backbone ou o comportamento de um conjunto de clientes, de acordo com os testes executados. Todo o tráfego gerado pelo D-ITG foi marcado através do campo ToS do protocolo IP (interpretado como DSCP pelo

D-ITG) para que os agentes da arquitetura pudessem distinguir entre os tipos de tráfego distintos.

5.1 TECNOLOGIAS E SISTEMAS UTILIZADOS

Para a elaboração da prova de conceito desta tese elaborou-se um ambiente composto de máquinas virtuais configuradas para operarem como roteadores de rede IP e diversas aplicações para geração e monitoração dos fluxos de dados para extração dos dados relevantes para a análise do comportamento dos agentes da arquitetura proposta.

As tecnologias utilizadas foram:

- Sistema operacional Linux Debian netinst 4.10, *kernel* 2.6.26;
- Aplicação IPFIX da Fokus;[19]
- D-ITG verão 2.7 Beta 2;
- *Traffic Control* (TC) e *IProute*2 para controle de caminhos, filas das interfaces de redes, dentre outros;
- NETEM.[20]

As tecnologias e suas configurações são detalhadas nos itens a seguir.

5.1.1 Infraestrutura utilizada

A infraestrutura para execução de testes foi elaborada em três grupos de elementos de comunicação distintos conforme ilustrado na Figura 12. Os elementos do grupo “Usuários Finais” devem representar os fluxos gerados pelos usuários finais de um sistema de comunicação. Nesses elementos está

[19] Agradeço a Tanja Zseby por ceder os códigos fonte do coletor e do probe IPFIX em desenvolvimento pelo Centro de Competência de Pesquisas em Redes da Fraunhofer Fokus (http://www.fokus.fraunhofer.de).

[20] Versão e instruções utilzadas disponíveis em (http://www.linuxfoundation.org/collaborate/workgroups/networking/netem)

instalado o gerador de tráfego D-ITG versão 2.7-beta2[21] para a geração e recepção do tráfego que atravessa toda a infraestrutura do sistema de comunicação. Os fluxos de dados gerados via D-ITG foram utilizados de forma a gerar distribuições similares em diversos trabalhos que se utilizam do D-ITG como Barolli, et.al (2009), Han, et.al. (2008) e Narayan; Graham e Barbour (2009).

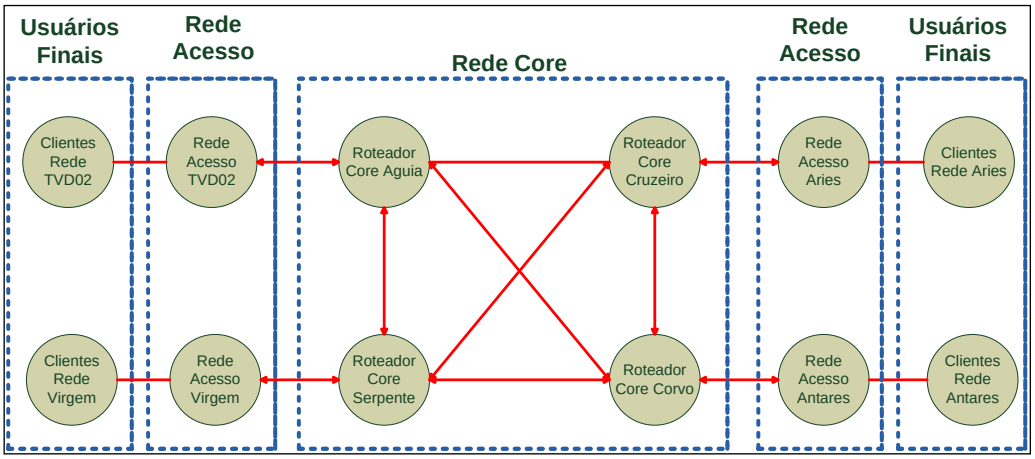

Figura 12 – Infraestrutura de rede utilizada nos testes do conceito da tese

O segundo grupo de elementos denominado “Rede Acesso” representam as redes de acesso e possuem configurações para representar as características de diversas tecnologias de acesso em relação a parâmetros como atraso, banda, variação de atraso, perda de pacotes e pacotes corrompidos. Tais alterações no tráfego são obtidas através do uso de duas aplicações integradas ao núcleo do sistema operacional (responsável pelo roteamento e encaminhamento dos pacotes). A primeira aplicação denomina-se *Traffic Control* (TC) e sua principal função é organizar as filas de uma interface e segmentar o tráfego de acordo com os parâmetros definidos, assim como controlar a largura de banda e demais características de uma

[21] Utilizou-se a versão beta da aplicação D-ITG devido à versão de kernel do sistema operacional utilizado. Segundo dados do site oficial da ferramenta D-TIG (http://www.grid.unina.it/software/ITG/) conusultado em novembro e dezembro de 2009, a versão beta apenas corrige questões de referencias à bibliotecas do kernel atual do sistema operacional Linux sem prejudicar quaisquer funcionalidades de geração e recepção de tráfego em relação às versões estáveis da aplicação D-ITG.

determinada interface (real ou virtual) de modo a se poder estimar comportamentos de canais com características diversas como canais de rede ethernet e de rede GSM, por exemplo. (Hubert,et.al. 2004). A segunda aplicação denomina-se NETEM e seu papel é emular propriedades de uma rede de dados IP. Com essa aplicação é possível causar atrasos em pacotes de diversas formas possíveis (como uma taxa constante ou uma distribuição normal). Da mesma forma o NETEM permite a geração de atrasos e variações de atrasos, pacotes corrompidos, perda e reordenação de pacotes, taxa de transmissão e controle de buffer, dentre outros aspectos. (Hemminger, 2005), (Choe, et.al, 2007)

Os elementos da "Rede *Core*" representam uma rede *backbone* com todos os elementos possuindo conexão com todos os demais elementos (infraestrutura *full-mesh*). Dessa forma, os agentes de controle da arquitetura podem utilizar diversos caminhos para segmentar diferentes classes de fluxos de dados para um destino específico (no caso de testes de existência de hubs no sistema de comunicação) ou para diversos destinos distintos. Tendo uma estrutura *full-mesh* e seu roteamento podem causar um efeito indesejado uma vez que há a possibilidade de formação de caminhos circulares que não permitem que um determinado destino seja alcançado. Portanto, deve fazer parte da decisão do agente não considerar caminhos que possam formar caminhos circulares. Para tal deve ser analisado se a origem do fluxo de dados é o próximo destino que o agente pode enviar o fluxo. Nestas condições o trecho que tem como extremidade a origem do fluxo de dados não deve ser considerado elegível. As mesmas aplicações existentes nas redes de acesso também estão presentes nos elementos da "Rede *Core*".

5.1.1.1 *IP Flow Information Export* (IPFIX)

Em todos os elementos da infraestrutura montada está instalada uma aplicação cuja meta é extrair dados através do protocolo IPFIX (Quittek; et.al., 2004), (Zseby, et. al, 2009), (Claise, 2008). Esse protocolo é similar ao protocolo NetFlow (Bin,et.al, 2008) e sua função é agregar dados sobre todos os fluxos de dados de uma determinada interface via um elemento de software denominado "*probe*" e enviar tais dados a uma outra entidade de software

denominada “coletor”. Os dados coletados pelo coletor IPFIX são organizados por fluxo de dados individuais, identificando os seguintes dados:

- Tempo de início de processamento do pacote e de seu término no elemento da rede (em milissegundos);
- Endereço IP origem e destino do fluxo de dados;
- Porta TCP ou UDP de origem e destino;
- Identificação de fluxo de dados via campo IP ToS;
- Quantidade de pacotes e octetos pertencentes àquela amostragem de dados.

Em relação às medidas de qualidade de serviço propostas para a prova de conceito estão o atraso e a perda de pacotes. O IPFIX auxilia na medição desses fatores porque para se ter o atraso total (equipamentos mais atraso de transmissão) basta ter a diferença entre o tempo que o fluxo de dados começou a ser processado em um equipamento e o tempo em que iniciou a mesma operação no equipamento adjacente. O tempo que uma determinada porção do fluxo de dados permaneceu no equipamento também é medido pelo IPFIX. Os elementos do sistema de comunicação estão todos sincronizados com o relógio da máquina hospedeira do ambiente de máquinas virtuais utilizados como roteadores de acordo com o especificado em Sun (2009), onde se utilizou como base de sincronismo a configuração ACPI[22] em todas as máquinas virtuais e verificação de sincronismo a cada um segundo.

O benefício de se utilizar a tecnologia IPFIX em detrimento de outras tecnologias de monitoração como o SNMP é o fato desse último considerar os dados por pacotes e, embora seja relevante, não traz informações sobre como o fluxo de dados se comporta. Logo, com o IPFIX é possível analisar o tempo gasto com o processamento do tráfego e sua transmissão, e em que ponto tal fato ocorre, assim como se percebe em intervalos de tempo qual fluxo causa variação na carga do *link* e como essa variação ocorre. A perda de pacotes em um *link* também é medida em termos de fluxos, sendo que a perda pode ser identificada como a quantidade de pacotes e octetos que há em um elemento

[22] *Advanced Configuration and Power Interface*

de rede e quantos pacotes e octetos chegam no elemento do elemento adjacente, como ilustrado na Figura 13.

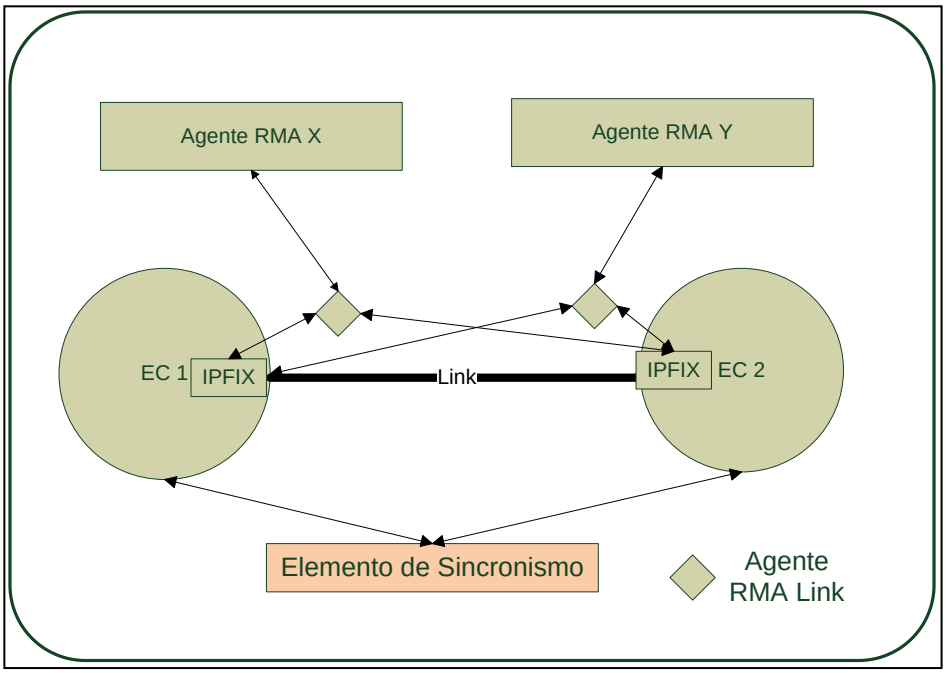

Figura 13 – Coleta de Dados pelo Agente RMA via IPFIX

Cada agente da Figura 13 recebe dados das duas extremidades do *link* e com isso é capaz de estimar o comportamento de todos os fluxos de dados que se utilizam daquele *link*. Em havendo sincronismo os agentes podem através de seus algoritmos de decisão determinar quais tipos de fluxo serão transportados por esse *link*.

Embora um agente não possa determinar como deve ser o comportamento dos fluxos de dados que chegam até ele, tais fluxos irão causar alterações no comportamento do *link* gerenciado pelo agente e tendo como conseqüência possíveis alterações tanto em P e Q que representam a preferência daquele *link* para cada tipo de fluxo de dados. O agente não necessita impedir a chegada de fluxos de dados uma vez que essa atividade é responsabilidade do agente adjacente. Contudo, o agente será o responsável por encaminhar todo fluxo que a ele é entregue para o destino final de acordo com os parâmetros estabelecidos de QoS, alterando as interfaces de envio de acordo com as condições do sistema de comunicação.

Um agente RMA não conhece um contrato de USLA, pois na arquitetura essa atividade pertence ao PA. O agente RMA controla o melhor caminho para

uma determinada classe de fluxo de dados dado um mesmo conjunto de requisitos do USLA, mas com valores para aquele segmento da infraestrutura. Isso é possível dado as características do IPFIX. O agente deve saber qual é o atraso e demais características que o equipamento que ele gerencia causa para manipular um determinado tipo de fluxo de dados por destino. Esses valores são enviados ao PA (juntamente com P e Q) para que a visão da rede seja estabelecida e seja possível identificar os agentes RMA que apresentam os melhores comportamentos (conceito similar ao PHB do *DiffServ*). Embora a tese não discuta mecanismos para alterar a preferência de um agente RMA sob outro (por razões de engenharia de tráfego em uma infraestrutura) pode-se ter essa situação alterando-se o valor do parâmetro A da equação de P. Dessa forma pode-se alterar o comportamento inicial dos agentes e alterar a forma como os fluxos de dados são encaminhados em um domínio administrativo.

5.1.1.2 Estrutura de Roteamento dos Elementos de Rede

De acordo com a topologia da Figura 12 apenas na estrutura “Rede Core” o agente poderá optar por três caminhos distintos para enviar um determinado fluxo de dados; um será o caminho determinado pelo roteamento (caminho padrão) e os outros dois caminhos serão considerados secundários.

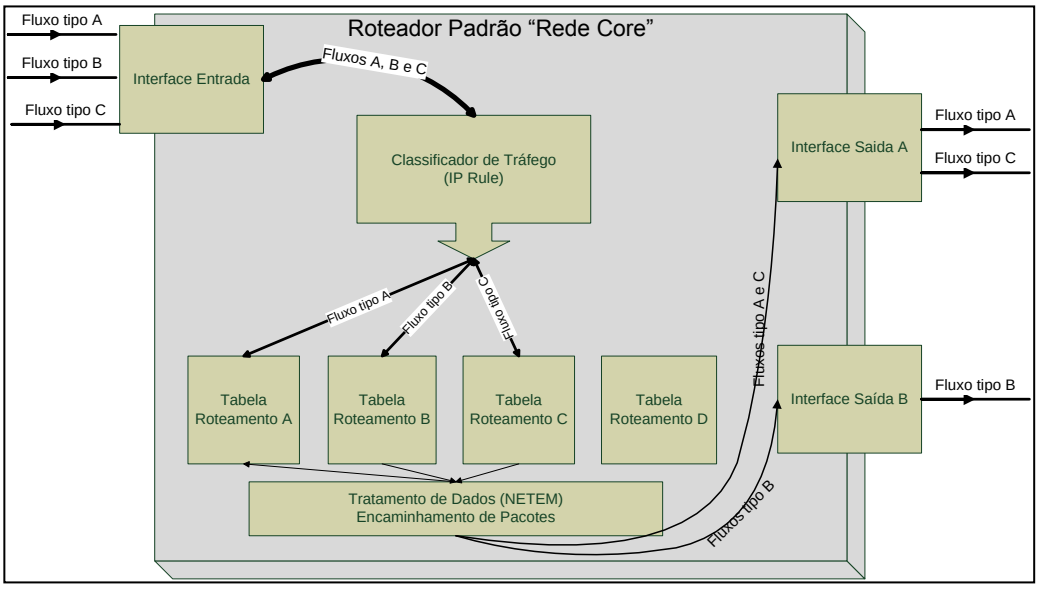

Figura 14 – Estrutura de Seleção de Tráfego e roteamento

Naturalmente o agente só poderá optar por um caminho que leve ao destino, e não qualquer caminho existente. Portanto, o roteamento IP se faz

interessante pois, em um domínio administrativo em geral utiliza-se protocolos de roteamento baseados em algoritmos *link state*, nos quais todos os caminhos existentes entre uma origem e um destino são conhecidos por todos os elementos do sistema de comunicação (Ross, Kurose, 2007), (Doyle,Carol,2005)

```
#aplicar filtro de roteamento
ip rule add from 192.168.3.0/24 table 9

#####################################################################
#Da rede de acesso conectada em Corvo para as demais redes de acesso
# visao de Aguia - nao pode enviar de volta para 30.0.0.2
#####################################################################
#Da rede de acesso conectada em Corvo para as demais redes de acesso
#de Corvo-chegando em aguia-> para o destino 192.168.3.0/24
echo 10 fromRede1921684 >> /etc/iproute2/rt_tables
###trafego de dados
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x10 via 10.0.0.2
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x10 via 40.0.0.2
metric 100
###trafego de voz
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x20 via 10.0.0.2
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x20 via 40.0.0.2
metric 100
###trafego de video
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x30 via 10.0.0.2
ip route add table fromRede1921684 to 192.168.3.0/24 dsfield 0x30 via 40.0.0.2
metric 100

#de Corvo-chegando em aguia-> para o destino 192.168.2.0/24
###trafego de dados
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x10 via 40.0.0.2
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x10 via 10.0.0.2
metric 100
###trafego de voz
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x20 via 40.0.0.1
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x20 via 10.0.0.2
metric 100
###trafego de video
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x30 via 40.0.0.1
ip route add table fromRede1921684 to 192.168.2.0/24 dsfield 0x30 via 10.0.0.2
metric 100

#de Corvo-chegando em aguia-> para o destino 192.168.1.0/24
#rota default para a rede de acesso "controlada" por serpente
ip route add table fromRede1921684 to 192.168.1.0/24 via 172.16.1.2
```

Figura 15 - Tabela de Roteamento de um roteador “Rede Core” (fragmento)

Baseado na premissa de roteamento IP, cada agente possui um conjunto de tabelas de roteamento, uma para cada possível origem existente de fluxos de dados. Em cada tabela há um conjunto de rotas para cada tipo de fluxo de dados existente, como pode ser observado na Figura 15. Nesta figura é descrito um trecho da implementação de uma tabela de roteamento em um agente no qual é tratada uma origem, todos os fluxos de dados utilizados na prova de conceito e todos os caminhos possíveis. Nota-se que para uma determinada origem há rotas para todos os tipos de fluxos de dados quando considerado uma rede de destino. Essa foi a forma escolhida para operar o

roteamento por ser possível aplicar-se filtros para todos os tipos de tráfego e saber quais as rotas válidas para aquela classe de fluxo de dados e destino em um ambiente Linux. As tabelas de roteamento são instaladas em cada roteador da “Rede Core” quando esse inicia sua operação, como ilustra a Figura 14. De acordo com as medidas obtidas através do IPFIX o agente altera na tabela de roteamento qual rota deve ser utilizada, e dessa forma altera o caminho por onde um determinado tipo de fluxo de dados é enviado.

De acordo com a Figura 14 todo o tráfego que chega em uma interface do roteador é analisado por um filtro que identifica qual a origem do fluxo de dados. Com essa informação o roteador utiliza uma das quatro tabelas de roteamento existentes e seleciona qual rota utilizar através do campo DSCP (ou ToS do protocolo IP). A Figura 15 ilustra a organização de uma (das quatro) tabela de roteamento de um roteador da “Rede Core”.

5.1.1.3 Geração de Fluxos de Dados com D-ITG

A geração de tráfego via a ferramenta D-ITG foi executada em clientes representados pelas máquinas virtuais "Clientes Rede TVD02" e "Clientes Rede Virgem" e destinada a provedores de serviços localizados em "Clientes Rede Aries" e "Clientes Rede Antares", sendo que alguns tipos de fluxos de dados apresentavam o comportamento de um serviço com requisição e resposta e outros fluxos de dados apenas enviavam conteúdo para o destino. Os fluxos de dados utilizados para a prova de conceito foram:

- fluxo de dados A: fluxo formado por pacotes de dados com a característica de tamanho variando em uma distribuição normal com média de 500 bytes e desvio padrão de 300 bytes e sendo enviados a uma taxa definida por uma distribuição de poisson com uma média de 1200 pacotes por segundo;
- fluxo de dados B: fluxo formado por pacotes de dados com a característica de tamanho variando em uma distribuição constante de 1500 bytes e sendo enviados a uma taxa definida por uma distribuição de Poisson com uma média de 1200 pacotes por segundo;

- fluxo de voz sobre IP (VoIP): fluxo formado por pacotes de dados com a característica de tamanho médio de 80 bytes e taxa de transmissão de aproximadamente 100 pacotes por segundo e utilizando como codec o G.711 com uma amostra de voz por pacote (Avalone, et.al, 2009).

5.1.1.4 Geração de Falhas com NETEM

O *software* NETEM foi utilizado nos testes para gerar atrasos em algumas portas de roteadores da "Rede Core" como forma de tornar um caminho para um determinada classe de fluxo de dados com menor preferência em relação aos demais caminhos. Na maioria dos testes a infraestrutura era colocada em uma situação onde as três rotas possíveis para um determinado destino e fluxo de dados possuíam a mesma preferência (*preferential attachment*). Contudo, uma delas era escolhida como a rota principal (com menor métrica em termos de roteamento), enquanto as demais não recebiam tráfego.

Cada agente possui limites para os parâmetros de rede para cada classe de fluxo de dados, sendo esses parâmetros configurados no agente como o limite máximo do valor de um parâmetro que é aceitável para uma determinada classe de fluxo de dados continuar respeitando o contrato de USLA. Caso esse limite seja ultrapassado o agente deve promover a escolha de um novo *link*, ou seja, de todos os *links* possíveis para aquele destino, verificar o valor de Q de cada *link* e esse valor representará a probabilidade do *link* ser escolhido para continuar a enviar o tráfego.

5.1.2 Software Desenvolvido

O software desenvolvido para a realização da prova de conceito é composto por agentes que possuem estrutura de coleta e organização de dados do IPFIX, a manipulação dos fluxos de dados e cálculo do *preferential attachment*, como descrito nos itens a seguir.

5.1.2.1 Estrutura de coleta e organização de dados IPFIX

A monitoração via protocolo IPFIX é realizada instalando-se um *probe* em cada uma das interfaces de comunicação de cada equipamento de comunicação (EC) da infraestrutura utilizada; e a função do *probe* é os dados sobre o comportamento dos fluxos de dados em uma determinada interface (Figura 16). A figura identifica o elemento *probe* de dados IPFIX e cada extremidade de um trecho entre dois elementos de comunicação. Os losangos representam processos do agente RMALink para os quais o *probe* de dados IPFIX envia dados periodicamente. Cada *probe* é questionado por duas aplicações que buscam dados: um coletor IPFIX utilizado para sumarizar os dados dos fluxos de dados independentemente do agente RMA; e o agente RMALink que também acessa os dados IPFIX para informar para o agente sobre o estado do *link* que monitora.

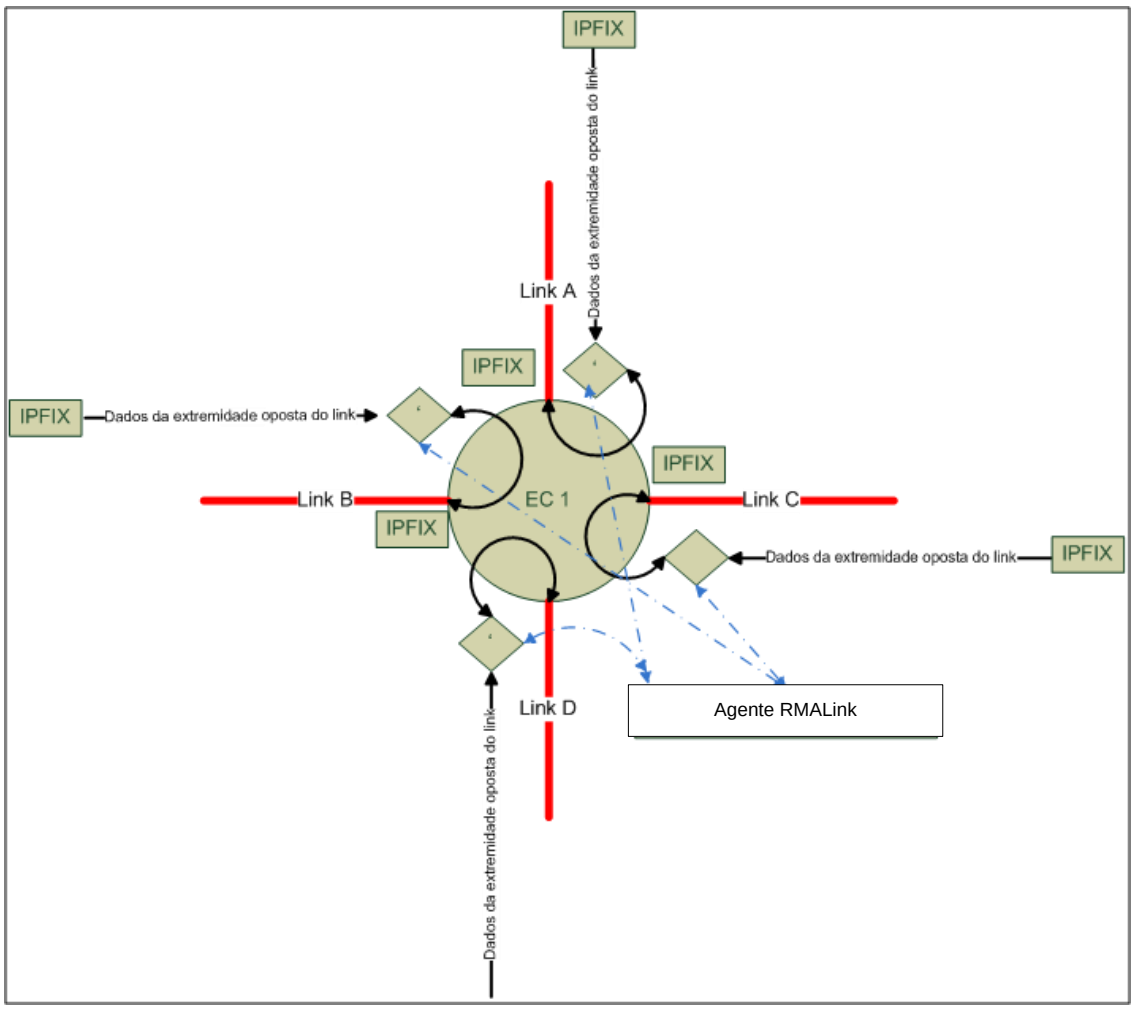

Figura 16 – Coleta de dados via IPFIX

O agente por sua vez cria uma tabela que representa os dados obtidos de cada *probe*. As duas tabelas (vindas de dois probes distintos e recebida por um agente RMALink são compiladas em uma única tabela denominada “Tabela IPFIX do *Link* X”, onde X é a identificação do *link*. Na Figura 17 X assume o valor 'A'.

