Segurança Baseada em Informações de Contexto para Redes Sem Fio

Francisco Gomes Milagres

Segurança Baseada em Informações de Contexto para Redes Sem Fio

Francisco Gomes Milagres

Orientador: *Prof Dr Edson dos Santos Moreira*

Monografia apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, para o Exame de Qualificação, como parte dos requisitos para obtenção do título de Mestre em Ciências de Computação e Matemática Computacional.

USP - São Carlos
Fevereiro/2003

Resumo

É notório o crescimento do segmento de computadores pessoais portáteis com características nativas de comunicação em redes sem fio em inúmeros cenários, como por exemplo, para acesso a informações em diversos outros tipos de dispositivos interligados de forma dinâmica e sem restrições de mobilidade por fios. Com o uso cada vez mais intenso destas novas ferramentas móveis para comunicação, surgem também novas ameaças contra a integridade dos dispositivos ou da informação que trafega nas redes que interconectam tais ferramentas. Com objetivo de realizar pesquisas na área de transmissão de vídeo em ambiente de redes sem fio e de forma segura, o projeto VIMOS (Vídeo, Mobilidade e Segurança) foi formado por pesquisadores membros de diversas instituições de pesquisa no país.

Visando contribuir com projetos em desenvolvimento na comunidade acadêmica brasileira como o VIMOS bem como prosseguir com as pesquisas realizadas no Laboratório Intermídia integrando diferentes linhas de pesquisa e conhecimento já adquirido, este presente trabalho foi definido. O objetivo deste trabalho é desenvolver um sistema de gerenciamento de segurança de clientes de uma rede sem fio utilizando para tal, a computação ubíqua — informações de contexto — do próprio sistema de transmissão, armazenamento e distribuição de vídeo.

Sumário

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

Introdução

" Precisamos lembrar que não somos os únicos que estamos diante de um problema quase insolúvel. Da mesma maneira que uma pipa só consegue levantar vôo quando é colocada contra o vento, mesmo o pior de nossos problemas serve para nos elevar a um degrau mais alto."

Dr. Rudolph Brasch

Desde a origem da Internet, o uso de redes de comunicação vem permitindo a efetivação de negócios e a troca de informação em velocidade e eficiência nunca antes imaginadas. Por meio destas redes, sejam elas públicas ou privadas, são também efetuadas transações entre parceiros de diferentes continentes e filiais de empresas que são localizadas a grandes distâncias. De acordo com estudos de três grandes grupos de pesquisa, o Brasil é um dos mercados mais emergentes e tende a atrair investimentos em diversos setores de tecnologia da informação.

Segundo o *International Data Corporation* (IDC)[1], devem ser investidos US$ 13,8 bilhões no Brasil até 2004 somente em comércio eletrônico. O *Yankee Group*[2] prevê um aporte de US$ 22,8 bilhões enquanto o *Forrester Research*[3] tem uma previsão ainda mais otimista para o mesmo período: US$ 59,4 bilhões.

Do mesmo modo que aumentam os investimentos nas áreas de tecnologia da informação no Brasil e em todo o planeta, observa-se também um grande

[1]Veja http://www.idcresearch.com/
[2]Veja http://www.yankeegroup.com/
[3]Veja http://www.forrester.com/

crescimento nos investimentos em áreas de comunicação móvel, redes sem fio de computadores e serviços de transmissão de dados via satélite. Este aumento facilita o acesso a informações com cada vez menos restrições físicas e maior mobilidade, seja através dos telefones celulares que permitem acesso à Internet até computadores portáteis (PDAs ou *personal digital assistants*) (Pickett et al. 2000) com dispositivos de acesso à redes públicas ou privadas de informação.

Devido ao crescimento do segmento de computadores pessoais portáteis com tais características nativas de comunicação, é cada vez mais comum pessoas portarem PDAs com capacidade de comunicação com outros computadores em rede bem como com outros dispositivos móveis como telefones celulares ou sensores e emissores de informação em instituições como universidades, empresas e hospitais, por exemplo. Com o uso cada vez mais intenso de novas ferramentas móveis para comunicação, surgem também novas ameaças e preocupações contra a integridade dos dispositivos ou da informação que trafega nas redes que interconectam tais ferramentas.

1.1 Motivação

Com o objetivo de realizar pesquisas na área de transmissão de vídeo em ambiente de redes sem fio e de forma segura, o projeto VIMOS foi formado por pesquisadores membros de diversas instituições de pesquisa no país, dentre elas UNICAMP, ICMC - USP, UFRJ, UERJ, UNIFACS e IBMEC. A principal motivação do VIMOS são os novos desafios relacionados às atuais redes sem fio de comutação de pacotes e transmissão de vídeo. (vide apêndice A)

Visando contribuir com projetos em desenvolvimento na comunidade acadêmica brasileira como o VIMOS bem como prosseguir com as pesquisas realizadas no Laboratório Intermídia integrando diferentes linhas de pesquisa e conhecimento já adquirido (vide apêndice B), este presente trabalho foi definido. A contribuição principal a ser realizada para ambos os grupos de pesquisadores em conjunto com outros trabalhos em desenvolvimento é desenvolver um sistema de gerenciamento de segurança de clientes da rede, utilizando para tal a computação ubíqua — informações de contexto — do próprio sistema de transmissão, armazenamento e distribuição de vídeo. (Goularte 2001; Santos 2003)

1.2 Organização desta monografia

O restante deste documento irá estabelecer as bases para a discussão da proposta de pesquisa a ser apresentada ao final deste. O capítulo 2 apresenta

os conceitos de redes sem fio de computadores e os protocolos de comunicação entre dispositivos em rede definidos a serem utilizados neste trabalho. O capítulo 3 apresenta o conceito de computação ubíqua e, mais especificamente, a área de pesquisa em consciência de contexto, que será a área a ser explorada durante a execução deste projeto. No capítulo 4 são apresentados resultados de pesquisas na área de segurança da informação, os padrões de gestão de segurança da informação que deverão ser adotados neste trabalho e são brevemente listadas as pesquisas mais recentes que relacionam segurança da informação em redes sem fio de computadores e computação ubíqua.

No capítulo 5 é apresentada a proposta de trabalho que é fundamentada com as informações apresentadas nos capítulos anteriores. São também detalhadas neste capítulo a metodologia de desenvolvimento, as etapas de trabalho já cumpridas, os resultados esperados e as etapas programadas com o cronograma de trabalho até a conclusão das tarefas definidas.

Este documento também inclui as referências bibliográficas consultadas para a sua pesquisa e redação e apêndices que descrevem o projeto VIMOS (apêndice A) e os projetos de pesquisa do grupo Intermídia que se relacionam com este trabalho em questão (apêndice B).

