UNIVERSIDADE ESTADUAL PAULISTA

"Júlio de Mesquita Filho"

Pós-Graduação em Ciência da Computação

Júnior César Rosante

Proposta de uma Ferramenta de Visualização e Realidade Virtual para o Monitoramento de Tráfego de Redes de Computadores

UNESP

2011

Júnior César Rosante

Proposta de uma Ferramenta de Visualização e Realidade Virtual para o Monitoramento de Tráfego de Redes de Computadores

Orientador: Prof. Dr. José Remo Ferreira Brega

Dissertação de Mestrado elaborada junto ao Programa de Pós-Graduação em Ciência da Computação – Área de Concentração Sistemas de Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

UNESP

2011

Júnior César Rosante

Proposta de uma Ferramenta de Visualização e Realidade Virtual para o Monitoramento de Tráfego de Redes de Computadores

Dissertação de Mestrado elaborada junto ao Programa de Pós-Graduação em Ciência da Computação – Área de Concentração Sistemas de Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

Prof. Dr. José Remo Ferreira Brega
Professor Adjunto Doutor
UNESP – Bauru
Orientador

Prof. Dr. Luis Carlos Trevelin
Professor Associado III
Universidade de Federal de São Carlos

Profª. Drª. Roberta Spolon
Professora Adjunto Doutora
UNESP – Bauru

Bauru, 01 de julho de 2011

Dedico este trabalho...
A Deus que me presenteou a alma,
A meus pais, Marin e Lene que me presentearam a vida,
A meu afilhado Lucas. Que eu consiga transmitir a Lucas
Olhos para enxergar a pureza da alma e garra para trilhar a verdade da vida!

AGRADECIMENTOS

Agradeço primeiramente a Deus pela vida, pela saúde e pela paz da alma, graças indispensáveis.

A minha família Lene, Marin, Juliana e Bela pelo total e incondicional apoio.

A minha namorada Paulinha pelo apoio e compreensão.

A meu orientador Prof. Dr. José Remo Ferreira Brega - Prof. Remo - por ter acreditado em meu potencial e pela paciência e dedicação à orientação deste trabalho.

Ao Prof. Dr. Aparecido Nilceu Marana que me recebeu de portas abertas para cursar o programa de mestrado e sempre me tratou com muito zelo e atenção.

Ao Prof. Dr. Aledir Silveira Pereira pela carta de recomendação e total apoio.

Ao Prof. Dr. João Paulo Papa pelo apoio, incentivo, e idéias e ao projeto.

Ao Prof. Dr. Henrique Luiz Monteiro - na ocasião diretor da FC - que foi favorável à minha liberação do STI para que eu pudesse assistir às aulas do programa, incentivando minha iniciativa em cursá-lo.

À Profa. Roberta, Prof. Marar, Prof. Ivan e demais docentes do programa, sempre dispostos a dar atenção e apoio.

Aos colegas de equipe do STI Lazanha, Andrezão, Hélio, Zóio, Mitsuo, Renatão, Marga que entenderam meus momentos de ausência do STI e meus momentos de "presença zumbi" pelas madrugadas mal-dormidas!

Aos colegas mestrandos Diegão, Anthony, Paty, Léo, Clayton pelos bons momentos de correria, angústia e glórias, sempre regados por um bom tereré; e graduandos Parra, Bruno, Flávio e Yuri pelo apoio ao desenvolvimento inicial do código.

Aos seguranças da Unesp que nunca reclamaram em ter de abrir e fechar o portão do STI por tantas madrugadas!

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SIGLAS

1D	Uma Dimensão
2D	Duas Dimensões
3D	Três Dimensões
DNS	Domain Name System
DoS	Denial of service
HMD	Head Mounted Displays
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection Systems
IMAPS	Internet Message Access Protocol Secure
IPv6	Internet Protocol Versão 6
LSTR	Laboratório de Sistemas de Tempo Real
NETBIOS	Network Basic Input/Output System
POP	Post Office Protocol
POPS	Post Office Protocol Secure
RV	Realidade Virtual
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VI	Visualização de Informação

RESUMO

O crescimento das redes de computadores e telecomunicações assim como do número de dispositivos conectados a essas provoca um aumento expressivo da quantidade de tráfego de dados gerando maior dificuldade no seu gerenciamento e demandas crescentes da necessidade de prover segurança dos dados e continuidade dos serviços de rede prestados pelas instituições. Existem ferramentas para auxiliar no trabalho de monitoramento de redes como o *Tcpdump* e o *Snort.* Este auxilia no trabalho de detecção e bloqueio de tráfegos maliciosos como *portscans* e ataques de *denial of services (DoS)* através da análise de tráfego por verificação de assinaturas e padrões. Ainda que sejam de suma importância, ferramentas deste tipo descartam a capacidade cognitiva do ser humano de aprendizado e reconhecimento de padrões. Para contornar essa carência e aproveitar a capacidade de cognição visual humana, este trabalho propõe o uso de conceitos de Realidade Virtual aliados a Visualização de Informação na implementação de uma ferramenta de visualização de informações. Esta deve apresentar os dados brutos do tráfego da rede através de novas perspectivas e metáforas visuais utilizando as técnicas de Realidade Virtual com suas características de imersão, interação e envolvimento em um espaço sintético tridimensional. A representação do tráfego de rede através de metáforas visuais pela ferramenta desperta o senso cognitivo do administrador de redes possibilitando a identificação de tráfego anômalo e de comportamentos estranhos. A ferramenta deve fornecer possibilidades de configurações para exibir diferentes aspectos do tráfego servindo tanto para auxílio administrativo de comportamentos dos usuários quanto para análise e detecção de acessos maliciosos.

PALAVRAS-CHAVE: Redes de computadores, Segurança, Visualização, Realidade Virtual.

ABSTRACT

The growth of computer networks and telecommunications as well as the number of devices connected to these causes a significant increase in the amount of data traffic generating greater difficulty in its management and growing demands on the need to provide data security and continuity of network services provided institutions. There are tools to assist in the work of monitoring networks such as Tcpdump and Snort. This helps in detecting and blocking malicious traffic and attacks such as portscans and denial of service (DoS) attacks by analyzing traffic for verification of signatures and patterns. Though they are very important, tool of this type discard the cognitive capacity of human learning and pattern recognition. To address this need and the ability to take advantage of human visual cognition, this work proposes the use of concepts of Virtual Reality to Information Visualization in the implementation of an information visualization tool. This should provide the raw data of network traffic through new perspectives and visual metaphors using Virtual Reality techniques to their characteristics of immersion, interaction and involvement in a synthetic three-dimensional space. The representation of network traffic through visual metaphors for the cognitive tool awakens the sense of enabling network administrators to identify anomalous traffic and strange behavior. The tool should give you plenty of settings to display different aspects of traffic serving both to assist administrators and users' behavior for analysis and detection of malicious access.

KEYWORDS: Networks, Security, Visualization, Virtual Reality.

1. INTRODUÇÃO

1.1. Contextualização

O crescimento das redes de computadores e telecomunicações, assim como do número de dispositivos conectados a essas provoca um aumento expressivo da quantidade de tráfego de dados. A disponibilização de serviços *on-line* como *webmails*, bancos de dados, servidores de páginas *web*, telefonia por voz sobre IP, vídeo conferência, *internet banking*, dentre outros, são cada vez mais comuns em corporações e universidades.

Paralelamente ao aumento dos serviços de rede e, consequentemente do tráfego de rede gerado, aumenta a necessidade de manter os serviços em funcionamento e prover segurança dos dados e sistemas envolvidos em suas comunicações, uma vez que informações confidenciais são enviadas constantemente entre os sistemas.

Dentre essas informações, trafegam senhas de contas de *e-mail*, senhas e dados de contas bancárias, dados de transações comerciais, números de cartão de crédito e de documentos de pessoas físicas e jurídicas.

Neste cenário, um administrador de redes tem de estar sempre atento às medidas de segurança dos sistemas de rede e dos servidores de aplicações sob seu domínio; deve monitorar os acessos aos dados que entram e saem do perímetro de sua rede a fim de manter os serviços em funcionamento; deve prezar pela segurança dos dados e coibir ações maliciosas como mau uso dos canais de comunicação, tentativas de invasão da rede e acessos indevidos às informações dos sistemas e dos usuários corporativos.

1.2. Motivação

Existem soluções para auxiliar no trabalho de monitoramento de redes e, dentre as ferramentas de segurança, há sistemas de captura e de classificação de tráfego que auxiliam no trabalho de detecção e bloqueio de tráfegos maliciosos como *portscans* e ataques de *denial of services (DoS).* Tais sistemas fazem sua análise através da verificação de assinaturas e padrões previamente conhecidos, ou seja, uma ferramenta deste tipo deve receber parâmetros de ataques conhecidos e regras pré-estabelecidas para, através de comparações, identificar possíveis tráfegos maliciosos.

A importância deste tipo de sistema é indiscutível, contudo, uma grande desvantagem deste tipo de ferramenta de análise de tráfego é o não provimento de meios para o reconhecimento e detecção de novos padrões de comportamento, descartando, assim, a capacidade cognitiva do ser humano de aprendizado e reconhecimento de padrões.

Tal capacidade, no entanto, pode ser aproveitada utilizando-se ferramentas de visualização de informações, que apresentam os dados brutos através de novas perspectivas e metáforas visuais, possibilitando ao analista de rede ter novas percepções sobre os dados e assimilar informações mais facilmente, podendo, inclusive, detectar anomalias e, desta forma, gerar conhecimento.

Portanto, metáforas de visualização, aliadas às técnicas de Realidade Virtual (RV) com suas características de imersão, interação e envolvimento, em um espaço sintético tridimensional, oferecem novas possibilidades de percepções e entendimento acerca dos dados e seus relacionamentos, o que apresenta uma forma inovadora de interação com a informação, abrindo um leque de possibilidades a serem exploradas pelo administrador humano.

1.3. Objetivos

Este trabalho sugere o estudo das técnicas envolvidas propondo o desenvolvimento do protótipo de uma ferramenta de monitoramento de tráfego de

redes que emprega técnicas de RV combinadas com as de Visualização de Informação (VI) sob um aspecto multidisciplinar de apoio aos conceitos de segurança e gerência de rede.

Pretende-se que o protótipo promova ao administrador humano uma ampliação de seu entendimento acerca da estrutura da rede e do tráfego desta, valorizando sua capacidade cognitiva através do uso de metáforas visuais em um ambiente tridimensional.

Alem disso, as técnicas implementadas devem servir de base para que novas funcionalidades possam ser incorporadas ao protótipo desenvolvido neste trabalho.

1.4. Estrutura da Dissertação

Além deste capítulo introdutório, em que foram apresentados os objetivos e motivações para este trabalho, a dissertação divide-se em outros cinco capítulos, descritos a seguir:

- **Capítulo 2**: Introduz a RV apresentando sistemas e aplicações, aglomerados gráficos e conceitos de estereoscopia, os quais são utilizados no projeto da ferramenta proposta.

- **Capítulo 3**: Apresenta conceitos de VI e aplicações desta área, destacando seus aspectos favoráveis para a cognição característica do sistema visual humano.

- **Capítulo 4**: Discute a necessidade do monitoramento do tráfego de rede pelo administrador humano e algumas dificuldades inerentes a esse processo. Apresenta trabalhos relacionados com visualização de tráfego destacando vantagens em se utilizar uma ferramenta que combine RV com VI.

- **Capítulo 5**: Apresenta o protótipo desenvolvido, bem como o ambiente

e as tecnologias utilizadas em seu desenvolvimento. As funcionalidades nele implementadas são testadas em um ambiente real através da avaliação por profissionais especialistas da área de redes. O resultado desta avaliação é compilado no final do capítulo.

- **Capítulo 6**: Apresenta as contribuições do projeto e sugestões para trabalhos futuros.

Partes do código desenvolvido com incorporação da Biblioteca Glass são apresentadas no Anexo A.

2. REALIDADE VIRTUAL

Este Capítulo define a Realidade Virtual (RV) apresentando os conceitos principais que devem ser obedecidos ao se desenvolver uma aplicação que se utilize dela. São apresentados alguns tipos de sistemas de RV e suas aplicações.

O Capítulo traz também discussões sobre aglomerados gráficos e estereoscopia os quais fazem parte do conjunto de conceitos aplicados à estrutura da ferramenta proposta.

2.1. Definição

Para KIRNER; SISCOUTO, 2008, a RV é uma interface avançada do usuário para acessar aplicações executadas no computador, propiciando a visualização, movimentação e interação do usuário, em tempo real, em ambientes tridimensionais gerados por computador.

Para Hancock (2005), a RV, de maneira simplificada, é a forma mais avançada de interface do usuário com o computador, caracterizando-se pela coexistência integrada de três idéias básicas: imersão, interação e envolvimento.

O computador, neste contexto, se torna elemento de transporte do usuário que se encontra em um cenário real para o cenário virtual, podendo ou não fazer uso elementos de hardware específicos como óculos estereoscópicos e luvas para prover a interação com o “novo mundo” (Figura 2.1).

Este transporte do usuário ao “mundo virtual” pode ocorrer de forma parcial como na Figura 2.1 ou total em que este está fisicamente “dentro” do novo mundo, Figura 2.2.

Figura 2.1 Utilização de óculos e luvas na interação com cenário virtual (STRICKLAND, 2007).

Figura 2.2 Exemplo de usuário “dentro” do mundo virtual (CUSIN, 2005).

Uma das principais características da RV é que seu ambiente deve fornecer interação, sendo que a mais simples delas é a navegação por este. Esta ocorre quando o usuário se movimenta no espaço tridimensional, através de algum dispositivo, como *mouse* 3D (Figura 2.3) ou gestos detectados por algum tipo de dispositivo de captura, gerando como resposta a visualização de novos pontos de vista do cenário. O ambiente pode conter elementos e objetos que possam ser manipulados pelos usuários, assim como visualizados de diversos pontos de vista. Alguns destes objetos podem ser animados e possuírem comportamentos autônomos ou disparados por eventos (TORI; KIRNER, 2006).

Figura 2.3 Exemplos de Mouse 3D (ABS-TECH, 2009).

Outros tipos de interação com o ambiente tridimensional como mover, segurar ou girar objetos são desejados pois aproximam o usuário do cenário real. É importante que o usuário tenha a sensação de estar atuando no ambiente virtual. Quanto mais natural forem os tipos de alterações causadas pelos comandos do usuário, maior facilidade este terá em interagir com a ferramenta virtual e maior a

possibilidade de sucesso na implementação de uma ferramenta de RV. Aplicações de RV que exijam maiores habilidades específicas por parte do usuário tendem a dificultar o transporte deste ao ambiente virtual causando desconforto e dificuldades de interação, exigindo, muitas vezes, treinamento adequado. Tais problemas acabam por inibir a popularização da RV como nova forma de interface (TORI; KIRNER, 2006).

Há diversas maneiras de se obter essa interação com o cenário virtual, seja através de dispositivos não convencionais, como capacetes de visualização *HMD - Head Mounted Displays* (Figura 2.4), óculos 3D (Figura 2.5), luvas ou *Datagloves* (Figura 2.6), o próprio corpo através de gestos e comando de voz ou através de dispositivos convencionais, como mouse, teclado e monitor de vídeo.

Figura 2.4 Capacete *HMD*
(HASEYAMA, 2008)

Para que esta sensação de interação se aproxime do mundo real, devem-se obter as atualizações em tempo-real. Ao ser humano, para se obter tal sensação, deve-se assegurar que os atrasos aos comandos não ultrapassem 100 milisegundos, o que impõe aos dispositivos de software e hardware envolvidos na aplicação o compromisso de funcionar com taxas mínimas de 10 quadros por segundo na renderização das imagens, sendo desejados 20 quadros por segundo para suportar cenas animadas (TORI; KIRNER, 2006).

Figura 2.5 Óculos 3D
(HASEYAMA, 2008)

Desta forma, faz-se necessário ajustar os equipamentos de hardware e modelagem de software envolvidos na aplicação a fim de se obter o desempenho mínimo da interface.

Figura 2.6. Datagloves (ABS-TECH, 2009).

A modelagem de ambientes virtuais faz uso de linguagens específicas e de bibliotecas gráficas como *OpenGL* (OPENGL, 2011), *Java 3D* (JAVA3D, 2011) e *toolkits* sob forma de bibliotecas *C/C++* (CPLUSPLUS, 2011). Seu desenvolvimento pode envolver etapas como modelagem 3D, manipulação de texturas, som e animações (TORI; KIRNER, 2006).

Embora a RV utilize múltiplas mídias, ela não se confunde com aplicações multimídia. A Tabela 2.1 compara seis características principais que diferenciam sistemas de multimídia – priorizam qualidade das imagens e capacidades de transmissão - de sistemas de RV, os quais priorizam as características que promovem interação, imersão e envolvimento do usuário.

Tabela 2.1 – Comparativo entre sistemas multimídia e sistemas de RV.

	Multimídia	RV
Imagens	Capturadas ou pré-processadas	Calculadas em tempo-real
Prioriza	Qualidade das imagens	Interação com o usuário
Exige	Alta capacidade de transmissão	Alta capacidade de processamento
Utiliza	Técnicas de compressão de dados	Técnicas e recursos de renderização
Espaço	2D	3D
Dispositivos necessários	Convencionais	Especiais

2.2. Tipos de sistemas de RV e aplicações

Sistemas de RV podem ser diferenciados de acordo com os níveis de imersão e interatividade proporcionados ao usuário, sendo que esses podem ser determinados pelos tipos de dispositivos de entrada e saída de dados do sistema, além da velocidade e potência do computador.

Pimentel (1995) classifica em cinco os tipos de sistemas de RV:

- **RV de Simulação**: são os primórdios da RV, originada com os simuladores de vôo desenvolvidos pelos militares americanos após a Segunda Guerra Mundial (JACOBSON, 1994) em que o interior de um carro, avião ou jato é imitado e o usuário é colocado dentro de uma cabine de controles. Nesta, telas de vídeo e monitores apresentam um ambiente virtual que reage à comandos do usuário. Em alguns sistemas as cabines são montadas sobre plataformas móveis, e os controles oferecem *feedback* tátil e auditivo.

- **RV de Projeção (Realidade Artificial):** foi criada na década de 70 por Myron Krueger. Na RV de Projeção o usuário está fora do ambiente virtual, entretanto, pode se comunicar com personagens ou objetos nele contidos (JACOBSON, 1994).

- **Realidade Aumentada:** caracteriza-se por informações geradas pelo computador sobrepostas ao mundo real. Para obtê-la, podem-se utilizar dispositivos visuais transparentes presos na cabeça do usuário, sendo que este pode ver dados, diagramas, animações e gráficos 3D sem deixar de enxergar o mundo real. Tais *displays* transparentes são chamados *heads-up-displays* (HUDs). O usuário pode, por exemplo, trabalhar em uma peça enquanto visualiza imagens sobrepostas com dados necessários a esta operação.

- **Tele-presença:** utiliza câmeras de vídeo e microfones remotos para envolver e projetar o usuário profundamente no ambiente virtual. Controle de robôs e exploração planetária são alguns exemplos de pesquisas em desenvolvimento. No entanto, existe um grande campo de pesquisa no uso de tele-presença em aplicações médicas. Médicos já utilizam câmeras de vídeo e cabos de fibra óptica em cirurgias para visualizar os corpos de seus pacientes. Através da RV eles podem, literalmente, “entrar” no paciente, indo direto ao ponto de interesse e/ou vistoriar a operação feita por outros.

- **RV de Mesa (*Desktop* VR):** é um subconjunto dos sistemas tradicionais de RV em que, ao invés de HDM, utilizam-se grandes monitores ou algum sistema de projeção para apresentação do ambiente virtual. Alguns sistemas permitem ao usuário ver imagens 3D no monitor com óculos obturadores, polarizadores ou filtros coloridos.

Há diversas aplicações em RV para as mais variadas áreas, como em Medicina (Figura 2.7 e Figura 2.8) para simulações de cirurgias laparoscópicas,

treinamentos com pacientes virtuais e tratamento de fobias.

Figura 2.7 Realidade Virtual na Medicina (CUSIN, 2005).

Existem sistemas que simulam situações de pânico e risco, tais como viagens aéreas, elevadores e medo de animais. Por exemplo, o *SPIDERWORLD* (Figura 2.8) é um sistema baseado em RV projetado para auxiliar pacientes em sua luta contra fobia de aranhas. A paciente usa um HMD que projeta uma aranha virtual. Através de um modelo sintético de aranha, o sistema rastreia a mão da paciente, permitindo que a mesma toque a criatura virtual (CARDOSO; LAMOUNIER JÚNIOR, 2009).

Figura 2.8 Sistema RV para fobia de aracnídeos (CARDOSO; LAMOUNIER JÚNIOR, 2009).

Destaca-se também o uso de RV na Educação, para modelagem de laboratórios de Física e Química, mostrando o comportamento dos materiais (Figura 2.9) e treinamentos (Figura 2.10).

Figura 2.9. Demonstração com o uso de Realidade Virtual (CUSIN, 2005).

Figura 2.10 Treinamento com o uso da Realidade Virtual (CUSIN, 2005).

Usa-se, ainda, RV para Visualização de Negócios (Figura 2.11) e Científica (Figura 2.12). Esta se preocupa em representar visualmente uma simulação tridimensional de algo físico real, por exemplo, nuvens fluindo através de uma cadeia de montanhas, dada certa condição do vento (CARMO, 2007 apud SPENCE, 2001).

Figura 2.11 Apresentação de negócios com o uso da Realidade Virtual (ABS-TECH, 2009).