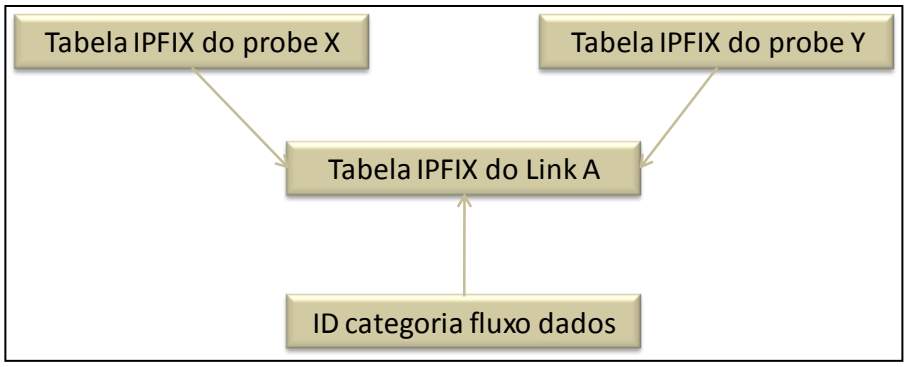

Figura 17 – Organização dos dados IPFIX em uma tabela que representa o *link*

Todas as tabelas de *link* (quatro nos experimentos realizados) são então enviadas ao agente RMA e esse compila-as para formar a tabela de resultados parciais a qual contém o estado de todos os *links* para cada classe de fluxo de dados. Aliando a tabela de resultados parciais com a tabela de roteamento podem-se classificar as rotas em relação a destino versus classe de fluxo de dados versus estado de um determinado *link* e determinar os melhores caminhos para uma determinada classe de fluxo de dados, como ilustrado na Figura 18.

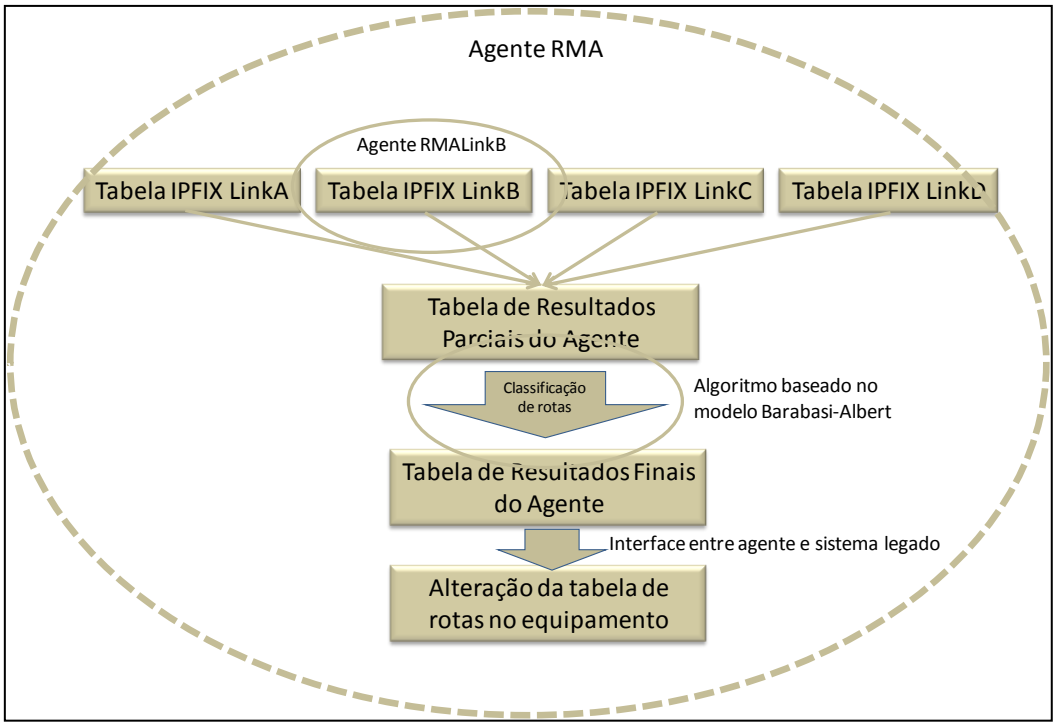

Figura 18 – Organização dos dados no agente RMA

5.1.2.2 Fluxo de dados

O fluxo de dados apresentado na Figura 19 representa o envio de um fluxo de dados da origem ao destino e como esse é tratado pelos elementos da rede. Destaca-se que um fluxo de dados é tratado pelo NETEM quando atinge uma determinada interface de um equipamento e após este tratamento é que há a medição pelo IPFIX e opção de roteamento. O módulo IPFIX controlado pelo agente RMALink executa a medidas do fluxo de dados após o tratamento do NETEM e informa o agente RMA. O agente então interfere na rota a ser escolhida para um determinado tipo de fluxo de dados de acordo com os critérios descritos em item a seguir desta tese.

5.1.2.3 Cálculo do *Preferential Attachment*

Cada agente possui limites para os parâmetros de rede para cada tipo de fluxo de dados, sendo esses parâmetros configurados no agente como o valor limite máximo aceitável de um parâmetro para um determinado tipo de fluxo de dados continuar respeitando o limite imposto pelo agente PA (com relação direta ao contrato de USLA). Caso esse limite seja ultrapassado o agente deve

promover a escolha de um novo *link*, ou seja, de todos os *links* possíveis para aquele destino, verificar o valor de Q de cada *link* e esse valor representará a probabilidade do *link* ser escolhido para continuar a enviar o tráfego.

A meta do agente é monitorar todos os seus *links* em relação às classes de fluxo de dados, periodicamente avaliar todos os *links* e optar por um dos possíveis caminhos para encaminhar determinada classe de fluxos de dados de acordo com o *preferential attachment* segundo as regras a seguir:

- verificar os limites estabelecidos para cada parâmetro de controle do fluxo de dados (atraso e perda de pacotes[23]) para verificação de falha;
- caso o *link* não apresente falha para um determinado tipo de fluxo de dados, então todos os fluxos são contabilizados como transmissão com sucesso e incrementam o valor de P;
- caso o *link* apresente falha para um determinado tipo de fluxo de dados, então o valor de Q é incrementado;
- é montada uma "Roleta de Monte Carlo" (Frenkel, 2004) com os valores de Q (normalizados), cujo significado é: "quanto menor o Q maior a probabilidade do *link* ser escolhido por apresentar menor falha no tratamento de determinado tipo de fluxo de dados";
- o *link* sorteado é instalado na tabela de roteamento apropriada pelo agente e o tráfego é enviado pelo novo caminho, o qual continua sendo monitorado pelo agente, independentemente de se ter sucesso ou falha do *link* para aquele determinado tipo de tráfego.

A escolha de um *link* independentemente de se ter sucesso ou falha via o algoritmo de “Monte Carlo” é uma forma se promover o *preferential attachment*, pois se dois *links* não apresentarem quantidades de falhas equivalentes para uma determinada classe de fluxo de dados, ambos tem iguais chances de

[23] Para efeitos da prova de conceito, apenas atraso e perda de pacotes foram considerados como parâmetros de controle. Essa restrição, contudo não representa nenhum tipo de limitação da arquitetura proposta.

serem escolhidos para aquela determinada classe de fluxo de dados, não ocorrendo dessa forma um desbalanceamento do valor de P (em princípio). Em ocorrendo falhas em um dos *links* ocorrerá uma diferenciação entre eles.

Cabe destacar que um *link* pode apresentar falha para um determinado tipo de fluxo de dados, e contudo não apresentar falha para outro tipo de fluxo de dados devido as diferenças de requisitos entre os fluxos. Logo, espera-se que após o estabelecimento do *preferential attachment* apenas o fluxo de dados que apresentou falha seja elegível para ser encaminhado por outro *link*, enquanto os demais fluxos de dados sejam elegíveis para alteração de caminho apenas em caso de *links* similares em termos de *preferential attachment*.

5.2 CENÁRIO DE TESTES

Os testes foram realizados em três etapas distintas. A primeira etapa consiste em validar o modelo de infraestrutura elaborado em ambiente virtual para verificar sua adequação em relação aos modelos e estimativas de operação de uma infraestrutura real (considerando redes IP). Para tal foram realizados ensaios para determinar a função cumulativa de tráfego, comumente utilizada para representar o comportamento de tráfego de um sistema de comunicação. Os testes foram realizados para dois tipos de tráfego distintos. O tráfego de dados é composto de três fluxos de dados distintos para que uma porcentagem dos pacotes IP possua valores pequenos (em torno de 64 bytes), ou outra porcentagem de pacotes com tamanho máximo de MTU de 1500 bytes o restante do tráfego com distribuição normal de tamanho de pacotes com média em torno de 500 bytes.

Os fluxos de dados de voz representam as características de chamadas VoIP com codificação G.711, pois de acordo com Botta; Dainotti e Pescapè, (2007) o gerador de tráfego D-ITG gera, com esse codec, um tráfego adequado para representação de fluxos de dados encontrados nas redes de dados atuais. Nos testes para a prova de conceito não foram utilizados fluxos de vídeo, pois seu tráfego característico no padrão MPEG4 exigia mais recursos do que os disponíveis no ambiente de testes.

5.2.1 Teste de validação da estrutura montada

Os testes realizados neste item visam identificar o comportamento característico da infraestrutura montada para a análise da arquitetura de controle de qualidade de serviços proposta.

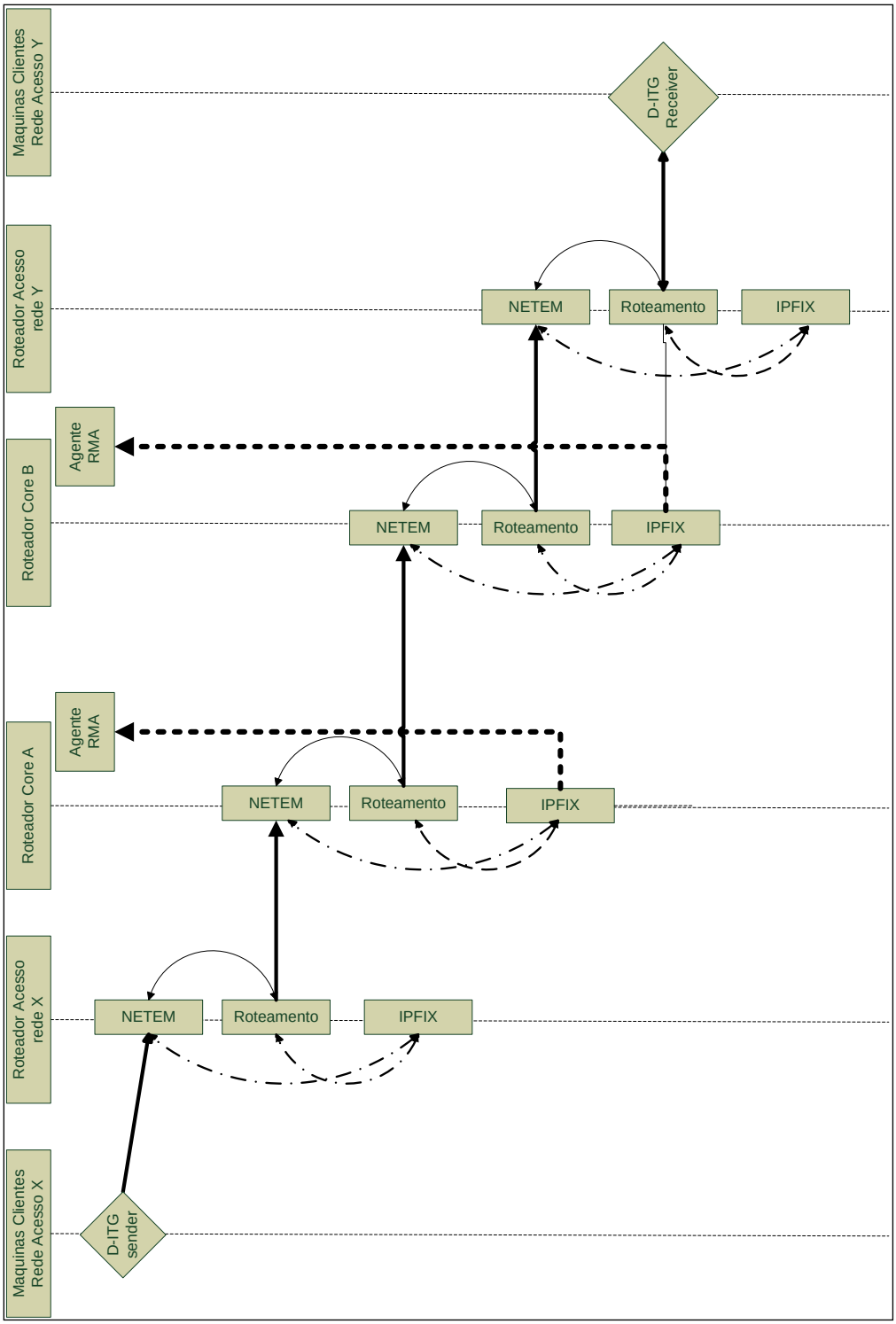

Figura 19 – Fluxo de dados entre os elementos do cenário de testes do conceito

De acordo com a Figura 20 para os fluxos de dados tipo dados e para os fluxos de dados tipo VoIP, as setas laranja indicam o caminho padrão (*rota default*) e as setas verdes e azuis os caminhos alternativos. Como os testes consideraram mudanças de caminho de fluxos de dados ocorrendo apenas em Aguia e Serpente, os demais caminhos configurados não foram representados na figura (embora houvesse tráfego entre clientes virgem e clientes Áries durante a preparação dos testes e verificação das funcionalidades da infraestrutura).

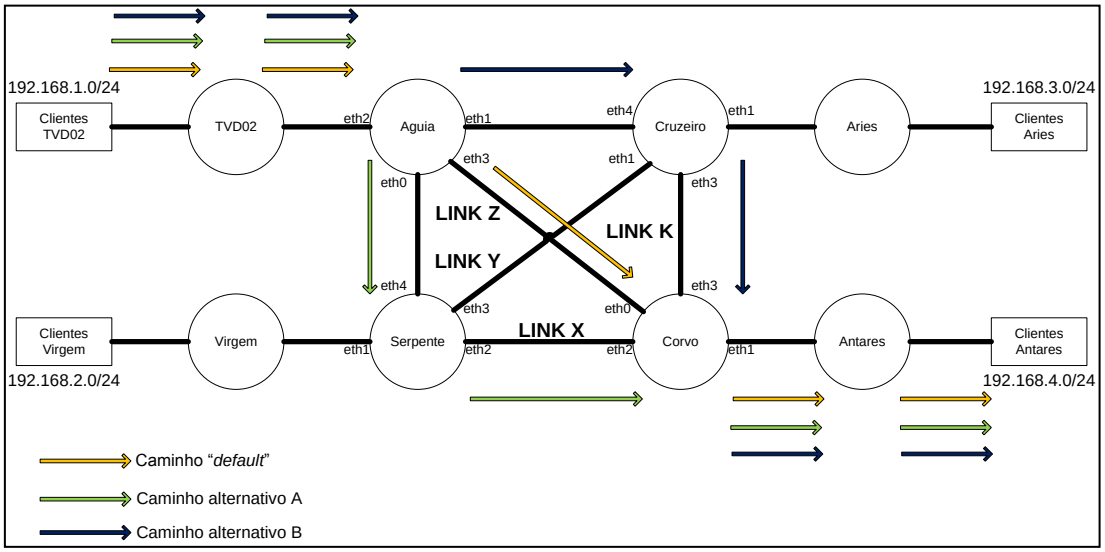

Figura 20 - Infraestrutura para prova de conceito e caminhos de acordo com Aguia

A Figura 21 identifica os caminhos padrão e alternativo do ponto de vista de Serpente.

Em todos os testes foram gerados dois conjuntos de fluxos de dados, ambos representando um serviço que utiliza fluxo de dados VoIP e fluxo de dados tipo dados. O fluxo 'A' descrito nesta tese representa fluxos de dados que podem ser utilizados em uma infraestrutura xDSL (devido aos recursos requeridos), enquanto o fluxo 'B' representa fluxos de dados que podem ser utilizados em uma rede 3G/UMTS. O fluxo de dados tipo VoIP é o mesmo para ambos os casos os fluxos de dados (A e B).

5.2.2 Teste de comportamento de tráfego sem influência de agentes

Neste conjunto de testes foram utilizados os mesmos tráfegos gerados para os testes anteriores, contudo nesses testes foram gerados atrasos em

Aguia e Corvo e Entre Serpente e Aguia como forma de verificar o efeito que as configurações de emulação de tráfego feitas pelo NETEM causam nos fluxos de dados utilizados para a experimentação proposta.

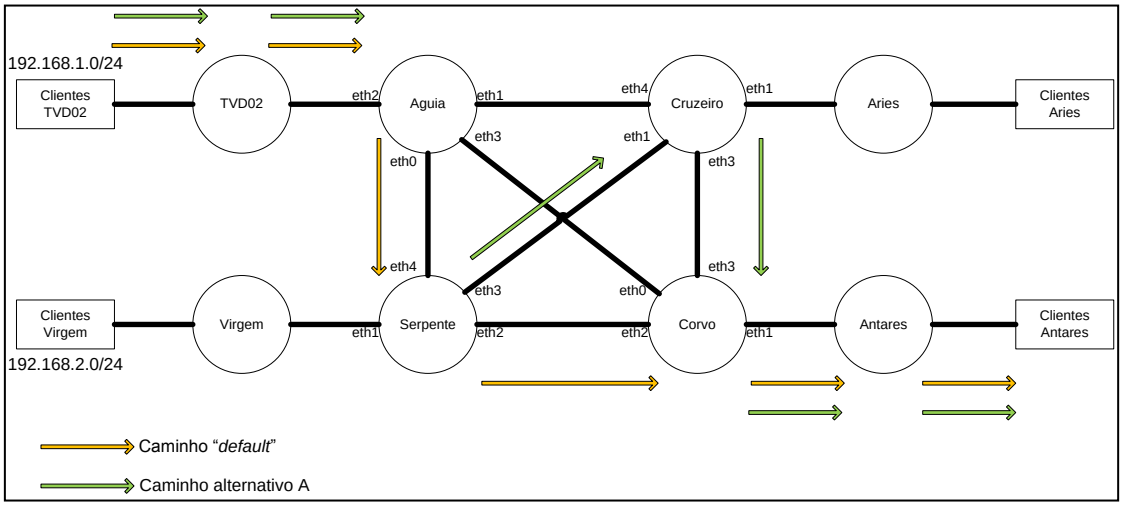

Figura 21 - Infraestrutura para prova de conceito e caminhos de acordo com Serpente

Os agentes estão ativos em todos os roteadores de "*core*" bem como seus coletores e *probes*. Este conjunto de testes também avalia se os agentes causam qualquer tipo de influência que não seja a de sua atuação, a qual não estará operando nesse teste (devido aos limites colocados para a atuação do agente serem muito superiores aos que a rede pode gerar).

5.2.3 Teste de comportamento de tráfego com agentes

5.2.3.1 Teste com agentes e um ponto de falha

Este teste avalia como um agente reage a uma determinada falha entre os equipamentos Aguia e Corvo, sendo que o agente sempre inicia em seu estado inicial, ou seja, todos os *links* possuem o mesmo valor de *preferential attachment*. Será aplicada uma configuração do NETEM nas interfaces ‘eth3’ de Aguia e ‘eth0’ de Corvo que aumentará o atraso dos pacotes segundo uma distribuição normal com média de 30ms e desvio padrão de 10ms.

As especificações do agente determinam que o fluxo de dados tipo VoIP não pode ter atrasos superiores a 20ms e não pode ocorrer perda de pacotes (perda deve ser zero). Já o tráfego de dados tem restrição de atraso de 150ms e, como no fluxo de dados tipo VoIP, não pode ocorrer perda de pacotes. As

medidas são relativas a atrasos e perdas no *link* durante o tempo de prestação de serviço pelo agente localizado em Aguia. Os demais agentes em Serpente, Corvo e Cruzeiro não devem ter ações nesse teste (os limites dos parâmetros de controle não devem ser ultrapassados de acordo com o comportamento da infraestrutura).

A Figura 22 ilustra o caminho por onde o fluxo de dados inicial tipo VoIP e dados deve passar e um dos possíveis caminhos finais a ser estabelecido pelo agente em Aguia.

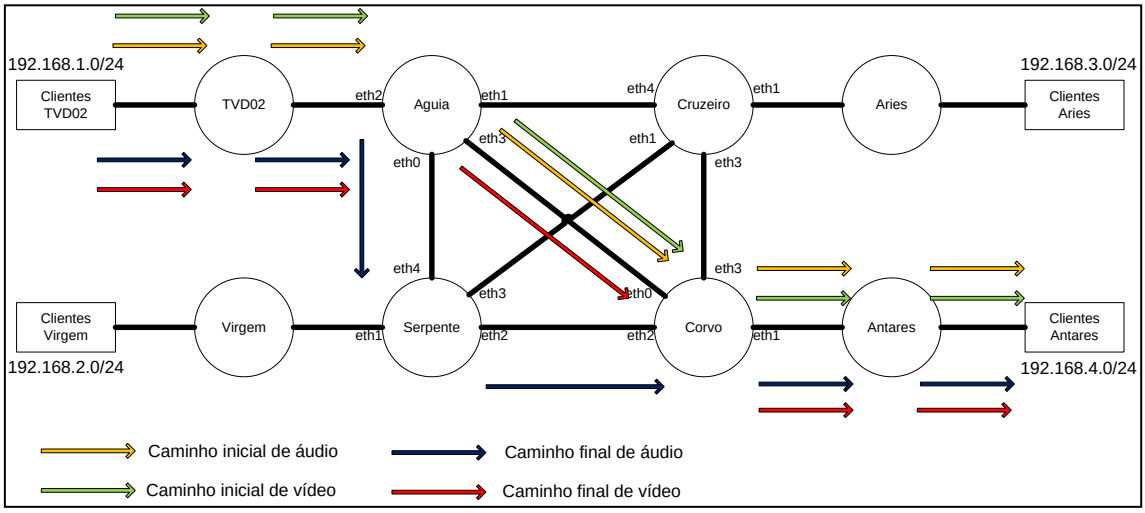

Figura 22 – Caminho do tráfego inicial e possível caminho após atuação do agente em Aguia

Os testes com as especificações descritas neste item são realizados com os agentes em seu estado inicial, ou seja, os agentes não tem preferência definida por nenhum *link* e todos os *links* possuem em princípio os mesmos valores de P e Q (ambos zero).

Os resultados desse teste indicam o comportamento inicial do agente e se este converge para uma escolha de *link* (ou um conjunto de *links*), ou seja, se ocorre o *preferential attachment* dado as variações de comportamento na infraestrutura.

5.2.3.2 Teste com agentes, um ponto de falha e agente com *preferential attachment* definido

Os testes desta seção avaliam como o agente se comporta dado uma determinada preferência por um *link*. Para se obter resultados estes testes foram realizados com a preferência estabelecida nos testes anteriores e verificou-se como o agente se comportava quando uma falha era implementada. Os testes foram realizados com a falha ocorrendo no mesmo local que do testes anteriores. Este conjunto de testes pretende verificar como o agente reage no momento em que o caminho preferencial sofre falhas.

A falha é aplicada no *link* que o agente mais utiliza para o fluxo de dados tipo VoIP, sendo a falha gerada pelo NETEM como um atraso segundo uma distribuição normal com média de 50ms e desvio padrão de 20ms.

5.3 RESULTADOS EXPERIMENTAIS

Os resultados apresentados nos próximos itens foram obtidos através da utilização dos dois conjuntos de fluxos de dados. Todos os testes foram realizados com as máquinas virtuais que representam os clientes das redes de acesso TVD02[24] e Virgem para os clientes das redes de acesso em Antares e Áries. Os fluxos medidos e apresentados foram gerados em "Clientes TVD02" foram enviados para "Clientes Antares". Entre Clientes Virgem e Clientes Aries houve geração de fluxos de dados, principalmente para monitoração dos processos da prova de conceito. Estes fluxos de dados compartilharam o seu meio de transmissão quando da ação dos agentes durante os testes realizados.