CAPÍTULO 2

Redes Sem Fio

" O segredo da guerra está nas comunicações."
Napoleão Bonaparte

As redes sem fio de dispositivos (do inglês *wireless networks*) constituíam anteriormente um nicho de mercado somente dedicado a negócios nos quais a adoção de redes tradicionais (*wired networks*) não poderiam ser instaladas por restrições de cabeamentos ou interconexões. Com a popularização do padrão para redes locais sem fio (WLANs, do inglês *Wireless Local Area Networks*) do *Institute of Electrical and Electronics Engineers*, IEEE 802.11, são cada vez mais comuns projetos de redes locais desta categoria em qualquer tipo de organização sem significativas diferenças de investimentos com relação às redes *wired*. (IEEE 1999a)

Apesar do protocolo de segurança do padrão de redes sem fio IEEE 802.11 WEP (*Wireless Equivalent Privacy*) ser vulnerável a diversos tipos de ataques e considerado fraco por muitos pesquisadores, (Temple & Regnault 2002; Arbaugh et al. 2001) este padrão de WLANs é, de acordo com pesquisa de mercado da In-Stat/MDR[1], o mais popular e responsável por absorver grande parte do mercado de redes de comunicação sem fio ainda por alguns anos. A figura 2.1 destaca o crescimento de aproximadamente 14% durante o ano de 2002 dos nós de redes sem fio instalados no mundo com o padrão IEEE 802.11 bem como os números para os padrões HomeRF (*Home Radio Frequency*) e HiperLAN (*High-Performance Radio LAN*)[2], que devido a questões de

[1] Veja http://www.instat.com
[2] Veja http://www.hiperlan2.com/

padronização, ainda está em desenvolvimento e em breve deve iniciar a disputa com os padrões IEEE por fatias de mercado.

Durante o primeiro semestre de 2002, segundo Aleen Nogee, analista senior da In-Stat/MDR, foram comercializados mais de 7 milhões de equipamentos de interconexão para acesso sem fio (AP – *access points*), que são equivalentes aos *hubs* ou *switches* nas redes tradicionais) e placas de rede compatíveis com o padrão IEEE 802.11a e 802.11b. As previsões para o ano de 2003 são ainda mais otimistas para o mercado de redes sem fio, afirma o analista Tim Mahon, do Banco de Investimentos *Credit Suisse First Boston*, que acredita que o número de equipamentos que possuam *chips* compatíveis com os padrões IEEE 802.11 — já incluindo o mais recente padrão IEEE 802.11g — alcance 11 milhões de unidades comercializadas no planeta no mesmo período. (Vaughan-Nichols 2002)

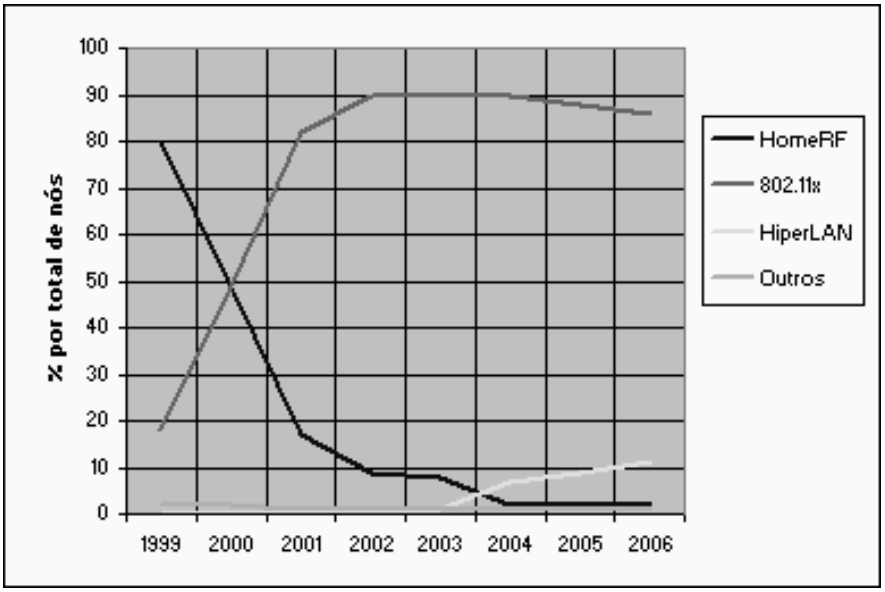

Figura 2.1: Pesquisa de mercado da In-Stat/MDR mostra que os padrões de redes sem fio IEEE 802.11x se manterão populares por alguns anos.

Nas seções a seguir serão apresentadas as classificações de redes sem fio e principais protocolos de comunicação utilizados na comunicação sem fio entre dispositivos eletrônicos como PDAs (*personal digital assistants*), (Pickett et al. 2000) computadores, periféricos e telefones celulares.

2.1 Classificações de redes sem fio

Há diferentes protocolos para comunicação entre dispositivos e periféricos de computadores e também para comunicação entre computadores em uma rede, cada um com suas restrições, áreas de alcance e outras características específicas. A figura 2.2.(a) ilustra a comunicação de um computador com

seus periféricos através de uma rede sem fios padrão *Bluetooth*[3] enquanto a figura 2.2.(b) destaca a comunicação entre computadores em uma rede sem fios *Ethernet* IEEE 802.11 com uma rede tradicional ou *wired*. (IEEE 1999b; IEEE 1999a; Haartsen 2000; Tanenbaum 2002)

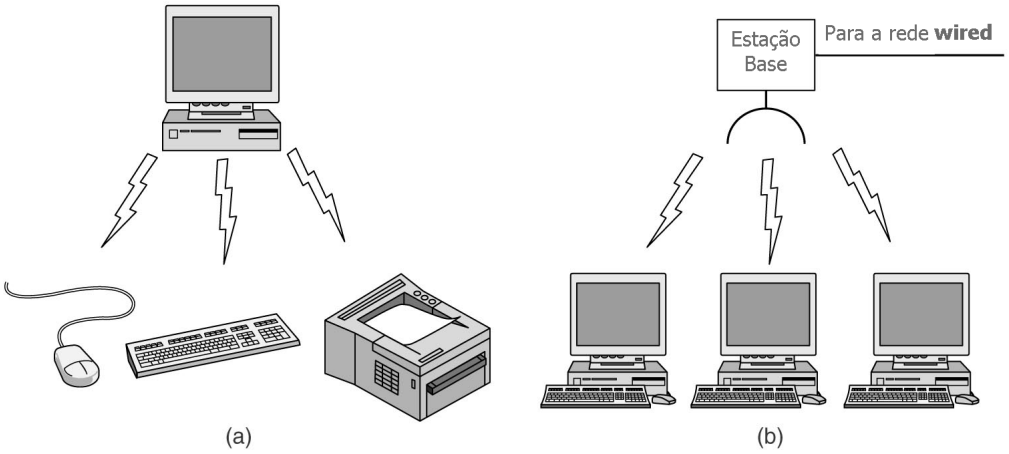

Figura 2.2: (a) Rede sem fio *Bluetooth* (b) Rede sem fio *Ethernet* IEEE 802.11

Há também duas classificações ou modos de operação para as redes sem fio, segundo o IEEE: modo infra-estruturado (BSS — *Basic Service Set*) ou *ad hoc* (IBSS — *Independent Basic Service Set*. (IEEE 1999a)

Em modo infra-estruturado, cada cliente se comunica diretamente com uma estação base ou ponto de acesso (*access point*). Esta estação base age como ponto de conexão entre a rede sem fio e a rede tradicional, de forma análoga aos roteadores em redes tradicionais. (Figura 2.3.(a))