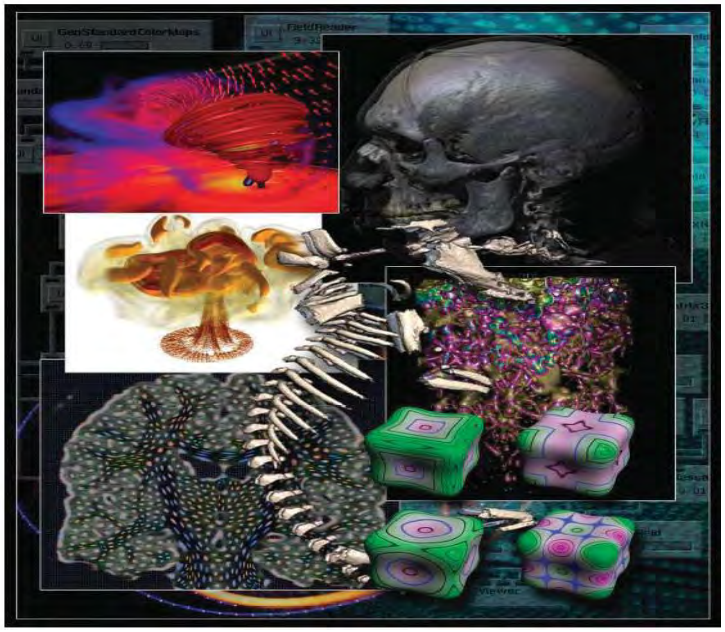


Figura 2.12 Visualização Científica (CARMO, 2007).

Na Indústria, várias são as áreas de aplicações de RV em seus vários ramos. Dentro destas diversas áreas pode-se destacar a área de petróleo (Figura 2.13) e aviação (Figura 2.14):

Figura 2.13. Realidade Virtual na exploração e busca de petróleo (CARDOSO; LAMOUNIER JÚNIOR, 2009).

Figura 2.14. Uso da Realidade na construção e simulação de aeronaves (CARDOSO; LAMOUNIER JÚNIOR, 2009).

2.3. Aglomerados gráficos

Aglomerados gráficos são um tipo especial de aglomerado com características específicas que os diferem dos tradicionais, como requisitos diferenciados de sincronismo das informações entre os nós (GUIMARAES, 2004).

Seu uso tem sido estudado por diversas áreas da Engenharia e, em Ciência da Computação, para as aplicações de RV.

Com o desenvolvimento acelerado de arquiteturas de redes e dos computadores pessoais, foram alcançados avanços significativos na área de processamento de alto desempenho. Os sistemas fortemente acoplados passaram a ser substituídos por aglomerados. Estes são caracterizados por uma coleção de nós interconectados por intermédio de uma rede local dando ao usuário a ilusão de um único sistema (KIWELEKAR, 2002). Segundo Buyya (1999), suas características como baixo custo, alta flexibilidade e escalabilidade expandiram rapidamente essa arquitetura.

Os aglomerados gráficos têm como objetivo oferecer uma visão múltipla do mesmo conjunto de dados e, para isto, cada nó processa apenas os dados referentes à sua parte de interesse, e então gera a imagem apenas daquela parte Enquanto os nós dos aglomerados tradicionais são geralmente idênticos, em RV é diferente, pois as aplicações requerem muitas tarefas variadas para serem realizadas, e em muitas aplicações, os dados são relativamente pequenos quando comparados com os dados dos aglomerados tradicionais. Por isso, os aglomerados gráficos não podem restringir-se a ter apenas nós idênticos, alguns deles podem ser específicos apenas para entradas, outros para saídas e outros para processamento. O aspecto de tempo real é outra importante diferença entre eles. Os aglomerados gráficos devem realizar as tarefas em tempo real, enquanto que os tradicionais, geralmente, realizam em forma de lotes (GUIMARAES, 2004). A interatividade e a geração de imagens em tempo real das aplicações gráficas requerem que as tarefas sejam executadas respeitando-se alguns limites de tempo. Por exemplo, as aplicações de multiprojeção precisam ser capazes de receber uma entrada, processar os dados, e produzir uma saída - para vários projetores ou monitores -,

mais de 15 vezes por segundo - preferencialmente 30 vezes, sem estereoscopia - enquanto que as aplicações que utilizam os aglomerados tradicionais não possuem este comprometimento. Isso é conhecido como taxa de atualização de quadros (CARDOSO, 2003). Se aplicação for estereoscópica, a taxa de atualização de quadros sobe para no mínimo 60 por segundo, sendo preferencialmente 120, pois para cada olho do usuário deve ser gerada uma imagem. Por isto, a sincronização das imagens e a comunicação estão entre os principais desafios a serem superados. A Figura 2.15 apresenta um esquema de aglomerado gráfico.

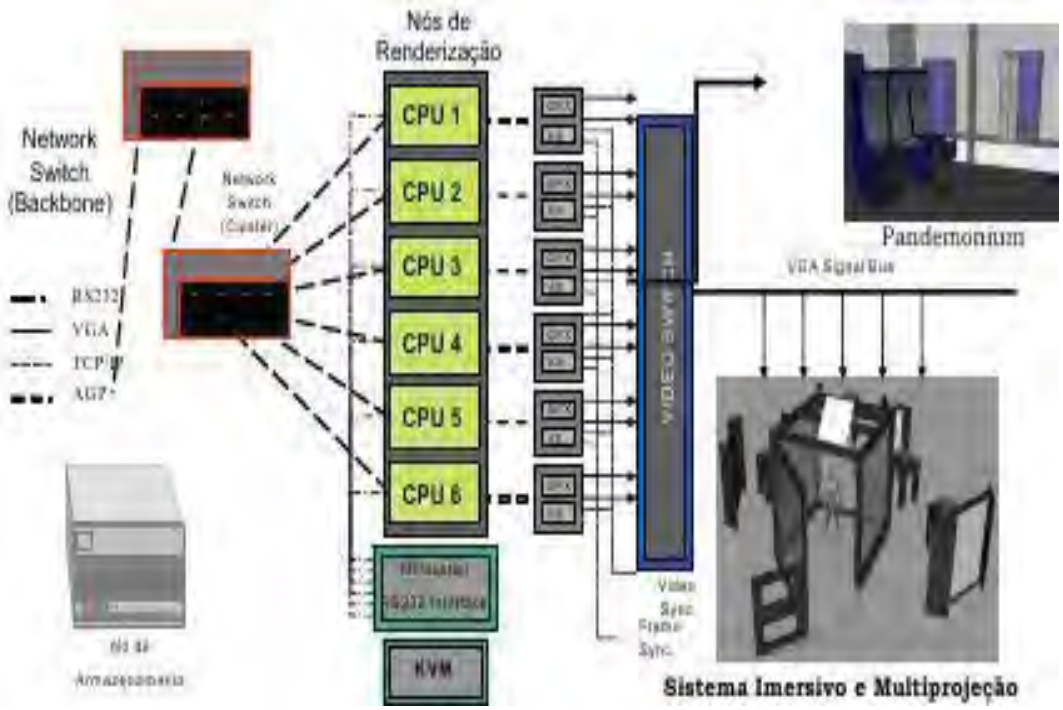


Figura 2.15 Aglomerado gráfico (GUIMARAES, 2004).

A comunicação é necessária para trocar informações entre os nós. E quando há comunicação, devem existir operações de sincronização, para fornecer controle de seqüência e controle de acesso. O controle de seqüência (também chamado de sincronização condicional ou sincronização de atividades) é utilizado para que se determine uma ordem na qual os processos (ou parte deles) devem ser executados. O controle de acesso é necessário quando há competição entre processos para a manipulação de algum recurso (deve-se garantir que acessos concorrentes a

recursos sejam controlados), para que se mantenha a consistência (GUIMARAES, 2004).

2.4. Estereoscopia

A visão monocular conta com elementos para uma percepção rudimentar de profundidade, valendo-se das leis da perspectiva, em que o tamanho aparente dos objetos diminui à medida que esses se afastam do observador, e da oclusão que ocorre quando um objeto encontra-se mais próximo e sob o mesmo eixo de perspectiva que outro (SEABRA, *et. al.*, 2005).

A estereoscopia é resultado da fusão e interpretação das imagens obtidas através dos pontos de vista de cada olho feitas pelo cérebro e que nos proporciona a percepção de profundidade dos objetos. (LIPTON, 1997).

Em média, os olhos dos seres humanos adultos são separados por 6,4 centímetros e assim, ao olhar para um objeto próximo, eles têm que se voltar para dentro para ver claramente e ainda permitir que a luz encontre a mesma parte sensível da retina. Este processo de virar os olhos para ver um objeto próximo é chamado de convergência. Crianças podem convergir seus olhos para enxergar objetos tão próximos quanto 7,5 cm, mas para adultos, a menor distância para uma visão clara é de 14 cm em média. Cada olho, então, vê uma figura ligeiramente diferente e esta diferença aumenta com a aproximação do objeto (BIOLOGIA, 2007).

Essa separação dos olhos causa a disparidade da retina que é a distância horizontal entre pontos correspondentes das imagens de um objeto obtidas por cada um dos olhos (RAPOSO, 2004). A Figura 2.16 representa de forma simplificada essa disparidade, onde a imagem mais a esquerda representa a visão do olho direito e a imagem mais a direita a visão do olho esquerdo.

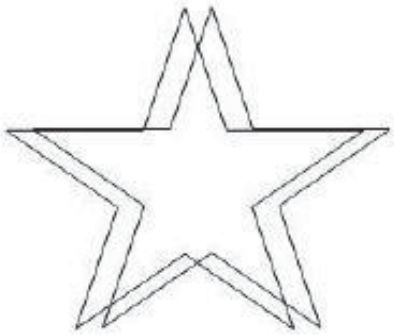
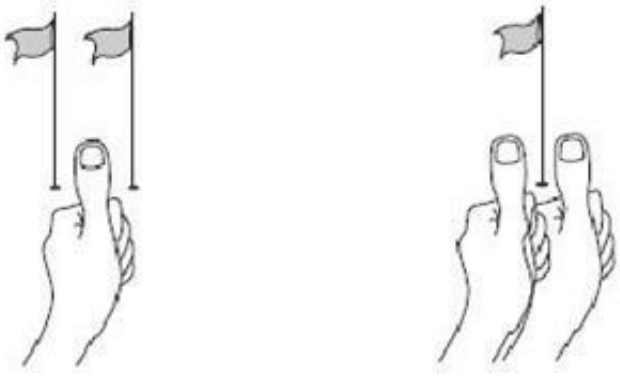


Figura 2.16 Disparidade da Retina (LIPTON, 1997).

A Figura 2.17-(a) exemplifica as diferentes percepções obtida por um observador com olhar fixo num objeto próximo (polegar), mas atento a um objeto distante (bandeira), enquanto a Figura 2.17-(b) exemplifica a percepção obtida por um observador com olhar fixo num objeto distante (bandeira), mas atento a um objeto próximo (polegar).



(a) (b)

Figura 2.17 Diferentes percepções do observador causadas pela variação da convergência (LIPTON, 1997).

A disparidade é zero para objetos onde os olhos convergem.

Outro conceito importante é a paralaxe: distância entre os pontos correspondentes das imagens do olho direito e do esquerdo na imagem projetada na tela. Segundo RAPOSO *et. al*. (2004), disparidade e paralaxe são duas entidades similares, com a diferença que paralaxe é medida na tela do computador e disparidade, na retina. É a paralaxe que produz a disparidade, que por sua vez, produz o estéreo.

Os três tipos básicos de paralaxe são (RAPOSO; *et. al*., 2004):

- **Paralaxe zero:** conhecido como ZPS (*Zero Paralax Setting*). Este tipo é ilustrado na Figura 2.18-(b). Um ponto com paralaxe zero se encontra no plano de projeção, tendo a mesma projeção para os dois olhos.

- **Paralaxe negativo:** significa que o cruzamento dos raios de projeção para cada olho encontra-se entre os olhos e a tela de projeção, como é visto na Figura 2.18-(a), dando a sensação de o objeto estar saindo da tela.

- **Paralaxe positivo:** indica que o ponto está atrás do plano de projeção, como ilustrado na Figura 2.18-(c), dando a sensação de que o objeto está atrás da tela de projeção.

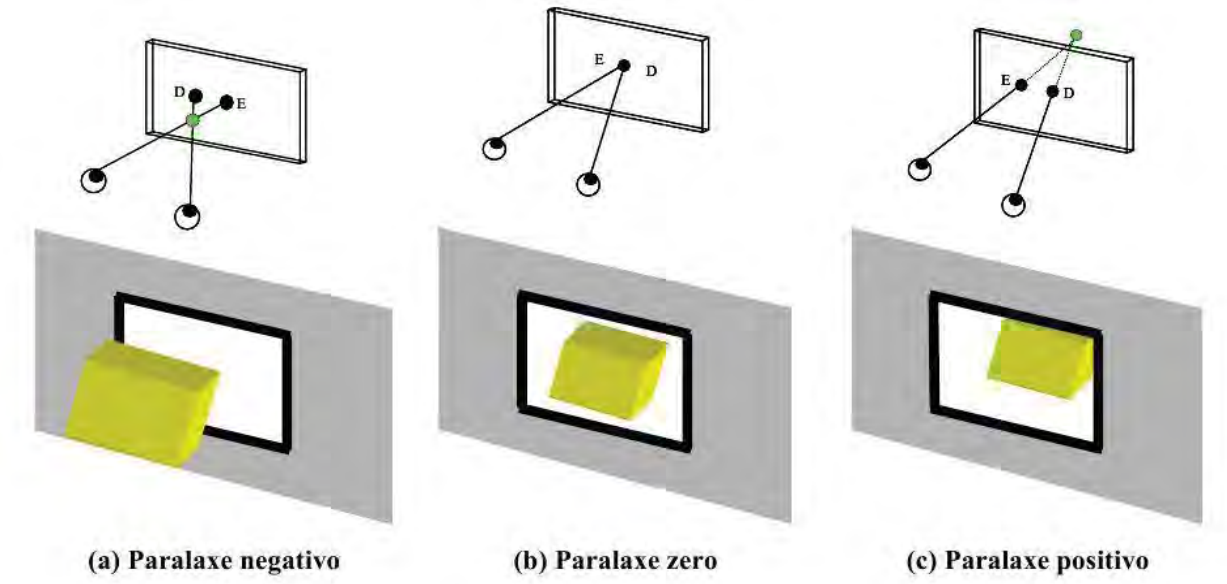


Figura 2.18 Tipos de paralaxe (RAPOSO; *et al.*, 2004).

Além do fenômeno da estereoscopia, há outros métodos que dão ao ser humano a percepção da profundidade que incluem aspectos tais como a nitidez das cores, a oclusão de objetos, e linhas de convergência. A Figura 2.19 exemplifica como o uso do efeito de iluminação transforma um círculo e um hexágono em uma esfera e um cubo.

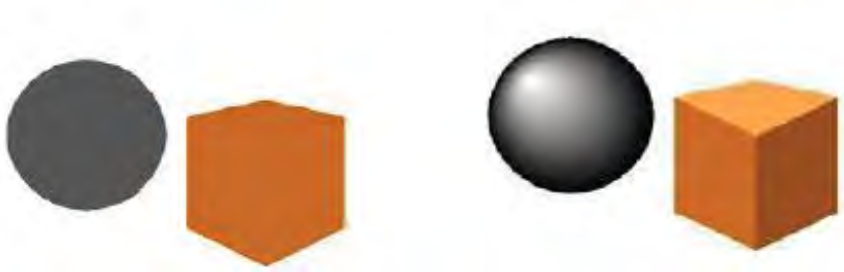


Figura 2.19 Efeito de iluminação (RAPOSO; *et al.*, 2004).

A Figura 2.20 exemplifica a sensação de profundidade através da oclusão que dá a sensação de ordem aos objetos.

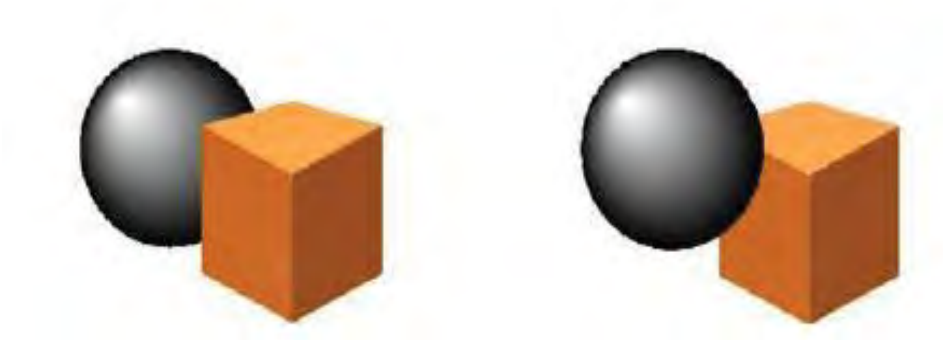


Figura 2.20 Efeito de oclusão (RAPOSO; *et. al*., 2004).

A Figura 2.21 aplica o efeito sombra dos objetos sobre um plano adicionado à cena. A esfera parece estar flutuando sobre o plano enquanto o cubo parece estar em contato com esse.

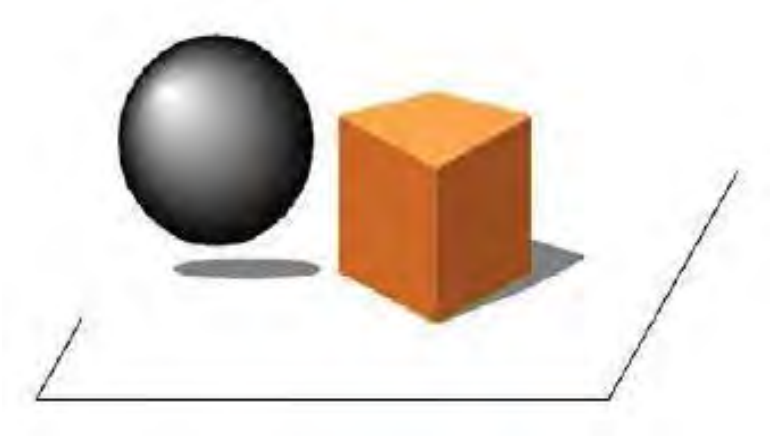


Figura 2.21 Efeito de sombra (RAPOSO; et al., 2004).

A figura 2.22 exemplifica o efeito perspectiva. Os dois paralelepípedos parecem estar afastados em profundidade, apesar de estarem desenhados sobre o mesmo plano.

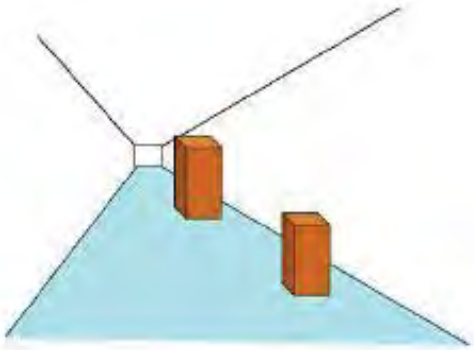


Figura 2.22 Efeito de perspectiva (RAPOSO; et al., 2004).

Em aplicações computacionais, geralmente as imagens são geradas a partir de uma única câmera virtual e visualizadas em monitor ou projeção em um plano.

De outro modo, procura-se, em aplicações estereoscópicas, simular a visão binocular humana gerando-se duas imagens a partir de câmeras virtuais separadas por uma determinada distância a fim de produzir a visão em 3D, Figura 2.23.

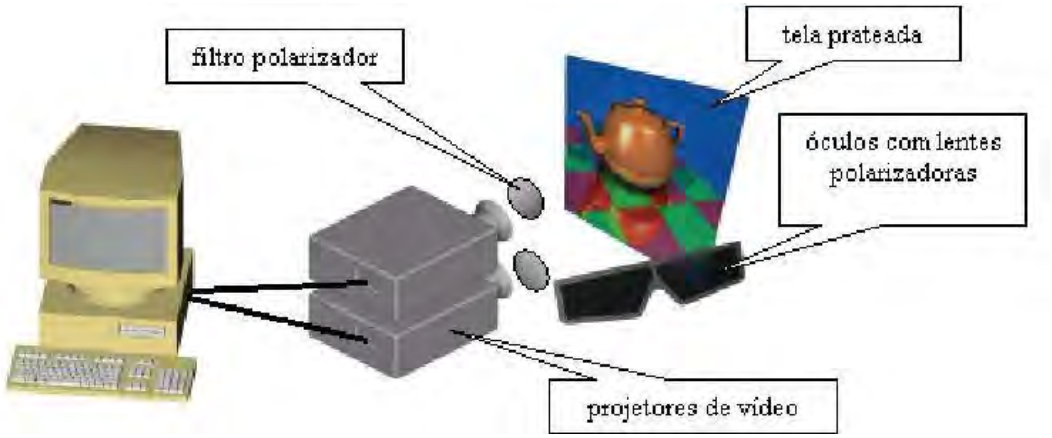


Figura 2.23 Esquema para projeção estereoscópica passiva (SEABRA; SANTOS, 2005).

Existem duas classificações de equipamentos para a estereoscopia – estéreo passivo e estéreo ativo. As duas utilizam óculos para separar as imagens (olho esquerdo e olho direito) (RAPOSO, 2004).

- **Passivo:** Nesse caso as duas imagens são exibidas juntas e os óculos servem de filtros, separando cada imagem em cada olho.

- **Ativo:** Nesse tipo de sistema os óculos – do tipo obturadores - são capazes de exibir em cada olho a sua correspondente imagem com a ajuda do sistema de exibição do estéreo.

2.5. Considerações finais

Foram apresentados neste capítulo, conceitos de RV explorados na implementação do protótipo da ferramenta de monitoramento, assim como aspectos biológicos da visão humana e a forma com que a computação gráfica e a RV procuram gerar ambientes virtuais o mais próximo possível da visão de mundo real. Tais aspectos devem ser considerados para que a ferramenta seja incorporada à estrutura de multi-projeção do LSTR – Laboratório de Sistemas de Tempo Real da Faculdade de Ciências - Unesp, a qual se utiliza de um aglomerado gráfico para projeção estereoscópica passiva.