5.3.1 Resultados validação da estrutura montada

A infraestrutura montada com máquinas virtuais gerou respostas compatíveis com o esperado de uma infraestrutura de um sistema

[24] Os nomes das máquinas virtuais são os nomes das máquinas utilizadas no Laboratório de Sistemas Abertos (LSA).

comunicação baseado no protocolo, conforme indica a função de distribuição acumulada da Figura 23.

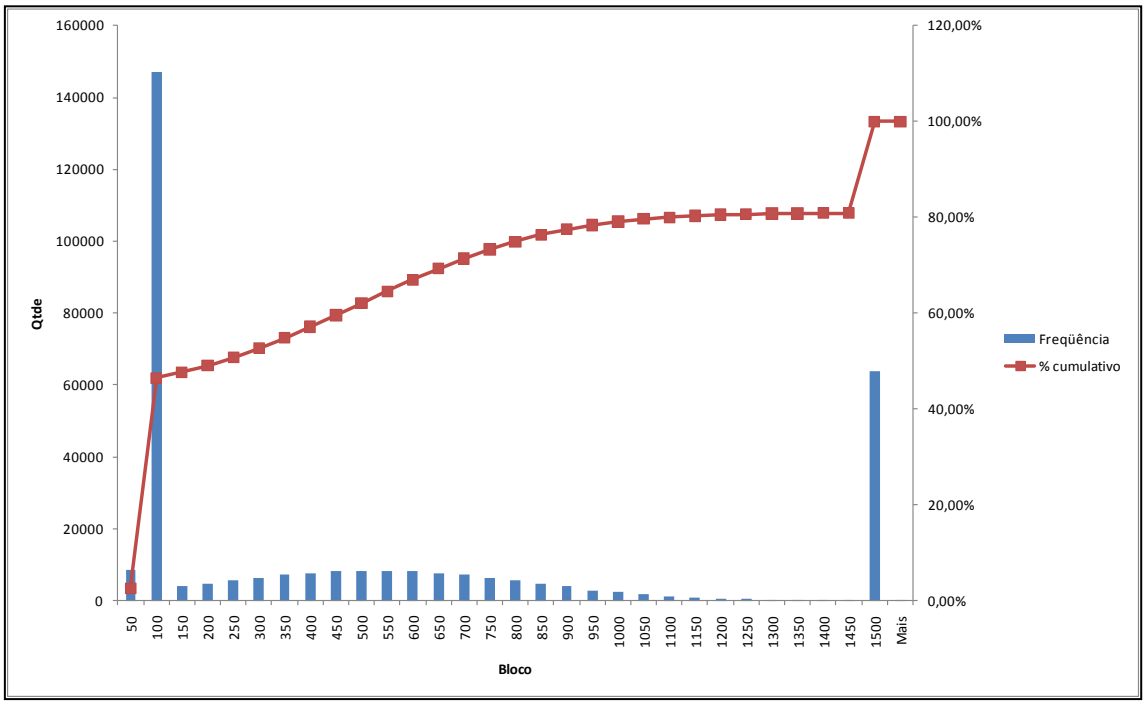

Figura 23 – Função distribuição acumulada

Para avaliação do comportamento dos fluxos de dados utilizados na prova de conceito foram elaborados dez experimentos para avaliar a taxa de transmissão, atraso e perdas de cada tipo de fluxo de dados, os quais apresentaram pequena variação de valores médio e variância, sendo suficientes para a análise requerida (Grinstead, Snell, 2006), como mostra a Tabela 5.

	Fluxo Dados A	Fluxo Dados B	Fluxo de dados C	Fluxo VoIP	Fluxo Agregado	
Medida 1	4856,8659	14384,3836	7,3522	73,5828	19322,1846	**Media**
	3498,9445	10473,2863	24,3443	31,1808	9394,4767	**Desvio Padrao**
Medida 2	4858,1977	14384,0037	7,3546	73,5828	19323,1389	**Media**
	3511,7930	10240,5985	24,3991	27,5997	9586,0385	**Desvio Padrao**
Medida 3	4866,5190	14384,9035	7,3472	73,5828	19332,3526	**Media**
	3499,2555	10159,2243	23,5850	28,6618	9581,7935	**Desvio Padrao**
Medida 4	4860,8968	14385,0635	7,3522	73,5828	19326,8953	**Media**
	3571,0216	10659,4188	23,6331	31,9599	9391,0466	**Desvio Padrao**
Medida 5	4855,7323	14385,1435	7,3497	73,5828	19321,8083	**Media**
	3580,2471	10105,9549	24,4431	23,9053	9245,0422	**Desvio Padrao**
Medida 6	4860,5015	14385,6234	7,3472	73,5816	19327,0537	**Media**
	3531,8118	10283,5736	24,7758	29,6654	9831,3026	**Desvio Padrao**
Medida 7	4850,4492	14385,1230	7,3585	73,5853	19316,5159	**Media**
	3599,7637	10166,5440	27,5332	27,2397	9390,6086	**Desvio Padrao**
Medida 8	4857,5852	14384,4836	7,3472	73,5828	19322,9989	**Media**
	3369,3703	10240,2642	24,6039	27,7188	9523,3833	**Desvio Padrao**
Medida 9	4858,6855	14385,6234	7,3509	73,5828	19325,2426	**Media**
	3333,9703	10148,8761	24,9535	30,6066	9589,6167	**Desvio Padrao**
Medida 10	4858,1977	14385,5434	7,3583	73,5828	19324,6822	**Media**
	3379,7922	10331,4951	24,2840	30,4958	9150,4080	**Desvio Padrao**
	4858,1255	**14384,8410**	**7,3511**	**73,5830**	**19324,1185**	**Media**

Tabela 5 – Taxa de transmissão para os fluxos de dados utilizados nos experimentos

O gráfico da Figura 24 apresenta o comportamento característico do fluxo de dados tipo A (dados com tamanhos de 300 a 500 bytes). De modo geral nota-se uma menor concentração de pontos ao redor da taxa de 5000 kbytes/seg., sendo que ocorre alguma concentração entre 8000 kbytes/seg. e 10000 kbytes/seg. Picos ocorreram em todas as medições, em geral dois ou três picos por teste como pode ser observado nas Figura 24. Já o fluxo de dados tipo B possui um comportamento diferente em relação ao fluxo de dados do tipo A, pois a maioria dos pontos segue taxas de transmissão regulares como podem ser observadas nas linhas formadas no gráfico da Figura 25. Contudo, essa transmissão não é sequencial no tempo, havendo várias taxas de transmissão em qualquer amostra de intervalo de tempo. O mesmo ocorre com o fluxo de dados do tipo VoIP, onde os pacotes apresentam taxas de transmissão bem definidas, como ilustra a Figura 27. Já o fluxo de dados tipo B possui um comportamento diferente em relação ao fluxo de dados do tipo A, pois a maioria dos pontos segue taxas de transmissão regulares como podem ser observadas nas linhas formadas no gráfico da Figura 26. Contudo, essa transmissão não é sequencial no tempo, havendo várias taxas de transmissão em qualquer amostra de intervalo de tempo. O mesmo ocorre com o fluxo de dados do tipo VoIP, onde os pacotes apresentam taxas de transmissão bem definidas, como ilustra a Figura 27. A taxa média de transmissão do fluxo A é de 14,38 Mbps/seg. e do fluxo B é de 4,8 Mbps/seg.

Como os fluxos de dados gerados para a rede 3G/UMTS exigiram maiores recursos do que aqueles descritos nas Tabela 3 e Tabela 4, foi utilizado então as especificações das redes 3G/UMTS HPSA+ e WCDMA, cuja capacidade de taxa de transferência pode variar entre 3,6 e 7,2 Mbps/seg. (Mader, Staehle; Gosswein, 2007); Oksman, et.al.; 2008).

A maior diferença entre os picos estava no momento em que ocorriam da transmissão. Contudo, são similares em amplitude e duração.

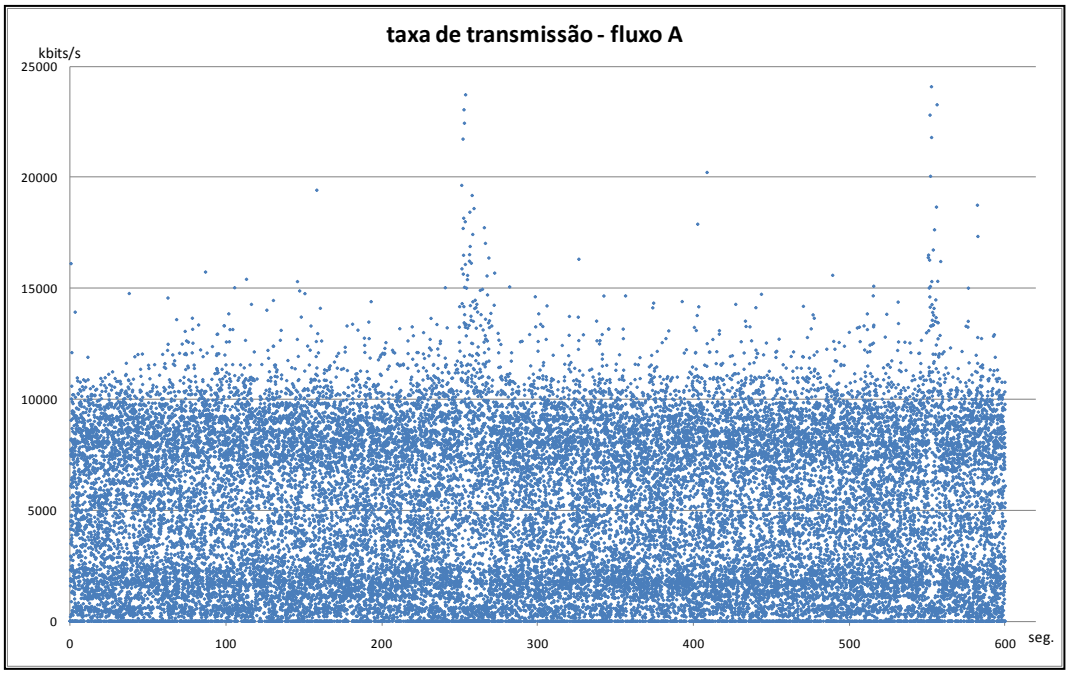

Figura 24 – Taxa de transmissão (bits/seg) do fluxo de dados A (teste 1)

Já o fluxo de dados tipo B possui um comportamento diferente em relação ao fluxo de dados do tipo A, pois a maioria dos pontos segue taxas de transmissão regulares como podem ser observadas nas linhas formadas no gráfico da Figura 26. Contudo, essa transmissão não é sequencial no tempo, havendo várias taxas de transmissão em qualquer amostra de intervalo de tempo. O mesmo ocorre com o fluxo de dados do tipo VoIP, onde os pacotes apresentam taxas de transmissão bem definidas, como ilustra a Figura 27.

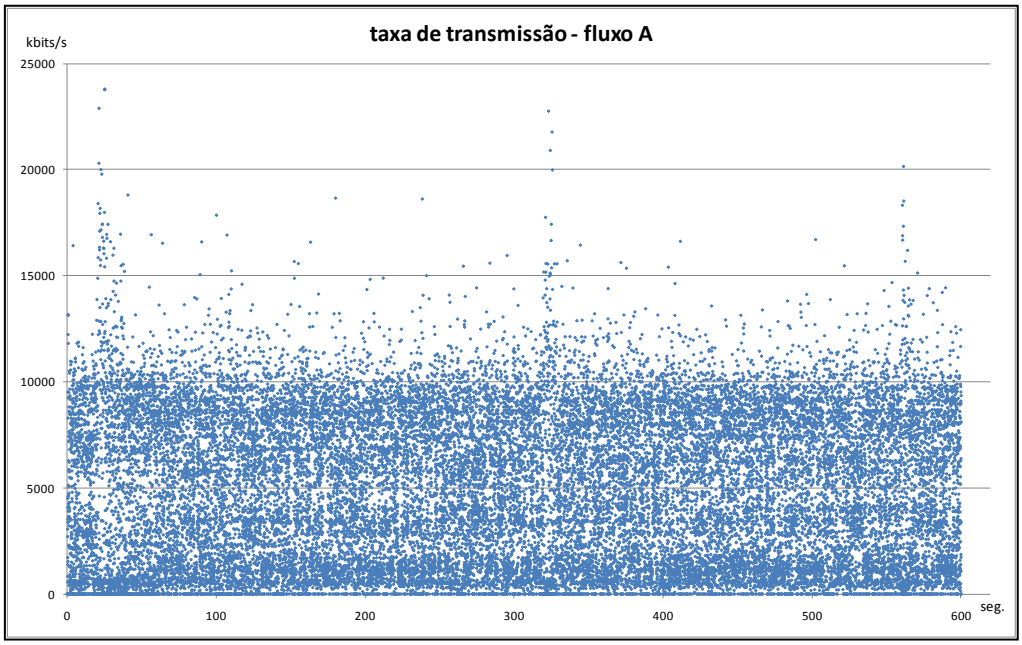

Figura 25 – Taxa de transmissão (bits/seg) do fluxo de dados A (teste 2)

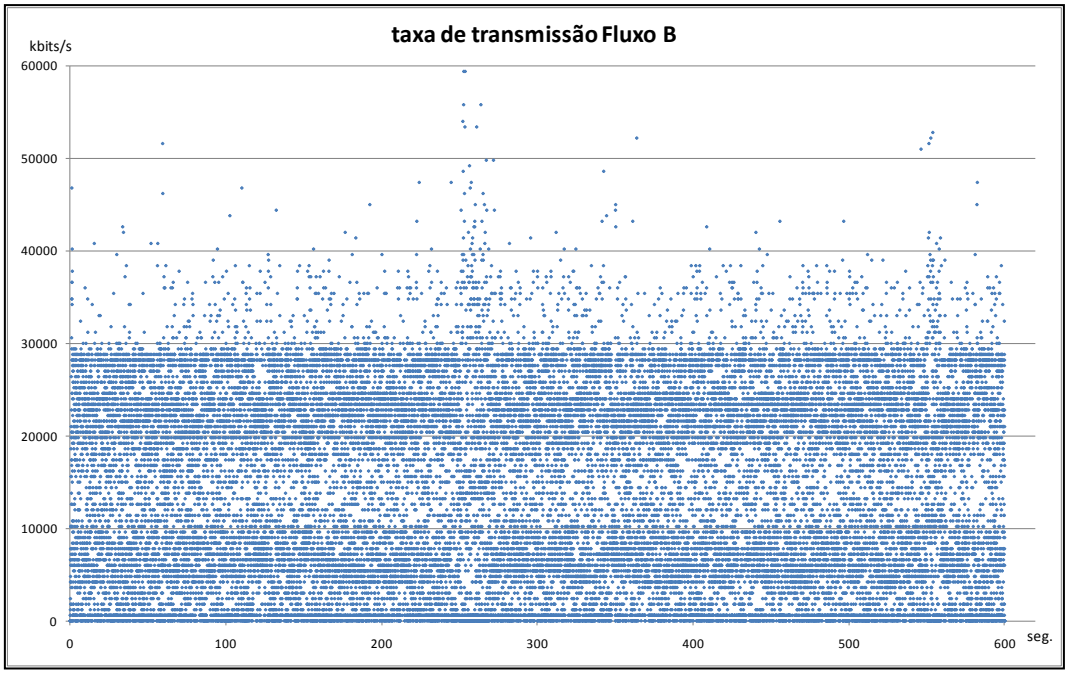

Figura 26 – Taxa de transmissão (bits/seg) do fluxo de dados B

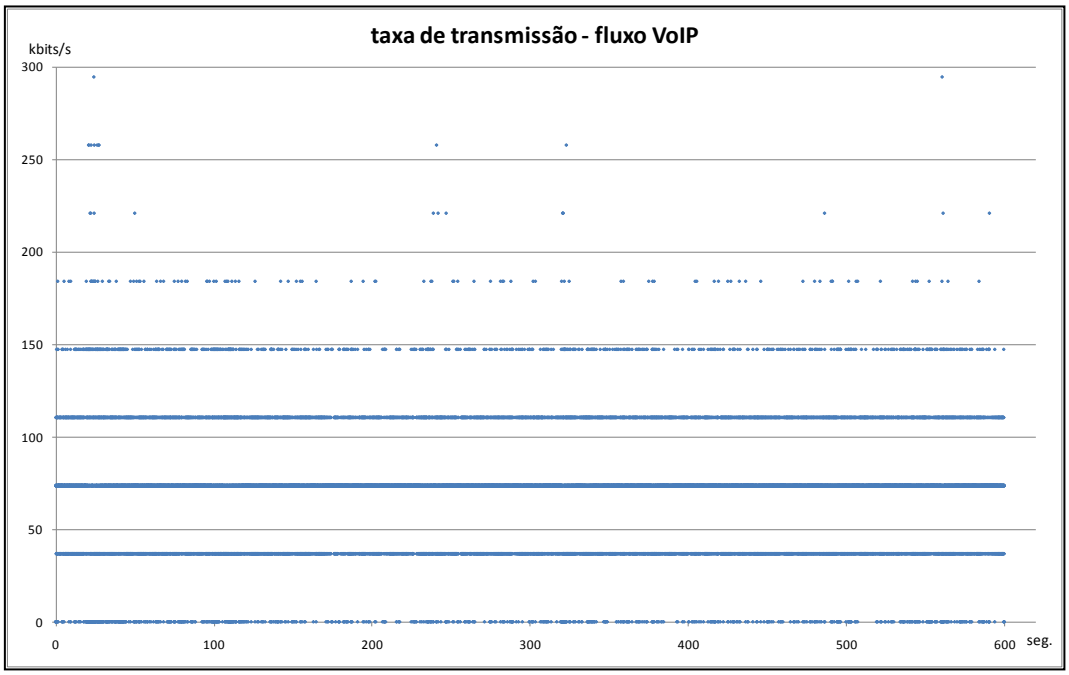

Figura 27 – Taxa de transmissão (bits/seg.) do fluxo de dados tipo VoIP

5.3.1.1 Atraso característico dos fluxos de dados tipo dados

O atraso apresentado pelos fluxos de dados do tipo A é menor do que o apresentado pelos fluxos de dados do tipo B. Enquanto o fluxo tipo A

apresentou atraso de 55,773ms e desvio padrão de 16,076ms (Figura 28), o fluxo tipo B apresentou atraso de 54,856ms e desvio padrão de 37,422ms (Figura 29). Os picos presentes nos gráficos de atraso correspondem aos respectivos picos de taxas de transmissão.

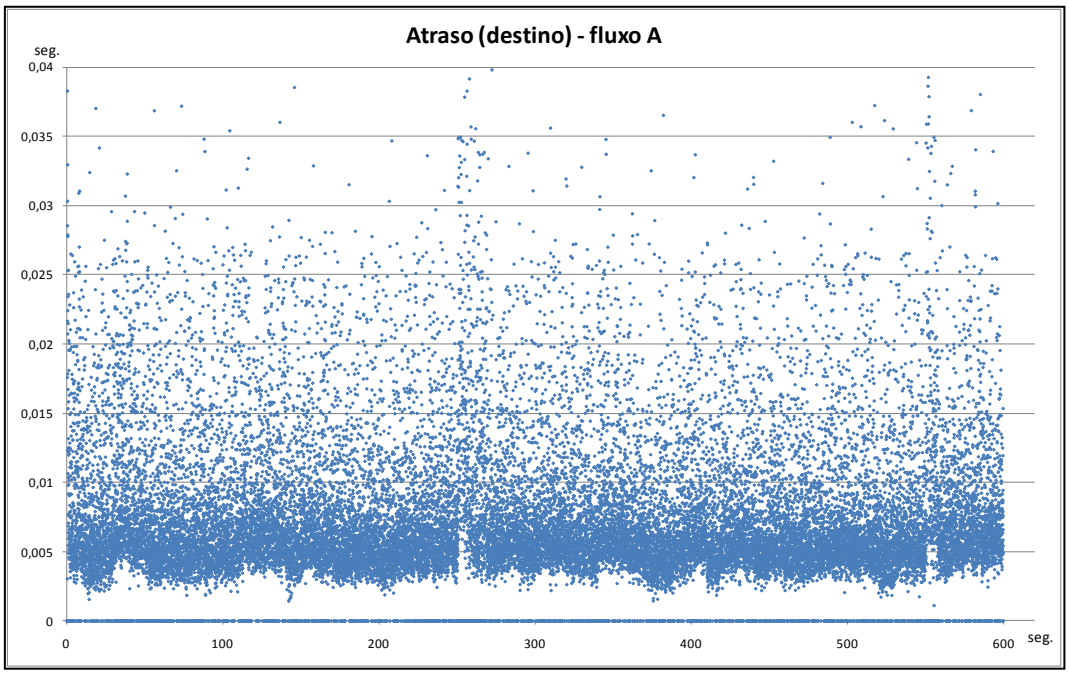

Figura 28 – Atraso apresentado pelo fluxo de dados tipo A (teste 1)

É importante destacar que ambos os fluxos de dados tipo A e B estão abaixo do limite estipulado pelo agente de 150ms de atraso.

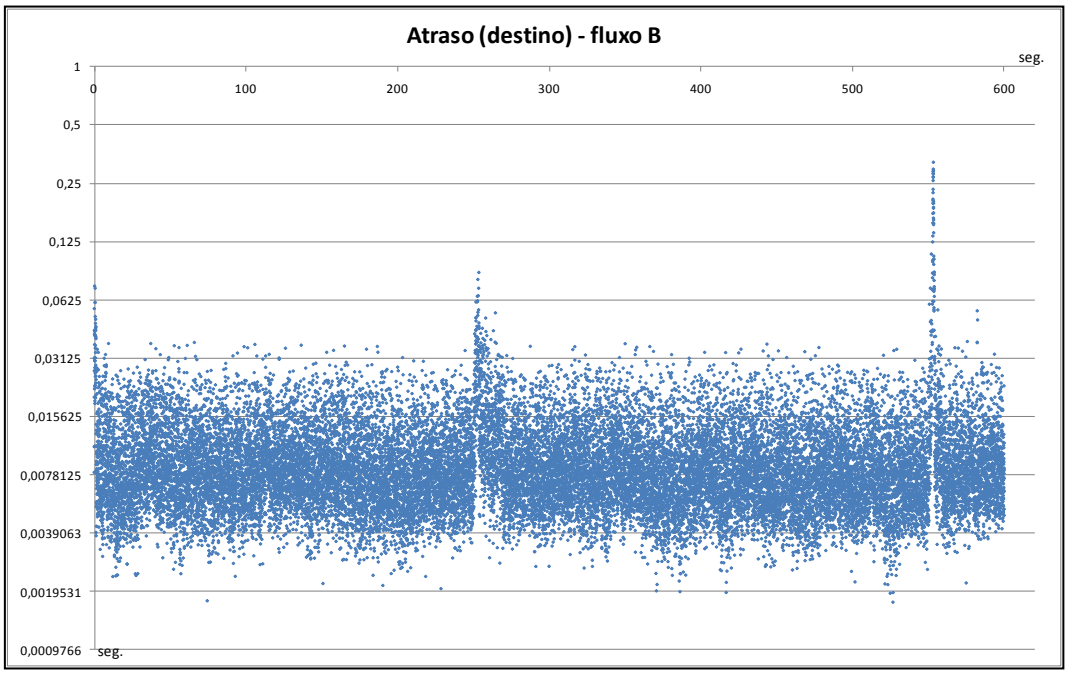

Figura 29 – Atraso apresentado pelo fluxo de dados tipo B

O tipo de fluxo VoIP, diferentemente dos demais fluxos, apresenta grande concentração dos pontos (Figura 30) em uma faixa que varia em torno de 4ms, sendo que a média do atraso é 37,188ms e desvio padrão de 11,611ms.

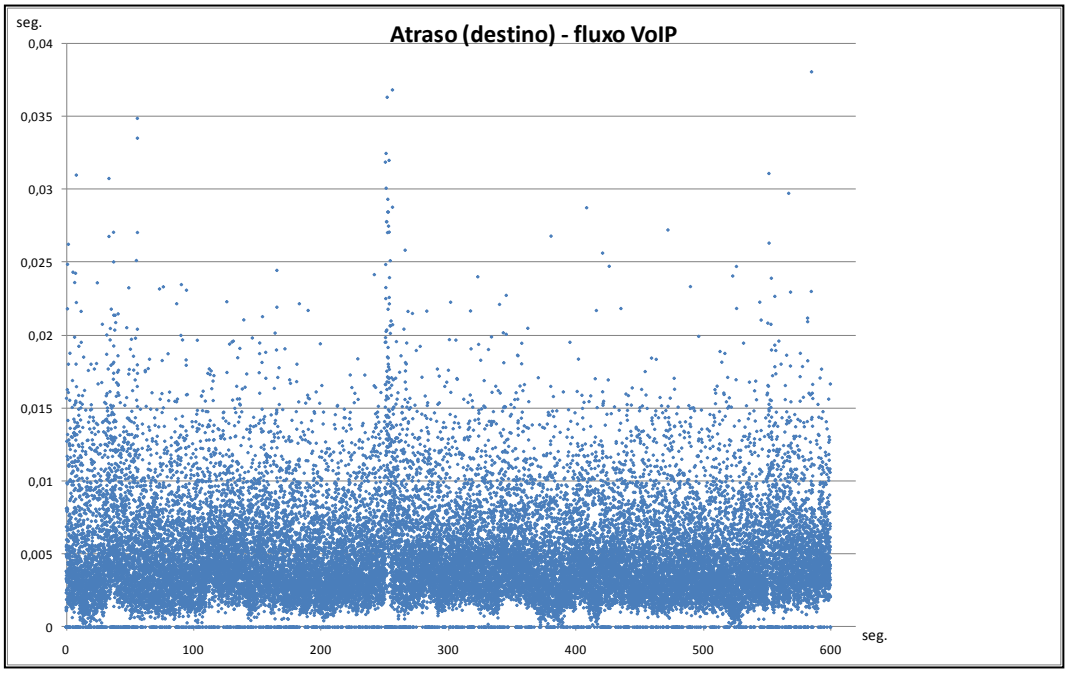

Figura 30 – Atraso apresentado pelo fluxo de dados tipo VoIP

Como pode ser observado no histograma a seguir (Figura 31) a distribuição de pacotes em relação ao atraso é similar para todos os tipos de fluxos de dados, considerando um deslocamento no tempo entre os fluxos de dados tipo A e B em relação ao fluxo de dados VoIP.