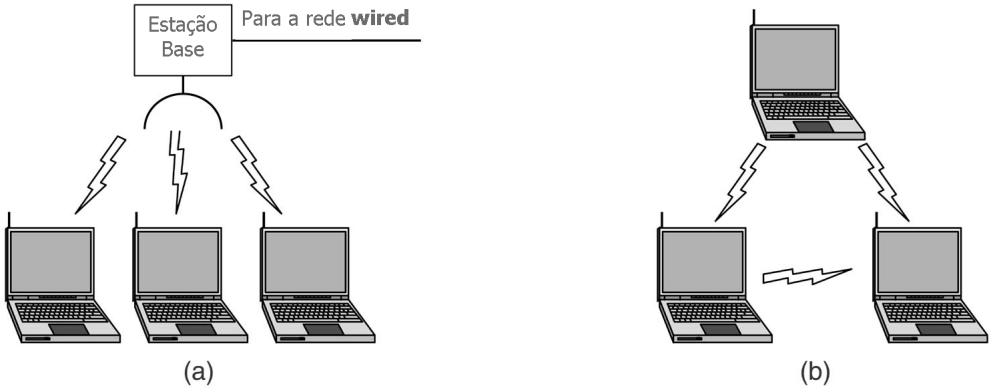

Figura 2.3: (a) Rede sem fio em modo infra-estruturado (b) Rede sem fio em modo *ad hoc*

No modo *ad hoc*, cada cliente se comunica diretamente com outros clientes da mesma rede. Este modo geralmente é destinado a comunicação de clientes que estejam na mesma área de alcance de seus sinais de comunicação ou

[3]Veja http://www.bluetooth.com/

célula e, se algum cliente na rede *ad hoc* deseja se comunicar a algum outro cliente externo à célula, um dos membros dela deve operar como um *gateway* e fazer o roteamento de tráfego adequado. (Figura 2.3.(b)) (Tanenbaum 2002)

2.2 Aplicações

Há muitas aplicações onde se podem fazer uso da flexibilidade das redes sem fio de dispositivos. Dentre as que podem ser listadas, se destacam: (Stajano & Anderson 2000)

- Coordenação de equipes em situações críticas como resgates, desastres ou confrontos;
- Troca de informações táticas em pesquisa de campo, confrontos abertos ou entre profissionais em hospitais;
- Compartilhamento de informação em salas de aula, reuniões corporativas, conferências e bibliotecas;
- Publicidade e informação direcionada em centros comerciais, competições esportivas e aeroportos.

É importante destacar que, com a adoção cada vez mais comum e a evolução tecnológica das redes sem fio, deve-se observar em breve melhorias nas relações de custo/benefício que justifiquem a escolha desta nova tecnologia em substituição às redes tradicionais.

2.2.1 Vantagens

São diversas as vantagens das redes sem fio sobre as redes tradicionais ou *wired networks*. Dentre elas, é importante destacar:

Flexibilidade de instalação: as redes sem fio, sejam elas infra-estruturadas ou *ad hoc*, possuem um diferencial com relação à facilidade de instalação já que não imprimem restrições físicas ao cabeamento e à topologia da rede como passagem de cabos e perfuração de paredes;

Alta tolerância a falhas: por serem formadas por dispositivos móveis e, em modo *ad hoc*, não possuírem um ponto central para estabelecimento de conexão, rotas dinâmicas podem ser estabelecidas em caso de entrada ou saída de clientes da rede ou ainda em caso de desastres, por exemplo;

Mobilidade: principal vantagem das redes sem fio sobre as redes tradicionais, visto que a mobilidade permite a criação de redes em locais restritos por

questões de cabeamento ou ainda por períodos limitados de tempo e com topologias flexíveis;

Redução do custo agregado: mesmo com investimento inicial maior que uma rede cabeada, estão agregadas às redes sem fio vantagens como: facilidade de expansão, menos necessidade de manutenção, robustez e outros fatores que ajudam a amenizar o investimento necessário para recuperar os recursos inicialmente empregados.

Nota-se também que, apesar de flexibilidade, alta tolerância a falhas e mobilidade, além de redução do custo agregado, há algumas restrições que devem ser observadas na adoção de redes sem fio ao invés das redes tradicionais.

2.2.2 Desvantagens

A seguir são listadas algumas das desvantagens da escolha de redes sem fio em substituição aos projetos de redes *wired*:

Localização e roteamento: a característica de mobilidade que é uma vantagem para os clientes de redes sem fio e de topologias dinâmicas dificulta a criação de algoritmos de roteamento para redes sem fio, estejam elas operando em modo *ad hoc* ou infra-estruturado;

Taxa de erros: a taxa de erros em redes sem fio é bem superior que as taxas de erro médias em redes tradicionais devido a interferências no meio de transmissão;

Taxa de transmissão: as taxas de transmissão em redes sem fio são inferiores à redes *wired*, chegando a taxas de no máximo de 20 Mbps enquanto há redes tradicionais que já alcançam taxas de transmissão da ordem de gigabits por segundo.

Segurança: intrinsecamente, os canais de comunicação sem fio são mais suscetíveis a interceptores não desejados já que o uso de ondas de rádio na transmissão de dados pode interferir em outros equipamentos. Além disso, equipamentos elétricos são capazes de interferir na transmissão acarretando em perdas de dados e alta taxa de erros na transmissão.

2.3 Principais protocolos

Nas subseções seguintes serão brevemente descritos os principais protocolos de comunicação de redes sem fio a serem utilizados no decorrer do trabalho.

2.3.1 IEEE 802.11

O padrão de redes locais sem fio do IEEE, 802.11, como já descrito anteriormente, (Vaughan-Nichols 2002) é o padrão que atualmente detém grande parte do segmento de mercado de redes locais sem fio. Definido pelo IEEE oficialmente em 1999 e já com revisões e atualizações até o ano de 2001, (IEEE 1999a) o padrão 802.11 acompanha os outros padrões 802.x estabelecendo a mesma interface com as camadas mais altas (e portanto, mantendo a conectividade com as redes cabeadas típicas) e especificando as camadas física e de acesso ao meio (MAC).

O primeiro dos padrões a se estabelecer foi o 802.11a, que é compatível com o original 802.11 nas camadas de acesso ao meio (MAC), apesar de em nível físico utilizar a banda de 5 GHz para transmissão de dados, possibilitanto taxas de transmissão na ordem de 20 Mbps. A segunda das revisões deste padrão foi a IEEE 802.11b, que trabalha com a previsão de uma alta taxa de transmissão a 2,4 GHz, que é a freqüência mais utilizada atualmente. (IEEE 2001)

Como meio de transmissão deste sinal sem fio das redes IEEE há algumas opções. O infravermelho, que é pouco usado, já que por sua faixa de freqüência ser pouco inferior à freqüência da luz visível, os sinais transmitidos devem ser de alta intensidade para não permitir a interferência da luz. Pode-se conseguir altas taxas de transmissão chegando em 10 Mbps e a distância máxima de comunicação não ultrapassa cerca de 30 metros mesmo com potentes dispositivos de ampliação de sinal. Pode-se utilizar também a transmissão por infravermelho com feixe direto — linha de visada desobstruída, semelhante à comunicação dos controles remotos ou com radiação a todas as direções por reflexão em superfícies e lentes de banda larga.

A transmissão via laser pode alcançar distâncias de 200 a 300 metros com visada direta, podendo ser utilizado, por exemplo, como conexão entre duas redes locais em prédios diferentes. As freqüências de rádio são as mais utilizadas em redes sem fio de computadores. Por sua natureza, ela é adequada tanto para ligações ponto a ponto quanto para ligações multiponto. As redes sem fio baseadas em radiodifusão são uma alternativa viável onde é restrita a instalação de cabos metálicos ou de fibra óptica. Seu emprego é particularmente importante para comunicações entre computadores portáteis em um ambiente de rede local móvel.