3. VISUALIZAÇÃO DE INFORMAÇÃO

Este Capítulo apresenta o conceito de VI e traz algumas características que devem ser observadas no desenvolvimento de ferramentas deste tipo uma vez que se devem apresentar os dados do tráfego da rede através de metáforas visuais na ferramenta proposta.

São apresentados, também, alguns exemplos de softwares já desenvolvidos na área.

3.1. Definição

Visualização pode ser definida como o uso de ferramentas computacionais interativas para representação visual de dados abstratos para amplificar a cognição. Seu objetivo é auxiliar pessoas no entendimento e análise de dados. É uma área de pesquisa que envolve diversas outras, dentre elas, Visualização Científica, Computação Gráfica, *Data Mining*, *Design* da Informação, assim como Ciências Cognitivas, Teoria da Percepção e Psicologia. Cada uma dessas áreas depende do tipo de dados a serem visualizados e da experiência do usuário, como pode ser ilustrado na Figura 3.1 (KERREN; *et. al.*, 2007).

Kerren, *et.al*. (2007) afirmam que a interação intuitiva com um sistema cujo desenho baseie-se nas capacidades cognitivas humanas pode aumentar a produtividade e a eficiência do trabalho.

Tal característica é desejável, haja vista que a sobrecarga de informações atualmente é considerada como um dos grandes problemas da interação humano-computador. Tomar uma decisão correta, em qualquer área do conhecimento, com uma enorme quantidade de dados e pouco tempo, quase sempre é uma tarefa difícil de realizar. O computador pode, em poucos segundos, recuperar informações que um ser humano levaria anos. Contudo, muitas dessas informações podem ser

irrelevantes para o usuário ou perdem-se informações úteis por não se conhecer o relacionamento entre os dados (MEIGUINS *et al*., 2009).

Técnicas de VI são utilizadas cada vez mais para melhorar o processo de busca e tomada de decisão sobre essa grande quantidade de informações. A Visualização objetiva auxiliar a análise e compreensão dos dados de maneira rápida, interativa e intuitiva, utilizando a capacidade de cognição humana para extrair informações dos dados utilizando representações visuais dos mesmos (KERREN; *et. al*., 2007) e (SPENCE, 2007).

Figura 3.1. Perspectiva dos mais importantes componentes das disciplinas ligadas às áreas da visualização humana. Modificada de (KERREN; *et. al.*, 2007).

Segundo DO NASCIMENTO, 2005, o processo de visualização está relacionado com a transformação de algo abstrato em imagens (mentais ou reais) que possam ser visualizadas pelos seres humanos com o objetivo final de auxiliar no entendimento de determinado assunto, o qual, sem uma visualização exigiria maior esforço para ser compreendido.

Busca-se, assim, em uma ferramenta de VI, permitir a fácil manipulação e

entendimento dos dados e seus relacionamentos, o que depende do domínio do problema e do tipo de relacionamento entre os dados a serem visualizados.

Neste contexto, VI mostra-se uma área emergente de pesquisa que estuda formas de transformar dados abstratos em imagens reais ou mentalmente visíveis de forma a facilitar o seu entendimento e/ou ajudar na descoberta de novas informações contidas nos mesmos (DO NASCIMENTO, 2005).

A Figura 3.2 ilustra, de modo simplificado, um processo automatizado de VI, em que uma imagem é produzida a partir de dados de entrada.

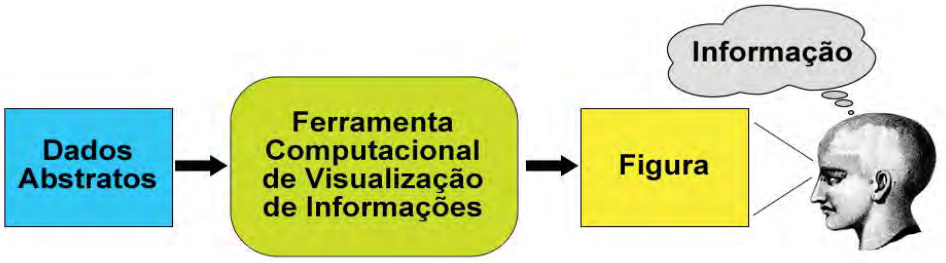


Figura 3.2. Processo simplificado de visualização de informações auxiliada por computador (DO NASCIMENTO, 2005).

Em VI, dá-se ênfase à capacidade visual humana devido a uma série de vantagens naturalmente apresentadas por esta, como a capacidade de reconhecimento de padrões. Esta característica é ilustrada através da dificuldade em se encontrar a palavra “estrela” na Figura 3.3. Porém, o ser humano encontra a figura da estrela com bastante facilidade na Figura 3.4. Caso fosse utilizada uma cor diferente na estrela, esta poderia ser mais facilmente reconhecida. Tais características do sistema visual humano nos permitem identificar e lidar com situações complexas do dia-a-dia que envolvem processamento visual.

quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado estrela quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado
quadrado quadrado quadrado quadrado quadrado quadrado quadrado quadrado

Figura 3.3 Identificação por texto

Visualizações podem, ainda, por si só, trazer benefícios uma vez que funcionam como uma extensão da memória humana num auxílio para o processo cognitivo.

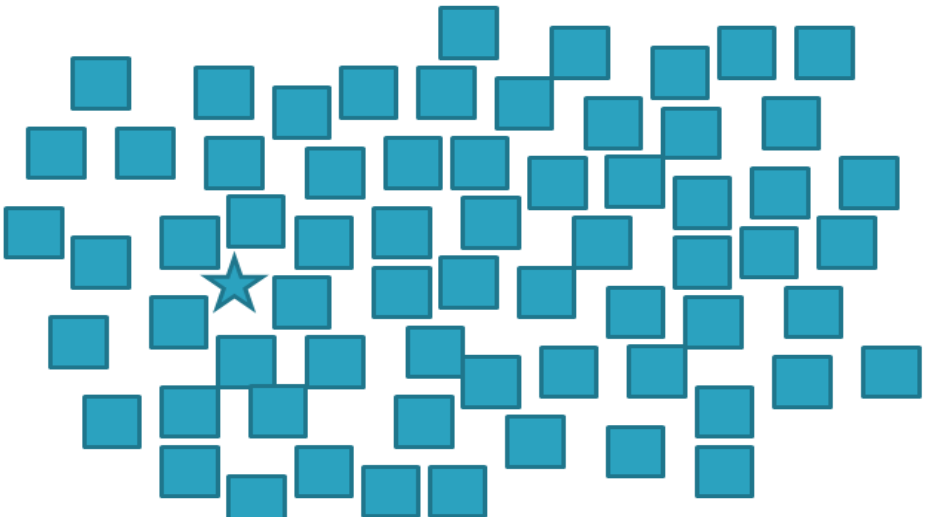


Figura 3.4 Identificação por imagem

Por exemplo, anotações em agenda ou em calendários para a lembrança de assuntos a serem discutidos ou de eventos que ocorreram ou irão ocorrer (DO NASCIMENTO, 2005).

Podem-se observar vantagens descritas acima através da aplicação a seguir. Através do *Tcpdump*, capturou-se o tráfego da rede por um período de trinta segundos, gerando-se um arquivo texto de 125456 linhas. A Figura 3.5 exemplifica parte deste arquivo.

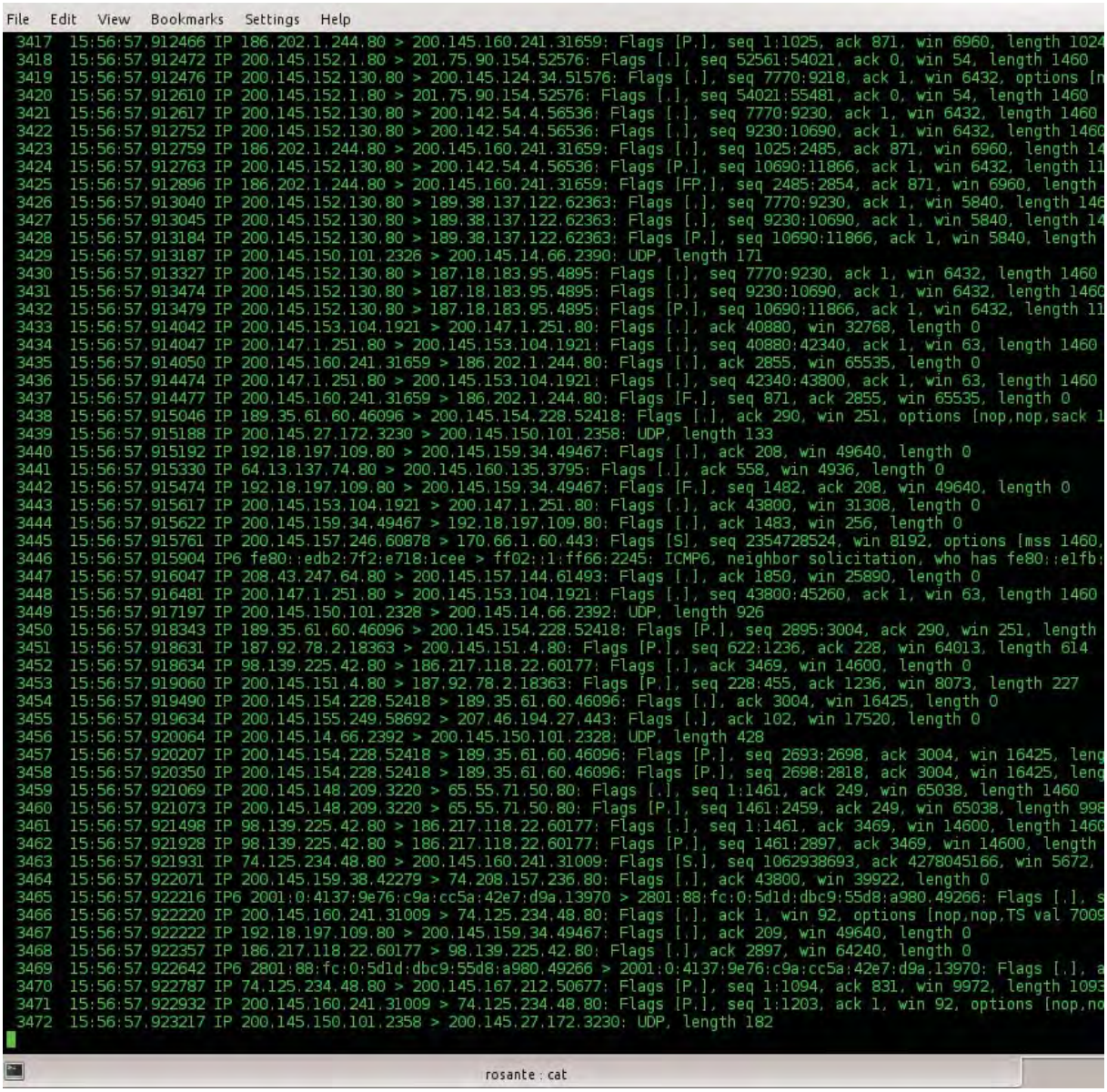


Figura 3.5 Parte do arquivo texto gerado pela captura do tráfego.

Uma questão interessante a se fazer acerca do tráfego capturado é “qual foi o serviço de rede mais utilizado?”. Seria muito penoso obter esta resposta analisando-se este arquivo puramente textual. Porém, analisando-se o *gráfico de pizza* da Figura 3.6, gerado a partir da distribuição de portas de destino, percebe-se imediatamente que o tráfego mais intenso foi o de HTTP.

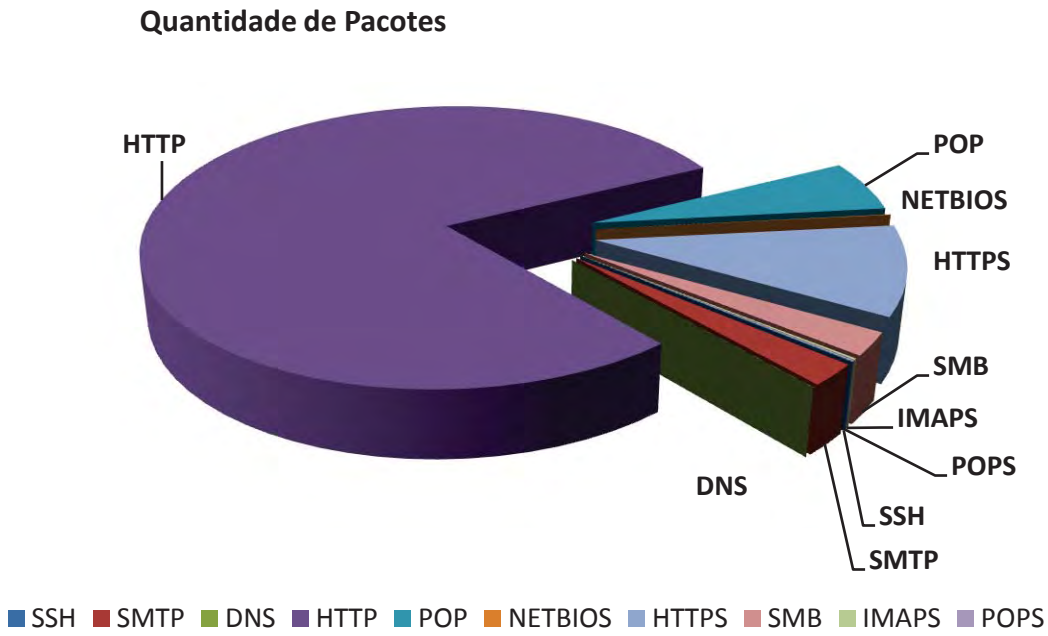


Figura 3.6 Gráfico de setores.

Evidencia-se, assim, que a constatação de padrões ou de características visuais presentes em imagens contribui de forma muito mais significativa para o processo de compreensão do que a simples observação dos dados em sua forma bruta.

A construção de uma visualização que possibilite essa observação pode ser conseguida organizando os dados segundo algum critério e apresentando-os de modo visual, como demonstrado nas figuras anteriores, o que, em geral, acabam

possibilitando a recuperação de informações relevantes e a construção de novos conhecimentos (DO NASCIMENTO, 2005).

3.2. Características das ferramentas de visualização

As ferramentas de visualização podem dar apoio ao usuário em todo o processo de análise dos dados. Tipicamente, podem apoiar três atividades:

- **Análise exploratória:** O usuário não tem nenhuma ideia de quais conhecimentos os dados podem conter e, através de um processo analítico, explora a representação visual e procura sinais que podem sugerir indicações sobre tendências particulares e relações que podem levar a alguma hipótese;

- **Análise de Confirmatória**: O utilizador tem uma hipótese e a meta será através da exploração visual achar a evidência para aceitação ou rejeição dessa hipótese;

- **Apresentação**: É utilizada para representação gráfica e exposição do relacionamento, estrutura, comportamento e outras características intrínsecas aos dados em questão.

Seja qual for o tipo de apoio da ferramenta, esta deve prover mecanismos de interação a fim de facilitar a visualização dos dados de diversas perspectivas, dentre eles (MEIGUINS *et al*., 2009):

- **Seleção**: possibilidade de selecionar dados pertinentes ao desenvolvimento de uma determinada tarefa;

- **Representação**: apresentação de dados abstratos, utilizando cores, formas, direções, entre outros;

- **Apresentação**: é a forma de disposição dos dados ao usuário, isso se

torna mais complexo se os recursos forem escassos como em celulares, *handhelds*, etc;

- **Escala e Dimensionalidade**: auxilia a visualização e a percepção do usuário, principalmente quando existe uma grande quantidade de dados sendo apresentada;

- **Rearranjo, interação e exploração**: uma nova visão sobre os mesmos dados com o objetivo de gerar uma nova percepção sobre os mesmos. Quanto melhor o conhecimento sobre os dados e seus relaciomentos, melhor será a tomada de decisão.

Wiss et. al (1998) implementaram em sua aplicação as tarefas que seguem, baseando-se em Shneiderman (1996), o qual afirma que uma ferramenta de VI deve permitir aos usuários realizarem:

- **Visão geral**: O usuário precisa ganhar uma noção sobre a totalidade dos dados que serão analisados, baseada nos parâmetros que este escolheu para a visualização, nos limites do gráfico usado e de sua percepção. A maioria dos atributos gráficos comuns são: posição, cor, tipo de representação e tamanho;

- **Zoom**: Permite focar em certo subconjunto dos dados para enfatizar a análise de um determinado contexto com maior precisão. Conforme se aplica o zoom, mais detalhes são mostrados sobre uma determinada visão dos dados, o que se chama de zoom semântico;

- **Filtro**: Possibilidade de o usuário reduzir o tamanho do conjunto de dados que está sendo analisado, eliminando itens baseados em seus atributos;

- **Detalhes sob demanda**: Disponibilização de informações e detalhes implícitos sobre um item em particular. Normalmente feito de forma

simples e direta como ao clique do mouse, por exemplo, onde as informações adicionais podem aparecer em uma janela auxiliar ou na própria visão dos dados;

- **Relacionamentos**: Se o usuário descobre um item de interesse, ele pode precisar saber outros itens com atributos similares;

- **Histórico**: Suporte ao usuário para desfazer uma ação, mostrar passos até aquele ponto, por exemplo.

Shneiderman (1996) agrupa em sete os diferentes tipos de dados que descrevem diferentes tipos de visualizações, sendo eles:

- **1-Dimensão**: Este tipo de dado é representado por texto ou dados similares, como linhas de código, podendo ou não haver outras informações associadas a ele, como data de criação, tamanho, data da última modificação, etc;

- **2-Dimensões**: Inclui dados geográficos, plantas de engenharia, entre outros. Pode-se associar uma grande quantidade de atributos com o uso de cores, tamanhos e formas diferentes;

- **3-Dimensões**: Dá-se importância ao volume de um objeto, um atributo a mais. Se for incluído o contexto do mundo real, melhor fica a percepção do usuário. Deve-se mencionar aqui, problemas inerentes como a oclusão (parte de um dado esconde outro) que deve ser tratada com transparência e *slicing*, por exemplo;

- **Temporal**: Reúne as características dos dados citados acima mais o atributo tempo. Costuma-se utilizar mais uma dimensão para este atributo e a animação deve ser considerada quanto há uma grande quantidade de dados a serem visualizados;

- **Multidimensional**: Base de dados relacional ou estatística pode ser considerada como pontos em um espaço multidimensional;

- **Hierárquico**: Representado por diagramas com nós, com ligações entre os mesmos. Útil para classificação de dados;

- **Rede**: Dados de rede são nós conectados por *links* previamente definidos que podem ser organizados em árvores ou em hierarquias sendo uma maneira ótima de manipulação a mudança de foco sobre os nós.

Há diversas ferramentas de VI com RV. Dentre elas destacam-se:

- **ThemeScape**: Desenvolvido pelo Laboratório Nacional Noroeste Pacífico, tenta organizar dados altamente multidimensionais como paisagens tridimensionais de terrenos, Figura 3.7:

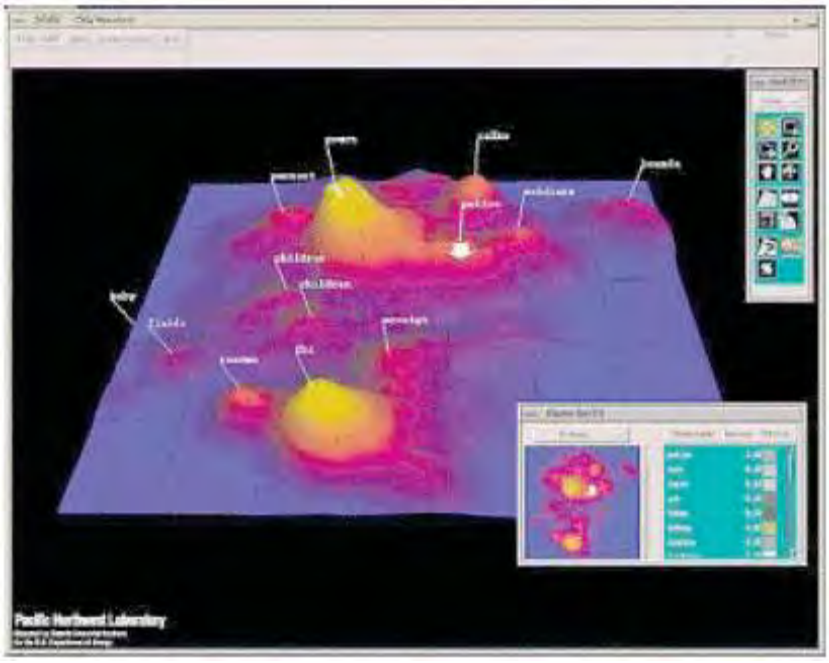


Figura 3.7. Aplicação ThemeScape (MEIGUINS et al., 2009 apud FURUHATA, 2004).

- **NetViz**: Baseia-se na representação de rede de dados importando dados de diversas fontes para auxiliar organizações a entender e administrar sua tecnologia de informação e sistema empresarial (Figura 3.8);

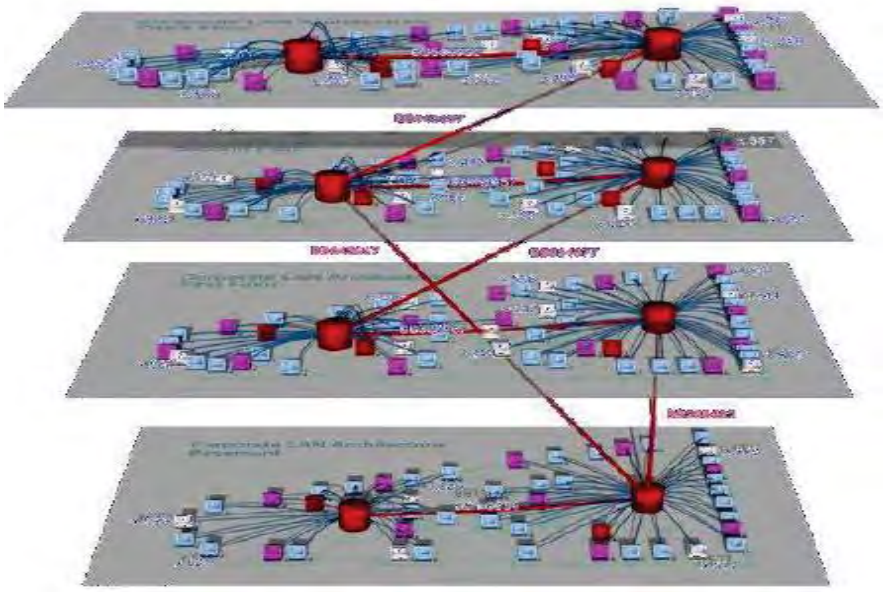


Figura 3.8. Uma aplicação de rede de dados em 3D (MEIGUINS et al., 2009 apud FURUHATA, 2004).