5.3.2 Resultados do comportamento de tráfego sem influência de agentes

Neste conjunto de testes não houve agentes realizando alterações de rotas para adequação do tráfego aos parâmetros de qualidade de serviço, pois o objetivo é determinar como o NETEM influencia o comportamento do tráfego e determinar o estado do cenário de testes para ser um caso de comparação em relação às mudanças executadas no cenário de testes pelo agente. Os testes realizados utilizam os mesmos fluxos de dados dos testes anteriores, e os atrasos gerados pelo NETEM seguiram uma distribuição normal com média em 30ms e desvio padrão de 10ms. As configurações do NETEM foram

aplicadas nas interfaces eth3 de Aguia e eth0 de Corvo, sendo esse o caminho registrado na tabela de rotas de Aguia para enviar qualquer tipo de fluxo de dados entre as redes 192.168.1.0/24 (origem) e 192.168.4.0/24 (destino).

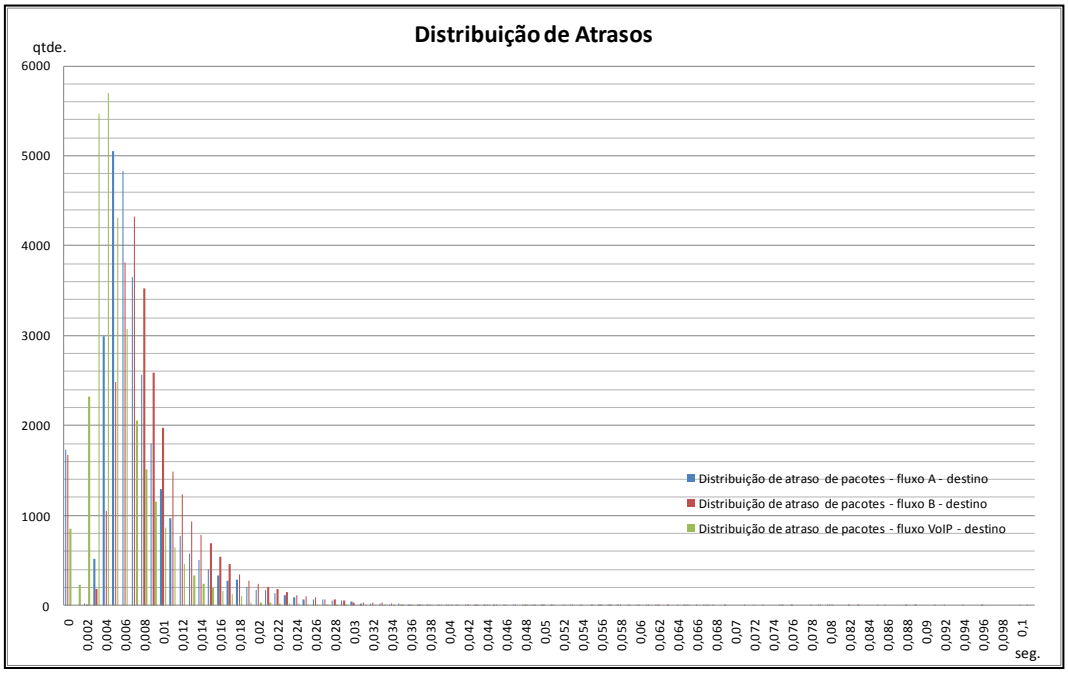

Figura 31 – Distribuição do atraso fluxo de dados

5.3.2.1 Análise do tráfego de dados

Como pode ser observado no gráfico da Figura 32, o NETEM alterou consideravelmente o atraso dos pacotes, mas não influenciou nas taxas de transmissão como observado na Figura 33 e Figura 34, onde as taxas de transmissão obtidas são similares aos testes anteriores, ou seja, se o agente não está programado para realizar interferências no tráfego (pois os limites dos parâmetros são superiores ao apresentado pela rede) não há alterações no comportamento do tráfego; independentemente do agente estar coletando e analisando o tráfego.

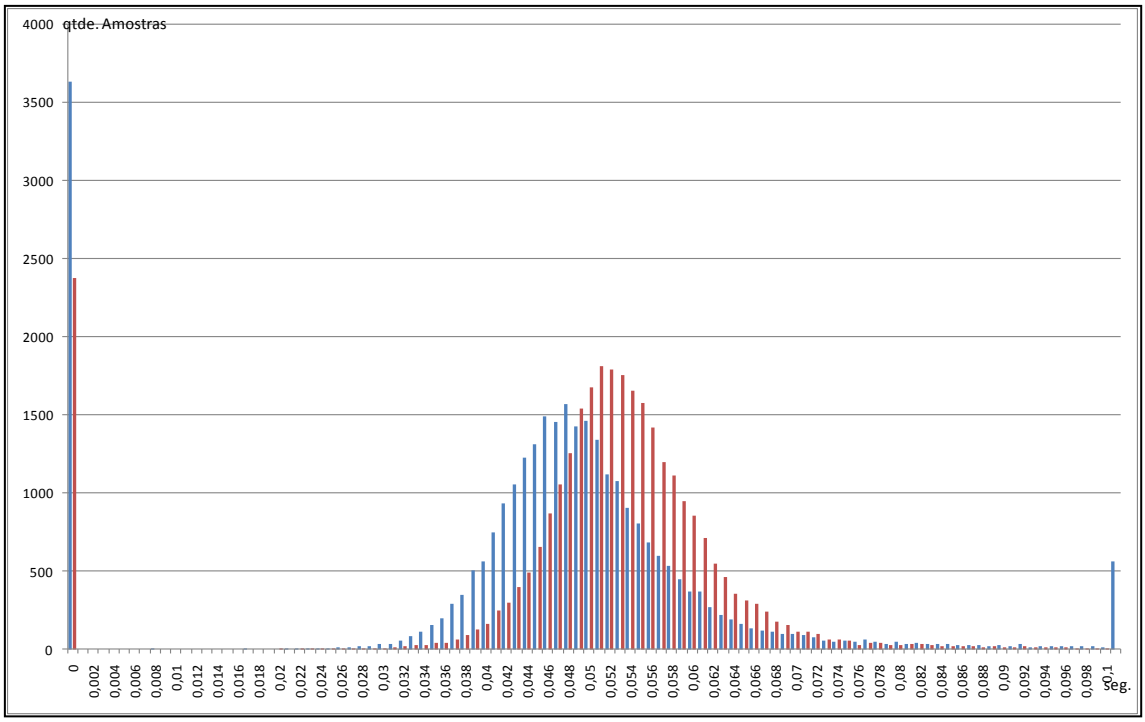

Figura 32 - Distribuição de amostras versus atraso

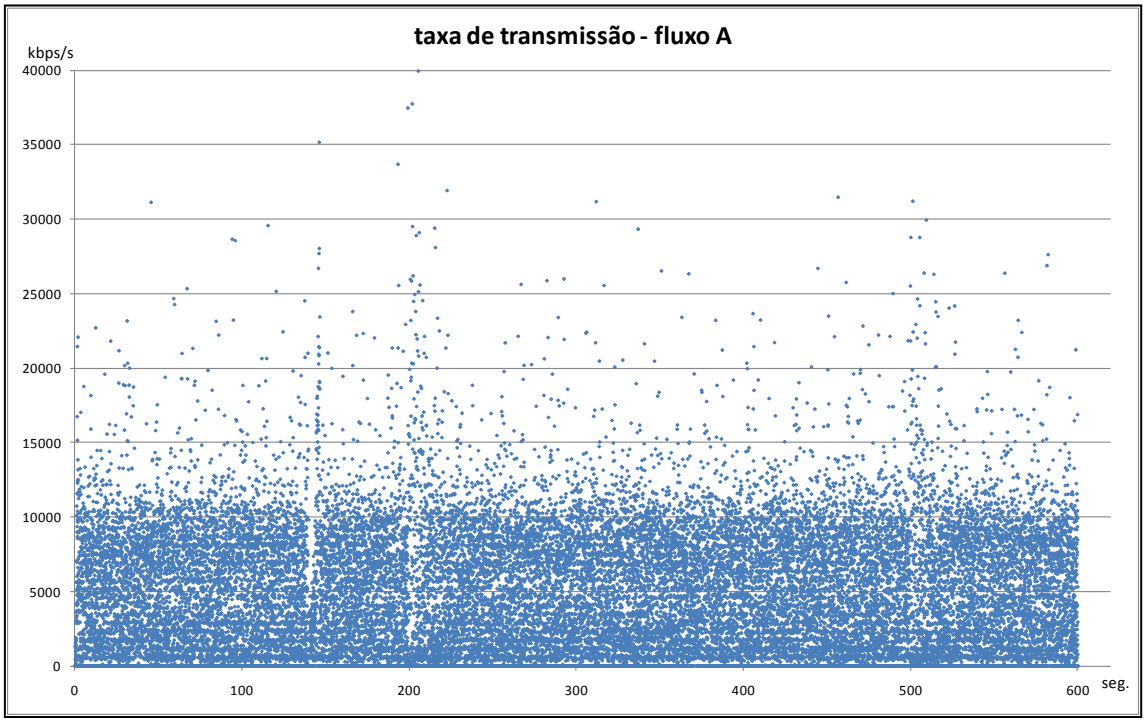

Figura 33 - Taxa de transmissão do fluxo de dados A sem atuação do agente

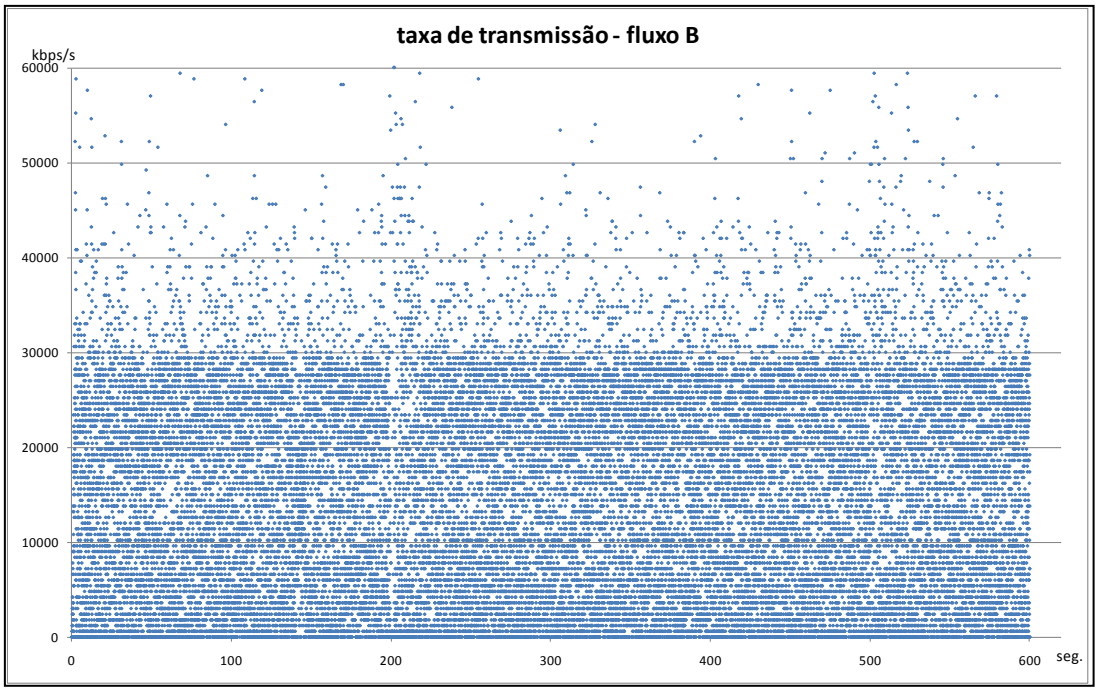

Figura 34 - Taxa de transmissão do fluxo de dados B sem atuação do agente

Como o agente não atua em relação ao atraso o resultado pode ser observado nos gráficos das Figura 35 e Figura 36, onde o atraso em cada classe de fluxo de dados deslocou-se em relação aos testes sem o uso do NETEM.

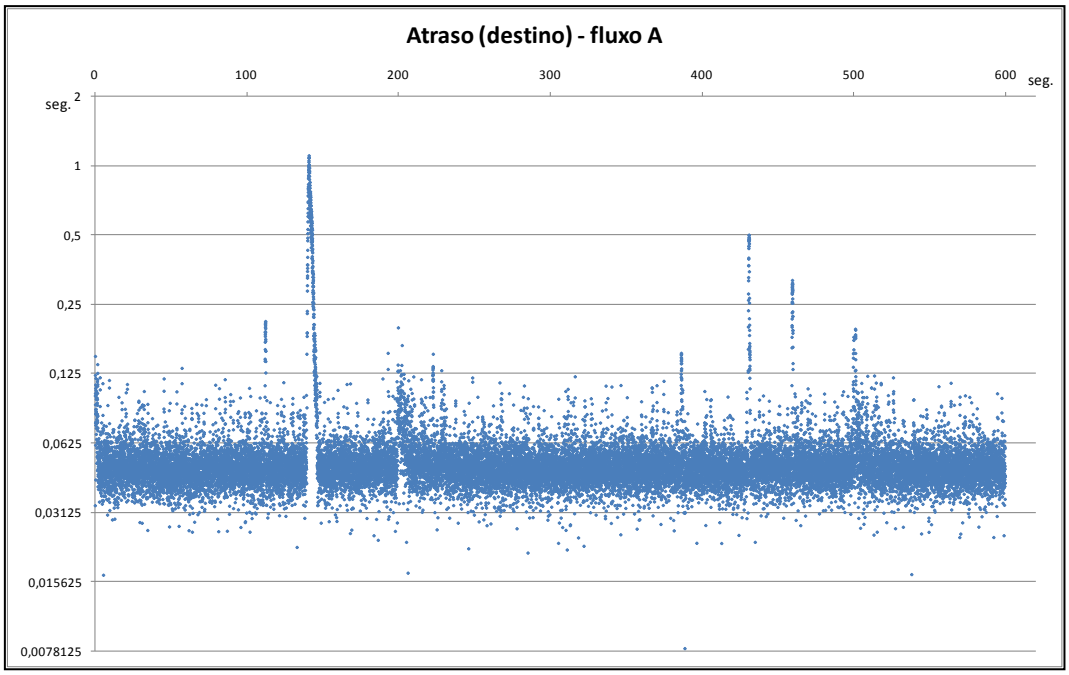

Figura 35 – Atraso do fluxo de dados A sem atuação do agente

Embora o agente também não influencie na perda de pacotes medida, esta ocorre devido ao atraso gerado pelo NETEM que aumenta a quantidade

de pacotes na fila de saída da interface, e por vezes não há espaço na fila alguns pacotes. A conseqüência é o descarte dos pacotes.

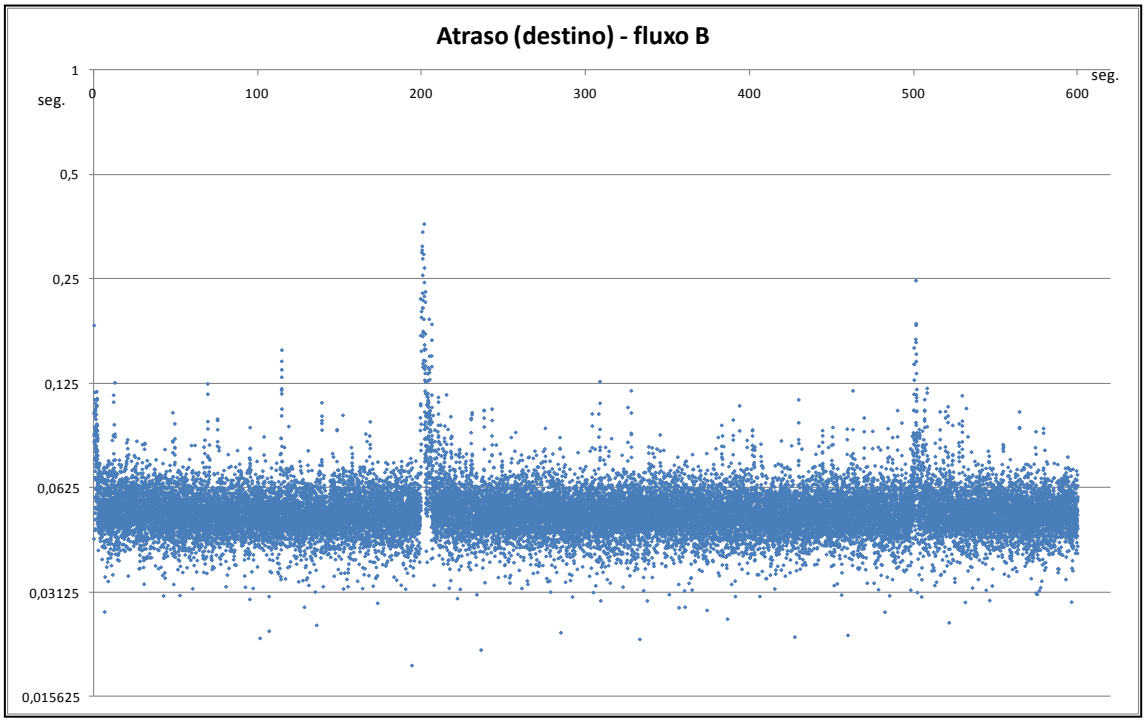

Figura 36 – Atraso do fluxo de dados B sem atuação do agente

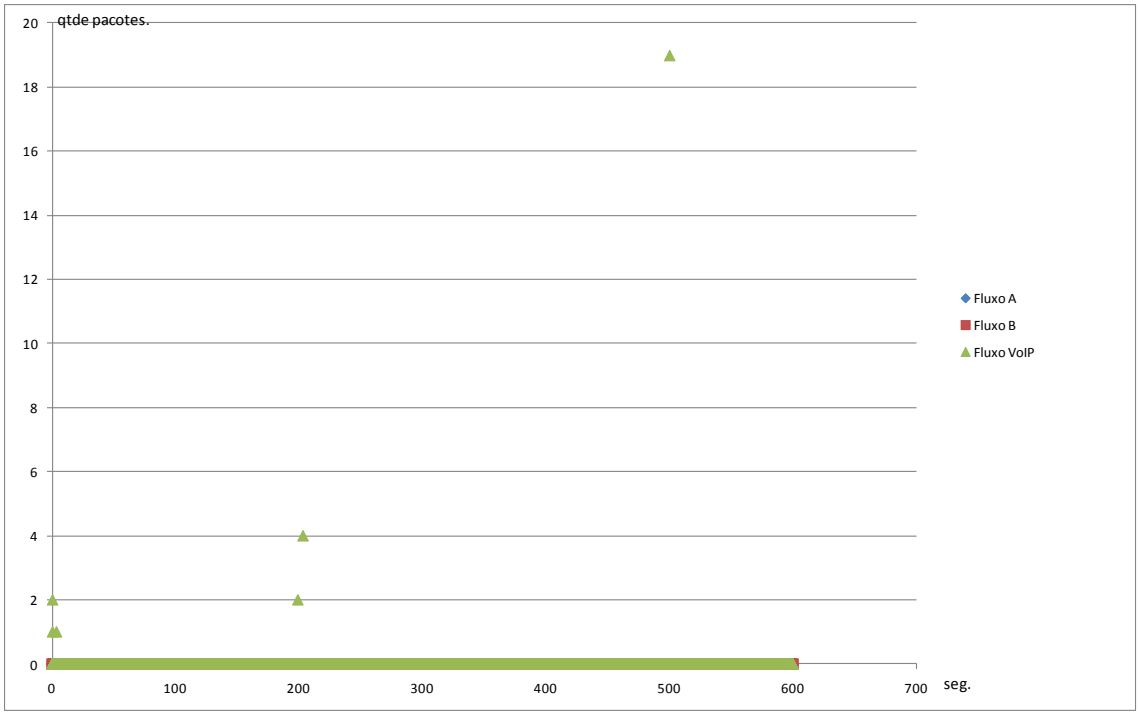

Figura 37 - Perda de pacotes sem atuação do agente

5.3.2.2 Análise do fluxo de dados tipo VoIP

O fluxo de dados tipo VoIP também não é influenciado pela presença do agente, pois todas as medidas são compatíveis com o que ocorre na rede sem agentes, com exceção do atraso (Figura 38 a Figura 40).

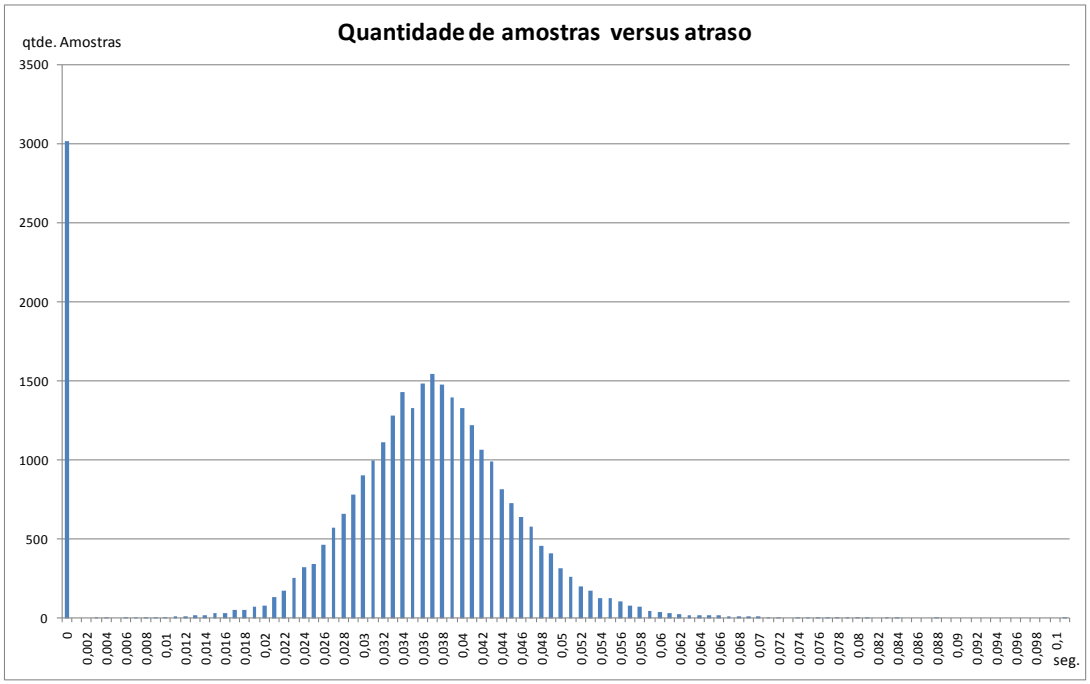

Figura 38 - Distribuição amostras versus atraso

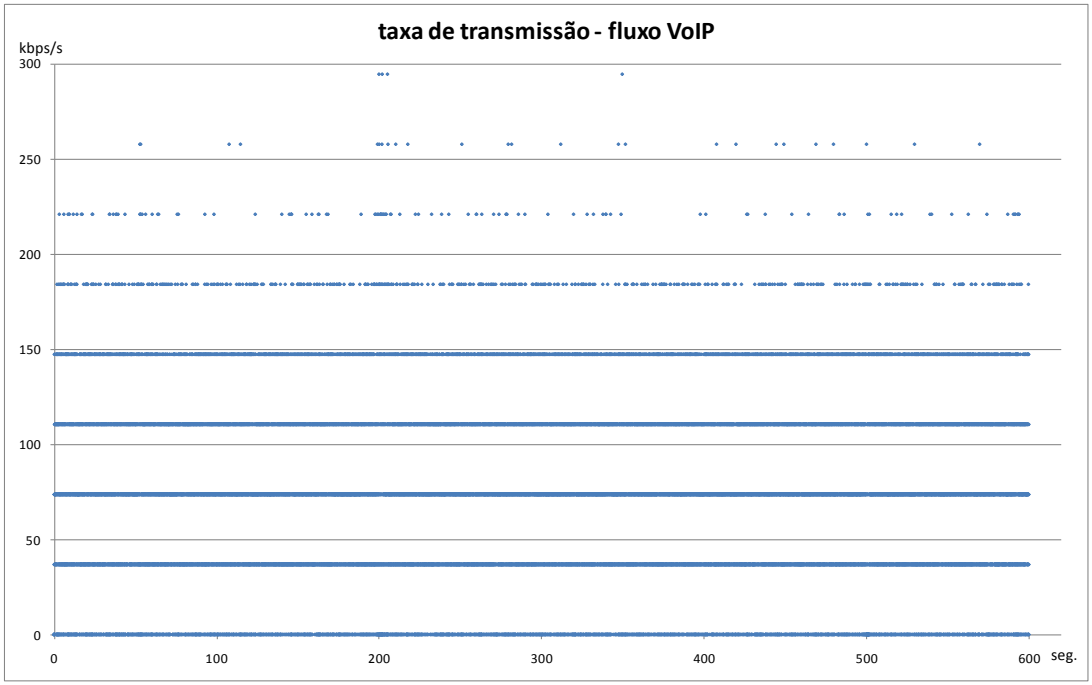

Figura 39 - Taxa de transmissão do fluxo de dados tipo VoIP sem atuação do agente