2.3.2 Bluetooth

Bluetooth é um sistema sem fio de telecomunicações de curto alcance — geralmente em torno de 10 metros — utilizado para conexão entre periféricos

e dispositivos sem fio de baixo consumo de energia a computadores, PDAs e telefones celulares, por exemplo. O principal objetivo da criação do padrão foi a substituição de cabos por ondas de rádio-freqüência de modo que pudesse ser difundido o mercado de dispositivos móveis. (Haartsen et al. 1998; Haartsen 2000)

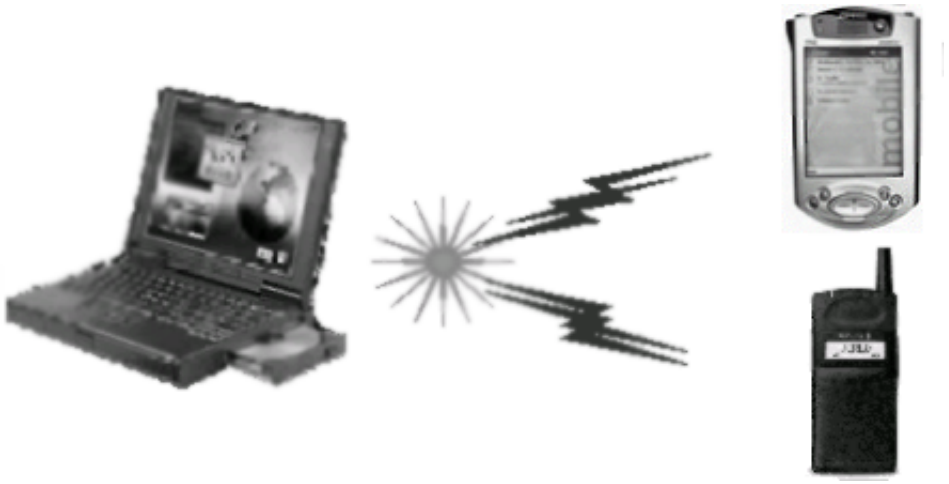

Figura 2.4: Um exemplo de uso do *Bluetooth*: a sincronização de dados entre um *notebook*, um PDA e um celular.

O *Bluetooth SIG* (*Special Interest Group*)[4] foi formado em 1998 por empresas como Ericsson, IBM, Intel, Nokia, Toshiba, 3Com e Motorola, sendo em breve adotado por mais de 1600 empresas no mundo. Entre suas principais características, pode-se destacar:

- Propriedade *ad hoc* nativa, o que permite rápida conexão e troca de dados entre dispositivos sem presença de um ponto de conexão ou central da rede sem fio;
- Projeto para baixo consumo de energia, o que facilita seu uso em dispositivos portáteis como celulares, PDAs e *notebooks*. A figura 2.4 ilustra uma situação de sincronização de informações entre os três dispositivos citados;
- Apesar da baixa taxa média de transmissão de dados (cerca de 1 Mbps), o *Bluetooth* permite até 59 conexões simultâneas em dispositivos em rede — *piconets* — e utiliza conceitos para reduzir chances de colisão de frequências de transmissão como alterações de suas frequências a cada envio de pacote de dados, que são também de tamanho reduzido;
- Para identificação dos dispositivos *Bluetooth*, o protocolo reconhece a identificação de cada cliente da rede com seu PIN (*Personal Identification Number*).

[4]Veja http://www.bluetooth.com/

Por ser um sistema de transmissão sem fio de baixo consumo de energia e restrito a pequenas áreas de alcançe, o *Bluetooth* tem se firmado como um padrão para comunicação sem fio em dispositivos de tamanho e capacidades reduzidos como telefones celulares, PDAs e computadores portáteis bem como tem sido apontado como uma tendência para a conexão de dispositivos domésticos em um futuro próximo, como geladeiras, fornos de microondas e aparelhos de TV, por exemplo.

2.4 Considerações finais

Este capítulo apresentou os conceitos básicos de redes sem fio de dispositivos, os números de pesquisas mais recentes que mostram o avanço deste setor de mercado. Foram também apresentadas aplicações destes padrões, suas vantagens, desvantagens e descrições dos padrões de transmissão de dados sem fio a serem utilizados neste trabalho: o IEEE 802.11 e o *Bluetooth*.

CAPÍTULO
3

Computação Ubíqua

" Não sendo capaz de controlar os eventos, eu me controlo. Me adaptarei a eles caso eles não se adaptem a mim."
Michel de Montaigne

Os protótipos foram a primeira tentativa de aproximar da realidade imagens para apresentação de conceitos. Com a apresentação de um novo conceito, Weiser introduziu a área de computação ubíqua e mostrou um cenário onde computadores podem prover informações e serviços quando e onde forem necessários. (Weiser 1991) A visão de Weiser descreveu uma proliferação de dispositivos de diferentes tamanhos como os pessoais (*inch-scale*), de médio porte (*foot-scale*) e grandes e de uso coletivo (*yard-scale*). Essa proliferação de dispositivos realmente aconteceu com os dispositivos usados normalmente, como por exemplo os PDAs, *laptops* e lousas eletrônicas. (Baldochi et al. 2002)

Segundo Weiser, criador da expressão *ubíqua* (do latim *ubique*, que está ao mesmo tempo em toda a parte, onipresente), (Ferreira 1986) esse novo conceito se propõe a expandir do paradigma de interação tradicional entre homem e máquina — teclado, *mouse* e monitor — através do modelo humano de interação natural.

3.1 Os conceitos de Mark Weiser

Em interações, pessoas não usam somente a fala mas também o olhar, a escrita, gestos e qualquer outra forma de comunicação implícita que tenha como objetivo a demonstração de algo que desejamos. Do mesmo modo que é

realizada de forma transparente pelos seres humanos esta rica comunicação, a principal motivação da computação ubíqua se destaca, já que na inspiração da comunicação humana, fazer a revolução da comunicação entre homem e máquina. (Weiser 1993)

Para justificar seus novos conceitos, Weiser apresentou concepções de novos dispositivos computacionais. Logo, foram desenvolvidos dispositivos de três tamanhos distintos: os chamados *Boards*, os quais podem ser comparados a lousas eletrônicas, *Pads*, análogos à cadernos de anotações e finalmente os dispositivos menores denominados *Tabs*, semelhantes a blocos de notas. (Figura 3.1)

Figura 3.1: Um exemplo de *Tab* (*Palm Tungsten T*) e um de *Pad* (*Tablet PC*).

Após alguns anos da apresentação das idéias de Weiser, atualmente é possível notar o uso cada dia mais comum das ferramentas idealizadas pelo pesquisador, como PDAs, *laptops* e lousas eletrônicas, apesar da infra-estrutura necessária ao suporte à computação móvel contínua, responsável pela interação constante entre usuário e dispositivos computacionais, ainda estar em desenvolvimento.

A influência de fatores chave para o desenvolvimento da computação ubíqua — o entendimento dos hábitos humanos, a criação de novos dispositivos interativos e a conexão e interação entre os dispositivos para permitir uma experiência realística — aliada ao avanço de tecnologias de reconhecimento e percepção, é essencial para a evolução das diferentes formas de captura de informações exigidas pela computação ubíqua. (Abowd & Mynatt 2002) Desse maneira, é possível fornecer capacidades bastante próximas à comunicação humana e efetivamente incorporar essas ações implícitas à computação ubíqua. Assim, a comunicação realizada entre o ambiente e o usuário também observará grandes melhorias.