Árvore de Cones: *Cat-a-Cone* é uma ferramenta para categorização de documentos em que os usuários navegam pela árvore de cones até o livro desejado e uma representação visual do livro se torna disponível (Figura 3.9.);

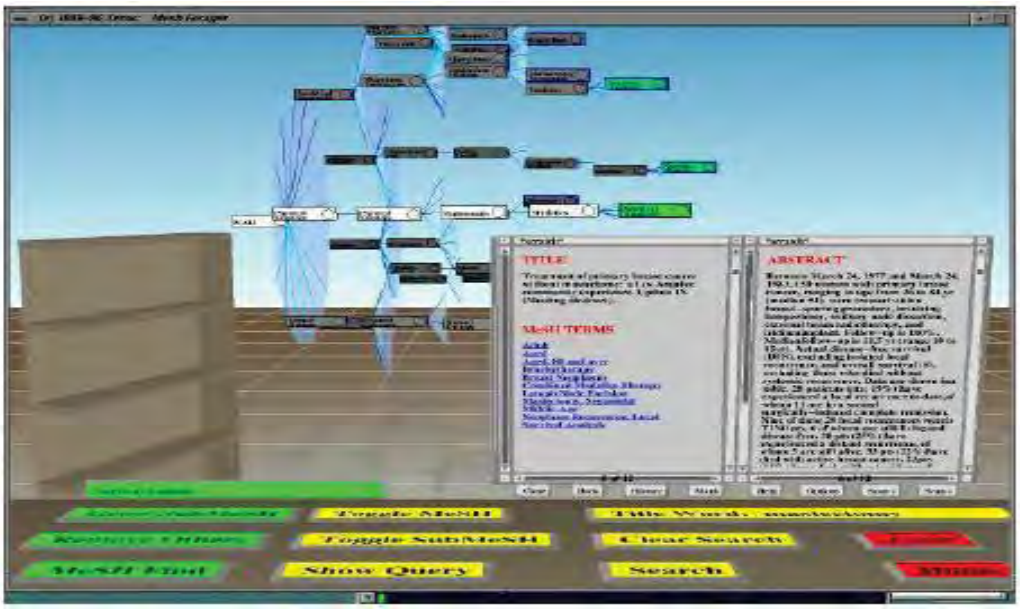


Figura 3.9. Aplicação Cat-a-Cone (MEIGUINS et al., 2009 apud FURUHATA, 2004).

- **Perspective Wall**: O usuário tem uma visão de dados em foco, podendo navegar na linha do tempo para poder analisar dados passados ou futuros. Não há filtro pois todos os dados no período são mostrados (Figura 3.10).

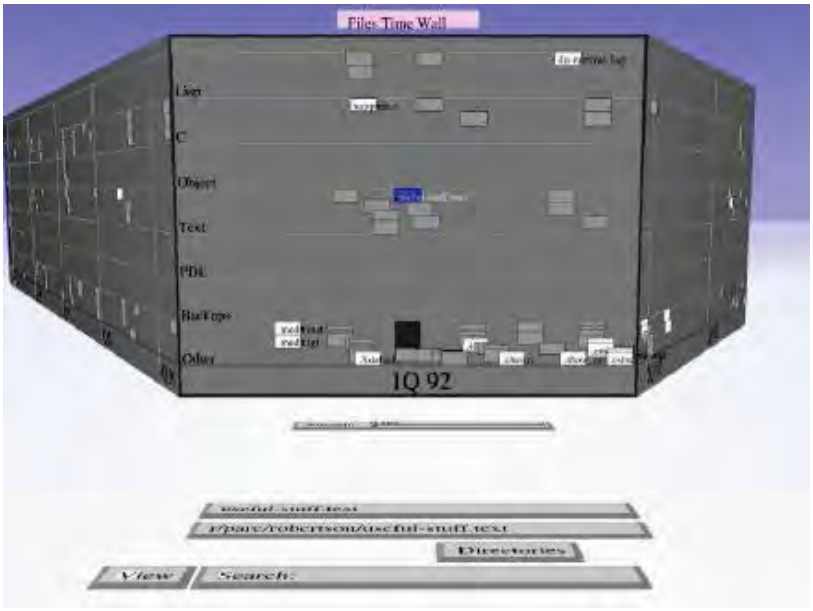


Figura 3.10. Aplicação com Perspective Wall (MEIGUINS et al., 2009 apud FURUHATA, 2004).

- **Histograma 3D**: Trata-se de uma técnica tipicamente bidimensional que pode ser estendida para o espaço tridimensional utilizando-se outras técnicas e metáforas como mapas ou redes de dados (Figura 3.11).

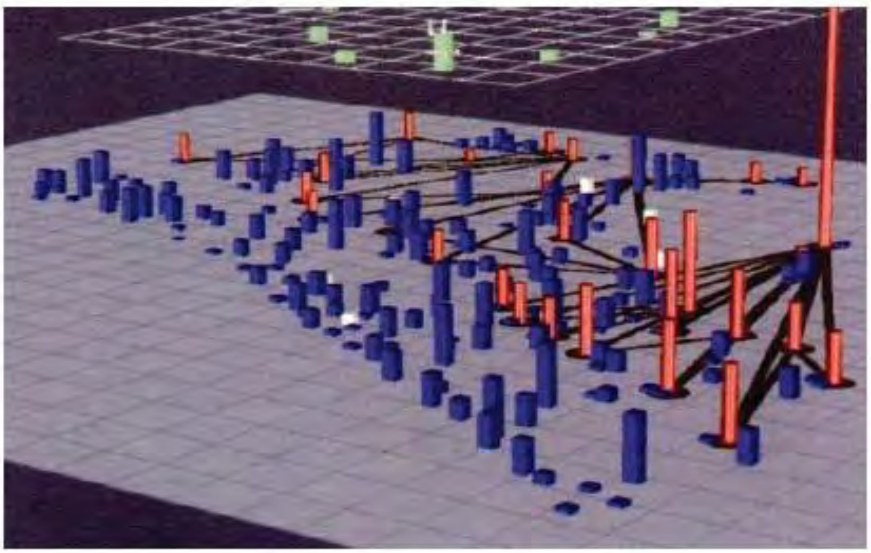


Figura 3.11. SAGE - Aplicação com histograma 3D (MEIGUINS *et al*., 2009).

3.3. Considerações finais

Objetivando a implementação de técnicas de visualização no protótipo de ferramenta proposto, foram apresentados seus conceitos e características da cognição humana em que pesa a maior facilidade do observador em obter conhecimento olhando para uma imagem em detrimento de informações puramente textuais.

Utilizando-se de diferentes formas e cores, enfim, lançando mão de metáforas visuais, obtém-se um ganho significativo para a percepção humana acerca dos dados sendo apresentados e das possíveis conexões, seus agrupamentos e relacionamentos intrínsecos. Algumas aplicações já desenvolvidas em outros trabalhos foram apresentadas para ilustrar tais conceitos.

4. TRÁFEGO DE REDES DE COMPUTADORES

Este Capítulo discute a necessidade de se monitorar tráfego de redes de computadores e algumas de suas dificuldades haja vista a quantidade excessiva de informação gerada pelos softwares de apresentação do tráfego, os chamados *sniffers*.

São apresentadas ferramentas de classificação e de monitoramento, atentando para a disjunção das informações entre elas e para a característica de funcionamento automático dos classificadores por padrões, que acabam por descartar a capacidade cognitiva do observador humano.

4.1. Monitoramento de tráfego de redes

Nos dias atuais, muitas organizações apóiam-se pesadamente e dependem de redes de computadores que se tornaram partes críticas de suas infra-estruturas. Paralelamente, o número de ataques contra tais redes explodiu em quantidade (MALÉCOT, 2006). Ainda, novos vírus e *worms* para os sistemas operacionais da família *Windows* e variantes tem sido desenvolvidos em taxa crescente o que tem aumentado em muito a quantidade de tráfego malicioso na Internet.

Este cenário torna-se ainda mais alarmante pelos dados da SYMANTEC (2011), que traz como principais fatos e números em seu relatório:

- 286 milhões de novas ameaças – Novos mecanismos de disparo, como os *toolkits* para ataques na rede, continuam a elevar o número de diferentes programas de *malware*. Em 2010, a Symantec identificou mais de 286 milhões programas maliciosos inéditos;

- 93% de aumento nos ataques baseados na rede – Os *toolkits* para ataques geraram aumento no volume de ataques 2010. O uso de *URLs* encurtadas também contribuiu para esse aumento;

- 260.000 identidades expostas por violação de dados;

- 6.253 novas vulnerabilidades – foram documentadas mais vulnerabilidades em 2010 do que em qualquer período anterior.

A Figura 4.1 mostra que, já em 2008, houve crescimento vertiginoso de ameaças via códigos maliciosos – um total de 1.656.227 - representando 60% do total dessas ameaças detectadas desde 2002 (SYMANTEC, 2009).

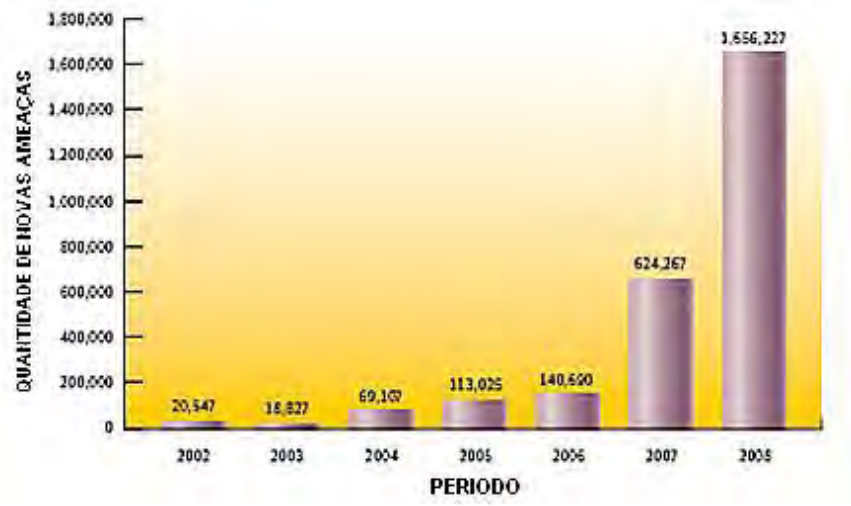


Figura 4.1. Novas ameaças por código malicioso na Internet (SYMANTEC, 2009).

Tais fatores impõem sérios desafios ao monitoramento e auditoria de segurança de redes. Enquanto aumenta o tráfego e a quantidade de dados das redes, acumulam-se o número de vulnerabilidades e tentativas de abuso.

Deste modo, a detecção e investigação de atividades intrusivas na Internet

apresentam-se como um desafio presente para administradores de rede e pesquisadores da área de segurança. O monitoramento de redes pode gerar grandes e ingerenciáveis quantidades de *logs* (registros) de dados, dificultando a distinção entre o tráfego legítimo e o malicioso.

Neste cenário figura o administrador de redes, sendo o profissional responsável por manter serviços de rede como conectividade com a Internet, servidor de *e-mail*, servidor de páginas, servidor de bancos de dados, entre outros para os usuários da rede corporativa. No caso de uma universidade, por exemplo, os usuários da rede compreendem essencialmente servidores docentes, discentes e servidores técnico-administrativos.

Para este propósito, existem ferramentas que podem auxiliar o administrador no processo de manutenção do funcionamento e da segurança de sua rede, como os *sniffers,* os *IDS - Intrusion Detection Systems* e as ferramentas de análise de tráfego.

Os *sniffers* são capturadores de pacotes que atravessam as interfaces de rede de dispositivos e podem ser utilizados tanto por usuários maliciosos, a fim de capturar informações sendo trocadas entre os dispositivos de rede quanto pelo administrador da rede no intuito de identificar problemas de conexão e falhas de segurança nos dispositivos. Nesta gama de softwares, destaca-se o *Tcpdump* (TCPDUMP, 2011). A Figura 4.2 apresenta um trecho de tráfego capturado por alguns centésimos de segundo.

Figura 4.2. Tráfego capturado pelo *Tcpdump*.

Apesar de ser esta um tipo de apresentação adequada aos softwares de análise de tráfego automatizados, tal forma de apresentação mostra-se demasiadamente complexa ao ser humano devido a ter informações puramente textuais e com altíssimas velocidades de apresentação.

As ferramentas de classificação como os *IDS*, trabalham com o conceito de verificação do tráfego a fim de encontrar assinaturas de ataques, ou seja, certos

padrões de tráfego, previamente conhecidos e configurados em suas regras, devem acontecer para que o dispositivo classifique o comportamento do tráfego como suspeito e isto leve a uma possível tomada de decisão. Tais regras são as chamadas “assinaturas de ataques”, ou seja, padrões de tráfegos maliciosos previamente estudados e conhecidos. Em (SNORT, 2011) há indicações para repositórios de regras, os quais são atualizados constantemente pelos seus mantenedores.

Geralmente tais ferramentas geram alertas que são gravados em arquivos de *log*, também, puramente textuais. A Figura 4.3 exemplifica algumas regras para detecçã do Snort.

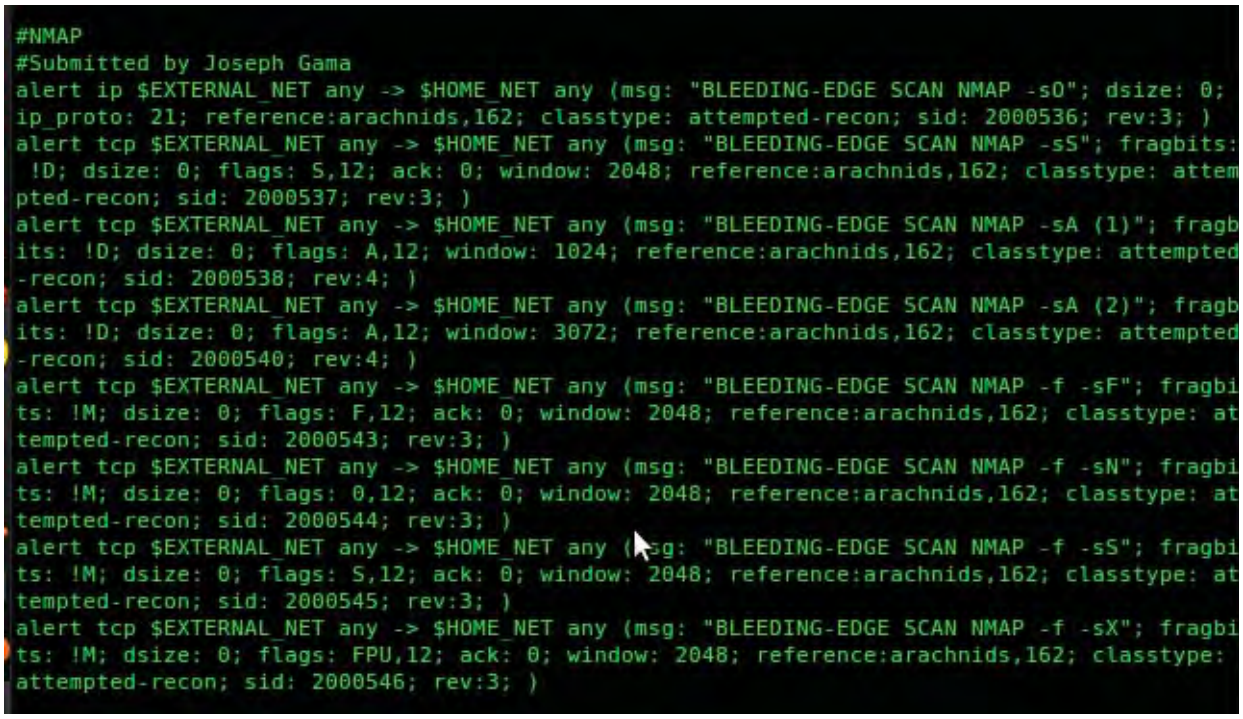


Figura 4.3. Exemplos de regras do Snort.

Por sua vez, os *logs* de alertas gerados pelo *Snort* através da verificação do tráfego da rede, baseada em suas regras pré-configuradas, são salvos em arquivos de texto. A Figura 4.4 traz parte do arquivo de *log* chamado de “*alert*”.

Figura 4.4. Alertas gerados em arquivo textual pelo Snort.

A partir da verificação do arquivo “alert”, um administrador pode tomar decisões administrativas relevantes. Desta forma, a importância de tais ferramentas de *IDS* é indiscutível, haja vista quantidade de informação e a velocidade com que os pacotes de dados passam pelos dispositivos, exigindo poderes computacionais para serem calculados.

Nessa gama de ferramentas para gerenciamento de redes, há as dedicadas não à detecção de tráfego malicioso, mas ao gerenciamento por monitoramento de aspectos da rede. Como exemplo de aplicação para monitoramento do tráfego da rede, pode-se citar o *Trafshow* (TRAFSHOW, 2011). Esta ferramenta com saída puramente textual imprime continuamente as informações do tráfego de pacotes, ordenando, por exemplo, pela quantidade de tráfego recebido ou enviado por cada computador da rede. A Figura 4.5 apresenta a interface do *trafshow*.

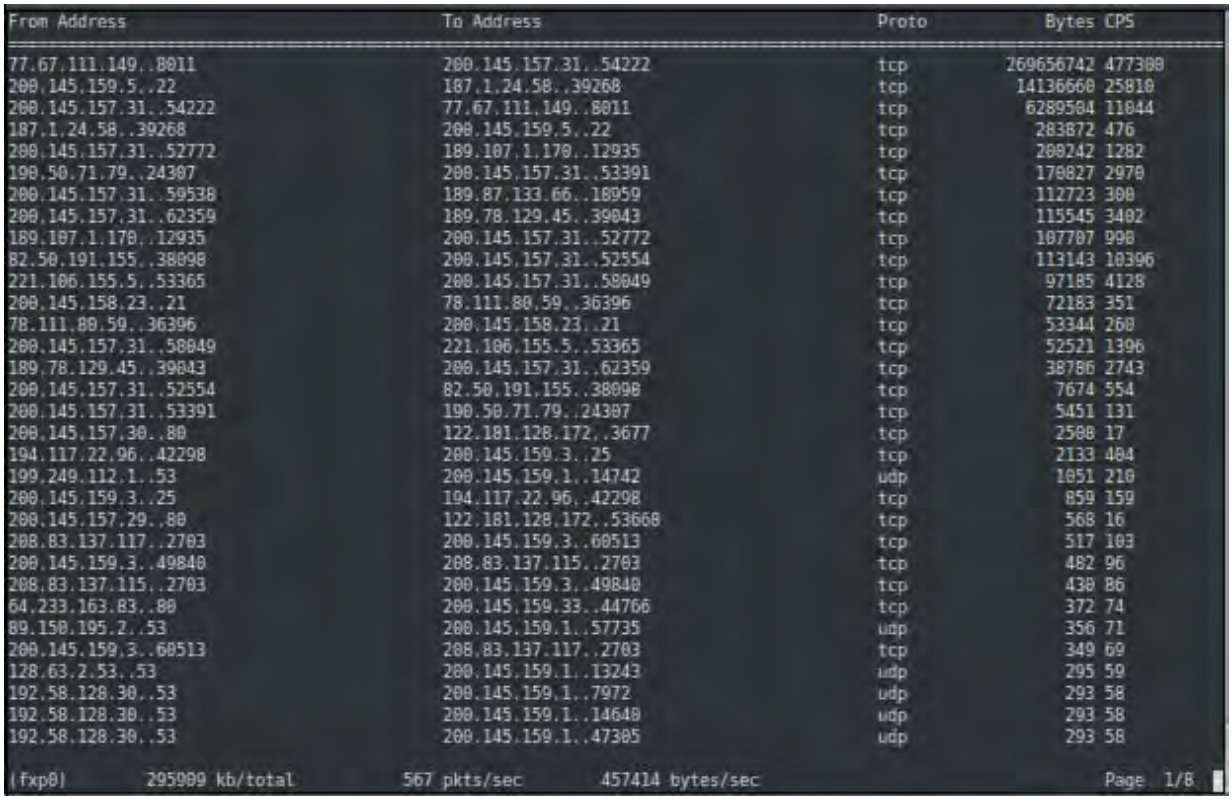


Figura 4.5. Interface do Trafshow.

Nota-se, na Figura 4.5, que o sistema apresenta pares de IP na primeira e segunda coluna, o protocolo em uso na terceira coluna e na coluna quatro, traz a somatória de *bytes* que trafegou pela conexão entre os dois equipamentos. Esta informação é importante para que o administrador da rede possa identificar mau uso da rede e clientes internos atuando como servidores de aplicações, por exemplo.

Um dos problemas que surgem em gerenciar uma rede apenas pelas abordagens das ferramentas apresentadas aqui é que elas acabam por descartar a capacidade cognitiva do ser humano em aprender e detectar novos padrões de comportamento, ficando simplesmente presas aos padrões previamente conhecidos e configurados nas ferramentas.