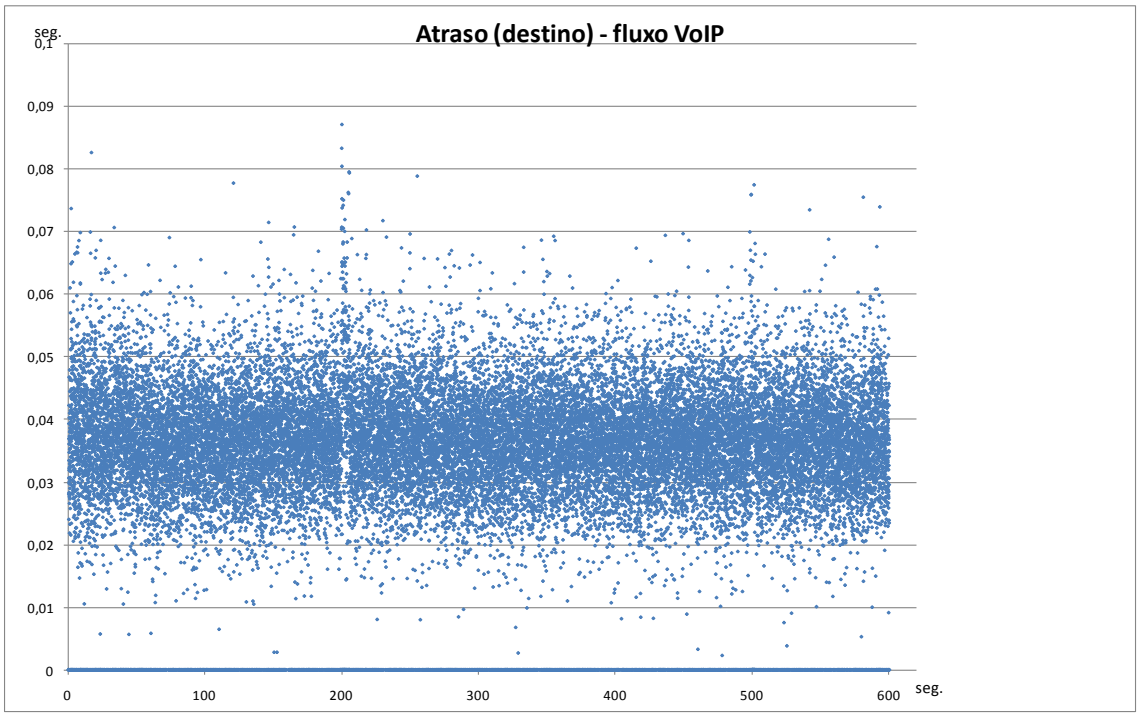

Figura 40 – Atraso do fluxo de dados tipo VoIP sem atuação do agente

Da mesma maneira que ocorre no tráfego de dados a perda de pacotes ocorrida com o fluxo de dados tipo VoIP também é decorrência da quantidade de pacotes na fila de saída da interface. Como se pode observar nos gráficos das Figura 35, Figura 36 e Figura 37, a perda de pacotes ocorre quando há picos de transmissão e por conseqüência de atrasos, uma vez que ambos os tráfegos estão sendo enviados pela mesma interface.

5.3.3 Resultados do comportamento de tráfego com agentes e um ponto de falha

Neste conjunto de testes os mesmos fluxos de dados dos testes anteriores foram utilizados com atraso gerado pelo NETEM com distribuição normal com média em 30ms e desvio padrão de 10ms. As configurações do NETEM foram aplicadas nas interfaces eth3 de Aguia e eth0 de Corvo, sendo esse o caminho inicialmente registrado na tabela de rotas de Aguia para enviar qualquer tipo de fluxo de dados entre as redes 192.168.1.0/24 (origem) e 192.168.4.0/24 (destino). Cada interface possui apenas uma fila de saída com

o esquema FIFO. O agente possui como critério que o flxuo de dados VoIP pode sofrer atraso de 20ms e não pode sofrer perda de pacotes (valor zero de perda) e o fluxo de dados do tipo dados tem atraso de até 150ms e perda zero.

Comparando-se os gráficos apresentados na Figura 41 e Figura 42 com as taxas de transmissão dos testes anteriores tem-se que as taxas apresentadas nos testes com a atuação dos agentes são bastante similares em todos os aspectos discutidos anteriormente neste trabalho, indicando claramente que todos os testes estão lidando com a mesma carga e tipo de tráfego. Logo, pode-se comparar se o agente alterou os valores de atraso e perda de pacotes de forma significativa em relação ao teste descrito no item anterior (infraestrutura com falha e sem atuação dos agentes[25].

5.3.3.1 Análise do tráfego de dados

Como pode ser observado no gráfico da Figura 41 e Figura 42 o agente não causou alteração na taxa de transmissão medida, embora esteja atuando diretamente sob os caminhos pelos quais o tráfego é transmitido.

[25] Neste tase não foram gerados ensaios com tráfego de vídeo, pois estes causaram demasiados atrasos na infraestrutura devido aos recursos exigidos para sua transmissão, independentemente da atuação dos agentes.

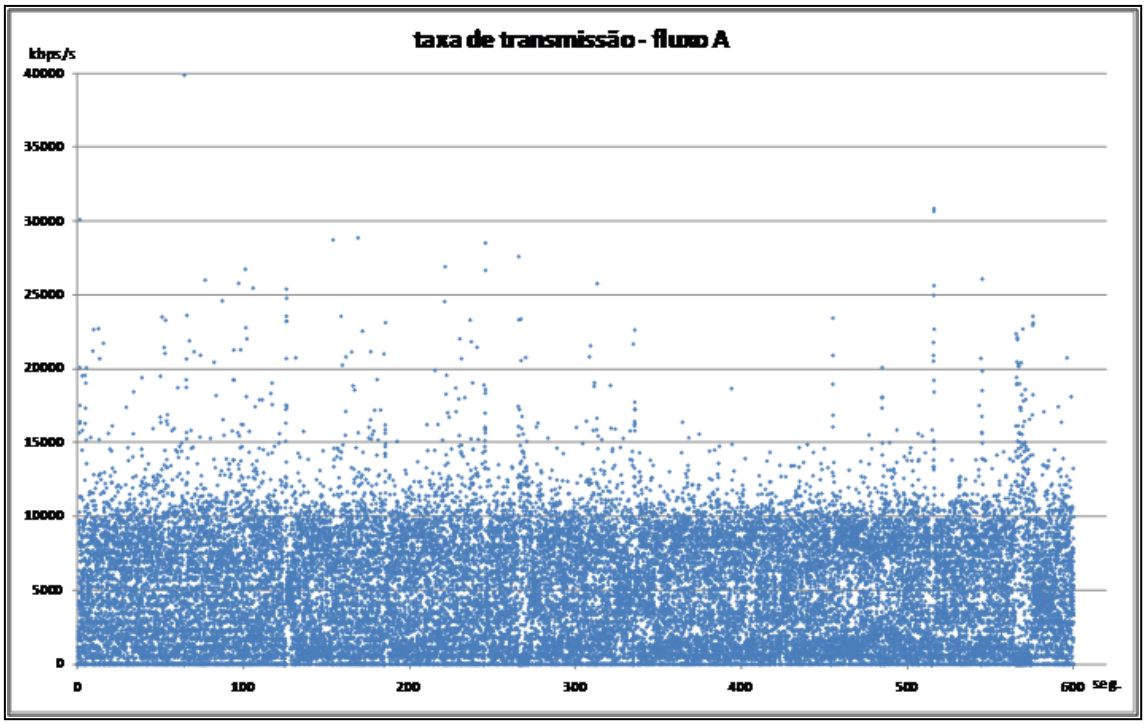

Figura 41 – Taxa de Transmissão do fluxo de dados A com atuação do agente

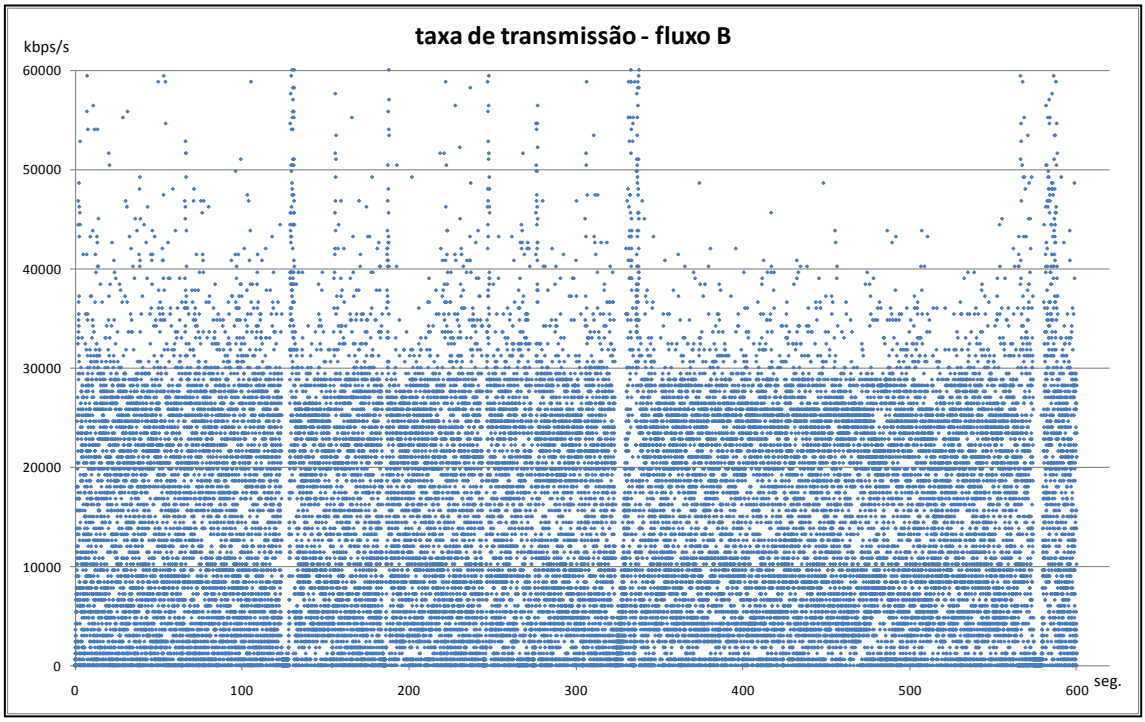

Figura 42 – Taxa de Transmissão do fluxo de dados B com atuação do agente

Já o atraso sofreu mudanças significativas como o esperado em ambos os fluxos de dados. Ambos os tráfegos apresentam o mesmo comportamento em relação ao atraso, pois são tratados em uma mesma categoria. Logo se o

fluxo de dados B não estiver sendo atendido em seus requisitos e sofrer uma mudança de caminho, essa mudança reflete-se no fluxo A, pois esse pertence à mesma categoria de fluxos de dados de B, independentemente de estar sendo atendido.

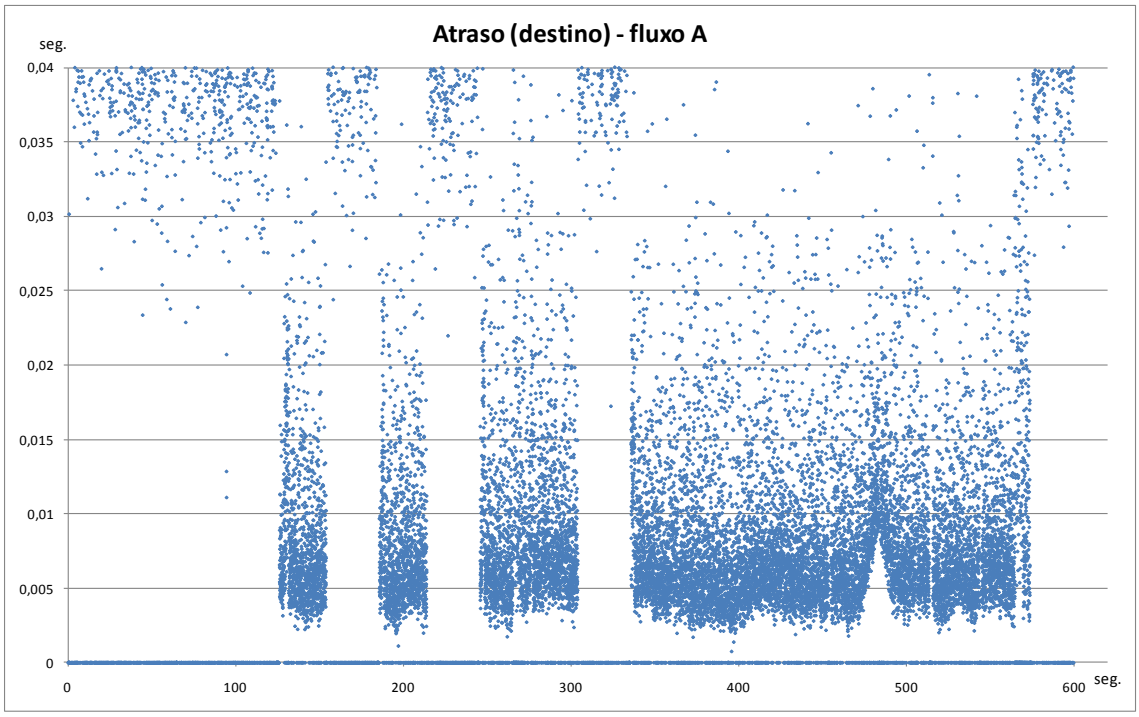

Figura 43 – Atraso do fluxo de dados A com atuação do agente (medida 1)

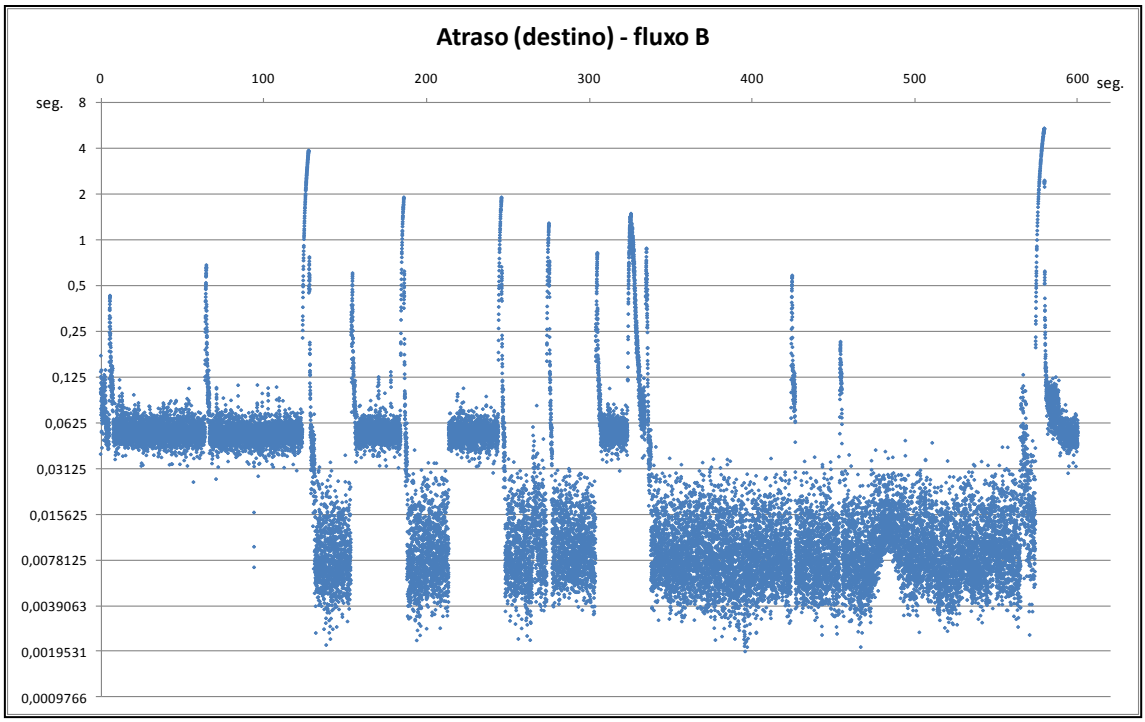

Figura 44 Atraso do fluxo de dados B com atuação do agente

As oscilações ocorridas nos gráficos da Figura 43 e Figura 44 são resultado dos valores iniciais de P e Q que resulta no *preferential attachment*. Como todos os *links* começam com valores iniciais de P e Q igual a zero em todos os *links*, o agente contabiliza as falhas e calcula a probabilidade de alterar o caminho. No gráfico da Figura 43 embora o agente tenha atuado o caminho escolhido foi o mesmo, logo o comportamento do gráfico não sofreu alterações nos primeiros 100 segundos.

Contudo em uma nova análise realizada entre 100 e 200 segundos o agente recalculou o *preferential attachment* escolhido foi aquele que não apresentava falhas. O comportamento oscilatório continuou até se estabilizar por aproximadamente 50% do tempo de transmissão pelo melhor caminho (que pode ser pela rota B ou rota C), notadamente devido aos valores de *preferential attachment* assumidos, como pode ser observador na Tabela 6.

Medida Agente	Preferential Attachment			Rotas Escolhida
	Rota A (next-hop 20.0.0.2)	Rota B (next-hop 40.0.0.2)	Rota C (next-hop 10.0.0.2)	
1	50%	33%	17%	A
2	40%	30%	30%	A
3	45%	28%	27%	B
4	40%	30%	30%	A
5	40%	29%	31%	B
6	39%	32%	29%	A
7	36%	32%	32%	C
8	37%	31%	32%	B
9	35%	31%	34%	A
10	38%	33%	29%	B
.....	.....	.....	.....	.....
20	28%	35%	37%	B

Tabela 6 – Valores de *Preferential Attachment* para tráfego de dados.

Embora o caminho com *preferential attachment* maior seja o caminho com as condições adequadas, pode ocorrer oscilações eventuais como pode ser observado nas figuras anteriores (próximo a 600s) uma vez que se trata de uma escolha probabilística. De acordo com a Tabela 6 tem–se que o caminho utilizado pelo fluxo de dados do tipo dados alterna entre a rota B e a rota C, e dado que ambos os caminhos possuem *preferential attachment* similar por apresentarem as mesmas condições, a oscilação de caminho não afeta os parâmetros dos fluxos de dados.

A evolução dos valores do *preferential attachment* possui a seguinte dinâmica:

- O valor de Q é calculado verificando quantidade de amostras de fluxos que falharam em determinado *link* em relação ao total de falhas em todos os *links* do equipamento controlado;
- A quantidade de erros é cumulativa;
- O *link* que não possui falhas porque não recebeu aquele tipo de fluxo de dados, tem seu valor calculado como a diferença entre o valor "1" menos a somatória dos demais *preferential attachments* dos demais *links* para aquele tipo de fluxo de dados (normalização dos valores).

É desta forma que mesmo sem receber um determinado tipo de fluxo de dados a rota C apresenta *preferential attachment* de 17%. Através desse mecanismo todos os *links* que possuem caminho para um determinado destino são elegíveis para ser escolhidos.

5.3.3.2 Análise do fluxo de dados tipo VoIP

O fluxo de dados tipo VoIP apresentou algumas oscilações em termos de atraso devido ora aos dois requisitos de tráfego que não estavam sendo cumpridos, ora por apenas um dos parâmetros, uma vez que as taxas de transmissão foram as mesmas apresentadas nos testes anteriores (Figura 45).

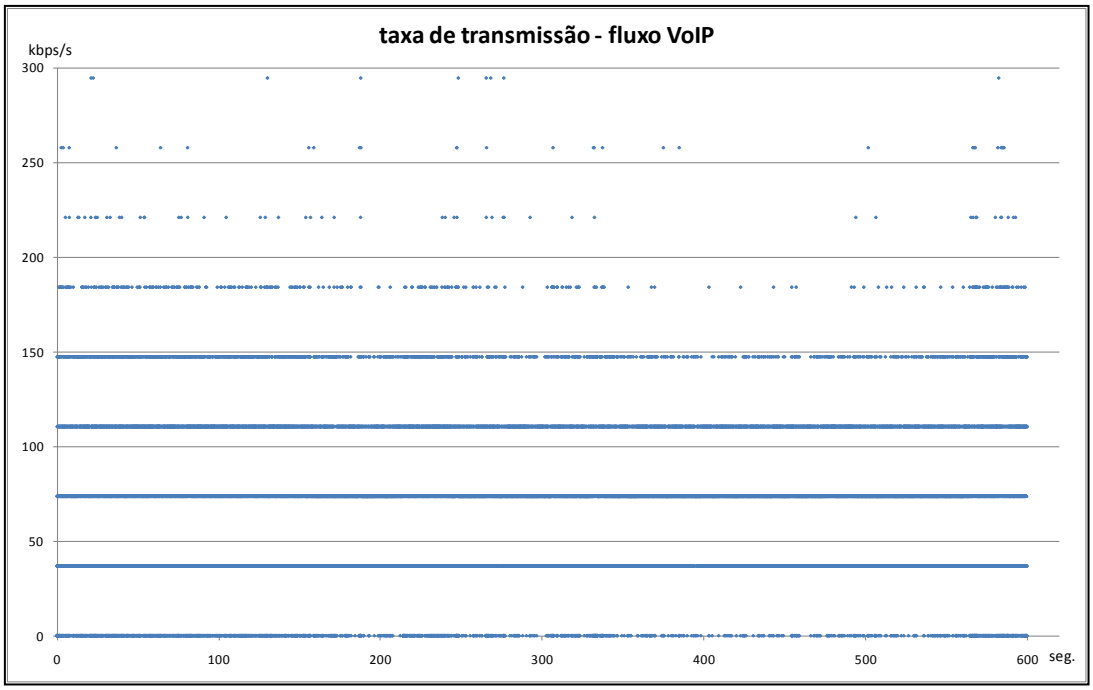

Figura 45 – Taxa de transmissão de um fluxo de dados tipo VoIP com atuação do agente

No segmento ‘X’ do gráfico da Figura 46 nota-se que tanto o atraso quanto a quantidade de pacotes perdidos (Figura 47) ultrapassa os limites estabelecidos e, portanto deve ocorrer uma mudança de caminho. Tal mudança só ocorre no trecho ‘Y’ que novamente será novamente alterado devido à perda de pacotes. Já no trecho K não ocorrem alterações de caminho devido ao *preferential attachment*, mesmo ocorrendo falhas intermitentes durante esse período de tempo o qual compreende o trecho K. Os valores de Q que os valores que determinam a comudança estão representados na Tabela 7.