Os novos aspectos de computação apresentados por Weiser foram idealizados com o surgimento de novas aplicações computacionais para explorar o uso de novos dispositivos como os apresentados e exemplicados na figura 3.1. O

desenvolvimento destas aplicações está associado a três áreas principais que são atualmente as principais motivações de pesquisa na área de computação ubíqua (*ubiquitous computing* ou *ubicomp*) e que serão descritas nas seções a seguir: interfaces naturais, captura e acesso de atividades humanas e computação consciente de contexto. (Abowd & Mynatt 2000) Convém destacar que devido à restrição de escopo deste trabalho, a seção de *Consciência de contexto* será a de principal destaque.

3.1.1 Interfaces naturais

De acordo com pesquisas recentes, interfaces computacionais que suportam formas naturais mais próximas das humanas de comunicação estão substituindo elementos do tradicional paradigma de interação homem-máquina das interfaces gráficas (*Graphical User Interfaces* ou GUIs). Estas interfaces são de fácil uso e já estabelecidas a alguns anos, além disso são fáceis de serem utilizadas e possibilitam tarefas como autoria sem grandes mudanças na sua forma de execução. Para o desenvolvimento de interfaces naturais mais efetivas, duas questões importantes devem ser consideradas: (Abowd & Mynatt 2000)

Tipos Básicos de Dados Naturais: para facilitar o desenvolvimento de aplicações com interfaces naturais, a manipulação de outras formas de entradas como *mouse* e teclado devem ser permitidas. As informações que são geradas em tais interfaces como áudio, vídeo, escrita e demais sensores precisam ser consideradas como tipos básicos no desenvolvimento de sistemas interativos;

Tendência a Erros por Interação Baseada em Reconhecimento: quando se utilizam interfaces naturais em tarefas baseadas em reconhecimento, surge um novo conjunto de problemas — elas permitem novos e diferentes tipos de problemas. A manipulação de erros em tecnologias de reconhecimento é um problema bem conhecido e é tema de pesquisa em tópicos como:

- Redução de erros: pesquisas para aperfeiçoamento de técnicas de reconhecimento, redução ou eliminação de erros;
- Descoberta de erros: antes mesmo do sistema ou do usuário serem capazes de efetuar alguma ação referente a algum erro, um deles deve ser comunicado a respeito da ocorrência dele;
- Infra-estrutura reusável para correção de erros: *kits* de ferramentas devem fornecer componentes reusáveis e são mais úteis quando há a existência de uma classe de problemas conhecidos;

3.1.2 Captura e acesso

São diversas as situações que nos levam a tentar absorver o máximo de informação de qualquer forma que ela seja nos apresentada, seja em qualquer forma cognitiva. Ferramentas projetadas para facilitar o trabalho de memorização suportam captura e acesso automatizados de diversos tipos das experiências mais tradicionais, como uma aula ou uma reunião de negócios, por exemplo. Assim, podemos nos preocupar apenas em fazer relações entre informações, resumir e interpretar tópicos, enquanto a ferramenta se encarrega da gravação das informações. (Abowd & Mynatt 2000; Abowd & Mynatt 2002)

A área de *Captura e Acesso* é definida como sendo responsável por preservar a gravação de alguma experiência de modo que futuramente ela possa ser retomada. Dentre os resultados de pesquisas desta área, pode-se citar o *PhoneSlave* e *Xcapture*, que capturam áudio; o *LiveBoard*, que auxilia na captura de informações de reuniões e, mais recentemente, o *Classroom2000* para captura de aulas acadêmicas. Há ainda exemplos de sistemas de captura individual, como o *Marquee*, o *Filochat*, *The Audio Notebook* e o *NotePals*. O primeiro sistema a prover tanto captura individual quanto em grupo foi o *StuPad* (*Student Notepad*). (Abowd & Mynatt 2002)

Um exemplo prático de uso, por exemplo, de um sistema de captura como o *Classroom2000*, seria nas revisões do conteúdo apresentado em sala de aula. Além da possibilidade de revisão completa da aula, seria possível a sua indexação de acordo com tópicos de relavância ou através de um resumo do conteúdo apresentado, por exemplo. (Abowd & Mynatt 2000).

3.1.3 Consciência de contexto

Ao interagirmos com outras pessoas, transmitimos idéias, pensamentos e opiniões, conseqüentemente, reagimos de maneira apropriada. Como fatores que possibilitam tal interação, podem ser citados uma rica e compartilhada linguagem e o entendimento implícito e recíproco do cotidiano. Logo, quando conversamos com outras pessoas, compartilhamos informações implícitas referentes à situação, ou seja, o contexto da situação. No entanto, ao interagirem com pessoas, os computadores não são capazes de tirar total proveito da situação contextual justamente por não haver uma interação rica como ocorre na interação entre pessoas. (Dey 2001; Morse, Armstrong, & Dey 2000) Portanto, a utilização de contexto torna-se relevante. Para que o conceito de *Consciência de Contexto* possa ser apresentado, antes devem ser definidos *contexto*, sua *representação* e sua *categorização*:

Definindo contexto

O primeiro trabalho a adotar o termo "consciência de contexto" foi o de Schilit e Theimer, os quais se referiam a contexto como localização, identidades de pessoas e objetos e mudanças desses objetos (Dey 2001). Outras abordagens definem contexto como o ambiente ou situação em que uma determinada interação ocorre. Dey ainda argumenta que tanto a definição de Shilit (a qual enfatiza que *"os principais aspectos do contexto são: onde você está, quem está com você, e quais recursos estão próximos"*) quanto a de Pascoe (*"contexto é o subconjunto de estados físicos e conceituais de interesse de uma entidade particular"*) são muito específicas, já que contexto é toda situação relevante a uma aplicação e seu conjunto de usuários.

Desse modo, Dey e Abowd definem contexto como *"qualquer informação que possa ser usada para caracterizar a situação de uma entidade. Uma entidade é uma pessoa, lugar ou objeto que é considerado relevante para a interação entre um usuário e uma aplicação, incluindo ambos"*. Se uma parte de informação pode ser usada para caracterizar a situação de um participante em uma interação, então tal informação é contexto. (Dey 2001; Dey & Abowd 2000)

Representação de contexto

Relacionada à definição de contexto está a questão de como representá-lo. Sem boas representações para contexto, desenvolvedores de aplicações são forçados a desenvolver esquemas limitados de armazenamento e manipulação de informações relevantes. Com o surgimento de representações mais sofisticadas, uma gama maior de capacidades surgirá e a separação da percepção de contexto da reação será facilitada.

Categorias de contexto

Para que seja possível diferenciar entre o que é contexto ou não, é proposta uma categorização de tipos de contexto capazes de ajudar projetistas de aplicações a descobrirem partes prováveis do contexto. Visando categorizar os tipos de contexto, Dey e Abowd definiram cinco dimensões conhecidas como *os Cinco W's*, as quais são descritas em seguida: (Dey & Abowd 2000; Abowd & Mynatt 2000; Truong, Abowd, & Brotherton 2001)

Who: (quem) os sistemas atuais focam a interação na identidade de um usuário em particular, raramente incorporando informações referentes a outras pessoas também pertencentes ao mesmo ambiente;

What: (o quê) a interação dos sistemas convencionais supõe o que o usuário está fazendo ou não suporta tal suposição. Perceber e interpretar a ativi-

dade humana não é um problema elementar, apesar disso, dispositivos que suportem contexto devem incorporar interpretações de atividades humanas para serem capazes de proverem informação relevante;

Where: (onde) é a dimensão mais explorada. Em particular, pesquisas apontam as relações de noções da dimensão *Where* e *When* mescladas, com objetivo de agregar novas funcionalidades;

When: (quando) embora poucos sistemas tenham suporte a esta dimensão, é geralmente utilizado em associação com *Where* para, por exemplo, determinar onde e quando um usuário realizou determinada ação;

Why: (porquê) é talvez a mais desafiante de todas as dimensões a ser captada, já que geralmente está associada a reconhecimento de informações vitais do usuário como humor, batimento cardíaco ou pressão arterial, por exemplo.