Outra dificuldade inerente diz respeito à disjunção das informações que são importantes ao administrador da rede, pois cada software exibe sua informação de

forma desconexa, sendo necessário fazer a junção lógica delas ao se fazer uma busca de verificação de tráfego anômalo. Por exemplo, caso o administrador perceba, através do *Trafshow*, que o tráfego de uma determinada máquina da rede está demasiadamente alto, ele deve abrir outro terminal remoto e utilizar o *Tcpdump* para verificar maiores informações sobre a conexão, tais como as portas envolvidas. Caso seja necessário tomar medidas de bloqueio, ele deve fazer uso de ainda outro software para tal, tornando o processo demasiadamente cansativo e complicado, passível de diversas falhas humanas.

Por outro lado, a observação do tráfego através de um detector de tráfego de rede dedicado reduz o volume de dados e alivia a preocupação de confundir tráfego malicioso de tráfego legítimo, além de que, a análise visual facilita uma rápida revisão e correlação de eventos pois utiliza a inteligência humana na identificação de padrões (VAN RIEL, 2006).

Procura-se, então, prover meios de possibilitar ao administrador de redes visualizar seu tráfego e monitorá-lo através de ferramentas visuais com interfaces intuitivas e amigáveis. Estas interfaces podem ser implementadas utilizando-se os conceitos de RV e VI, de forma a se obter uma complementação aos sistemas de segurança de rede automatizados já existentes procurando uma integração entre eles.

4.2. Ferramentas de visualização de tráfego de redes

Técnicas de VI tem sido utilizadas para tarefas de monitoramento apoiando-se na idéia de se obter vantagem através do processo visual humano e do reconhecimento de padrões. Diversas ferramentas de visualização foram criadas, em sua maioria com gráficos 2D entre outras que exploram cenas em 3D, o que possibilita a criação de representações mais complexas (MALÉCOT, 2006).

Há diversos trabalhos na área de visualização de tráfego de redes, como:

- **EtherApe:**. É baseado em visualização 2D e apresenta os hosts como nós de um círculo. A atividade da rede é simbolizada pela largura das

linhas entre os nós e as cores denotam os protocolos reconhecidos (ETHERAPE, 2011), Figura 4.6;

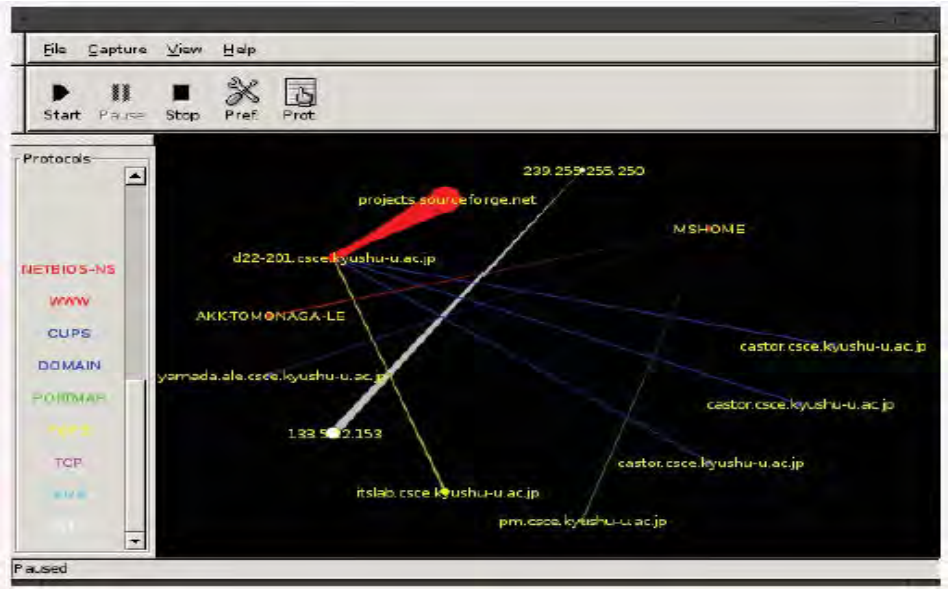


Figura 4.6 Tela do EtherApe (MALÉCOT, 2006).

Na Figura 4.7 pode-se observar que a visualização torna-se de difícil entendimento quando há muitos hosts se comunicando na rede.

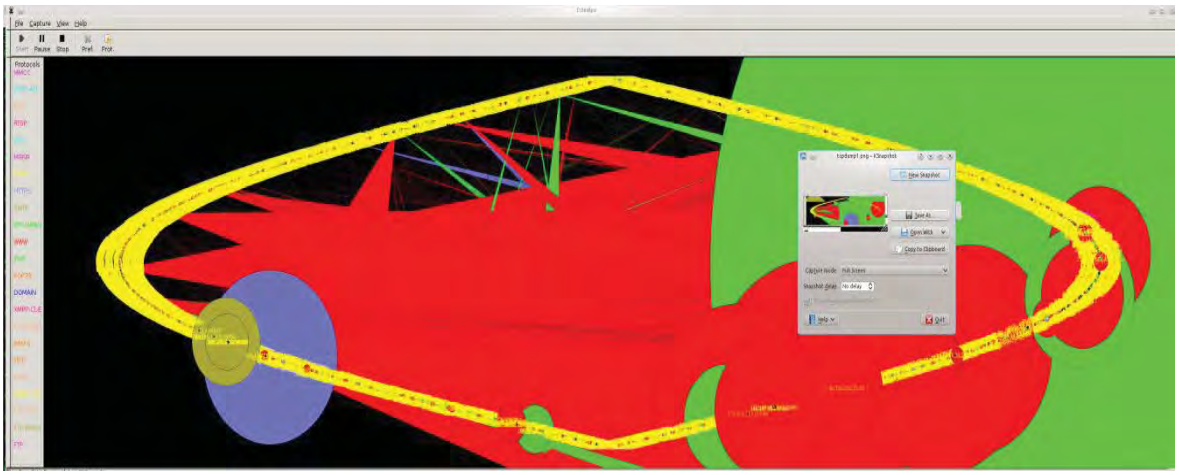


Figura 4.7 EtherApe com muitos hosts se comunicando.

- **VISUAL** (BALL, 2004): É outro aplicativo de visualização 2D. Ele foca na apresentação da comunicação entre a rede local e o mundo externo. A rede monitorada é representada por um *grid* sendo que cada quadrilátero significa um *host* da rede. Os *hosts* externos são representados por marcas fora do *grid*. As conexões entre *hosts* internos e externos são representadas por segmentos ligando os quadriláteros às marcas sendo que suas cores indicam a forma de comunicação unidirecional ou bilateral. A quantidade de tráfego da comunicação é apresentada pelo tamanho dos quadriláteros - *hosts* externos, Figura 4.8;

Figura 4.8. Tela do VISUAL (BALL, 2004).

- **Spinning Cube of Potential Doom** (LAU, 2004): Utiliza Visualização 3D para apresentar dados acerca de conexões TCP realizadas e tentativas de conexões em um cubo, Figura 4.9;

(a) **(b)**

Figura 4.9 Telas do Spinning Cube of Pontential Doom: (a) indica tráfego normal, (b) indica portscan sendo executado (LAU, 2004).

O eixo x do cubo lista os endereços IP internos da rede, o eixo z lista o espaço global de endereços IP externos à rede e o eixo y lista as portas TCP. Cada conexão TCP é apresentada como um ponto que pode ser branco para uma conexão estabelecida ou colorido, de acordo com o número da porta da tentativa de conexão. Desta forma, tentativas de conexão são enfatizadas e *scans* de portas são facilmente detectados pois linhas coloridas são formadas dentro do cubo. Apesar da facilidade em se visualizar os ataques de *portscan*, as exatas origens destes são difíceis de se visualizar e a aplicação não oferece interatividade sendo que a rotação do cubo a única forma de alteração do ponto de vista.

- **NvisionIP;** Desenvolvido por (LAKKARAJU *et al*., 2004), usa uma representação gráfica de uma rede classe B em uma única tela. A visualização apresentada é baseada na quantidade de *bytes* transmitidos partindo de ou destinados aos *hosts* da rede e pode ser

filtrada baseando-se em atributos, como, por exemplo, pode-se fazer um *"drill-down"* para ver estatísticas sobre uma pequena porção de *hosts* ou informações detalhadas de um único *host*. A Figura 4.10 apresenta a tela do *NvisionIP*.

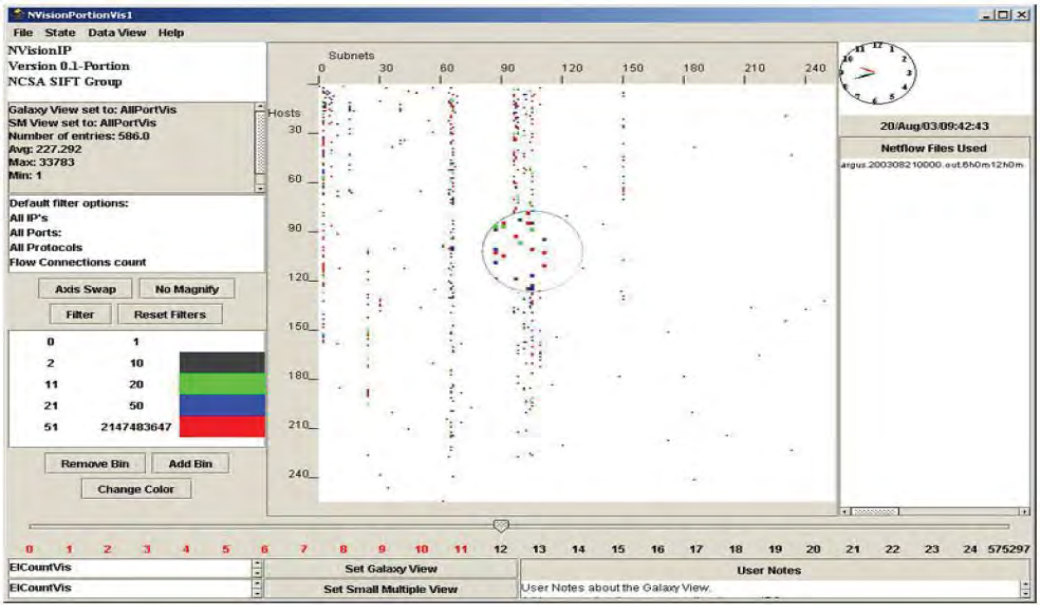


Figura 4.10 Tela do NvisionIP (LAKKARAJU et al., 2004).

4.3. Considerações finais

Neste capítulo foram apresentados os conceitos de gerência de rede tangíveis à manutenção de serviços e segurança de acesso. Discutiram-se as dificuldades em se utilizar softwares que apresentam o funcionamento da rede por interfaces simples de texto, e as desvantagens cognitivas inerentes aos classificadores automáticos por padrões.

Foram apresentadas, também, algumas ferramentas já descritas na literatura, as quais procuram, de forma gráfica, representar dados de redes através de diferentes formas de visualização. Foi apresentado o problema do EtherApe quando o tráfego é intenso. Tal questão é resolvida utilizando-se a visualização através de

um cubo forma proposta pelo protótipo desenvolvido neste trabalho.

Uma comparação entre tais ferramentas e o protótipo proposto é dada na Tabela 4.1. Em sua última linha, são apresentadas as características que o protótipo proposto neste trabalho deve fornecer, dentre as principais:

- meios de interação;
- filtros;
- formas, cores e posicionamento de objetos em seu cenário.

Tabela 4.1 Comparativo das características das ferramentas.

Ferramenta	Tipo de dados	Interação	Filtros	Características apresentadas	Representação
EtherApe	3D	Clique do mouse	Protocolo	Quantidade de tráfego	Cores Formas Ligações
Visual	2D	Alteração de foco	Porta Protocolo	Quantidade de tráfego	Cores Formas Ligações
Spinning Cube of Pontential Doom	3D	Rotação do cubo	Range de IP	Tentativas de conexão	Cores
NvisionIP	2D	Alteração de foco	Protocolo	Quantidade de tráfego	Cores
Tcpdump	1D	-	Informações de cabeçalho	Pacotes na interface de rede	Parâmetros de informações do cabeçalho
Snort	1D	-	Regras	Alarmes	-
Trafshow	1D	Alteração de foco	Range de IP	Quantidade de tráfego	Tabela
Protótipo proposto	3D	Rotação dos eixos; Zoom-in/out; Clique do mouse	Parâmetros do cabeçalho; Quantização; Placa de rede	Quantidade de tráfego; Relacionamentos; Detalhes por demanda	Formas; Cores; Posição

5. PROTÓTIPO DA FERRAMENTA 3D

Este capítulo descreve aspectos do sistema de visualização de tráfego de redes proposto, apresentando o ambiente no qual este está inserido, as metodologias utilizadas em sua concepção e conceitos de VI e de RV implementados.

O sistema consiste numa ferramenta para visualização de tráfego de redes de computadores capaz de apresentá-lo em um ambiente sintetizado representando seus nós através de metáforas visuais de objetos tridimensionais em um cenário de RV.

5.1. Ambiente do sistema

As tecnologias envolvidas no desenvolvimento do software são baseadas em software livre, dentre as quais destacam-se:

- Sistema operacional Linux Ubuntu; Fornece repositórios de pacotes de software *Open Source* para inúmeras ferramentas de desenvolvimento, comunicação, serviços de rede dentre outros, além de contar com uma vasta comunidade organizada em grupos e fóruns com amplas discussões acerca de soluções para problemas e dificuldades encontradas por seus usuários.

- IDE de desenvolvimento *QT Creator*: Trata-se de uma IDE multi-plataforma que oferece suporte ao desenvolvimento de aplicações. Torna mais ágil o processo de criação de ferramentas com interfaces gráficas.

- Linguagem de programação *C++*: Linguagem de programação que

combina características de linguagens de alto e baixo níveis. Oferece grande desempenho, sendo esta uma importante necessidade de sistemas de RV por envolver pesado processamento gráfico.

- Biblioteca *Ogre 3D*: *Object-oriented Graphics Rendering Engine.* Motor gráfico 3D orientado a objetos. Trata-se de uma biblioteca para auxílio ao desenvolvimento de aplicações e jogos com 3D.

- Biblioteca *Libpcap*: Fornece mecanismos para a captura de pacotes em interfaces de rede. Apresenta-se como uma das principais bibliotecas utilizadas no desenvolvimento da ferramenta proposta, haja vista que ela fornece meios para captura do tráfego da rede que se transforma em dados a serem apresentados pela ferramenta.

- Biblioteca *Glass*: Biblioteca para programação distribuída.

- *miniCAVE*: Estrutura de multiprojeção do LSTR.

As seções seguintes apresentam a Biblioteca Glass e a miniCAVE.

5.1.1 Biblioteca Glass

Esta seção define a biblioteca *Glass*, uma vez que ela é utlizada para a incorporação da ferramenta proposta ao Sistema de Multiprojeção apresentado na próxima seção.

Segundo GUIMARÃES (2004), o aumento do interesse pelas aplicações de RV motiva a pesquisa e o desenvolvimento de aglomerados de computadores, bibliotecas de desenvolvimento e de estratégias de desenvolvimento de aplicações de RV. Nesse intuito, a *Glass* é uma biblioteca para programação distribuída que consiste em um conjunto escalável de componentes que podem ser utilizados pelas aplicações. As aplicações são construídas reutilizando-se, conforme a necessidade, os componentes que estão disponíveis, habilitando-se assim a execução dos

serviços oferecidos pela biblioteca. Foi inicialmente criada no Laboratório de Sistemas Integráveis do departamento de Engenharia de Sistemas Eletrônicos da Universidade de São Paulo para dar suporte ao desenvolvimento de aplicações que necessitavam de sincronização entre os nós de um aglomerado gráfico. Trata-se de um ambiente avançado para o desenvolvimento de aplicações de RV baseadas em aglomerados gráficos (GNECCO, *et. al,* 2003).

A *Glass* pode ser utilizada para:

- Desenvolvimento de aplicações baseadas em aglomerados gráficos.
- Portabilidade de aplicações de RV já desenvolvidas para sistemas fortemente acoplados para serem executadas em aglomerados gráficos sem a necessidade de se refazer todo o projeto.

A Figura 5.1 apresenta uma visão geral dos seus componentes, quais sejam o componente *Arcabouço Glass* e o componente *Aplicações*.

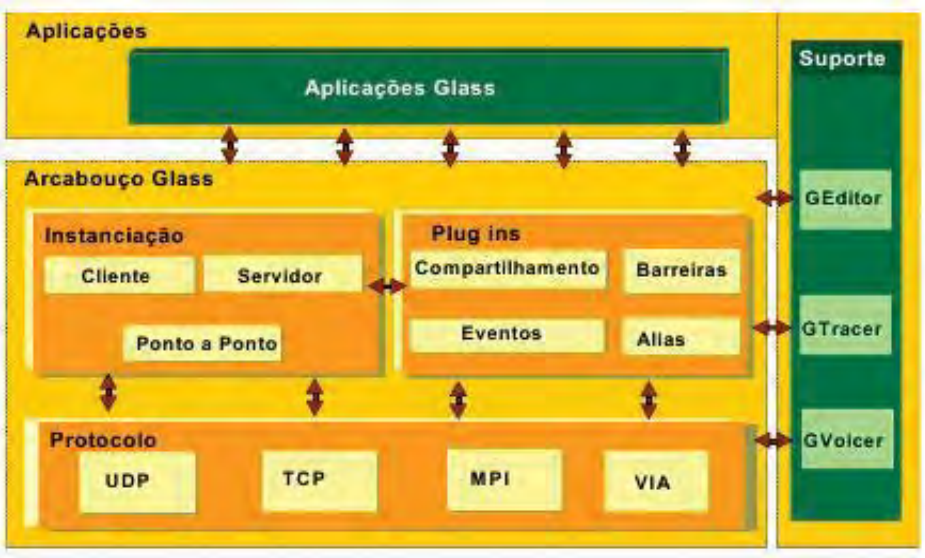


Figura 5.1 Arquitetura Glass (GUIMARÃES, 2004).

O Arcabouço *Glass* é composto por:

- Instanciação: tem como objetivo inicializar as aplicações conforme a arquitetura interna da *Glass*, que permite a aplicação ser cliente ou servidor.

- Protocolo: encapsula (*wrapper*) bibliotecas de protocolos de comunicação. Este componente possui uma infra-estrutura de empacotamento/desempacotamento de mensagens. Esse empacotador/desempacotador provê interoperabilidade entre sistemas.

- Plugins: gerencia todos os plugins da *Glass*. Os *plugins* fornecem serviços de transmissão de Eventos (*plugin* Eventos), de compartilhamento de dados (*plugin* Compartilhamento), de barreiras de sincronização (*plugin* Barreiras) e de associação de funções (*plugin Alias* – Pseudônimo).

O componente Aplicações é composto por:

- Aplicações *Glass*: são aplicações de RV baseadas em aglomerados gráficos. Elas podem ser desenvolvidas em *C/C++* ou em *Java*

- Aplicações de Suporte (*GTracer*, o *GEditor* e o *GVoicer*), são ferramentas que auxiliam o desenvolvimento de Aplicações *Glass*.

5.1.2 A miniCAVE

É uma estrutura de multiprojeção do LSTR – Laboratório de Sistemas de Tempo Real da FC, Figura 5.2. É composta de três telas medindo 2,5m x 1,5m cada, um aglomerado contendo seis *PC - Personal Computers* - interligados por um *switch gigabit ethernet* - visando prover um alto poder de processamento para a realização das renderizações necessárias às aplicações desenvolvidas e seis projetores de alta definição para que o sistema possibilite o uso de estereoscopia passiva.

Dessa maneira, torna-se necessário o uso de dois projetores para cada tela do sistema, um gerando imagem para o olho direito e, o outro, para o olho esquerdo. As duas imagens são sobrepostas, portanto, havendo necessidade de se “filtrar” os sinais gerados pelos projetores. Pares de lentes polarizadoras são posicionados nas saídas dos projetores, havendo assim, uma diferenciação nos sinais emitidos (DIAS; BREGA, 2011).

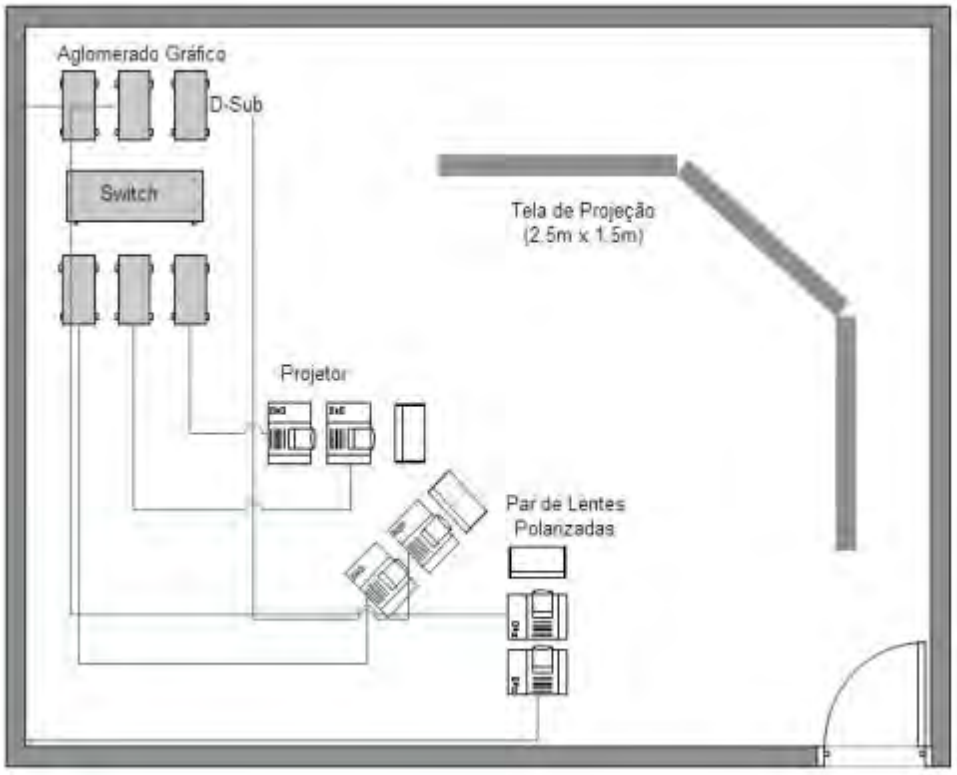


Figura 5.2 Planta baixa do Sistema de Multiprojeção (DIAS; BREGA, 2011).