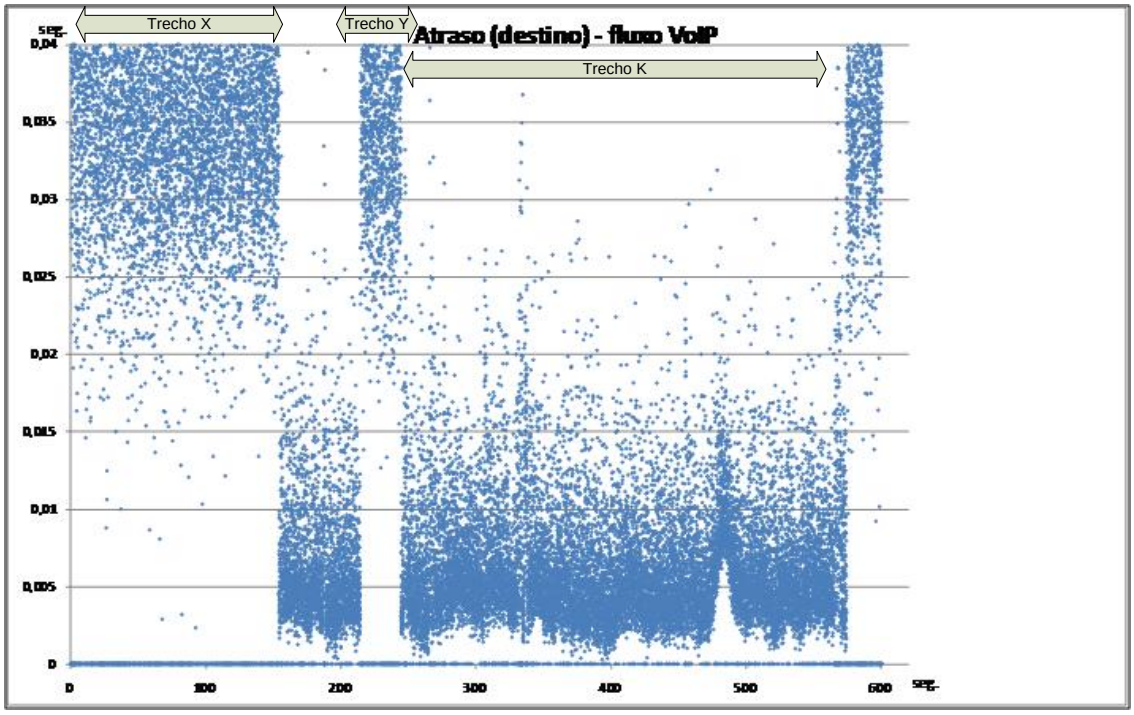

Figura 46 – Atraso de um fluxo de dados tipo VoIP com atuação do agente

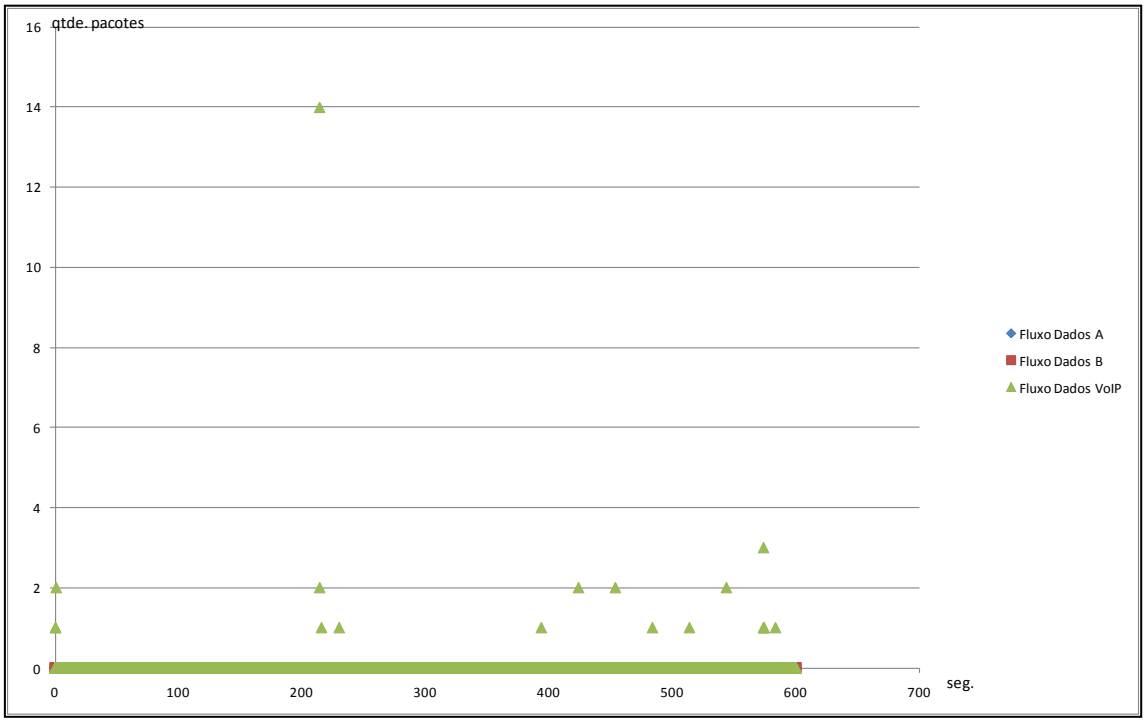

Figura 47 – Perda de pacotes de um fluxo de dados tipo VoIP com atuação do agente.

Medida Agente	Preferential Attachment			Rotas Escolhida
	Rota A (next-hop 20.0.0.2)	Rota B (next-hop 40.0.0.2)	Rota C (next-hop 10.0.0.2)	
1	50%	0%	50%	A
2	25%	25%	50%	B
3	17%	50%	33%	B
4	25%	50%	25%	A
5	17%	50%	33%	C
6	22%	42%	36%	C
7	17%	44%	39%	B
8	23%	45%	32%	B
.....	.....	.....	.....	.....
20	28%	35%	37%	B

Tabela 7 – Valores de *Preferential Attachment* para fluxo de dados tipo VoIP

A Tabela 7 apresenta o mesmo tipo de comportamento do *preferential attachment* em relação aos fluxos de dados do tipo dados. No caso do fluxo de dados VoIP o *preferential attachment* de B iniciou em zero e cresceu ao longo da quantidade de falhas apresentada pela rota A.

5.3.4 Resultados do teste com agentes, um ponto de falha e agente com *preferential attachment* definido

Neste conjunto de testes foram gerados os mesmos tipos de atraso do item anterior, sendo a única diferença é que este conjunto de testes foi feito após os agentes trabalharem por uma hora com o mesmo padrão de fluxo de dados gerado. O *preferential attachment* gerado está representado na Tabela 8 e medida 1 do agente no final da primeira hora utilizada para a definição do *preferential attachment* para os fluxos de dados tipo Dados e a medida 1 da Tabela 9 para os fluxos de dados VoIP.

Nestes testes o agente calcula o *preferential attachment* e reorganiza o caminho independentemente do fluxo de dados estar sendo ou não atendido. Esta foi uma alteração para este teste de forma a verificar se a reorganização de todos os fluxos de dados causaria oscilações nos valores de *preferential attachment*.

5.3.4.1 Análise do tráfego de dados

De acordo com o gráfico da Figura 48 a taxa de transmissão dos fluxos de dados de testes apresenta o mesmo padrão dos testes anteriores; já em relação ao atraso tem-se que esse se manteve na maior parte do tempo de teste dentro dos parâmetros esperados (Figura 49).

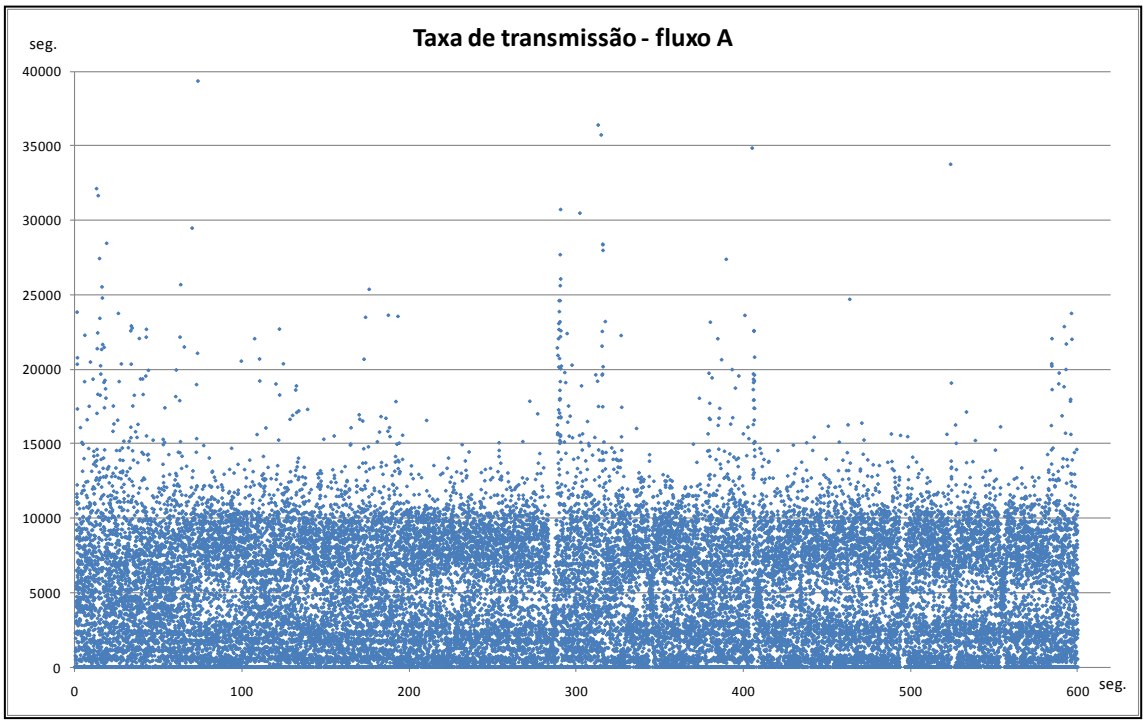

Figura 48 – Taxa de transmissão de um fluxo de dados

A variação de atraso dos fluxos de dados de dados (Figura 50) ficou em média em 1,2ms para fluxos de dados com taxa de transferência média de 14,38 Mbps/seg. e atraso médio de 11ms (fluxo A); e com variação de atraso de 1,34ms para fluxos de dados com taxa de transmissão de 4,86Mbps/seg. e atraso de 32,8ms (fluxo B).

Medida Agente	*Preferential Attachment*			Rotas Escolhida
	Rota A (next-hop 20.0.0.2)	Rota B (next-hop 40.0.0.2)	Rota C (next-hop 10.0.0.2)	
1	24,85%	32,57%	42,58%	C
2	23,97%	33,14%	42,89%	C
3	24,21%	32,94%	42,85%	C
4	23,80%	33,23%	42,97%	B
5	23,92%	32,95%	43,13%	C

Tabela 8 – *Preferential Attachment* do fluxo de dados tipo dados

Analisando os dados da Tabela 8 tem-se que o *preferential attachment* não se alterou significativamente, pois cada medida da tabela apresenta uma medida a cada 10 minutos (da medida 2 até a medida 5). Nota-se que nesse ponto ocorreu uma alteração de caminho para a rota B apenas, sendo que no restante do tempo os fluxos de dados se mantiveram na rota C.

Na Tabela 8 tem-se que tanto a rota C quanto a rota B possuem em princípio condições de trafegar os fluxos de dados do tipo Dados, embora eventualmente, o fluxo de dados A (Figura 49) alterou seu caminho por um caminho inadequado.

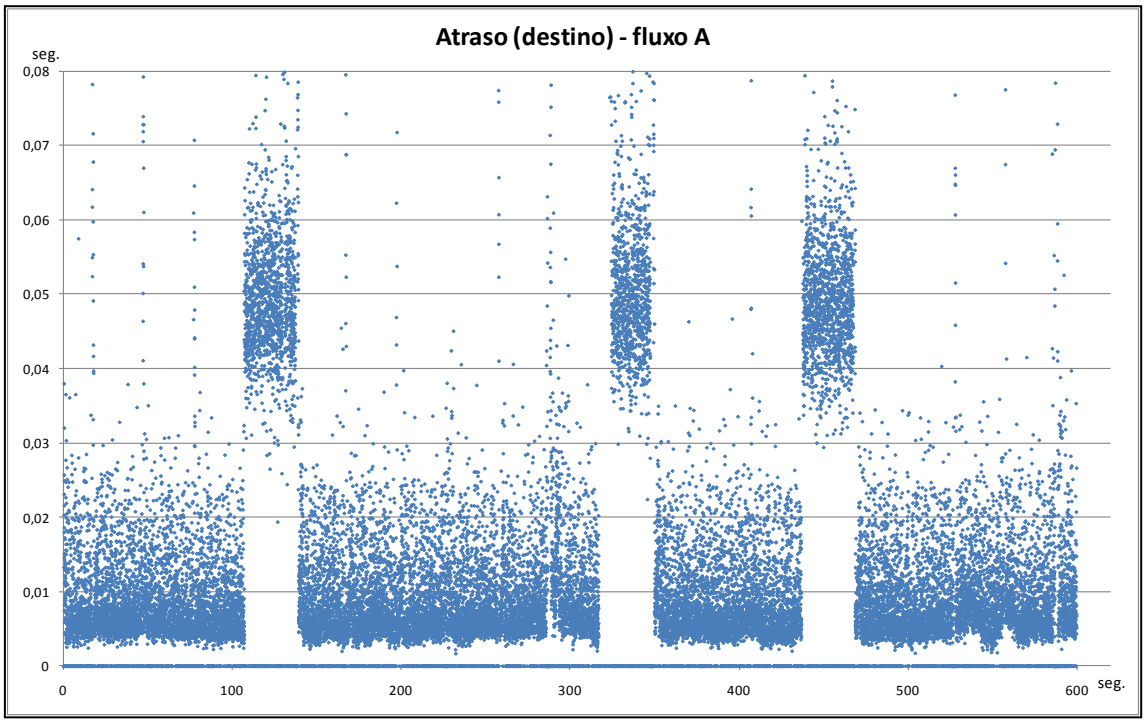

Figura 49 – Atraso de um fluxo de dados tipo dados

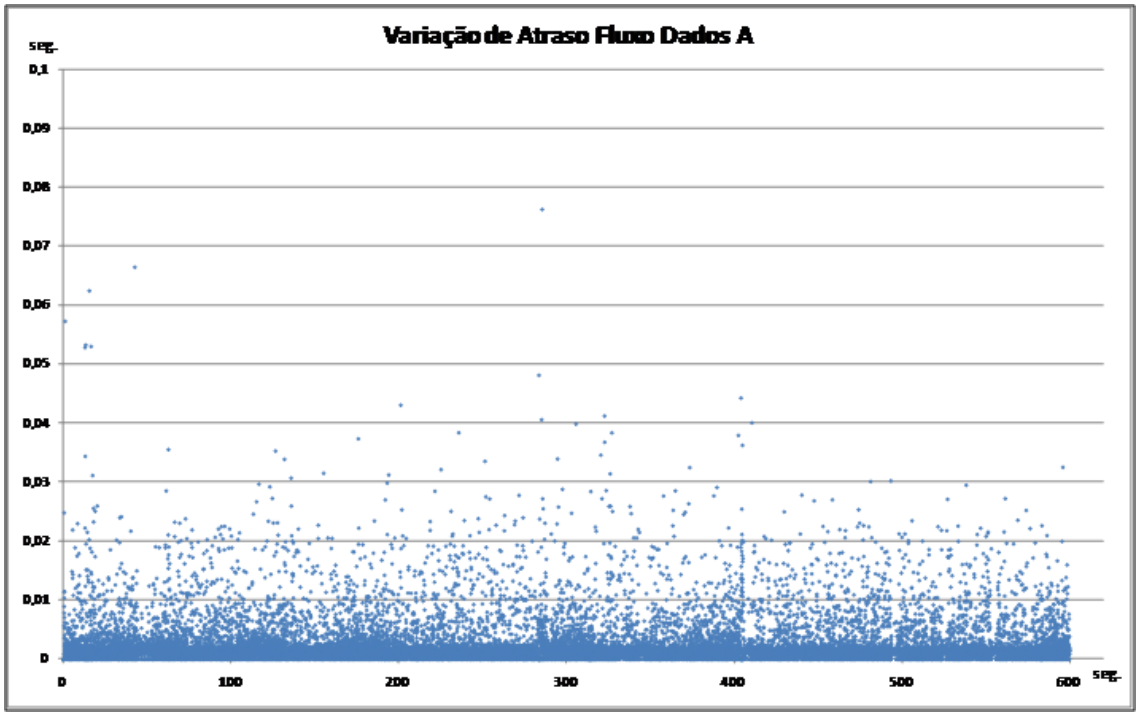

Figura 50 – Variação de atraso de um fluxo de dados tipo dados

5.3.4.2 Análise do fluxo de dados tipo VoIP

Os fluxos de dados tipo VoIP por sua vez apresentaram estabilidade similar aos fluxos de dados do tipo dados. O gráfico da Figura 51 indica a mesma taxa de transferência e o gráfico da Figura 52 mostra o momento em que a decisão do agente foi alterar o caminho para um caminho inadequado, voltando à estabilidade do caminho após essa oscilação.

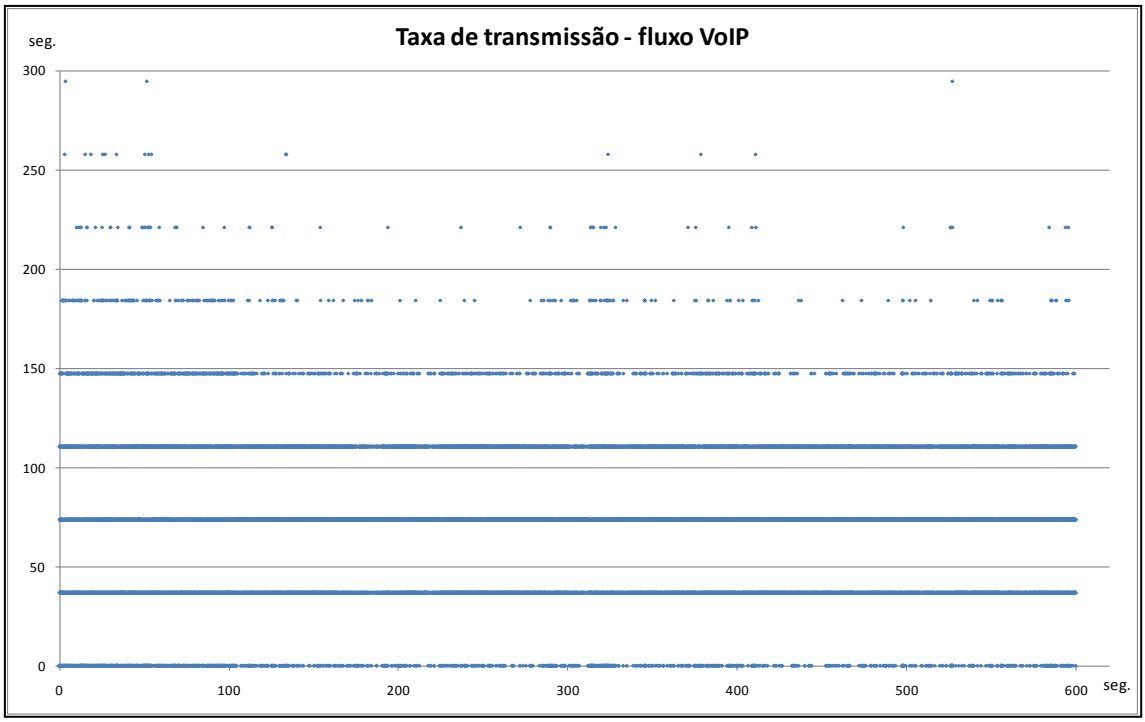

Figura 51 – Tráfego de um fluxo de dados tipo VoIP (com atraso)

A Tabela 9 identifica esse momento na medida 3, e as demais medidas apresentam amostras feitas a cada 10 minutos da mesma forma que feito para os fluxos de dados do tipo Dados. Nota-se a estabilidade do caminho. O gráfico da Figura 53 identifica que nenhum caminho apresenta o valor de variação de atraso adequado para fluxo de dados tipo VoIP de acordo com a Tabela 4 (página 33).

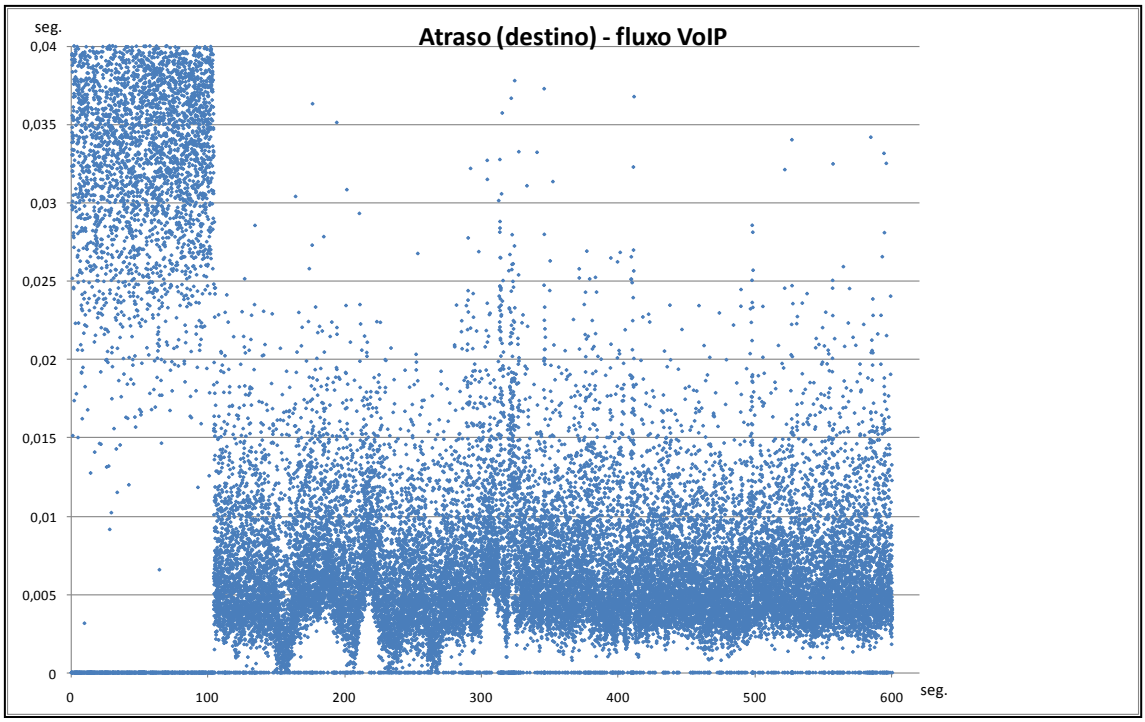

Figura 52 – Atraso de um fluxo de dados tipo VoIP (com atraso)

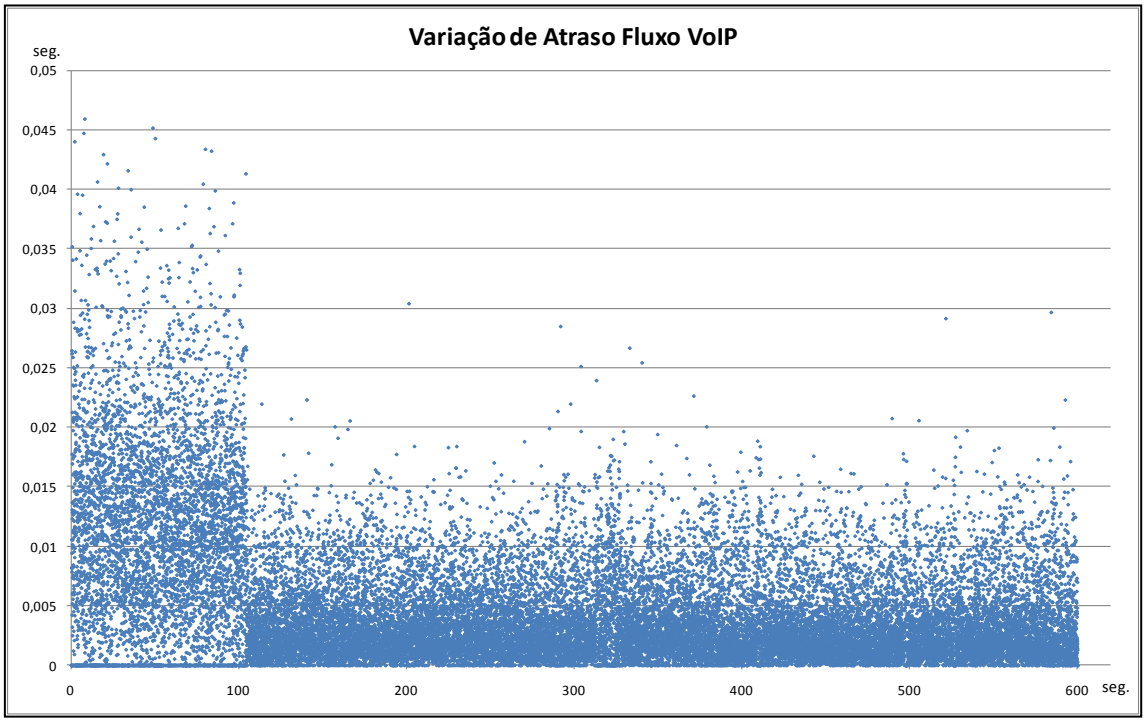

Figura 53 – Variação de atraso de um fluxo de dados tipo VoIP

Medida Agente	Valores de Q			Rotas Escolhida
	Rota A (next-hop 20.0.0.2)	Rota B (next-hop 40.0.0.2)	Rota C (next-hop 10.0.0.2)	
1	24,11%	29,17%	46,72%	C
2	23,55%	29,65%	46,80%	C
3	26,18%	26,95%	46,87%	A
4	25,26%	27,82%	46,92%	C
5	25,41%	27,62%	46,97%	C

Tabela 9 – *Preferential Attachment* para fluxo de dados tipo VoIP

5.4 DISCUSSÃO DOS RESULTADOS OBTIDOS

Os resultados obtidos através dos testes realizados indicam claramente o comportamento do *preferential attachment*, o qual pode ser observado pela evolução dos valores de Q e por conseqüência as oscilações dos parâmetros de atraso dos fluxos de dados.

Embora oscilações possam ocorrer devido à proximidade dos valores de Q, principalmente durante o início das operações do agente, a tendência do *preferential attachment* é respeitada e os resultados iniciais demonstram que pode ocorrer “especialização de *links*”, ou seja, os valores de P e Q podem fazer com que um determinado tipo de fluxo de dados seja enviado por apenas um caminho, enquanto outro tipo de dados seja enviado por outro caminho, mesmo que o destino seja o mesmo dado as condições de cada parâmetro da infraestrutura.