Definindo consciência de contexto

A primeira definição de *Consciência de Contexto* (Dey 2001) foi restrita a aplicações que são simplesmente informadas sobre contexto para se adaptarem de acordo com estas informações. Segundo Dey e Abowd, definições anteriores podem ser incluídas em duas categorias: o uso de contexto e adaptação ao contexto e ainda acrescentam que, nas duas classes as definições são muito específicas e definem de maneira geral um sistema consciente de contexto como sendo *"um sistema que utiliza contexto para prover informação relevante e/ou serviços ao usuário, onde a relevância depende da tarefa do usuário"*. Considerando então esta definição, três aspectos importantes nesta área de computação ubíqua devem ser identificados: (Morse, Armstrong, & Dey 2000; Dey & Abowd 2000)

- Apresentação de informações e serviços ao usuário;
- Execução automática de um serviço a um usuário;
- Vinculação do contexto à informação para futuras consultas.

3.2 Considerações finais

Neste capítulo foram apresentados os conceitos de computação ubíqua que são necessários para a apresentação da proposta de trabalho. É possível perceber que a área de pesquisa definida para este projeto — a consciência de contexto — tem como alvo a representação de informações de contexto de

qualquer tipo de sistema, neste caso, de um sistema computacional com ações e reações humanas em tempo real. Para este trabalho, conceitos apresentados como a representação de contexto em *Cinco W's* são essenciais na representação de informação natural para adaptação de segurança de acordo com o contexto do ambiente em questão.

CAPÍTULO 4

Segurança da Informação

" Segurança é ortogonal a funcionalidade – se um sistema de proteção funciona adequadamente, isto não significa que ele seja seguro."
Bruce Schneier

Segundo pesquisa mais recente sobre segurança da informação no país, realizada pela *Módulo Security Solutions S.A.*[1], 78% das empresas no Brasil reconhecem que tiveram perdas financeiras devido a alguma violação de segurança no último ano, porém, 56% ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança da informação. Em 22% das organizações que conseguiram contabilizar estes valores, o total de perdas registradas foi de R$ 39,7 milhões.

A preocupação crescente pela segurança da informação foi redobrada no ano de 2002 a partir de ameaças que não podiam sequer ser previstas, como a que se abateu sobre o *World Trade Center* (WTC) e o Pentágono em Setembro de 2001, quando muitas empresas perderam, além de seus funcionários, todas as suas bases de dados e sistemas de informação devido a um ataque terrorista.

Em 21 de Janeiro de 2003, durante a *Microsoft Exchange Conference* (MEC) 2002, a *Aladdin Knowledge Systems*[2], em pesquisa avaliou opiniões de mais de 500 profissionais de tecnologia da informação sobre os planos de gastos com tecnologia de segurança de rede para o ano de 2003. Em contraste aos resultados amenos do mercado em 2002, 67% dos entrevistados revelaram seus planos em aumentar gastos com segurança.

[1] Veja http://www.modulo.com.br/pdf/oitava-pesquisa-modulo.pdf
[2] Veja http://www.ealaddin.com/news/2003/all/mec.asp

O objetivo deste capítulo é apresentar os conceitos principais de segurança da informação, os padrões de gestão de segurança de informação para tecnologia da informação definidos para o Brasil e também para o exterior, bem como pesquisas nas áreas específicas a serem pesquisadas durante este trabalho: redes sem fio e computação ubíqua.

4.1 Definição de segurança

Para apresentar as ferramentas e estudos nos quais serão baseados as justificativas deste trabalho, inicialmente deve-se definir o conceito de segurança da informação. São cinco [3] os requisitos básicos para definir a segurança de um sistema, apresentados graficamente na figura 4.1 e descritos a seguir: (Spafford & Garfinkel 1996)

Figura 4.1: Os princípios básicos para a definição de segurança.

Autenticidade: a certificação que um sistema se comporta como esperado por usuários autorizados é garantia de autenticidade;

Privacidade: consiste na proteção de acesso a leitura ou cópia de informação por quem não está explicitamente autorizado pelo seu proprietário;

Controle de acesso: consiste na definição e controle de regras para acesso a um sistema ou informação;

Integridade: proteção de qualquer informação ou sistema contra remoção ou alteração de qualquer forma sem a permissão explícita de seu proprietário;

[3] Veja http://www.nsa.gov/isso/ (NSA – *National Security Agency* — Agência de Segurança dos EUA)

Não repúdio: como garantia contra negação de execução de alguma tarefa, a característica de não repúdio deve ser implementada de modo a permitir também auditoria de acessos, sejam autorizados ou não, a uma informação ou sistema.

É importante destacar que não há uma definição estabelecida do que seja segurança da informação e há conflitos de conceitos na literatura com relação aos pontos básicos para sua garantia. De acordo com Spafford, ainda deve-se incluir, por exemplo, a característica de disponibilidade para que seja garantida a segurança de um sistema —- proteção a um sistema de modo que ele não se degrade ou se torne indisponível sem autorização — conceito este que para a definição acima é considerado segurança no funcionamento (*safety*) e não de segurança no uso (*security*). (Spafford & Garfinkel 1996; Pickett et al. 2000)

A seguir serão apresentados os padrões para gestão de segurança da informação e que serão utilizados neste trabalho na definição de regras do perfis de segurança a serem modelados e implementados.

4.2 Códigos de prática para segurança

Atualmente, a segurança da informação é preocupação de todos que integram as organizações e sua cadeia de valor e a ausência de processos e controles de segurança pode resultar em diversos impactos, como por exemplo, perda de faturamento, aumento de custos e conseqüente perda de valor da empresa. Por estas razões, uma dúvida que sempre acompanha os profissionais responsáveis pela administração de segurança da informação nas organizações é como medir e verificar se as recomendações e controles usados são efetivos e completos.