A Figura 5.3 apresenta o sistema de multiprojeção em funcionamento. A tela da esquerda contém a interface do Trafshow, a tela central contém o protótipo em execução e a tela da direita contém a interface do Tcpdump.

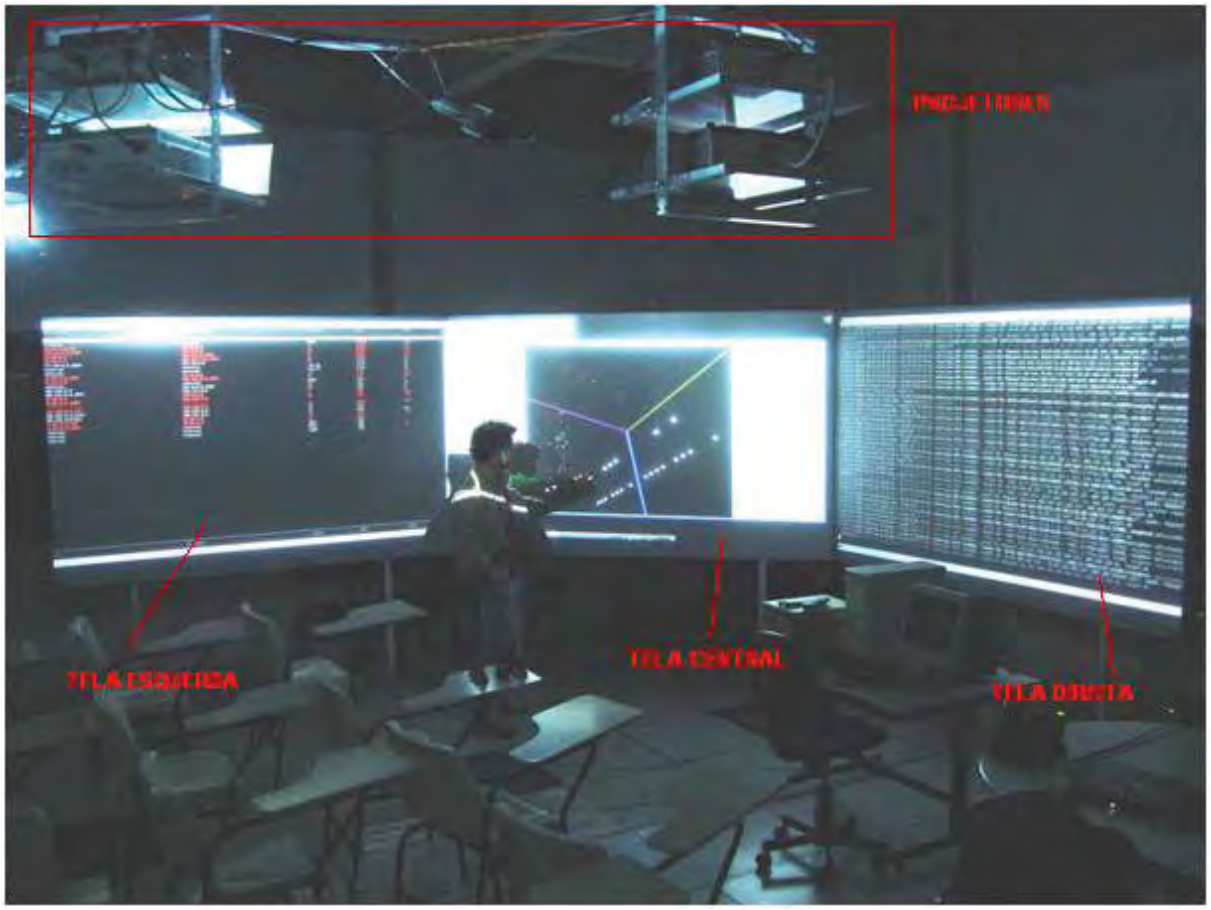


Figura 5.3 Aplicação sendo executada no sistema de multiprojeção

5.2. Projeto do protótipo

Para o desenvolvimento do software de visualização, foram elaborados diagramas de casos de uso da UML - *Unified Modeling Language* – Figura 5.4.

Descreveu-se a ferramenta em oito casos de uso que serão descritos a seguir. No diagrama, os atores descritos são os seguintes:

- Administrador de Redes: O usuário final do sistema, responsável pela manutenção e bom funcionamento da rede de computadores;

- Interface de Visualização: Módulo do sistema responsável pelas formas

como os dados estarão dispostos para o usurário, faz a interface entre a rede e o usuário final. Nesse módulo estão os recursos de RV;

- Interface de Redes: Módulo do sistema responsável pela leitura e interpretação dos dados lidos da rede de computadores. Esse ator é responsável pela transformação de dados em informações que serão mostradas ao usuário final.

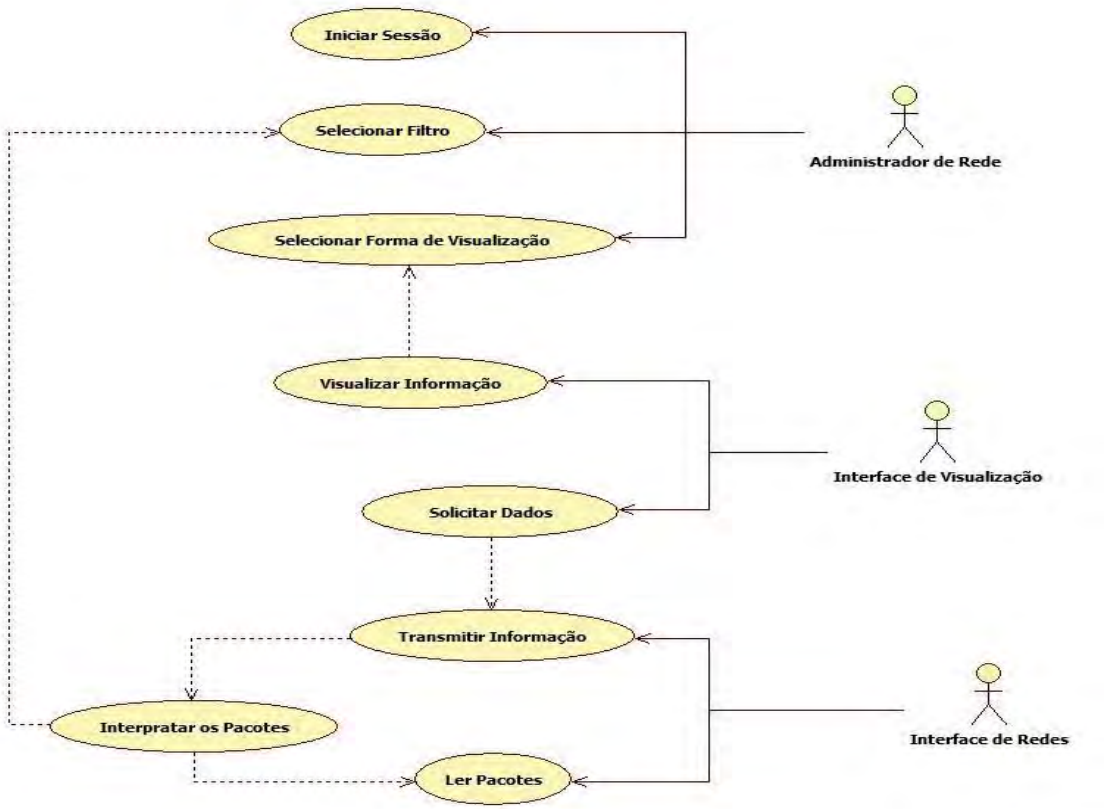


Figura 5.4 Diagrama de casos de uso.

A seguir, descrevem-se os Casos de Uso:

- Iniciar a Sessão:
  - Ator: Administrador de Redes.
  - Descrição: O administrador de rede executará o sistema através do terminal de comandos com usuário *root*.

- Selecionar Filtro:
    - Ator: Administrador de Redes.
    - Descrição: O administrador de redes seleciona quais filtros serão aplicados para análise e amostragem dos dados na interface. Esses filtros serão utilizados na interpretação dos dados lidos pela interface de rede.

- Selecionar Forma de Visualização:
    - Ator: Administrador e Redes.
    - Descrição: Apresenta relação de dependência com as formas de visualização proporcionadas pela interface de visualização. O administrador de rede escolherá duas opções de visualização dos pacotes de dados que trafegarão pela rede: Modo texto e Modo 3D. Serão descritas no próximo caso de uso.

- Visualizar Informação:
    - Ator: Interface de Visualização.
    - Descrição: A interface de visualização oferece ao administrador de redes duas formas de visualização de dados. Modo 3D e Modo texto. No primeiro, com elementos de RV, os pacotes serão representados dentro de um cubo cujas arestas representam IP origem, IP destino e porta. Em ambos os modos, as informações dos pacotes são detalhadas através do clique do mouse sobre o objeto que referencia o pacote.

- Solicitar Dados:
    - Ator: Interface de Visualização.
    - Descrição: A interface de visualização solicitará à interface de redes os pacotes de dados que serão ilustrados em seus modos de visualização.

- Transmitir Informação:

- Ator: Interface de Redes.
- Descrição: A interface de redes enviará à interface de visualização as informações por ela solicitadas.

- Interpretar Pacotes:
  - Ator: Interface de Redes.
  - Descrição: A interpretação dos pacotes de dados se dá pelos filtros pelo administrador de redes, ”Transformação de dados em Informações”. Estabelece relação de dependência com a leitura de pacotes e a transmissão de dados.

- Ler Pacotes:
  - Ator: Interface de Redes.
  - Descrição: A interface de redes é responsável pela leitura dos pacotes que trafegam pela rede. Para que desempenhe essa função utiliza de funções existentes na biblioteca *LibpCap*.

O fluxo lógico de funcionamento do sistema pode ser descrito pelo diagrama de sequência da Figura 5.5.

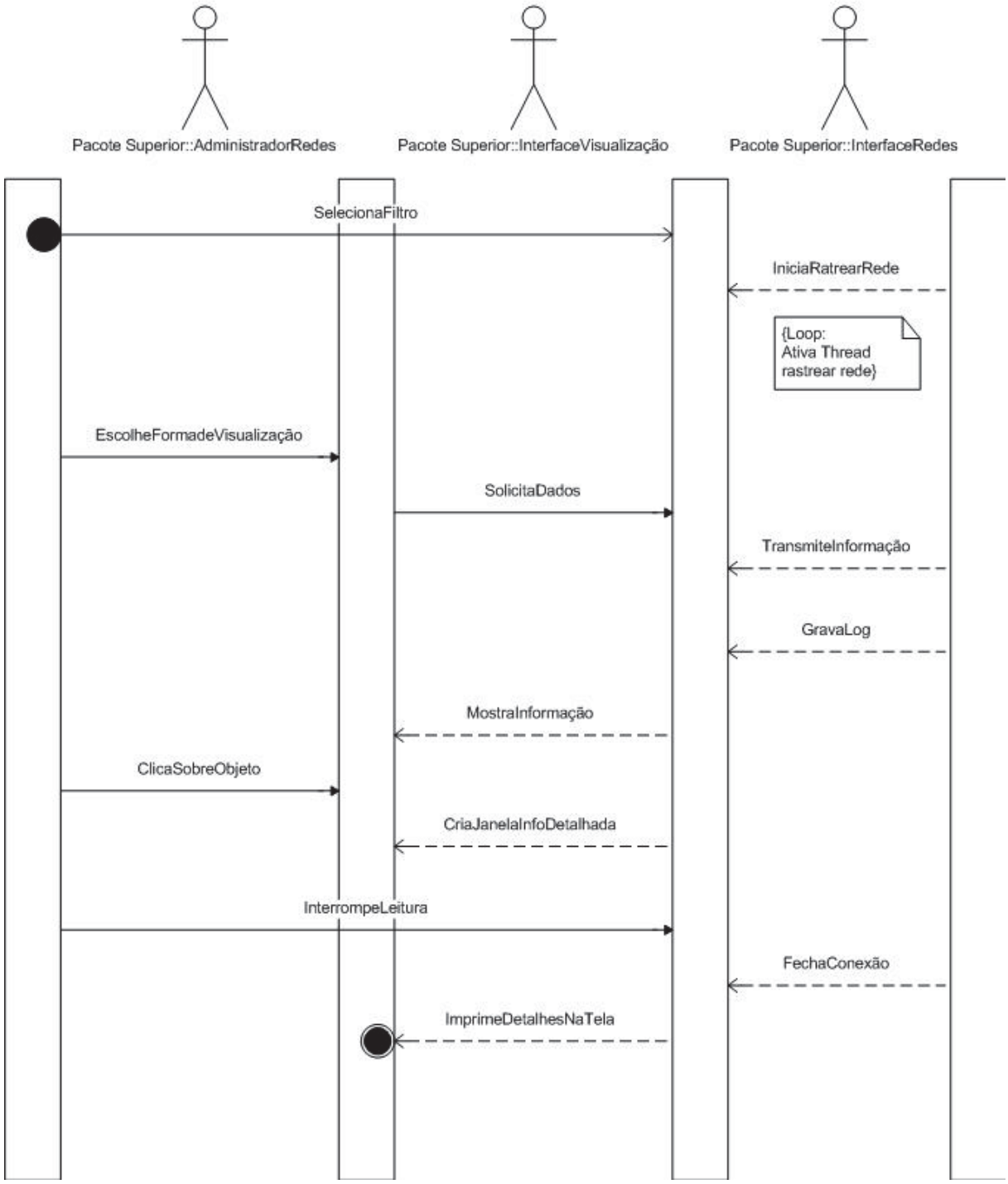


Figura 5.5 Diagrama de sequência

Para a obtenção de estereoscopia através do aglomerado gráfico e da miniCAVE, utilizou-se a biblioteca Glass.

O papel principal dos objetos *glass* é fazer o compartilhamento dos dados de transformação do ambiente virtual. Os objetos do *Ogre* responsáveis pela transformação são:

- **Vector3:** utilizado para o efeito *zoom-in/zoom-out* do ambiente.
- **Quaternion:** utilizado pelas transformações de *pitch* (rotação em x), *yaw* (rotação em y) e *row* (rotação em z).

Esses dois tipos de dados do *Ogre* devem ser distribuídos no aglomerado e para isso foram utilizados objetos da *Glass* definidos no *TestWidge.h*:

```
Shared<Ogre::Vector3, rawPack, rawUnpack> *glassCameraPos;

        Shared<Ogre::Quaternion, rawPack, rawUnpack> *glassCameraYaw;

        Shared<Ogre::Quaternion, rawPack, rawUnpack>
*glassCameraPitch;

        Shared<Ogre::Quaternion, rawPack, rawUnpack> *glassCameraRow;
```

Objetos *Shared*, como descrito em GUIMARÃES (2004), fazem a distribuição dos dados. A declaração é definida deste modo:

- **Shared:** tipo do objeto *glass*;
- **<Ogre::Vector3**: tipo do objeto que será distribuído;
- **rawPack, rawUnpack>:** atributos estão ligados à distribuição dos objetos. São serializados para o envio e de-serializados no recebimento dos dados pelos nós;
- ***glassCameraPos;** nome do objeto glass.

A utilização dessa estrutura no código do protótipo é feita baseando-se na interação com a cena, sendo que um estímulo do teclado deve ser distribuído para todos os nós da Glass. O método que realiza a essa distribuição de estímulos está na classe *TestWidget.cpp.* e é apresentado no Apêndice.

A atribuição de valores o objeto Glass é feita por:

```
glassCameraRow->assign(crow);
```

Depois de atribuído a todos os objetos, estes devem ser enviados aos demais nós do aglomerado:

```
if (g->isMaster()){
glassCameraPos->sendUpdate();
glassCameraYaw->sendUpdate();
glassCameraPitch->sendUpdate();
glassCameraRow->sendUpdate();
}
```

É necessário sincronizar os dados dos nós na renderização do ambiente, médodo da classe *QOgreWidget.cpp*. Para isso, são definidas as seguintes barreiras da *glass*:

```
Barrier   *datalock, *swaplock;
```

Depois de definidas, são inicializadas:

```
            this->datalock = new Barrier(1, false);
            this->swaplock = new Barrier(2, false);
```

O *datalock* sincroniza os dados antes de renderizar. O *swaplock* sincroniza a troca de quadros.

```
voidQOgreWidget::update(void) {
if (m_renderWindow) {
datalock->sync();
            m_ogreRoot->_fireFrameStarted();
            m_renderWindow->update();
swaplock->sync();
            m_ogreRoot->_fireFrameEnded();
}
}
```

5.3. Execução e testes

A ferramenta desenvolvida foi posicionada no perímetro da rede para o monitoramento de todo o tráfego que entra ou sai dele.

A Figura 5.6 apresenta a interface 3D da ferramenta a qual consiste em um cubo cujas arestas representam informações como IP origem, IP destino, porta origem ou porta destino.

Figura 5.6 Interface 3D da ferramenta

Esse cubo é de um mapa 3D em que cada ponto projetado sobre cada um dos três eixos representa a troca de informações entre dois dispositivos na rede. Conforme os dados são capturados, o ambiente é modificado, seja por meio de mais objetos sendo desenhados dentro do cubo a fim de representar novas estruturas de conexão, seja por meio de atualização das características dos objetos já existentes, representando novas informações acerca de uma conexão já existente. Na Figura 5.6, obtem-se uma visualização geral da estrutura, sendo que todo o tráfego da rede é apresentado, sem a ocorrência do problema apresentado pelo EtherApe.

Ao lado direito do gráfico 3D, Figura 5.7, há uma interface de configuração que permite ao usuário escolher entre diversas opções de visualização. As principais

configurações são:

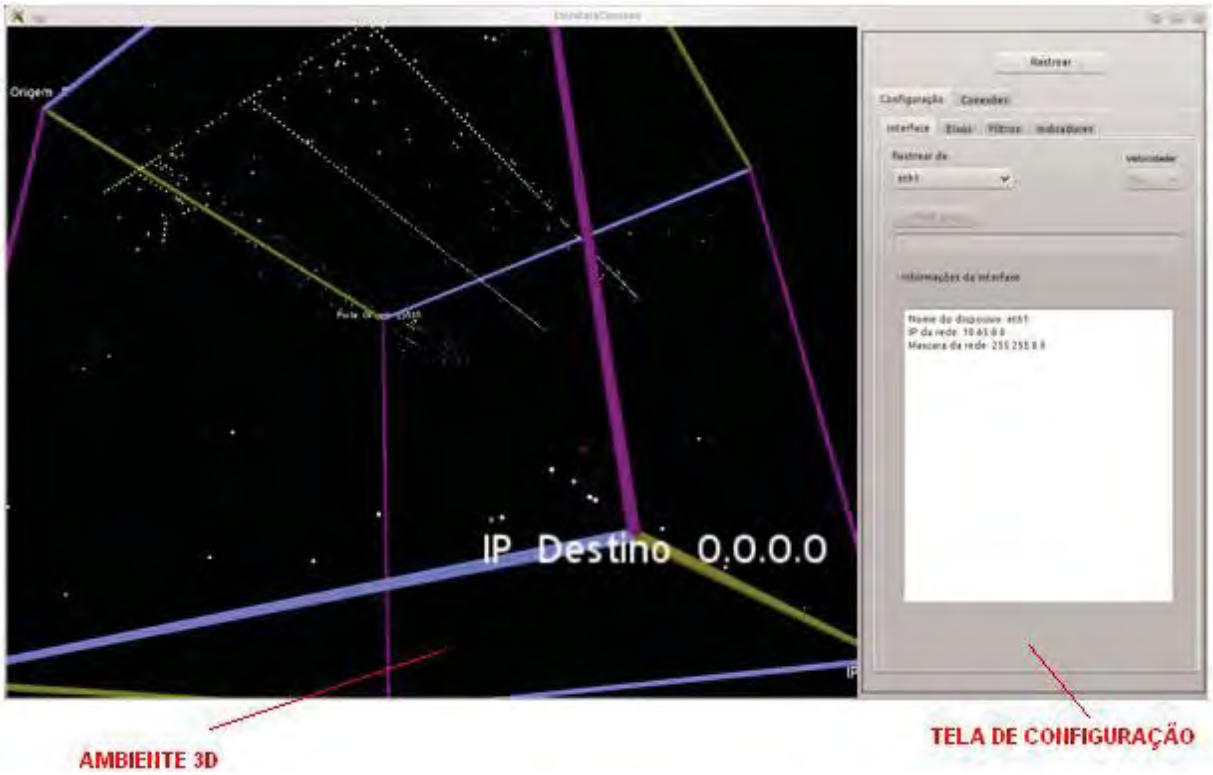


Figura 5.7 Interface de configuração

- **Aba de configuração da interface de rede**: permite ao usuário escolher a interface de rede a ser rastreada, no caso de existir múltiplas interfaces no equipamento ou leitura de um arquivo de *log* que tenha sido previamente salvo no formato da LibPcap.
- **Aba de configuração dos Eixos**: nessa tela o usuário escolhe quais informações devem ser representadas em cada aresta do cubo; Esta funcionalidade prove inúmeras possibilidades de cruzamento de características do tráfego no cubo.
- **Aba de configuração de filtros**: podem-se construir filtros de pacotes com base nas diversas funções de filtro da *LibpCap*;
- **Aba de configuração dos indicadores**: nessa tela o usuário pode definir classificações para cada conexão encontrada, como cores

representando um intervalo de valores que pode ser número de pacotes, porta origem, porta destino, tamanho em *Kbps* ou tempo. Esta funcionalidade prove ao sistema de visualização importante valor cognitivo para a percepção de detalhes sobre o tráfego.