O *preferential attachment* também mostra-se robusto em relação às oscilações dos parâmetros para controle de um fluxo de dados, mesmo em se tendo um algoritmo simples em termos do que considerar falha. O algoritmo para cálculo de P e Q da forma como foi desenvolvido para a prova de conceito desta tese considera que se uma amostra do fluxo de dados analisado não atender aos requisitos em qualquer um dos parâmetros, tal fluxo de dados deve ser considerado como falho. Certamente há casos de fluxos de dados que, mesmo que uma amostra não esteja de acordo com os requisitos determinados, ainda assim o fluxo de dados como um todo estará de acordo com a expectativa do usuário e, portanto, respeitando o contrato de qualidade de serviço. Dessa forma não seriam necessárias alterações no caminho do

fluxo de dados. A robustez apresentada pela arquitetura distribuída está em mesmo se considerando qualquer desrespeito aos requisitos estabelecidos, não ocorrem alterações de caminho em todos os casos devido à probabilidade de se manter no caminho. Apenas em casos de grandes variações, ou seja, de diversos pacotes de um tipo de fluxo de dados não respeitarem os requisitos é que o agente tenderá a alterar o caminho. Portanto, para falhas intermitentes a tendência é que o caminho não seja trocado quando o *preferential attachment* estiver estabelecido (ou seja, os valores de P e Q não sofrem variações que alterem a organização da distribuição de fluxos de dados). Contudo, se estas falhas intermitentes ocorrerem com freqüência, o caminho poderá ter sua preferência eliminada dependendo de quantos fluxos de dados são afetados pela falha intermitente.

Os resultados também indicam que a robustez do conceito de *preferential attachment* para o tratamento da qualidade de serviço está na forma de ajuste do caminho dado a independência dos parâmetros de controle, pois mesmo com dois caminhos apresentando cada qual um tipo de falha, o agente foi capaz de determinar um melhor caminho por uma terceira via. Foi o caso dos testes com *preferential attachment* definido (e por consequencia caminho definido), pois a rota C foi aquela que não apresentou falhas durante o experimento. O agente apenas oscilará e não terá um caminho determinado para a maioria de suas decisões se ocorrerem de todos os caminhos para um determinado destino apresentem quantidade de falhas próximas, independente de qual o parâmetro em que a falha ocorra.

Também se pode observar a influência entre os fluxos dados, pois se um tipo de fluxo exige mais de um *link* os efeitos são sentidos pelo outro tráfego e dessa forma pode ocorrer a mudança do caminho de um dos fluxos de dados, ou do que está exigindo mais ou daquele que sente o efeito, dependendo de qual parâmetro é afetado e do tempo de análise do agente. Comparando os momentos onde ocorre perda de pacotes fica claro ao longo dos testes que na maioria dos casos tal perda ocorre quando ambos os tipos de fluxos de dados estão passando por um mesmo caminho. Isso significa que uma alteração em um determinado fluxo de dados influencia os outros tipos de fluxos de dados, pois ambos compartilham a mesma fila de saída. O agente RMA da arquitetura

proposta é capaz de considerar tais falhas e alterar o caminho dos fluxos de dados se necessário.

6 CONCLUSÕES

A abordagem distribuída da arquitetura proposta apresenta um conjunto propriedades que aliadas à teoria dos sistemas complexos e à hierarquia de agentes traz pontos interessantes para a questão do controle da qualidade de serviço em sistemas de comunicação.

O primeiro ponto é em relação ao tempo de resposta para uma determinada falha em um ponto qualquer do sistema de comunicação e de como o conhecimento sobre as condições do sistema de comunicação é distribuído. Por se tratar de um sistema distribuído e composto por agentes autônomos as falhas são tratadas no ponto onde ocorrem e independem de um sistema central para atuações que resolvam a falha ou envie instruções para o agente atuar. Contudo, nem sempre é possível resolver uma determinada falha localmente, pois se o agente RMA não possuir outra opção de caminho para tratamento daquela falha, então ele será incapaz de determinar uma solução. Essa situação pode ser tratada como falta de recursos (*starvation*) e para esse tipo de caso se faz necessária a atuação da hierarquia superior composta do agente PA.

O agente PA não fere o princípio da autonomia dos agentes RMA, uma vez que não influencia na decisão do agente RMA onde a falha ocorre. Se o agente PA atuar apenas no agente RMA que não possui recursos para tratar a falha, provavelmente não obterá sucesso devido à mesma falta de recursos. Contudo, o agente PA pode atuar em pontos anteriores do sistema de comunicação por onde o fluxo de dados falho passa, sejam tais pontos no interior do domínio administrativo ou em suas nas bordas. Uma primeira ação é determinar um alto valor de Q para aquele destino e classe de fluxo de dados para os agentes EA, indicando para os agentes UA e SA que o domínio administrativo não é capaz de lidar com aquele tráfego. Outra forma de atuação pode ser enviar uma mensagem para os agentes RMA vizinhos ao agente RMA que apresentou a falha indicando que há uma falha que não pode ser tratada. Neste caso, os agentes vizinhos de posse desta informação podem ajustar de forma autônoma seus valores de P e Q e com essa ação podem alterar o

caminho para que o fluxo de dados não passe pelo equipamento controlado pelo agente que apresentou a falta de recurso para lidar com a falha.

A comunicação com a hierarquia superior se faz mais interessante do que a comunicação entre os pares devido à forma de propagação. Uma vez que os agentes da hierarquia superior possuem uma visão do domínio administrativo maior do que os agentes da hierarquia inferior, a decisão de avisar os vizinhos do agente RMA com falha pode ser substituída apenas por um aviso de valores de parâmetros para o agente PA, uma vez que o agente RMA em cuja falha ocorreu pode ser caminho único para aquele tipo de fluxo de dados e destino. Este tipo de decisão deve ser feito pelo agente PA, cujo algoritmo deve tratar esse tipo de situação e intervir na rede no menor tempo possível.

Em se tratando de uma classe de fluxo de dados e de quando esse é elegível para ter seu caminho alterado, todos os fluxos de dados daquela categoria mudam independentemente se estão sendo ou não atendidos, dado que eu um deles não está sendo atendido. Essa situação pode ocorrer, por exemplo, pelo excesso de fluxos de dados de um determinado tipo para um destino devido a presença de hubs (pontos de concentração) em algum ponto do sistema de comunicação. Mesmo que todos os fluxos de dados sejam considerados como falha por causa de apenas um fluxo não atendido, os testes indicam que as oscilações não causam prejuízo aos fluxos de dados, uma vez que tendem a serem transmitidos por um caminho mais adequado. É por essa razão que todos os fluxos de um mesmo tipo são registrados como falha e são contabilizados no *preferential attachment*. Isto não significa que todos os fluxos de dados mudem de caminho obrigatoriamente, pois cada fluxo de dados pode ser independentemente submetido ao algoritmo de Monte Carlo para decidir por qual *link* deve ser enviado.

De certa forma o comportamento descrito influencia positivamente o *preferential attachment* e não causa demasiadas oscilações, pois como está demonstrado nos testes realizados uma vez definido o *preferential attachment*, ou seja, um determinado tipo de fluxo de dados passa por um determinado caminho para alcançar um destino, falhas intermitentes não causam alteração de caminho devido aos valores de Q e P, mas se causarem a tendência é que os fluxos de dados sejam enviados por um caminho que em princípio possui

um valor adequado de P e Q similares ao caminho atual. Como não há relação direta entre os valores de P e Q de classes de fluxos de dados distintas, a mudança de caminho de um determinado tipo de fluxo de dados pode apenas causar influência indireta nos valores de P e Q de outras classes de fluxos de dados, sendo que tais mudanças podem ser positivas para algumas classes de fluxos de dados que terão um caminho com menor competição pelos recursos, e outros caminhos que podem se tornar menos interessantes para algumas classes de fluxos de dados.

A arquitetura proposta não oferece garantias que a mudança de caminho será sempre positiva para todos os tipos de fluxos de dados; daí está um dos comportamentos complexos do sistema de controle de qualidade de serviço proposto. Como os fluxos de dados são tratados de forma distinta e independente, então se um caminho não recebeu um determinado tipo de fluxo de dados, sua taxa de erro é zero, assim como sua taxa de sucesso. Dependendo da condição da infraestrutura do sistema de comunicação este caminho por se elegível pode receber o fluxo de dados. Neste momento duas situações podem ocorrer: o caminho realmente possui os recursos necessários ou o caminho não possui os recursos necessários.

Na primeira situação em que o caminho possui os recursos necessários então o valor de P para aquele tipo de fluxo de dados e destino irá aumentar, enquanto Q continuará em um valor que faça com que o novo caminho seja em algum momento o caminho preferencial daquele tipo de tráfego. Enquanto isto não ocorrer transições de caminho podem ocorrer, como os testes da prova de conceito indicaram. Contudo, independente das oscilações um caminho adequado foi encontrado.

Já na segunda situação o novo caminho também pode ser falho por pelo menos dois motivos: ou por não ter recursos totais suficientes (independentemente da quantidade de tráfego existente no *link*) ou porque está transmitindo um determinado tipo de fluxo de dados que consome recursos em tal ordem que não há excedentes suficientes para o tipo de fluxo de dados recém chegado. Em princípio não há forma de se determinar o que ocorrerá de forma determinística; contudo os dois tipos de fluxos de dados terão suas influências refletidas em seus valores de P e Q e, dependendo do estado de P

e Q dos caminhos alternativos os fluxos de dados podem ter seus caminhos alterados.

Independentemente de qual das duas situações ocorram, pode existir propagação de alterações para diversos pontos do domínio administrativo como forma de adequá-lo à exigência de todas as classes de fluxos de dados e suas quantidades transmitidas. O limite é alcançado se não se encontrar caminhos para todos os fluxos e, portanto haverá a decisão do agente PA de como tratar tal situação.

Um caso em particular de falha é aquele em que a falha ocorre próximo ao destino final do tráfego, pois quanto mais próximo do destino menor a quantidade de caminhos disponíveis. Contudo, quanto mais próximo do destino o agente estiver, maior a probabilidade do agente já receber aquele tráfego, e portanto menor a probabilidade de se ter falha causado por uma mudança no caminho do fluxo de dados, afinal o tráfego converge para um mesmo local na infraestrutura.

Embora as falhas com menor chance de serem tratadas estarem localizadas próximo do destino ou da origem do fluxo de dados, podem ocorrer casos de falhas em outros pontos do domínio administrativo nos quais impliquem na impossibilidade de todo o domínio administrativo atender aos requisitos de qualidade de serviço. Em ambos os casos a situação de *handover* deve ser analisada. O *handover* é considerado nesta tese como ocorrendo entre domínios administrativos distintos visíveis por um agente UA ou SA, independentemente da sua tecnologia (do ponto de vista dos agentes). Logo a decisão de ocorrer *handover* é prerrogativa dos agentes UA e SA, dependendo do estado do domínio administrativo em relação ao contrato de qualidade de serviço que o agente UA ou SA esperam ter. O agente PA, em seu nível hierárquico apenas apresenta dados sob ,seu domínio administrativo e propaga dados de todos os níveis hierárquicos superiores (incluso seu nível) para os agentes do nível inferior.

A informação enviada do agente PA mostra-se relevante para os agentes UA e SA tomem decisões de *handover* em se comparando os dados fornecidos pelo agente EA de cada domínio administrativo ao qual o agente UA e SA possam ter acesso. Contudo, para a informação ser coerente deve ser

composta por dados fim a fim e nenhum agente RMA ou PA podem possuir tal informação, pois estes apenas gerenciam um domínio administrativo. Portanto, tal tarefa cabe ao agente SCA, pois este é capaz de ter todos os dados de seus agentes PA, sendo então capaz de determinar os dados de maneira global em seu sistema autônomo. A informação fornecida por um sistema autônomo só pode ser utilizada como dado fim a fim se tanto a origem como o destino pertencerem ao mesmo sistema autônomo controlado pelo agente SCA. Caso contrário o agente SCA utilizará os dados recebidos de outros agentes SCA para determinar o *service level management* fim a fim e com isso determinar quanto recurso o seu domínio administrativo custa para o transporte fim a fim. Dessa forma, o ciclo de qualidade de serviço fim a fim é fechado já que ocorre uma forma de realimentação de controle, uma vez que o SCA conhece os dados de seu domínio e os dados totais, desta forma podendo determinar se seu sistema autônomo é capaz de transmitir um tipo de fluxo de dados.

Notadamente no teste realizado todo o tráfego é desviado devido à forma montada de roteamento. Contudo, não é uma limitação da arquitetura proposta, pois outros dados podem ser adicionados na análise do agente para tomada de decisão diferenciada, como, por exemplo, número de porta TCP ou UDP. Esse refinamento é similar ao que é proposto na arquitetura IntServ, com a diferença de não se ter de propagar pedidos de alteração na rede, o que melhora o desempenho, embora também aumente a quantidade de estados de um fluxo a serem controlados. Atualmente, matrizes de comutação dedicadas em diversos equipamentos de rede IP podem solucionar a questão de desempenho promovida pelo aumento de estados de controle; contudo não solucionam a troca de dados entre equipamentos se esta for necessária.

Como foi observado nos testes realizados pode ocorrer com determinados serviços a segmentação de caminhos, ou seja, entre uma mesma origem e destino, um fluxo de dados de determinada classe pode ser encaminhado por um determinado caminho diferente de outra classe de fluxo de dados. Contudo, ambos os fluxos de dados que seguem por caminhos distintos podem pertencer a um único serviço, como aulas online onde há fluxos de dados tipo vídeo e fluxos de dados tipo texto que guardam entre si uma relação de sincronismo. Nestes casos a arquitetura proposta não possui mecanismos para

controlar esse sincronismo entre as classes de dados de tipos distintas e, portanto o destino de tal serviço deverá se preocupar por quais redes os fluxos são entregues e tratar quaisquer questões de sincronismo.

6.1 CUMPRIMENTO DOS OBJETIVOS E INEDITISMO

O objetivo da tese foi cumprido pois um passo foi dado na elaboração e análise das características de uma arquitetura de controle de qualidade de serviço para um ambiente heterogêneo composto de *backbones* IP e redes de acesso de diversas tecnologias. Embora os testes da prova de conceito tenham sido construídos sob a plataforma IP, a estrutura da prova de conceito permitiu de forma satisfatória a criação de canais de comunicação que foram ajustados para representar a conexão de um usuário final em diversos tipos de redes de acesso, notadamente redes xDSL e redes 3G/UMTS HSPDA+ e WCDMA.

A hipótese da tese de que uma arquitetura distribuída para controle de QoS possa responder às exigências de dos contratos de qualidade de serviço de um usuário para um serviço dito convergente em um ambiente heterogêneo mostrou-se viável através da aplicação de sistemas multiagentes e conceitos de sistemas complexos. As alterações de caminhos determinadas pelos agentes de forma autônoma e localizada no equipamento que este agente controlava mostraram que a decisão descentralizada de qualidade de serviço pode obter resultados satisfatórios como forma de escolher os caminhos que se mostram adequados para um determinado tipo de fluxo de dados, e com isso determinando uma tendência para a prestação do serviço de acordo com os requisitos estabelecidos. A hipótese de agrupamento de fluxos de dados devido às decisões de um agente baseado no conceito de *preferential attachment* também se mostrou consistente nos testes realizados com agentes RMA localizados no "*backbone*" da infraestrutura proposta.

Com relação ao ineditismo desta tese pode-se considerar o modelo proposto, a aplicação do conceito de *preferential attachment* no âmbito de controle de qualidade de serviço, e o mecanismo de malha de realimentação criado pela hierarquia de agentes, pois não foi encontrado na literatura e nem em empresas de mercado, até o presente momento, nenhuma arquitetura com

as características e mecanismos propostos neste trabalho. Este trabalho também propõe uma visão única de qualidade de serviço e relação entre parâmetros de um serviço de forma independente da tecnologia de um sistema de comunicação.

6.2 TRABALHOS FUTUROS

Este trabalho propõe uma arquitetura de controle de qualidade de serviço da qual foi explorada algumas de suas características. Contudo, novas pesquisas e aplicações podem ser realizadas tendo esta pesquisa como subsídio, desde o estudo de algoritmos para decisão e cálculo dos valores de P e Q até o estudo do comportamento do tráfego e o resultado do comportamento dos agentes em outros cenários e organizações de infraestruturas e sistemas de comunicação.

Algumas propostas de pesquisa que podem ser realizadas e guardam relação com esta tese são:

- estabelecimento do comportamento da arquitetura proposta em termos de grandes volumes de fluxos de dados quando estes são entregues ao sistema de comunicação em um curto intervalo de tempo (*burst* de tráfego). Esse tipo de pesquisa auxiliará na identificação da forma de resposta e o controle de admissão dos agentes EA;
- proposta de ontologia para a comunicação entre os agentes e suas hierarquias de forma a que a malha de controle proposta possa ser analisada, assim como pode ser elaborada uma relação entre os diversos parâmetros de qualidade de serviço de diversas tecnologias de sistemas de comunicação;
- estudos de algoritmos para determinação de P e Q de outras formas que tomem em consideração propriedades apresentadas pelos fluxos de dados, assim como sua interação com outras arquiteturas de qualidade de serviço. Trabalhos nesta linha de pesquisa podem considerar como os diversos algoritmos de filas de uma interface de comunicação podem ser utilizados para aprimorar

a decisão dos agentes, assim como quais classes de algoritmos respondem em menor tempo a oscilações e falhas em um sistema de comunicação. Podem ser estudados algoritmos para considerar diversos tipos de perfis de tráfego e de usuários para determinação de "casos" ou situações que se podem esperar de um sistema de comunicação e de um conjunto de serviços;

- pode ser estudado como diferentes técnicas de engenharia de tráfego podem ser aprimoradas através dos dados fornecidos pelos agentes e como decisões distribuídas podem ser utilizadas de forma conjunta com técnicas de engenharia de tráfego existentes, principalmente em se considerando terminais móveis e com capacidade de operar em diferentes tecnologias e padrões de sistemas de comunicação;
- estudos sobre se a segmentação de fluxos de dados e controle de caminhos em um sistema de comunicação pode trazer algum grau de previsibilidade para um sistema de comunicação baseado em redes de pacotes e compartilhamento de recursos (como ocorre atualmente em redes IP). Esses estudos podem auxiliar na elaboração de técnicas de engenharia de tráfego e projetos de sistemas de comunicação, pois indicariam comportamentos que se poderiam esperar de um sistema de comunicação e de seus usuários em relação aos serviços que utilizam e de como os utilizam.

Ainda se pode estudar classes de algoritmos para todos os agentes da arquitetura proposta para os agentes organizarem e tomarem decisões baseadas em políticas de um domínio administrativo ou de um sistema autônomo, ou ainda como forma a se adequarem a questões de *handover* e engenharia de tráfego.

REFERÊNCIAS BIBLIOGRÁFICAS

2008a FIPA. FIPA Abstract Architecture Specification. FIPA, 2008. Disponível em http://www,fipa.org/specs/fipa00001.

2008b FIPA . FIPA Contract Net Interaction Protocol Specification Disponível em: http://www.fipa.org/specs/fipa00029/index.html

2008c FIPA. Agent Management Specification, 2008. Disponível em: http://www.fipa.org/specs/fipa00023/index.html.

Adler, J.L.;et.al. "A multi-agent approach to cooperative traffic management and route guidance". In: Transportation Research Part B: Methodological, v. 39, n. 4, Elsevier, 2005. p.297-318.

Ahmad, I.; Kamruzzaman, J. "Preemption-aware Instantaneous request call routing for networks with book-ahead reservation". In: IEEE Transactions on Multimedia. v. 9, n.7. 2007. p. 1456-1465.

AMIDST Project. Deliverable 3.2.1 – QoS archictecture. 1999. Disponível em: amidst.ctit.utwente.nl/amidst_publications.html. Acessado em Ago. 2007.

Anisetti, M.; et.al. "Accurate Localization and Tracking of Mobile Terminal". In: International Conference on Wireless Communications, Networking and Mobile Computing, 2006. p. 1-4.

ANS T1.523-2001, Telecom Glossary 2000. Disponível em: http://www.atis.org/glossary/

Aurrecoechea, C.; Campbell, A. T.; Hauw, L. A survey of QoS architectures. In: Multimedia Systems, n. 6, 1998; pp. 138-151.

Avalone, S.; et.al.; "D-ITG v. 2.6.1d Manual". 2008, Disponível em: http://www.grid.unina.it/software/ITG/codice/D-ITG2.6.1d-manual.pdf. Acessado em: Ago/2009.

Baschieri, F.; Bellavista, P.; Corradi, A. Mobile Agents for QoS tailoring, Control, Adaptation over the Internet: the ubiQoS Video on Demand Service. IN: Proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02).

Barabási, A.L.; Albert, R.; "Emergence of Scaling in Random Networks," In: Science J., vol. 286, 1999, pp. 509–512.

Barabási, A.L.; Albert, R. Jeong, H.; "Scale-free characteristics of random networks: the topology of the world-wide web". In: Physica A: Statistical Mechanics and its Applications, v 281, n. 1-4, 15, 2000. p. 69-77.

Barabási, A L.. Linked: how everything is connected to everything else and what it means for business, science and everyday life. A Plume Book, 2003. 294p.

_____; “The Architecture of the Complexity: from network structures to human dynamics”. In: IEEE Control Systems Magazine, 2007. pp. 33 – 42.

_____; “Scale-free networks: a decade and beyond”. In: Science, v 325, n. 5939. 2009, pp. 412-413

Barakat, C. et.al. A flow-based model form internet backbone traffic. IN. Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement, p. 35-47, 2002.

Baroli, et.al. “Performance Analysis of OLSR and BATMAN Protocols Considering Link Quality Parameter”. In: International Conference on Advanced Information Networking and Applications, 2009. p. 307-314.

Bhargava, B. et. al.; "Multimedia Data Transmission and Contol Using Active Networks." Special Issue on Activated and Programmable Internet, Journal of Computer Communications, v. 28, n. 6, 2005, p. 623-639.

Bellavista, P.; Corradi, A.; Stefanelli, C. Application-level QoS Control for Video-on-Demand. In: IEEE Internet Computing, November, 2003. pp. 16-24

Bellifemine, F.; Caire, G.; Trucco, T.; Rimassa, G. JADE Programmer’s Guide. CSELT, 2008. Disponível em http://jade.cselt.it/

Bellifemine, F. et. al. Jade: a software framework for developing multi-agent applications. Lessons learned. In: Information and Software Technology v. 50, n.1-2, 2008. p.10-21.

_____, “JADE: A software framework for developing multi-agent applications. Lessons learned”. In: Information and Software Technology, v. 50, n. 1-12, 2008. p. 10-21.

Bellifemine, F.; Poggi, A.; Rimassa, G. “Developing multi-agent systems with JADE”. In: Intelligent Agents VII Agent Theories Architectures and Languages - Lecture Notes in Computer Science, v. 1986, 2001.p. 42-47.

Bentahar, J. “A pragmatic and semantic unified framework for agent communication”. Faculté des Sciences et de Génie Université Laval (tese). 2005. 233pp.

Beydoun, G. et.al; “A security-aware metamodel for multi-agent systems (MAS)”. In: Information and Software Techonlogy, v.51, n. 5, Elsevier, 2009. p. 832-845.

Bin, L.; et.al.; “A NetFlow based flow analysis and monitoring system in enterprise networks”. In: Computer Networks, v. 52, n. 5, Elsevier, 2008. p. 1074-1092.

Bless, R. “Dynamic Aggregation of Reservation for Internet Services”. In: Telecommunication Systems. v. 26, n. 1, 2004. pp. 33-52.

Bless, R. et. al. A Quality of service signaling architecture for seamless handover support in next generation, IP based mobile networks. In: Wireless Press Communications. n. 43. 2007. Springer Science + Business Media. p.817-835.

Bonabeau, E. Routing in Telecommunication Networks with Like-Agent Agents. In: IATA'98, LNAI 1437. 1998, 60-72.

Botta, A.; Dainotti, A; Pescapè, A.; "Multi-protocol and multi-platform traffic generation and measurement". In: IEEE 26th Annual IEEE Conference on Computer Communications, Anchorage, USA, 2007.

Bradshaw, J. M. . An Introduction to Software Agents. In: BRADSHAW, J. M Software Agents. MIT Press, 1997. p. 3-46.

CAIRE, G. JADE TUTORIAL: Jade Tutorial for Begginers. CSELT, 2008. Disponível em http://jade.cselt.it/. Acessado em 10 abr. 2008.

Calisti, M; Greenwood, D. Enabling Adaptive Service Access Management for Next Generation Multi-Service Networks. In: Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07), 2007. 10pp.

Calyam, P.; Leem C. "Characterizing voice and video traffic behavior over the Internet". In: Proceedings of the international symposium on computer and information sciences (ISCIS). 2005. Acessado em 01/Dez./2009. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.4605&rep=rep1&type=url&i=0

Camarillo, G; Garcia-Marti´n, M.; The 3G IP multimedia subsystem (IMS): merging the internet and the cellular worlds. 2ed. Wiley, 2006

Carneiro, G; et.al. "The DAIDALOS Architecture for QoS over Heterogeneous Wireless Networks", In: 14th IST Mobile & Wireless Communications Summit, Dresden, Germany, 2005.

Chalmers, D. "Quality of Service in Mobile Environments". Imperial College of Science, Technology and Medicine. Department of Computing of the University of London (dissertação). 1998. 132p.

Chalmers, D. Sloman, M. A Survey of Quality of Service in Mobile Computing Environments. In IEEE Communications Surveys. 2nd quarter, 1999.

Chen, B.; Chen, H. H.; Palen, J.; "Integrating mobile agent technology with multi-agent systems for distributed traffic detection and management systems". In: Transportation Research Part C: Emerging Technologies, v.17, n. 1, 2009. p.1-10.