Com base nesta necessidade, o BSI (*British Standard Institute* — Instituto Britânico de Padrões)[4] criou a norma BS 7799, (BSI 1998) considerada até o momento o mais completo padrão para o gerenciamento de segurança. Com ela é possível ter recomendações para implementar um sistema de gestão de segurança baseado em controles definidos por normas internacionais. Em dezembro de 2000, a Parte 1 da BS 7799 se tornou norma oficial da ISO (*International Organization for Standardization*)[5] sob o código ISO/IEC 17799. (ISO 2000) Em agosto do ano seguinte, o Brasil adotou esta norma ISO como seu padrão, através da ABNT (Associação Brasileira de Normas Técnicas)[6], sob o código NBR ISO/IEC 17799 (2001). (ABNT 2001)

[4]Veja http://www.bsi-global.com/
[5]Veja http://www.iso.ch/
[6]Veja http://www.abnt.org.br/

O objetivo do código 17799 é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança da informação em qualquer tipo de organização. A norma estabelece uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas da gestão da segurança, facilitando testes e medições dos processos e provendo confiança nos relacionamentos entre as organizações. A norma BS 7799, que deu origem aos padrões ISO e NBR e compõe a base destas, é dividida em duas partes:

4.2.1 Código de prática para gestão da segurança da informação

Esta parte contém recomendações de segurança divididas em dez seções com requisitos gerais de vários grupos de controles e devem ser usados de acordo com o escopo onde será aplicada a gestão de segurança da informação. A seguir serão listados os tópicos que compõem esta primeira parte: (BSI 1998)

- Política de Segurança
- Segurança Organizacional
- Classificação e Controle dos Ativos de Informação
- Segurança em Pessoas
- Segurança Física e do Ambiente
- Gerenciamento das Operações e Comunicações
- Controle de Acesso
- Desenvolvimento e Manutenção de Sistemas
- Gestão de Continuidade do Negócio
- Conformidade

De acordo com a necessidade, os controles acima devem ser definidos na gestão de segurança da informação para implementação deste trabalho.

4.2.2 Especificação de sistema de gestão de segurança da informação

Esta parte da norma define um SGSI – Sistema de Gestão de Segurança da Informação, que é um objeto de certificação. A adoção da BS 7799 –

Parte 2 como norma ISO está em estudo e não há previsão para conclusão desse trabalho em curto prazo. Diversas empresas no mundo já foram certificadas na norma BS 7799, como bancos, empresas de telecomunicações, indústrias, prestadores de serviços, consultorias e organizações governamentais. São empresas que optaram pela certificação por vários motivos e benefícios que variam desde a redução de prêmios de seguro, até uma estratégia de propaganda utilizando a certificação como diferencial competitivo e como demonstração pública do compromisso da empresa com a segurança das informações de seus clientes. (BSI 1998) De acordo com a BSI, há somente duas empresas no Brasil certificadas com a norma britânica de segurança, dentre elas a empresa de informações financeiras SERASA e a empresa de segurança da informação Módulo Security Solutions.

Nas seções seguintes serão apresentados brevemente os resultados dos principais trabalhos em segurança nas duas áreas de pesquisa que serão integradas neste trabalho: as redes móveis sem fio de computadores e a computação ubíqua.

4.3 Segurança em redes sem fio

Como mencionado no capítulo 2, são conhecidas diversas vulnerabilidades dos protocolos de comunicação em redes sem fio. (Temple & Regnault 2002; Arbaugh et al. 2001) O protocolo WEP (*Wireless Equivalent Privacy*), que deveria garantir segurança às redes sem fio, foi desde a primeira versão do padrão IEEE 802.11 até a sua mais recente revisão bastante criticado e atualmente é alvo de estudos de pesquisadores que implementam neste protocolo diretivas específicas de segurança de acordo com suas necessidades. (IEEE 1999a; IEEE 2001)

4.4 Segurança em computação ubíqua

Em 2000, Frank Stajano e Ross Anderson publicaram o primeiro trabalho que tratou de questões de segurança na recente área de pesquisa de computação ubíqua. (Stajano & Anderson 2000) A apresentação de um cenário considerado para muitos como sendo futurista como a integração de dispositivos como DVDs, aparelhos de TV, computadores e sensores em residências em trabalhos de Weiser em 1993, (Weiser 1993) neste trabalho de 1999 houveram novas considerações de segurança que antes não foram abordadas.

Stajano e Anderson relacionaram neste trabalho os processos de um sistema de computação úbiqua com algumas necessidades para que um nível de segurança possa ser garantido: disponibilidade, autenticidade, integridade

e sigilo. Cada uma destas características podem ser garantidas com protocolos apresentados pelos pesquisadores neste trabalho, que posteriormente teve uma nova publicação ampliada e posteriormente um livro dedicado ao assunto. (Stajano 2001; Stajano 2002)

4.5 Considerações finais

Este capítulo apresentou resultados de recentes estudos e pesquisas na área de segurança, que mostram que esta área em pesquisas bem como no mercado é um foco de estudiosos e investidores, em grande parte preocupados com os números que mostram um constante aumento de riscos contra seus ativos.

Foram apresentados neste capítulo também os padrões de gestão de segurança da informação que servirão de base para a definição da política de uso e segurança na modelagem e implementação deste trabalho. Brevemente também foram apresentadas pesquisas em segurança nas duas áreas que devem ser integradas de modo a prover segurança para o sistema de transmissão de vídeo a ser assegurado neste trabalho com uso de informações de contexto: as redes móveis sem fio e a computação ubíqua. É importante destacar que estudos aprofundados de protocolos de segurança estabelecidos nestas duas áreas são resultados esperados deste trabalho e não foram detalhados neste documento.

CAPÍTULO 5

Proposta de Trabalho

Conforme apresentado nas seções anteriores, estão em constantes avanços e são temas de pesquisas as áreas de redes móveis e sem fio, computação ubíqua e segurança da informação. Visando a integração de pesquisas destas áreas, a contribuição direta com o Projeto VIMOS (vide apêndice A) no qual pesquisadores do Intermídia estão inseridos e a continuidade das pesquisas em desenvolvimento pelo mesmo grupo de pesquisas com integração de áreas paralelas de pesquisa (vide apêndice B), este trabalho é proposto.

O presente trabalho tem como objetivo estudar as principais pesquisas em desenvolvimento e protocolos estabelecidos para segurança de redes móveis e sem fio de computadores e em computação ubíqua, definir, implementar e validar um módulo denomidado *Gerente de Segurança* para um ambiente de comunicação de dispositivos sem fio utilizando para tal gerenciamento das informações de contexto do próprio sistema.

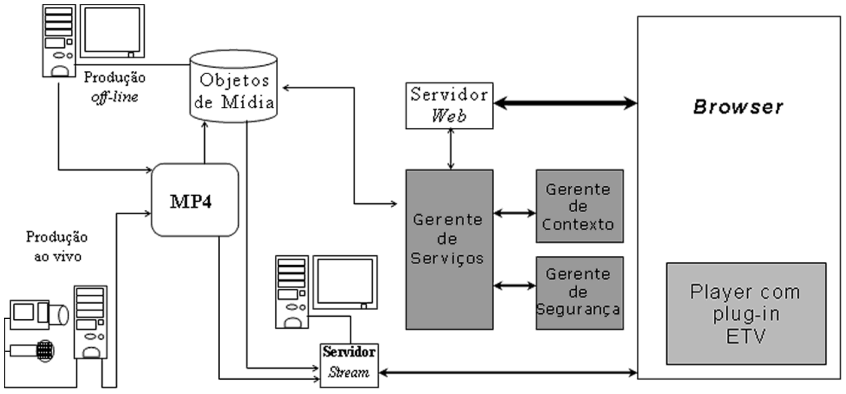

Figura 5.1: Modelo resumido dos Gerentes de Serviço, Contexto e Segurança.

A figura 5.1 ilustra de forma resumida o cenário onde será aplicado este

trabalho. (Goularte 2001) Em princípio, o sistema a ser desenvolvido será composto basicamente de três módulos integrados: o Gerente de Contexto, Gerente de Segurança e o Gerente de Serviços. O Gerente de Contexto tem como objetivo realizar as funções de obtenção de informações da infra-estrutura, do ambiente e dos usuários do sistema através de sensores e efetuar uma filtragem, a qual decidirá quais informações capturadas são referentes ao contexto. O Gerente de Serviços proverá serviços como controle de qualidade de transmissão de vídeo baseado em informações de contexto do sistema.