Foram incorporados à Interface de Visualização recursos de imersão, interação e envolvimento, característicos das aplicações em RV, tais como:

- **Rotação**: o cubo pode ser girado em todos os seus eixos, Figura 5.10.;
- **Clique do mouse**: clicando-se nas esferas, obtem-se, em uma nova tela, informações acerca do tráfego passante para aquele objeto selecionado, Figura 5.8. Ainda nessa nova tela, o clique sobre as linhas apresentadas apresentam as informações do protocolo;
- ***Zoom-in, zoom-out***: pode-se aumentar o *zoom*, dando a impressão de se estar dentro do cubo, a fim de obter-se uma visualização mais detalhada de determinado objeto, Figura 5.9 e Figura 5.11.

Na Figura 5.8 nota-se a formação de uma estrutura linear, causada pela execução de um ataque de *portscan*. Em situações de tráfego normal, deve-se obter um arranjo esparso de objetos, indicando diferentes máquinas da rede externa trocando dados com diferentes máquinas da rede interna. Formações de estruturas pela interação dos objetos no cubo podem ser entendidas como tráfego anormal, indicando uma possível ação maliciosa.

Tal característica de configurações variadas dos eixos do cubo deve trazer inúmeras possibilidades de uso da ferramenta para obtenção de diferentes aspectos do tráfego.

Ao lado direito, na Figura 5.8, apresenta-se a tela de detalhes do tráfego, aberta pelo clique do mouse sobre o objeto em vermelho, apontado na Figura.

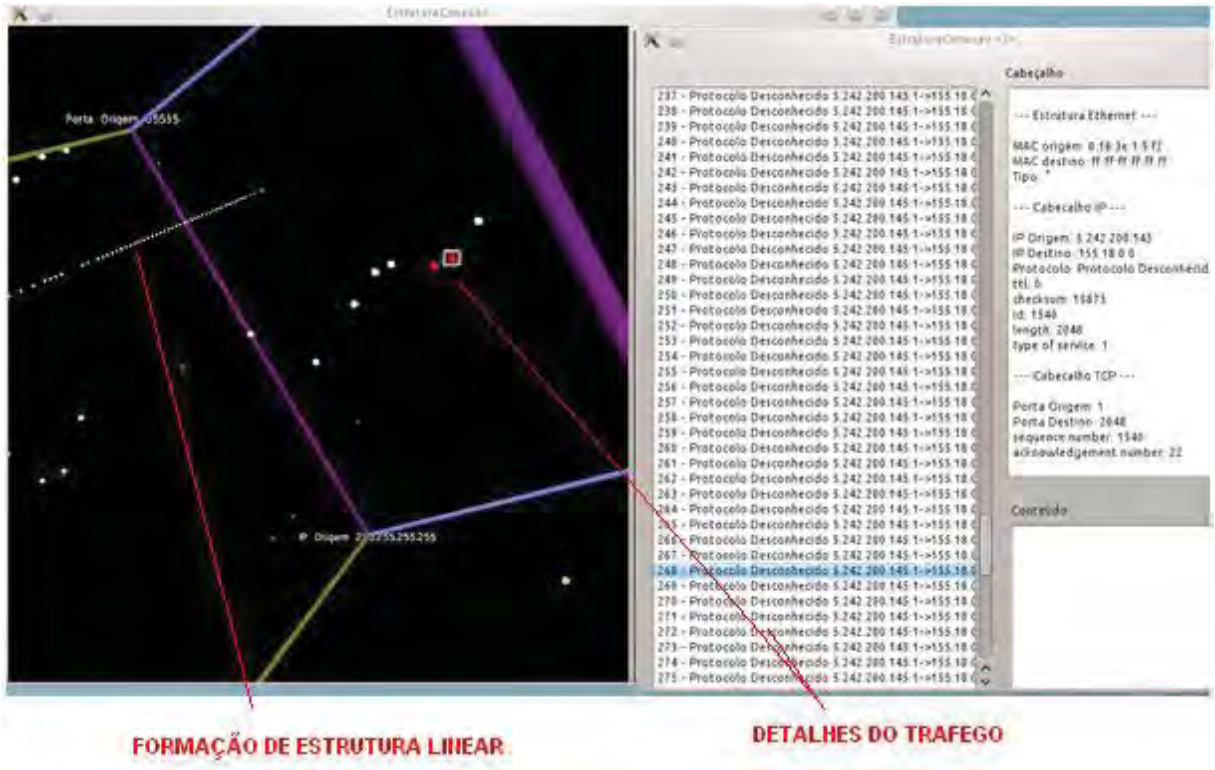


Figura 5.8 Exemplificação do recurso de interação através de clique do mouse.

Na Figura 5.9, percebe-se que foi executado um *zoom-in* de forma que tem-se a impressão de estar “dentro” do cubo.

Os objetos mais próximos do observador aparecem maiores e ocorre o efeito da oclusão.

Nota-se, também a utilização de diversas cores, sendo que, neste caso, a ferramenta foi configurada para classificar a quantidade de tráfego através delas (Figura 5.11). A cor branca indica pouco tráfego e, conforme os pacotes da conexão classificada vão sendo contabilizados, as cores vão sendo alternadas até chegar ao vermelho indicando tráfego intenso.

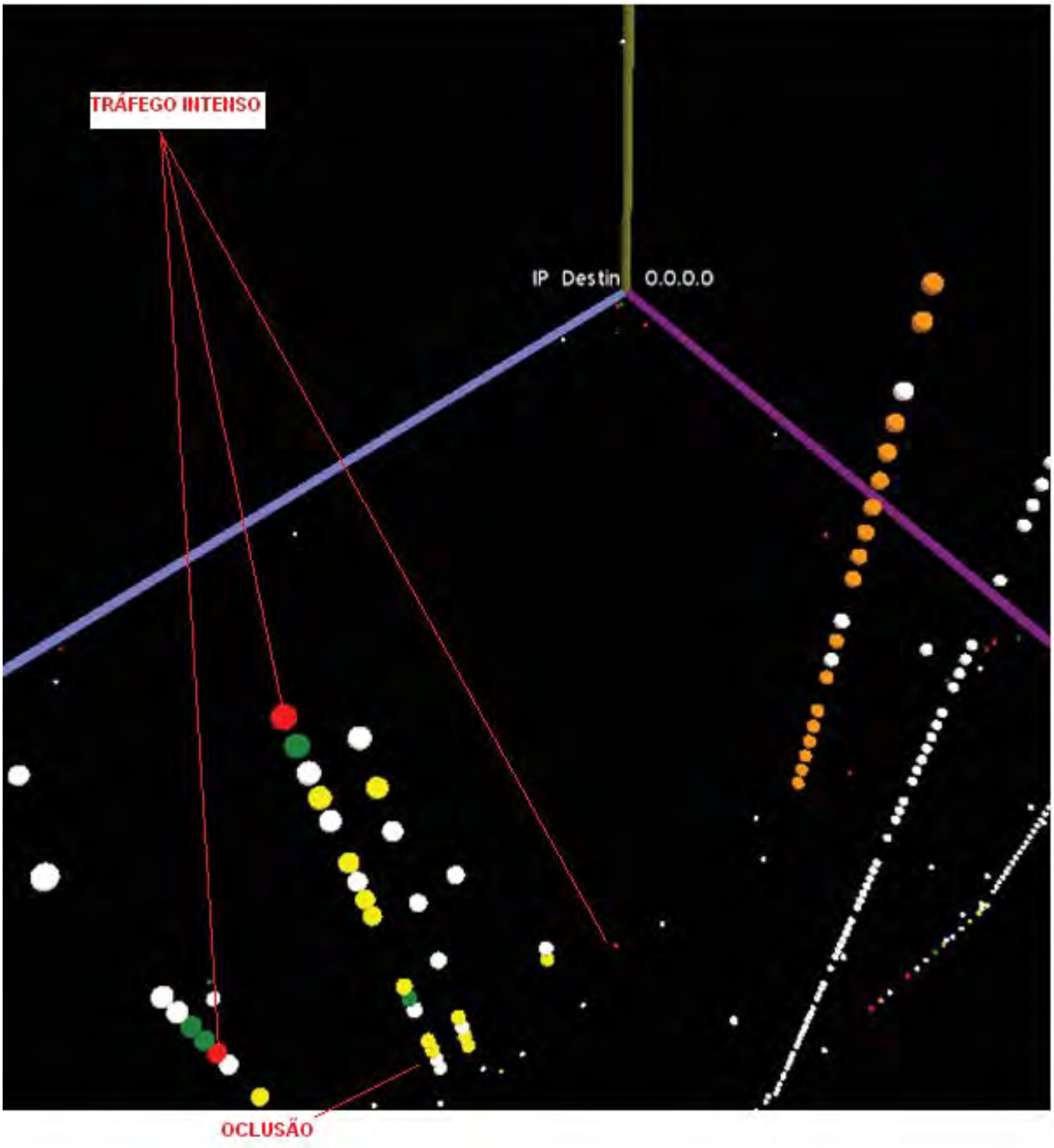


Figura 5.9 Exemplificação do recurso de zoom.

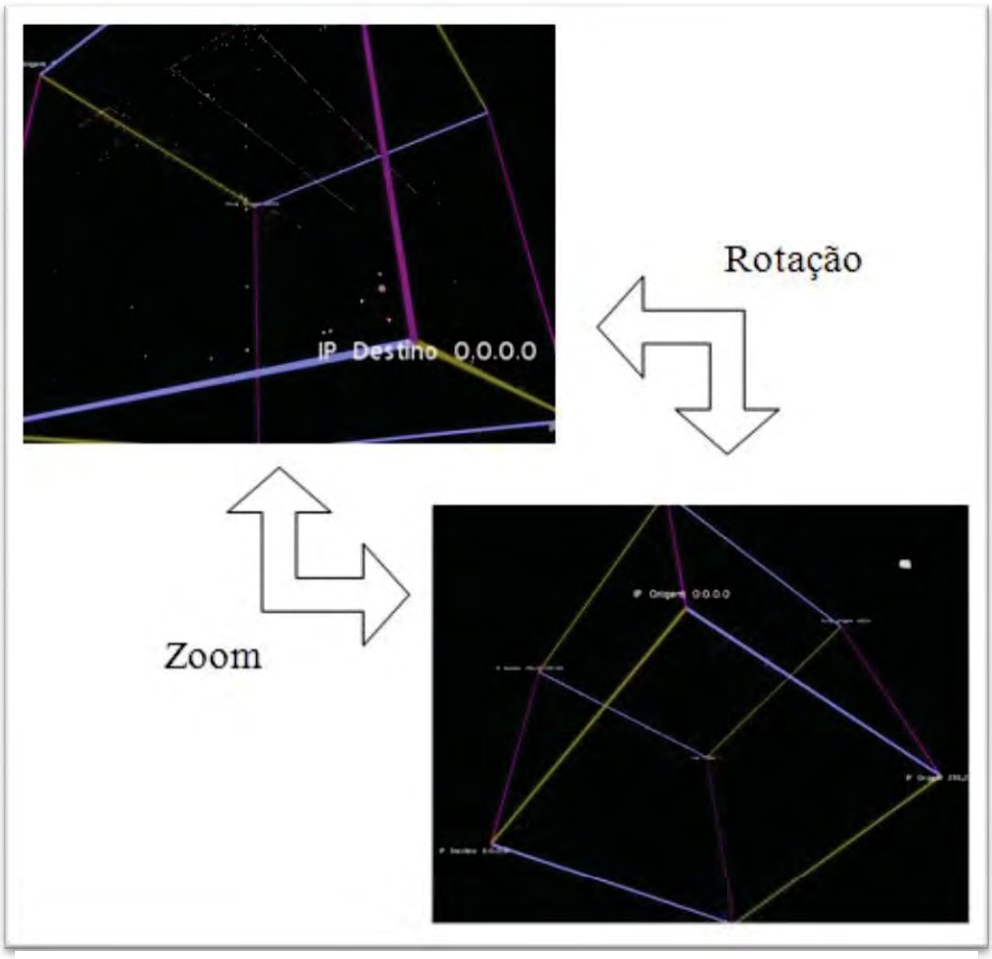


Figura 5.10 Exemplificação dos recursos de rotação e zoom.

Recursos desejados nas ferramentas de VI também foram contemplados no protótipo, tais como:

- **Representação:** escolha de alternadas cores para os objetos, indicando diferentes estados da conexão, Figura 5.11;
- **Visão Geral/ Zoom:** escolha de foco em subconjuntos de dados, Figura 5.10;
- **Filtro:** possibilidade de redução do tamanho do conjunto de objetos a ser analisado.

Na figura 5.11, foi escolhida a característica “número de pacotes” para a

classificação por cores, sendo esta característica se dá pelas faixas indicadas para cada uma:

- **Branco**: 0 a 5 pacotes;
- **Verde**: 6 a 10 pacotes;
- **Amarelo**: 11 a 20 pacotes;
- **Laranja**: 21 a 40 pacotes;
- **Vermelho**: 41 ou mais pacotes.

Diversas opções de classificação podem ser utilizadas, como por exemplo, tipo de protocolo e número de porta.

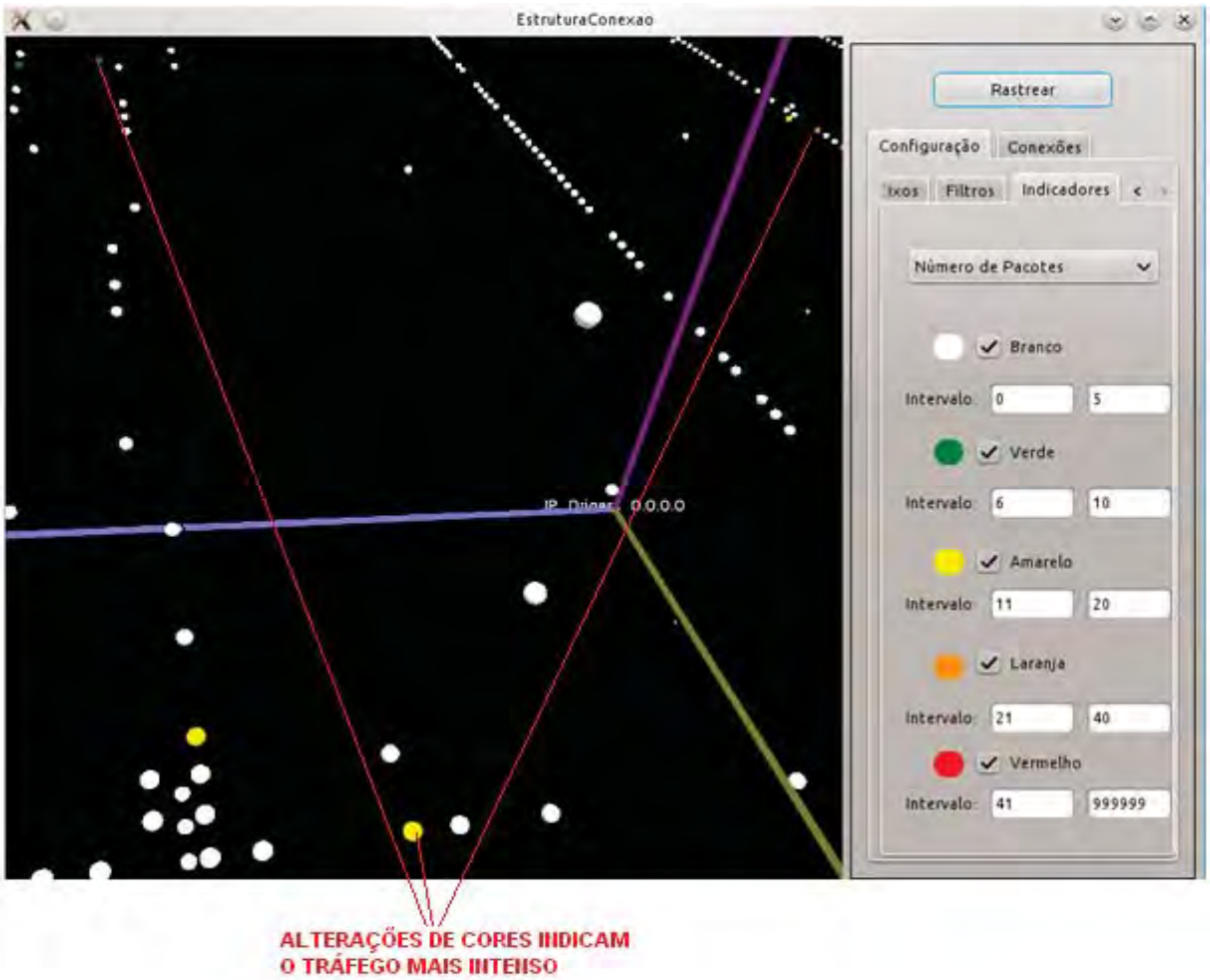


Figura 5.11 Exemplificação do recurso de representação.

5.4. Avaliação do protótipo

Com o intuito de avaliar o protótipo desenvolvido, este foi apresentado a um grupo de 7 profissionais da área de redes em atuação. O protótipo foi apresentado aos profissionais e suas funcionalidades foram exploradas. Ao fim da apresentação, cada profissional respondeu um questionário para que se avaliasse:

- Experiência prévia com aplicações de VI e/ou RV para o gerenciamento de redes;
- Opinião sobre a contribuição do protótipo para o entendimento da rede;
- Opinião sobre a contribuição do protótipo para a capacidade cognitiva do profissional;
- Opinião sobre a possibilidade de o protótipo servir de base para acoplamento de novos módulos;
- Opinião sobre a característica de o protótipo oferecer diversas possibilidades de cruzamento de informações do tráfego;
- Opinião sobre a importância das formas de interação implementadas para interação com o cenário;
- Opinião sobre a importância das formas de interação implementadas para a congnição;
- Opinião sobre a facilidade de interação promovida pelas formas de interação implementadas;
- Opinião sobre a importância do clique do mouse para a obtenção de informações detalhadas do tráfego;

- Opinião sobre a importância do uso de cores para facilitar o entendimento de características do tráfego;

- Opinião sobre a importância da ferramenta que combina RV com VI para o monitoramento de redes;

- Opinião sobre o ganho de interatividade através da projeção na miniCAVE;

- Opinião sobre a usabilidade e resultados da ferramenta através de um monitor; e

- Opinião e sugestões livres acerca do sistema apresentado.

O questionário apresentado foi o seguinte:

- Q1 – Você já teve alguma experiência prévia com aplicações de Visualização e/ou Realidade Virtual para gerenciamento de redes?

- Q2 – Você concorda que o módulo 3D do sistema apresentado oferece meios de obter maior entendimento e informações importantes acerca da rede?

- Q3 – Você concorda que o módulo 3D do sistema apresentado valoriza a capacidade cognitiva do analista?

- Q4 – Você concorda que o módulo 3D do sistema apresentado oferece uma base para que novas funcionalidades e módulos possam ser acoplados em projetos futuros?

- Q5 – Você concorda que a interface de configuração da ferramenta oferece possibilidades interessantes de cruzamento de informações

pelos eixos do cubo?

- Q6 – Você concorda que as funcionalidades de zoom-in/zoom-out são interessantes para a interação com o cenário 3D?

- Q7 – Você concorda que as interações com o cenário 3D (rotação do cubo, zoom, clique do mouse) são fáceis e intuitivas?

- Q8 – Você concorda que as interações com o cenário 3D (rotação do cubo, zoom, clique do mouse) são importantes pois a alteração da forma de representação dos dados pode revelar informações novas?

- Q9 – Você concorda que a interação por clique do mouse é interessante pois apresenta informações detalhadas sobre o tráfego?

- Q10 – Você concorda que a utilização de cores para visualização é interessante e facilita o entendimento das características do tráfego?

- Q11 – Você concorda que o sistema apresentado que combina Visualização com Realidade Virtual para o monitoramento de redes é uma ferramenta interessante de apoio aos analistas de rede?

- Q12 – Você concorda que o uso da miniCAVE proporciona melhor interação com a ferramenta?

- Q13 – Você concorda que mesmo visualizando a ferramenta por monitor pode-se obter resultados interessantes?

- Q14 (questão dissertativa para livre resposta) – Qual sua opinião geral sobre o sistema apresentado?

Possíveis alternativas de resposta para as questões optativas (escolha de

uma das seguintes alternativas):

- Q1:
  - Sim; ou
  - Não.

- Q2 a Q13:
  - Concordo plenamente (CP); ou
  - Concordo um pouco (CUP); ou
  - Não tenho certeza (NTC); ou
  - Discordo um pouco (DUP); ou
  - Discordo totalmente (DT).

5.5. Resultados

Os resultados obtidos por meio dos questionários foram compilados e apresentados na Tabela 6.1.

Tabela 5.1. Resultado do questionário de avaliação do sistema para as questões optativas.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13
P1	N	CP	CP	CP	CP	CP	CP	CP	CUP	CP	NTC	NTC	CP
P2	N	CP	CP	CP	CUP	CP	CP	CP	CUP	CP	CP	CUP	CP
P3	N	CUP	CP	CP	CUP	CP	CP	CP	CP	CP	CP	CP	CP
P4	N	CP	CP	NTC	NTC	CP	CUP	CP	CP	CP	CP	CP	CP
P5	N	CP	CP	CP	CP	CP	NTC	CP	CP	CP	CP	NTC	CP
P6	N	CUP	CUP	CUP	CP	CP	CP	CP	CUP	CP	CP	NTC	CUP
P7	N	CP	CUP	CP	CP	CP	CUP	CP	CP	CP	CP	CUP	CP

Legenda dos dados apresentados na Tabela 6.1:

- P – Profissional;
- Q – Questão;
- N – Não;
- CP – Concordo Plenamente;
- CUP – Concordo um pouco;
- NTC – Não tenho certeza;

A partir da Tabela 5.1 foram gerados os gráficos da Figura 5.12.