Chimento, P.F. "Tutorial on QoS Support for IP". Acessado em: 20/11/2009. Disponível em: https://doc.novay.nl/dsweb/Get/File-6929/qos-tutorial.pdf. 1998. 18pp.

Choe, Y.R.; et.al.; “Improving VoD server efficiency with bittorrent”. In: Proceedings of the 15th international conference on Multimedia, Augsburg. Alemanha, 2007. p. 117-126.

Chuah, M.C; Zhang, Q.; Introduction to Traffic Engineering. In: Design and Performance of 3G Wireless Networks and Wireless Lans. Springer US, pag. 39-59, 2005.

Ciancetta, et.al, 1999. “Convergence Trends for Fixed and Mobile Services”. In: IEEE Personal Communications, v. 6, n. 2, 1999. pp 14-21.

Cisco, Internetworking Technologies Handbook, 4 ed., Cisco Press, 2003.

Claise, B.; “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information”. RFC 5101. 2008.

Colcher, S.; et. al. VoIP: Voz sobre IP, Rio de Janeiro, Elsevier, 2005.

Cucurull, J., et.al. “Agent mobility architecture based on IEEE-FIPA standards” In: Computer Communications, v.32 n.4, 2009. p. 712-729.

Dash, R.K.; et.al. “Market-Based Task Allocation Mechanisms for Limited-Capacity Suppliers”. In: IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, v. 37, n.3, 2007. p. 391-405.

Deora, V.; et.al. “A Quality of Service Management Framework Based on User Expectations” In: Lecture Notes in Computer Science, v. 2910, 2003. p. 104-114.

Dezso, Z; et.al. “Dynamics of information access on the web”. In: Physical Review E, v. 73 n. 6, 2006.

Dorogovtsev, S.N.; Mendes, J.F.F.; Samukhin, A.N.; “Structure of Growing Networks with Preferential Linking”. In: Physical Review Letters, v. 85 n. 21, 2000.

Douligeris, C.; Pitsllides, A. Computational intelligence in telecommunications networks. In. Computer Communications, n25, 2002 p.1413-1414.

Doyle, J.; Carroll, J. Routing TCP/IP v.1; 2 ed., Cisco Press, 2005.

Endrei, M.; et. al. Patterns: service oriented architecture and web services. IBM, 2004.

Egawa, T; Kiriha, Y; Arutaki, A. Tackling the Complexity of Future Networks. In: Lecture Notes in Computer Science, v. 3912, 2007. p78-87.

Evangelista, L. G.; Guardieiro, P.R.; Novo Mecanismo baseado em DiffServ para provisionamento de QoS na rede de núcleo de sistemas celulares 3G. In: Simpósio Brasileiro de Redes de Computadores, Paraíbda, 12 pp. 2007.Acessado em 10, abril de 2009. Disponível em: http://www.sbrc2007.ufpa.br/anais/2004/1940.pdf

ETSI, 2005, ETSI TS 185 001 V1.1.1, TISPAN; NGN QoS Framework and Requirements, November 2005.

ETSI, 2006 - ETSI ES 282 003 V1.1.1, TISPAN RACS Functional Architecture, June 2006

ETSI, 2009a, ETSI. TS 123 107 – Quality of service (QoS) concepts and architecture. v. 9.0.0, 2009.

ETSI 2009b; ETSI. TS 123 207 – End to End Quality of Service (QoS) concept and architecture. v. 9.0.0, 2009.

ETSI, 2009c, ETSI; TS 123 228 – IP Multimedia Subsystem Stage 2. v. 7.7.0 release 7, 2009.

Feldmann, A. et.al. The changing mature of network traffic: scaling phenomena. In. ACM SIGCOMM Computer Communication Review, v. 28, n.2, 1998. p.5-22.

Ferguson, P.; Hustion, Quality of Service: Delivering QoS on the Internet and in Computer Networks, John Wiley and sons, Inc, 1998.

Fok,C.; Roman, G.; Lu,C.;" Agilla: A mobile agent middleware for self-adaptive wireless sensor networks".In: ACM Transactions on Autonomous and Adaptive Systems (TAAS), v.4, n. 3, 2009,

Freire, V. A; Soares, L. C. Redes Convergentes. Rio de Janeiro: Alta Books, 2002, 346 p.

Frenkel, D.; Introduction to Monte Carlo Methods. John von Neumann Institute for Computing, NIC Series, v. 23. 2004.

Gani, A. et. al. "TCP/IP suite significant enhancement for 4G mobile multimedia internet networks.". In: Proceedings of the 8th WSEAS International Conference on Multimedia systems and signal processing, Hangzhou, China, 2008. p. 229-235.

Gao, X.; Wu, G.; Miki, T.; "End-to-end qos provisioning in mobile heterogeneous networks". In: IEEE Wireless Communications, v. 11, n. 3, 2004.

Geer, D. Building Converged Networks with IMS technology. In: Computer. Nov. 2005.

Geihs, K. Middleware Challenges Ahead. In: Computer, v. 34, i. 6, 2001. pp. 24-31.

Giri, N.; et.al.; "Multi agent system based service architectures for service level agreement in cellular networks". In: Proceedings of the 2nd Bangalore Annual Compute Conference on 2nd Bangalore Annual Compute Conference. Bangalore, India. 2009.

Gozdecki, J., Jajszczyk, A., Stankiewicz, R. "Quality of Service Terminology in IP Networks". In. IEEE Communication Magazine, v. 42, n. 3. 2003. p.153-159.

Greenwood, D.,et.al, The IEEE FIPA approach to integrating software agents and web services". In: Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems, Honolulu, Estados Unidos, 2007.

Griffin, D.; et.al. "Interdomain routing through qos-class planes". In: IEEE Communications Magazine, v. 45, n 2, 2007. p. 88-95.

Grinstead, C.M.; Snell, J.L. Introduction to Probability, 2ed., American Mathematical Society, 2006.

Hadim, S.; Mohamed, Nader. "Middleware: middleware challenges and approaches for wireless sensor networks". In: IEEE Distributed Systems Online. V. 7, N. 3. 2006.

Hafajee, H.; Chan, H.A.; "Low-cost qos-enabled wireless network with interworked wlan and wimax". 2005. Acessado em: Nov/2009. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/versions;jsessionid=E48A6B0713A355769A80F60AEBEF00F3?doi=10.1.1.84.455,

Hagen, L; Breugst, M; Magedanz, T. "Impacts of Mobile Agent Technology on mobile communication system evolution". In: IEEE Personal Communications. 1998.

Halabi, S.; McPherson, D.; Internet Routing Architectures, 2ed. Cisco Press, 2000. 498pp.

Han, M.; et.al.; "Evaluation of VoIP Quality over WiBro". In: Lecture Notes in Computer Science - Passive and Active Network Measurement. V. 4979, 2008. p. 51-60.

Hemminger, S.; "Network Emulation with NETEM". In: Linux Conf Au. 2005. Disponível em: http://www.citeulike.org/group/250/article/355636. Acessado em: Set/2009.

Hillebrand, J. et. al. Quality of Service signaling for Next-Generation IP-Based Mobile Networks. In: IEEE Communications Magazine, jun. 2004. pp. 72-79.

Horlait, E.; Rouhana,N. Differentiated Services and Integrated Services use of MPLS. In: Computers and Communications, 2000. Proceedings. ISCC 2000. Fifth IEEE Symposium on. 2000. pag. 194-199.

Houaiss, A. Dicionário Houaiss da Lingua Portuguesa, 2009.. Disponível em http://houaiss.uol.com.br/. Acessado em: Jan/2010.

Houéto,F.; Pierre, S.; "Quality of Service and Performance Issues in Multiservice Networks Subject to Voice and Video Traffics". In: Computer Communications, vol 28, 2005. pp. 393-404.

ITU-T, International Telecommunication Union Y.2001 - General Overview of NGN, 2004a.

ITU-T, International Telecommunication Union Y.2011 - General Principles and General Reference Model for Next Generation Networks, 2004b.

Hubert, B.; et.al. “Linux Advanced Routing & traffic control howto”. 2004. Disponível em: http://lartc.org/. Acessado em: Ago/2009.

Huhns M.N.; Stephens, L.M.. Multiagent Systems and societies of agents. In: WEISS, G. Multiagent Systems: a modern approach to distributed artificial intelligence. Massachutsetts Institute of Technology, 1999. p 79-120.

Issarny, V.; Caporuscio, M.; Georgantas, N.; “A Perspective on the Future of Middleware-based Software Engineering”. In: International Conference on Software Engineering-
Future of Software Engineering, 2007, p. 244-258.

ITU-T M.3060/Y2401 – Principles for the Management of Next Generation Networks. 2006.

Jamalipour, A.; Lorenz, P.; End-to-end QoS support for IP and multimedia traffic in heterogeneous mobile networks. In: Computer Communications, n. 29, 2006. P. 671-682.

Jennings, R.N.; Wooldridge, M.; “Applying Agent Technology”. In: Applied Artificial Inteligence, v.9, n.4, 1995, p. 357-369.

Jezic, G.; Kusek, M.; Sinkovic.. Teamwork Coordination in Large-Scale Mobile Agent Networks. In: Kes 2006, Part I, LNAI 4251, pp.236 – 243. 2006.

Jia et.al. “Next Generation Networks Architecture and Layered End-to-End QoS Control”. In: In: Lecture Notes in Computer Science, v. 3758, 2005.

Jonker, C.M.; Robu, V.; Treur, J.; “An agent architecture for multi-attribute negotiation using incomplete preference information”, In: Autonomous Agents and Multi-Agent Systems, v.15, n. 2 2007. p. 221-252.

Karam, D. “Modelo de Negocio para sistemas heterogenos moveis convergentes’”. Escola Politécnica da Universidade de São Paulo (tese). 2006. 80p.

Karlich, et.al., 2004. “A Self-Adaptive Service Provisioning framework for 3G+/4G Mobile Applications”. In: IEEE Wireless Communications, v. 11, n. 5, 2004. pp. 48-56.

Kim, B.; Sebuktekin, I.; “An integrated IP QoS architecture - performance”. In: Proceedings of MILCOM 2002. v.2,, 2002 p. 1189-1193.

Kim, C.C; et. al. “End to End QoS Monitoring Tool Development and Performance Analysis for NGN”. In: Lecture Notes in Computer Science, v. 4238, 2006

Kim, M; Won, Y. J.; Hong, J.W. “Characteristic analysis of internet traffic from the perspective of flows”. In. Computer Comunications. v. 29, n. 10, 2006, p. 1639-1652.

Kim, H. et.at. “Internet Traffic Classification Demystified: myths, caveats and best practices”. In: Proceedings of the 2008 ACM CoNEXT: International Conference On Emerging Networking Experiments And Technologies. Madrid, Espanha, 2008.

Knightson, K; , Morita, N; Towel, T. “NGN Architecture: Generic Principles, Functional Architecture, and Implementation”. In: IEEE Communications Magazine, v. 43, n10. 2005. pp. 49-56.

Kone, M.T.; Nakajima, T.; “An Architecture of a QoS-based Mobile Agent System” In: Proceedings of Fifth International Conference on Real-Time Computing Systems and Applications, 1998.

Koukoulidis, V.; Shah, M. The IP multimedia domain: service architecture for the delivery of voice, data and next generation multimedia applications. In: Multimedia Tools and Appl. n. 28, Springer Science + Business Media, Inc., 2006. p. 203-220.

Kumar, N.; Saraph, G. “” In: International conference on Networking and Services, 2006. ICNS '06. Bombay, India. 2006.

Kurant, M.; Thiran, P.; “Layered Complex Networks”. In: Physical Review Letters, v. 96, n. 13, 2006.

Laboratory of Open Systems (LSA). Discussions of research group. Department of Digital Systems and Computing Engineering. Escola Politécnica da Universidade de São Paulo. 2006.

Laurel, B. Interface Agents: Metaphors with Character. In: BRADSHAW, J. M Software Agents. MIT Press, 1997. p. 67-77.

Li, X.; et.al.; “Mix-bandwidth data path design for 5G real wireless world” In: Proceedings of the 12th WSEAS international conference on Communications, Herakilion, Grecia, 2008, p. 316-320.

Lin, N; Qi, H.; “A QoS Model of Next Generation Network based on MPLS”. In: International Conference on Network and Parallel Computing Workshops, 2007. NPC Workshops, 2007. P. 915-919.

Lynch, C.; Pesch, D.; “A Middleware Architecture Supporting Native Mobile Agents for Wireless Sensor Networks” In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering - Mobile Wireless Middleware, Operating Systems, and Applications – Workshops Mobilware 2009 Workshops, Berlim, Alemanha, 2009, p.65-74.

Mader, A.; Staehle, D.; Gosswein, C.; "Performance of Internet Services over the UMTS Enhanced Uplink". In: The 2007 International Conference on Next

Generation Mobile Applications, Services and Technologies, n.12-14, 007, p. 298-303.

Magedanz, Th; Gouveia, F.C. IMS – the IP Multimedia System as NGN Service Delivery Platform. In: Elektrotechnik & Informationstechnik, 2006, v. 123. pp. 271-276.

Maia,R.F. Sistema Multi-agentes para acompanhamento e auxílio de avaliação de alunos em ambientes de ensino à distância. Dissertação (Mestrado), São Paulo, 167pp. 2004. Escola Politécnica da Universidade de São Paulo. São Paulo, 2004.

_____ et.al.; Issues of Quality of Service in Convergent Environments. WSEAS Transactions on Communications, Athens, v. 4, n. 11, p. 1298-1305, 2005

_____ et. al. Middleware Orientado a Objetos e Sistemas Multi-Agentes. Trabalho apresentado na disciplina PCS 5002, 2006.

Manvi, S.S.; Venkataram, P. Applications of agent technology in communications: a review. In: Computer Communications, n. 27, 2005 p. 1493-1508.

Marques, V. et al, “An Architecture Supporting End-to-End QoS with User Mobility for Systems Beyond 3rd Generation”, In Proc. of IST Mobile and Wireless Telecommunications Summit 2002, June 2002, Thessaloniki, Greece.

Martini, B.; et.al,; “Dynamic QoS control based on VPLS in service oriented transport networks” In: 10th Anniversary International Conference on Transparent Optical Networks, 2008. ICTON 2008, v. 1, 2008, p. 29-32.

Mařík, V.; Lažanský, J.; “Industrial applications of agent technologies”, In: Control Engineering Practice. V. 15, n. 11, Elsevier, 2007, p. 1364-1380.

Mellouk, A.; Zeadally, S.; Mueller,P.; “Foreword: Routing and QoS over heterogeneous networks”. In: Annals of Telecommunications, v.63, n.11-12, Springer Paris, 2008, p. 543-544.

Meloni, S.; et.al. “Scaling Breakdown in Flow Fluctuations on Complex Networks”. In: Physical Review Letters, v. 100, n. 20, 2008.

Mykoniati,E. et.al.; *Admission Control for Providing QoS in IP DiffServ Networks: the TEQUILA Approach*, IEEE Communications, special issue on QoS Advances: the European IST Premium Projects, vol. 41, no. 1, pp. 38-45, IEEE, 2003.

Narayan,S.; Graham,D.; Barbour, R.H.; “Generic factors influencing optimal LAN size for commonly used operating systems maximized for network performance”. In: International Journal of Computer Science and Network Security, v. 9, n. 6. 2009

Nwana, H. Software Agents: An Overview. Knowledge Engineering Review. Cambridge University Press. v.3, p.1- 40. 1996.

Nichols, K., Jacobson, V. and L. Zhang, "A Two-bit Differentiated Services Architecture for the Internet", RFC 2638, July 1999.

Odom, W.; Cavanaugh, M.J. Cisco QOS Exam Certification Guide (IP Telephony Self-Study), 2nd Edition, 2004, 768pp.

Oliveira, J. C. C; et. al. Simulações da rede de conexões da Internet Brasileira. Documento: CBPF-NT-016/04, Centro Brasileiro de Pesquisas Físicas, 2004.

Onnela, J.P.; et.al.; “Structure and tie strengths in mobile communication networks”. In: Proceedings of the National Academy of Sciences of the United States of America (PNAS), v.104. 2007. p. 7332-7336.

Oksman, V.; et.al.; "‘Podracing’: experimenting with mobile TV content consumption and delivery methods". In: Multimedia Systems, v. 14, n.2, 2008. p. 105-114.

Papavassiliou, S.; et. al. “Mobile agent-based approach for efficient network management and resource allocation: framework and applications”. In: IEEE Journal on Selected Areas in Communications. V. 20, N. 4, 2002. p. 858-872.

Park, J.; Barabási, A.L.; “Distribution of node characteristics in complex networks”. In: Proceedings of the National Academy of Sciences of the United States of America (PNAS), v.104 n. 46. 2007. p. 17916-17920.

Parunak. H.V.D. Go to ant: engineering principles from natural multi-agent systems. In: Anals of Operations Research 75, 1997, 69-101

PAXSON, V. “End to End Routing Behavior in the Internet”. In: Computer Communication Review; v. 36 n. 5, 2006, p.43-56.

Penna, M.C.; Wandresen, R.R.; “On-line control of service level aggrement”. In: Network Control and Engineering for QOS, Security and Mobility, III, Springer, 2005. p. 15-26.

Qiang N.; Romdhandi,L.; Turletti, T.; “A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN”, In: Journal of Wireless Communications and Mobile Computing, Wiley. 2004, v. 4, n. 5 p.547-566.

Quitteck,J. et.al.; “Requirements for IP Flow Information Export (IPFIX)” RFC 3917. 2004. 33 pp.

Rao, K.R; Bojkovic, Z.S.; Milavanovic, D. A. Introduction to Multimedia Communications: applications, middleware, networking. John Wiley & Sons, 2006. 733p.

Rejeb, S. B; et. al. Modelling end to end QoS management and real time agreement protocols for resource reservation for multimedia mobile radio network. In: Computer Communications. n. 30, 2007. pp 1953 – 1963

Rezende, S. O.; Prati, R.; Sistemas Inteligentes, fundamentos e aplicações, Editora Manole, 2003.

Roberts, J.W. Traffic theory and the Internet. In: IEEE Communications Magazine. January, 2001 p94-99.

Ross, K.W.; Kurose, J.F. Redes de Computadores e a Internet: uma nova abordagem. 3 ed. Addison Wesley Bra. 2007. 656pp.

Rubinstein, M; Duarte, O.C.; Pujolle, G.; Reducing the response time in network management by using multiple mobile agents, Proceedings of the 4th International Conference on Autonomous Agents, Agents'2000, June 2000, pp. 165–166.

Russel, S. T.; Norvig, P. Inteligência Artificial. 2ed. Editora Campus, 2004.

Saad, E.M.; El-Ghandour, O.M; Jehan, M.K.; Evaluation of QoS in UMTS backbone network using Differentiated Services. In: 25th National Radio Science Conference, 2008. Acessado em: 03, set. 2009.

Scerri, P.; Vincent, R.; Mailler, R. Comparing three approaches to large-scale coordination. In: Coordination of Large Scale Multiagent Systems. Springer, 2006, 53-71.

Schmidt, D. C. "Middleware for Real-Time and Embedded Systems". In: Communications of the ACM, June 2002/Vol. 45, No. 6.

Serra, A. P. G. "Método para identificação de parâmetros de qualidade de serviços aplicados a serviços móveis e interativos". Escola Politécnica da Universidade de São Paulo (tese). 2007. 123p.

Shannon, C. "A mathematical theory of communication". In: ACM SIGMOBILE Mobile Computing and Communications Review. V. 5, n. 1, 2001. P.3-55.

Sebuktekin, et.al.; "Aggregate RSVP implementation experience and performance analysis for applicability in tactical IP networks". In: Proceedings of IEEE Military Communications Conference, MILCOM, 2008, p. 1-7.

Simon, H. The Architecture of Complexity. In: Proceedings of the American Philosophical Society, v. 106, n. 6. 1962 pp. 467-482. Acessado em; 10, ago, 2009. Disponível em: http://links.jstor.org/sici?sici=0003-049X%2819621212%29106%3A6%3C467%3ATAOC%3E2.0.CO%3B2-

Sinha, R; Papadopoulos, C; Heidemann, J. "Internet packet size distributions: some observations. In: Technical Report ISI-TR-2007-643, USC/Information Sciences Institute, 2007. Acessado em 10/Dez/2009. DIsponível em: http://www.isi.edu/~johnh/PAPERS/Sinha07a.html

Sun. Sun VirtualBox user manual v.3.1.2. 2009. Disponível em: http://www.virtualbox.org.

Stal, M. Web Services: beyond component-based computing. In: Communications of the ACM, v. 45, n. 10, 2002.

Tanembaum, A.S.; Steen, M. Distributed Systems: principles and paradigms. New Jersey, Prentice Hall, 2002. 803pp.

Tang, J.; Jin, Z.; **"**Requirement Driven Service Agent Collaboration and QoS Based Negotiation". In: Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology - Volume 02, Washington, 2009. p. 585-588.

Tommasi, F.; Molendini, S.; Trico, A. "Experience-driven selective scan for 802.11 networks" In: International Conference on Software in Telecommunications and Computer Networks, 2006.

Toral, H. et.al. "Self-similarity, packet loss, jitter and packet size: em pirical relationships for VoIP". In: Procedings of IEEE 18th International Conference on Electronics, Communications and Computers, 2008. P. 11-16.

Trimintzios, et.al.; "A management and control architecture for providing IP differentiated services in MPLS-based networks." In: IEEE Communication Magazine, v. 39, n. 5, 2001, p. 80-88.

Tsigkas,O.; Pavlidou, F.; "Providing QoS support at the Distributed Wireless Mac Layer: a comprehensive study" In: IEEE Wireless Communications, v.15, n.1, 2008. p. 22-31.

Urushidani, S.; Matsukata, J. "Next-generation science information network for leading-edge applications". In: Proceedings of the 6th IAEA Technical Meeting on Control, Data Acquisition, and Remote Participation for Fusion Research, 2007. P. 498-503.

Vasconcelos, S.V. Provisionamento de Recursos e QoS em redes de núcleo IP para sistemas celulares de 3ª geração, Dissertação (Mestrado), Rio de Janeiro, 107pp. 2002. Acessado em 01, agosto de 2009. Dispoível em: http://www.pee.ufrj.br/teses/Resumo?=2002090301

Verdi, F.; et. al.; "The Virtual Topology Service: A Mechanism for QoS-Enabled Interdomain Routing". In: Lecture Notes in Computer Science: Autonomic Principles of IP Operations and Management, v. 4268, 2006, p. 205-217.

Verma, D. 1999 Supporting Service Level Agreements on IP Networks. Macmillan Technical Publishing.

Vishwanath, K. V.; Vahdat, A. "Realistic and Responsive Network Traffic Generation". In: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications. Pisa, Italia, 2006. P. 111-122.

VINOSKI, S. An Overview of Middleware. In: Lecture Notes in Computer Science. v. 3063, Berlim, Spring-Verlag, 2004. pp. 35-51

Wang, N. et. al. “Towards and Adaptive and Reflective Middleware Framework for QoS-enabled Corba Component Model Application”. 2000. Disponível em: http://www.cs.wustl.edu/~schmidt/papers/NASA/dsonline.html. Acessado em: marc. 2008.

Wang, Z. Internet QoS: Architecture and Mechanisms for Quality of Service. Bell Labs, Lucent Technology. Morgan Kaufmann Publishers. USA, 2001.

Wang, N. et.al. “Qos-enabled Middleware”. In: Middleware for Communications. John Wiley & Sons, 2002.

Wang, W.; et.al. “Traffic dynamics based on local routing protocol on a scale-free network”. In: Physical Review E, v. 73, n. 2, 2006.

Wang, H.; Lee C.; Ho, T.; “Combining subjective and objective QoS factors for personalized web service selection”. In: Expert Systems with Applications, v. 32, n. 2, 2007, p. 571-584.

Ward, et. al. Domain Management of IMS. In. Bell Labs Technical Journal. n. 10, v. 4, 2006. p. 233-254.

Watts, J.D. Six Degress: the science of a connected age. WW Norton & Company. 2003.

Weiss, G. Multiagent systems a modern approach to distributed artificial intelligence, MIT Press,1999, 619pp.

WONG, H.C.; SYCARA, K. Adding security and trust to multiagent systems. In Applied Artificial Intelligence. Taylor & Francis, 2000.pp 927-941.

Wooldridge, M.; Jennings, N. Intelligent Agents: Theory and Practice. In Knowledge Engineering Review, v. 10, n. 2, 1995.

Wooldridge, M. An Introduction to multi-agent systems. 1ed. John Wiley & Sons, 2002.

Xia, Y.; et.al.; “Scale-free user-network approach to telephony network traffic analysis”. In: Physical Review E, v. 72, n. 2, 2007.

Xu, F; Zhang, L; Zhou, Z. Interworking of Wimax and 3GPP Networks based on IMS. In: IEEE Communication Magazine. 2007 pp. 144-150.

Yannuzzi, M.; et.al. **“**On the challenges of establishing disjoint QoS IP/MPLS paths across multiple domains”. In: IEEE Communications Magazine, v. 44, n. 12, 2006. p. 60-66.

Zhani,M.F., Elbiaze, H., Kamoun, F.; Analysis of prediction perfornmance of training-based models using real network traffic, v. 37, n. 1, 2010, p.10-19.

Zhao, L. et.al. “Onset of traffic congestion in complex networks”. In: Physical Review. v. 71 n. 026125, 2005. p. 026125-1 – 026125-8.

Zseby, T.; et.al.; “IP Flow Information Export (IPFIX) Applicability”. RFC 5742. 2009.