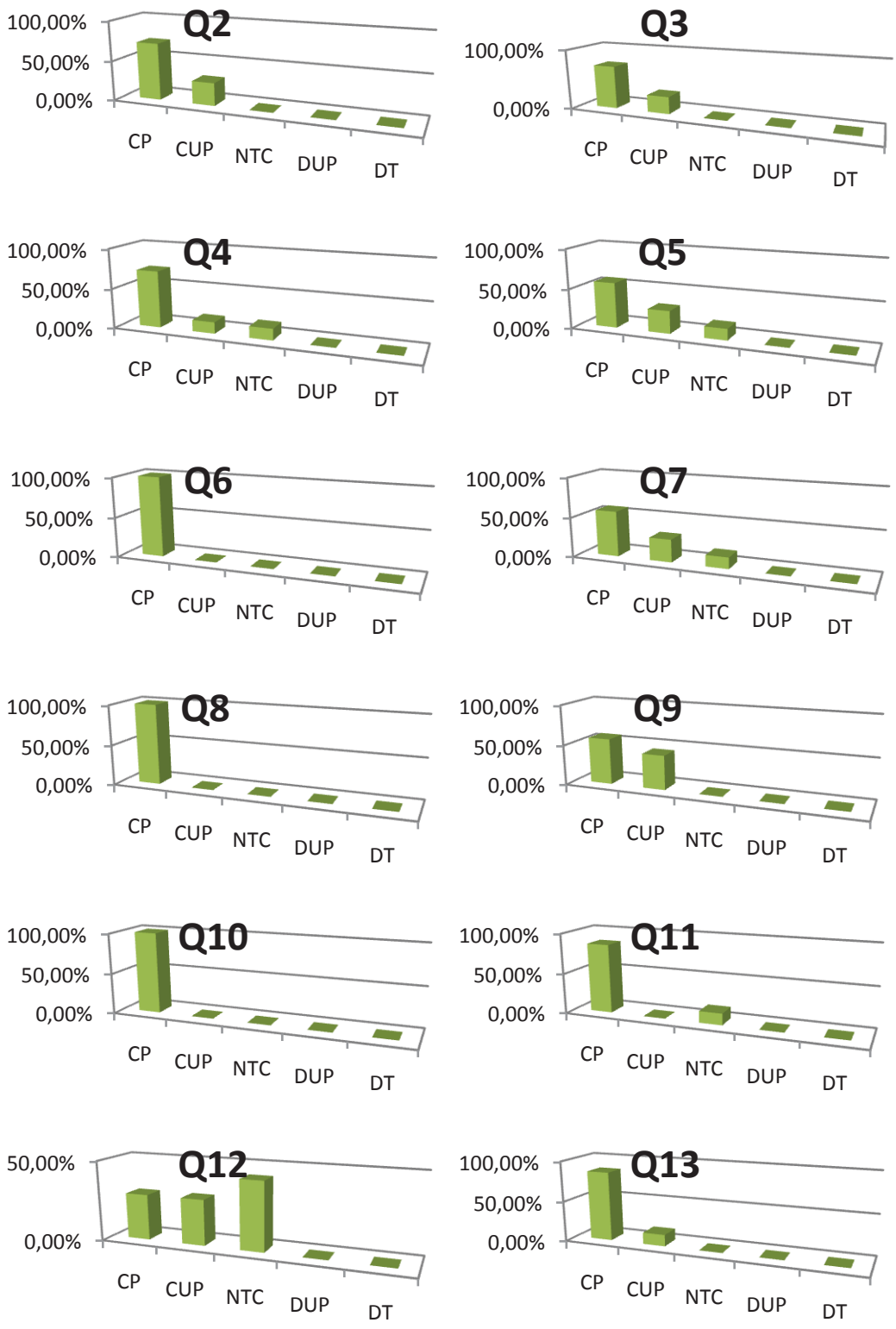


Figura 5.12 Percentagem das repostas por questão.

Além das discussões fomentadas acerta do funcionamento do protótipo da ferramenta e dúvidas levantadas e respondidas durante a apresentação da ferramenta em ambiente real, cada profissional deu um parecer livre como resposta dissertativa para a questão 14:

- Prosissional 1 – “Interessante. Poderia ser desenvolvido como aplicação para a área de rede.”

- Prosissional 2 – “O sistema possibilita a inclusão de inúmeras funcionalidades que podem ser adaptadas para cada tipo de aplicação.”

- Prosissional 3 – “ Interessante. É importante que comecemos a utilizar tecnologia de Realidade Virtual com o objetivo de trazer resultados mais eficientes na execução das mais variadas tarefas. É uma estratégia importante utilizá-la.”

- Prosissional 4 – “Trata-se de uma ferramenta interessante de visualização rápida de ataques e uso intensivo da rede”.

- Prosissional 5 – “Ferramenta muito interessante pois combina a capacidade cognitiva humana com a coleta de dados oferecida pelas ferramentas de monitoramento de tráfego existentes formando uma opção para monitoramento de múltiplos nós de rede. Buscarei utilizar ferramentas de Visualização para colaborar com a validação dessas ferramentas em desenvolvimento.”

- Prosissional 6 – “O sistema apresenta o tráfego de forma visual dando uma noção geral. As idéias apresentadas de detalhamento dos dados e na forma de apresentação poderiam tornar o sistema mais detalhado e interativo.”

- Prosissional 7 – “Existe grande potencial de desenvolvimento da ferramenta. A idéia é bastante interessante e abre possibilidades para um novo conceito em monitoramento de rede.”

Dos 7 profissionais participantes da avaliação, nenhum relatou ter experiência prévia com aplicações de VI e/ou RV para o gerenciamento de redes.

A avaliação demonstrou que, diferentemente de outras metáforas de visualização estudadas, em que o tráfego intenso torna a cena ininteligível, a visualização 3D em cubo é uma forma interessante para quaisquer situações de tráfego e quantidade de *hosts* envolvidos. Porém, em situações extremas de tráfego, ocorreram quedas do sistema, também percebidas por testes com o EtherApe. As quedas foram reduzidas utilizando-se filtros de entrada, de forma que a quantidade de dados processada fosse menor.

A representação do tráfego através dos objetos 3D despertou o senso cognitivo dos profissionais. A disposição dos objetos na cena, assim como suas cores possibilitam identificação de tráfego anômalo e de comportamentos estranhos, possivelmente maliciosos, tarefa quase impossível de se alcançar visualizando a saída textual do *Tcpdump*.

Segundo os avaliadores, as funcionalidades implementadas como *zoom-in e zoom-out* obtidas via interação por teclado é fácil e intuitiva. A interação do mouse na cena através do clique sobre os objetos é intuitiva e traz benefícios ao administrador na medida que traz informações detalhadas sobre a conexão sendo apresentada, descartando a necessidade de utilizar outras ferramentas para obter tais informações.

Percebeu-se que o efeito da oclusão dos objetos na cena pode trazer dificuldades de visualização, porém, a alteração do ponto de vista do cenário através da rotação em seus eixos reduz este problema.

De acordo com os avaliadores, a interação com a ferramenta através da projeção na miniCAVE, proporciona maior imersão do usuário na cena e pode ser utilizada como painel de monitoramento da rede em tempo real, entretanto, mesmo

através de um monitor de vídeo, o sistema pode trazer bons resultados.

Ainda, houve entendimento de que o protótipo serve de base para que novos módulos possam ser incorporados, potencializando a ferramenta, seja através de novos objetos no cenário, classificação automatizada de ataques, leitura de pacotes IPv6 ou por utilização de fluxo de dados como entrada em alternativa ao pacotes.

6. CONCLUSÕES

Foram discutidos e apresentados conceitos e dificuldades inerentes ao gerenciamento de redes, procurando encontrar pontos de interligação entre suas necessidades e as características oferecidas por sistemas de RV, as peculiaridades do sistema visual e cognitivo humano e a representação de dados por metáforas de visualização.

A existência de trabalhos correlatos na área motivou o desafio em aliar RV e VI no desenvolvimento do protótipo de uma ferramenta de visualização para auxílio ao gerenciamento de redes.

Os resultados obtidos e a avaliação do protótipo demonstrou que a utilização de conceitos de RV com VI aplicados a ferramentas de gerência de rede se apresenta como um caminho de pesquisa promissor.

Partindo-se do protótipo desenvolvido neste trabalho, e com base nos resultados de sua avaliação por profissionais da área de redes, propõe-se que novos módulos e formas de interação sejam acopladas como proposta de trabalhos futuros, tais como:

- Implementação de ajustes no código para evitar quedas do sistema por situações de tráfego extremo;

- Desenvolvimento de módulo para gerenciamento por SNMP e interação com ferramentas que utilizam esse protocolo;

- Desenvolvimento de módulo para obtenção de um gráfico hierárquico da rede, inicando seus dispositivos sendo interessante implementar novas funcionalidades de interação através do clique do mouse;

- Desenvolvimento de módulo para envio de comandos remotos a dispositivos de rede;

- Desenvolvimento de módulo de interface da ferramenta para acesso via web;

- Módulo para classificação de automática de tráfego malicioso.

REFERÊNCIAS BIBLIOGRÁFICAS

ABS-TECH. **Absolut Technologies: Visualizações Inteligentes**. Disponível em <http://www.abs-tech.com>. Acesso em 01 dez. 2009.

BALL, R.; FINK, G. A.;NORTH C.. **Home-centric visualization of network traffic for security administration.** Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, October 29-29, 2004, Washington DC, USA.

BIOLOGIA. O olho e a visão. Disponível em: <http://www.mundovestibular.com.br/articles/469/1/O-OLHO-E-A-VISAO/Paacutegina1.html>. Acesso em 10 de maio de 2011.

BUYYA,R. High performance cluster computing. Programming and Applications. Volume 2. Prentice Hall PTR.1999.

CARDOSO, Alexandre; LAMOUNIER JÚNIOR, E. A. . **Aplicações de RV e RA na Educação e Treinamento**. In: Rosa Maria Costa; Marcos Wagner S. Ribeiro. (Org.). Aplicações de Realidade Virtual e Aumentada. 1 ed. Porto Alegre-RS: Sociedade Brasileira de Computação, 2009, v. 1, p. 53-68.

CUSIN, C. A. **Um Sistema Multimodal com Movimentos Interpretados em Linguagem Natural Controlada**. Dissertação (Mestrado em Ciência da Computação) - Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2005.

CARDOSO,A. Ambientes Virtuais: projeto e implementação. PortoAlegre.. Capítulos 4 e 5. 2003.

CARMO, Ricardo Melo Casseb do. **MVC-RA:** múltiplas visões coordenadas em ambientes de realidade aumentada. 2007. 81 f. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciência da Computação, Instituto de Ciências Exatas e Naturais, Universidade Federal do Pará, Belém, 2007.

COMEAU, C. P. & Bryan, J. S. **Headsight television system provides remote surveillance**,Electronics, pp. 86-90, November, 1961.

CPLUSPLUS. C**plusplus.com - The C++ Resources Network.** Disponível em: <http://www.cplusplus.com/>. Acesso em: 10 maio. 2011.

DIAS, D.R.C; BREGA, J.R.F. **Sistema Avançado de Realidade Virtual para Visualização de Estruturas Odontológicas**. I Workshop do Programa de Pós-Graduação em Ciência da Computação (I WPPGCC). 2011

DO NASCIMENTO, H. A. D.; FERREIRA, C. B. R. **Visualização de Informações – Uma Abordagem Prática** . XXV Congresso da Sociedade Brasileira de Computação, XXIV JAI. UNISINOS, S. Leopoldo – RS, 2005.

ELLIS, S. R. What are virtual environments?, IEEE Computer Graphics and Application, 31 pp. 17-22, January, 1994.

ETHERAPE. **A graphical network monitor.** Disponível em: <http://etherape.sourceforge.net/**>.** Acesso em: 01 maio. 2011.

GNECCO,B. B & GUIMARÃES, M. P & ZUFFO, M.K. Um Framework Flexível e Transparente para Computação Distribuída de Alto Desempenho. Simpósio de Realidade Virtual. Ribeirão Preto. 2003.

GUIMARÃES, M. P. “Um ambiente para o desenvolvimento de aplicações deRealidade Virtual baseadas em aglomerados gráficos”. Tese de Doutorado. EscolaPolitécnica da Universidade de São Paulo. São Paulo. 2004.

HANCOCK, D. **Viewpoint: Virtual Reality in Search of Middle Ground**, IEEE Spectrum, 32(1):68, January, 1995.

HAND, C. Other faces of virtual reality, First International Conference MHVR’94 - Lecture Notes in Computer Science n.1077 , pp. 107-116, Ed. Springer, Moscow, Russia, September, 1994.

JACOBSON, L. **Realidade virtual em casa** . Rio de Janeiro, Berkeley, 1994.

JAVA3D.**The Source for Java Technology Collaboration.** Disponível em: <https://java3d.dev.java.net/>. Acesso em: 10 maio. 2011.

KERREN, A.,EBERT, A.,MEYER, J..**Introduction to Human-Centered Visualization Environments**. In Human-Centered Visualization Environments, volume 4417 of LNCS Tutorial, Springer, 2007.

KIRNER, C.; SISCOUTO R. A. **Fundamentos de Realidade Virtual e Aumentada**. In: Robson Siscoutto, Rosa Costa. (Org.). Realidade Virtual e Aumentada: Uma Abordagem Tecnológica. 1 ed. Porto Alegre - RS: SBC, 2008, v. 1, p. 1-20.

KIWELEKAR,A.W. & SINHA,P.H. Evaluating CORBA as a Cluster ADCOM. 9th International middleware for Heterogeneous Cluster. Conference on Bhubaneshwar. Advanced India. Computing December. And 2001. Communications. Disponível em: http://www.csse.monash.edu.au/~rajkumar/ADCOM/. Acesso em: 11 mar. 2002.

LAKKARAJU, K.; YURCIK, W.; LEE, A. J. 2004. **NVisionIP: netflow visualizations of system state for security situational awareness**. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining For Computer Security* (Washington DC, USA, October 29 - 29, 2004). VizSEC/DMSEC '04. ACM, New York, NY, 65-72. DOI= http://doi.acm.org/10.1145/1029208.1029219

LAU, S. **The Spinning Cube of Potential Doom.** Communications of the ACM, v.47

n.6, June 2004.

LIPTON, L., “Stereographics Developers Handbook.” Stereographics Corporation, 1997.

MALÉCOT, E. L. **Interactively combining 2D and 3D visualization for network traffic monitoring**, Proceedings of the 3rd international workshop on Visualization for computer security, November 03-03, 2006, Alexandria, Virginia, USA.

MEIGUINS, B.S.; MEIGUINS, A. S. G.; ALMEIDA, L.H... **Aplicações de Visualização de Informação em Ambientes de Realidade Virtual e Aumentada**. In: Rosa Maria Costai; Marcos Wagner S. R.. (Org.). Aplicações de Realidade Virtual e Aumentada. Sociedade Brasileira de Computação - SBC, 2009, Livro do Pré-Simpósio, XI Simpósio de Realidade Virtual e Aumentada p. 128-146.

NMAP. **NMap network scanning utility**. Disponível em: <http://nmap.org/>. Acesso em: 10 dez. 2011.

OPENGL. **The Industry's Foundation for High Performance Graphics.** Disponível em: <http://www.opengl.org/>. Acesso em: 10 maio. 2011.

PIMENTEL, K.; TEIXEIRA, K. **Virtual reality - through the new looking glass**. 2.ed. New York, McGraw-Hill, 1995.

RAPOSO, A. B., SZENBERG, F., GATTASS, M., CELES, W. Visão Estereoscópica, Realidade Virtual, Realidade Aumentada e Colaboração. In: A. M. S. Andrade, A. T. Martins, R. J. A. Macêdo (eds.), Anais do XXIV Congresso da Sociedade Brasileira de Computação, Vol. 2, XXIII JAI - Livro Texto, Cap. 7, p.289 - 331. SBC, Brazil, 2004 (ISBN 85-88442-95-7).

SEABRA, R. D.; SANTOS, E. T. Utilização de técnicas de realidade virtual no projeto de uma ferramenta 3D para desenvolvimento da habilidade de visualização espacial. Revista Educação Gráfica, Bauru, n.9, p.111-122, 2005.

SHNEIDERMAN, B. The eyes have it: a task by data type taxonomy for information visualizations. Proceedings of IEEE Symposium on Visual Languages , Boulder, CO,September 3-6, 1996. pp. 336-343.

SNORT. **Snort network intrusion prevention and detection system**. Disponível em: <http://www.snort.org>. Acesso em: 10 maio. 2011.

SPENSE, R. **Information Visualization.** Barcelona: Acm Press. 2001

SPENSE, R. **Information Visualization: Design for Interaction.** Barcelona: Acm Press. 2 ed. 2007

STRICKLAND, Jonathan. **How Virtual Reality Works**. 2007. Disponível em: <http://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm>. Acesso em: 01 dez. 2009.

SYMANTEC. 2009. **Symantec Global Internet Security Threat Report,** Trends for 2008. Volume XVI, April 2011. Disponível em: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>. Acesso em 02 dez. 2009.

SYMANTEC. 2011. Relatório de Ameaças à Segurança na Internet. Volume XVI, April 2011. Disponível em: <http://www.symantec.com/pt/br/business/theme.jsp?themeid=gin>. Acesso em 30 abril. 2009.

TCPDUMP. **TCPDump packet capture utility and LibPCap packet capture library**. 2011. Disponível em: <http://www.tcpdump.org>. Acesso em: 10 maio. 2011.

TRAFSHOW. **Network traffic monitoring utility.** Disponível em: <http://linux.maruhn.com/sec/trafshow.html>. Acesso em: 10 maio. 2011

TORI, R.; KIRNER, C. **Fundamentos de Realidade Virtual**. In: Romero tori; Claudio Kirner; Robson Siscouto. (Org.). Fundamentos e Tecnologia de Realidade Virtual e Aumentada. 1 ed. Sociedade Brasileira de Computação - SBC, 2006, Livro do Pré-Simpósio, VIII Symposium on Virtual Reality, v. 1, p. 2-21.

VAN RIEL J. ;IRWIN, B.. **InetVis, a visual tool for network telescope traffic analysis.** Proceedings of the 4th international conference on Computer graphics, virtual reality, visualisation and interaction in Africa, January 25-27, 2006, Cape Town, South Africa.

WISS, U., CARR, D., and JONSSON, H. **Evaluating Three-Dimensional Information Visualization Designs**: A Case Study of Three Designs. In *Proceedings of the international Conference on information Visualisation,* July 29 - 31, 1998. IV. IEEE Computer Society, Washington, DC, 137.

ANEXO A – INCORPORAÇÃO DA GLASS

Este Anexo traz a forma com que o código foi modificado para a incorporação da Glass.

```
voidTestWidget::keyPressEvent(QKeyEvent *e)
{    Ogre::Vector3 vet;
static Ogre::Vector3 posinicial = m_mainNode->getPosition();
static Ogre::Quaternion oriinicial = m_mainNode->getOrientation();
static double m_move = 5;

if ((e->key()== (Qt::Key_1 )))
    {
m_mainNode->setPosition(posinicial);
m_mainNode->setOrientation(oriinicial);
    }

if ((e->key()== (Qt::Key_Z )) )
    {
vet = glassCameraPos->getData();
vet.z +=m_move;

m_mainNode->setPosition(vet.x,vet.y,vet.z);
if (g->isMaster()){
glassCameraPos->assign(vet);
        }
```

```
    }
if ((e->key()== (Qt::Key_X )) )
    {
vet = glassCameraPos->getData();
vet.z -=m_move;

m_mainNode->setPosition(vet.x,vet.y,vet.z);
if (g->isMaster()){
glassCameraPos->assign(vet);
          }
    }

if ((e->key()== (Qt::Key_Up )) )
    {
if(g->isMaster()){
m_mainNode->pitch(Ogre::Degree(-2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion cpy(m_mainNode->getOrientation());
glassCameraPitch->assign(cpy);
    }
m_mainNode->setOrientation(this->glassCameraPitch->getData());
    }

if ((e->key()== (Qt::Key_Down )) )
    {
if(g->isMaster()){
m_mainNode->pitch(Ogre::Degree(2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion cpy(m_mainNode->getOrientation());
glassCameraPitch->assign(cpy);
```

```
    }
m_mainNode->setOrientation(this->glassCameraPitch->getData());
    }


if ((e->key()== (Qt::Key_Left )) )
    {
if(g->isMaster()){
m_mainNode->yaw(Ogre::Degree(-2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion cyaw(m_mainNode->getOrientation());
glassCameraYaw->assign(cyaw);
    }
m_mainNode->setOrientation(this->glassCameraYaw->getData());
    }

if ((e->key()== (Qt::Key_Right )) )
    {
if(g->isMaster()){
m_mainNode->yaw(Ogre::Degree(2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion cyaw(m_mainNode->getOrientation());
glassCameraYaw->assign(cyaw);
    }
m_mainNode->setOrientation(this->glassCameraYaw->getData());
    }
if ((e->key()== (Qt::Key_A )) )
    {
if(g->isMaster()){
m_mainNode->roll(Ogre::Degree(2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion crow(m_mainNode->getOrientation());
```

```
glassCameraRow->assign(crow);
    }
m_mainNode->setOrientation(this->glassCameraRow->getData());
}

if ((e->key()== (Qt::Key_D )) )
    {
if(g->isMaster()){
m_mainNode->roll(Ogre::Degree(-2.5), Ogre::Node::TS_WORLD);
        Ogre::Quaternion crow(m_mainNode->getOrientation());
glassCameraRow->assign(crow);
    }
m_mainNode->setOrientation(this->glassCameraRow->getData());
    }

if (g->isMaster()){
glassCameraPos->sendUpdate();
glassCameraYaw->sendUpdate();
glassCameraPitch->sendUpdate();
glassCameraRow->sendUpdate();
}
}
```