Todas as informações trocadas entre os gerentes utilizarão formato XML (W3C 2000) — padrão adotado pelo grupo para o desenvolvimento do gerente de serviços — e transmitidas aos Gerentes de Segurança e de Serviços de acordo com a demanda, visto que o contexto é variável e somente válido por um determinado período de tempo. É importante destacar que as informações de contexto geradas farão parte de um documento contextual que será armazenado em uma base de dados para manutenção de um histórico. É um requisito que esta base seja compartilhada por todos os módulos do sistema e deverá ser utilizada, por exemplo, para históricos referentes a infra-estrutura, ambiente e usuários do próprio sistema. Poderão ser usados também para análises da rede através de cálculos estatísticos ou para tomada de decisão de perfis de segurança relacionadas às ações prévias de um determinado usuário, bem como oferecer aos clientes do sistema serviços específico de acordo com suas escolhas antecedentes referentes a uma determinada classe de serviços.

O Gerente de Segurança, que é o objetivo deste trabalho, será responsável pelos perfis de segurança atribuídos a ações de usuários, utilização de dispositivos e disponibilidade do sistema de acordo com informações de contexto. Para tal, o Gerente de Segurança terá inicialmente definidos os perfis para cada tipo de cliente, aplicação e usuário do sistema de transmissão e recepção de vídeo em rede. De acordo com informações de contexto disponibilidadas pelo Gerente de Contexto e de serviços da infra-estrutura do Gerente de Serviços, o Gerente de Segurança deverá controlar o acesso aos recursos e auditar o sistema de acordo com as primitivas definidas em cada um dos perfis de segurança e com a política de uso e segurança definidas com auxílio de uma recomendação estabelecida. (ABNT 2001)

Os módulos de Gerência de Contexto e de Gerência de Serviços estão sendo implementados respectivamente em trabalhos de mestrado e doutorado e os resultados, em conjunto com o do presente trabalho, serão integrados no projeto VIMOS. (Goularte 2001; Santos 2003)

5.1 Resultados esperados

São diversos os resultados a serem alcançados até a conclusão deste trabalho. A seguir, são listados os principais deles a serem atingidos:

- O presente trabalho deve apresentar em sua conclusão um módulo de gerenciamento de segurança para um sistema de transporte e armazenamento de multimídia utilizando informações de contexto e serviços providos por módulos em desenvolvimento paralelo a este; (Goularte 2001; Santos 2003)

- Como contribuição ao projeto VIMOS (vide apêndice A), este trabalho deve possuir características de portabilidade e prover controle dos níveis de segurança estabelecidos para este projeto, de modo a, de acordo com a necessidade, ser integrado parcial ou completamente à aquele;

- Para apresentação dos resultados à comunicade científica e de pesquisa nas áreas relacionadas a este projeto, devem ser submetidos a periódicos e eventos de relevância publicações apresentando os resultados deste trabalho.

5.2 Etapas já realizadas

Durante as fases de projeto que antecederam a dissertação deste documento, foram realizadas etapas que serão listadas abaixo e que são consideradas importantes na contribuição para a execução deste trabalho de mestrado.

Definição de principais protocolos e padrões: de acordo com estudos de mercado e definições de projetos com os quais o presente trabalho está integrado, foram definidos, dentre os diversos existentes, os procolos e padrões alvo a serem estudados neste trabalho e que foram apresentados neste documento;

Modelagem do cenário a ser aplicado: com a definição dos projetos com os quais esta pesquisa está integrada, foi definido o cenário de aplicação deste (figura 5.1) bem como os trabalhos de mestrado e doutorado do mesmo grupo de pesquisa que estão sendo desenvolvidos em conjunto; (Goularte 2001; Santos 2003)

5.3 Ferramentas de apoio

A seguir serão brevemente descritas algumas das ferramentas de apoio à execução deste trabalho:

5.3.1 Unified Modeling Language (UML)

A *Unified Modeling Language* (UML)[1] é uma linguagem para a modelagem de sistemas que define uma série de diagramas apropriados a visualização, especificação, construção e documentação de artefatos de softwares com processos como definição de casos de uso, hierarquias básicas de classes, entre outras.

5.3.2 Linguagem de Programação Java

Linguagem de programação da *Sun Microsystems*[2] utilizada no desenvolvimento de sistemas orientados a objetos[3]. Das vantagens de sua utilização, convém mencionar: a existência de ferramentas de edição, desenvolvimento e compilação gratuitas; um padrão apropriado e popular para documentação do código fonte (JavaDoc) e a fácil portabilidade e reutilização de código de implementações entre diversos sistemas operacionais.

5.3.3 XML - eXtenxible Markup Language

A *Extensible Markup Language* (XML)(W3C 2000) é uma linguagem de marcação criada pelo *World Wide Web Consortim* (W3C)[4] para descrever conteúdo e fornecer sua semântica. Deriva do padrão *SGML* (*Standard Generalized Markup Language*, que descreve uma linguagem aberta não proprietária para estrutura de documentos.

É importante destacar que outras ferramentas para conclusão deste trabalho e que não foram previstas e descritas nesta seção previstas devem surgir e serão documentadas na dissertação de mestrado.

5.4 Metodologia

No intuito de alcançar os objetivos deste trabalho, serão descritas a seguir as etapas a serem realizadas durante este trabalho:

[1] Veja http://www.uml.org
[2] Veja http://www.sun.com
[3] Veja http://java.sun.com
[4] Veja http://www.w3c.org

(1) Acompanhamento dos trabalhos em desenvolvimento: com objetivo de acrescentar conhecimentos ao grupo de pesquisa e também de auxiliar o desenvolvimento integrado dos módulos projetados para o projeto VIMOS (apêndice A), este trabalho está em desenvolvimento de forma cooperativa com outros projetos no Laboratório Intermídia (apêndice B); (Goularte 2001; Santos 2003)

(2) Levantamento e Análise de Requisitos: a tarefa de análise de requisitos é um processo de descoberta, refinamento, modelagem e especificação. O passo inicial será identificar os casos de uso do Gerente de Segurança e suas interações de acordo com a norma de gerenciamento de segurança da informaçao NBR 17799. (ABNT 2001) A partir deste ponto, será possível ter uma visão mais precisa das funcionalidades que o ambiente deve fornecer suporte para que decisões mais explícitas possam ser tomadas durante as fases de projeto e implementação;

(3) Estudo e avaliação de ferramentas de apoio: após o levantamento e análise dos requisitos do módulo de gerenciamento de segurança proposto, deve ser feita uma avaliação das ferramentas a serem utilizadas durante o trabalho para a criação e implementação do módulo de gerência de segurança;

(4) Projeto e Modelagem: nessa fase será realizada a modelagem do Gerente de Segurança de acordo com o levantamento e a especifição de requisitos. Para tal, deve ser usada a linguagem de modelagem UML (*UML - Unified Modeling Language*), que, em conjunto com a especificação e modelagem dos outros módulos em desenvolvimento, (Santos 2003) deve ser, de acordo com a necessidade, adaptada;

(5) Implementação do Modelo: consiste da implementação em linguagem de programação Java do módulo de gerenciamento de segurança, executada a partir da especificação e análise de requisitos de projeto;

(6) Teste e Validação da Implementação: após implementação e testes isolados do módulo de gerência de segurança, serão efetuados testes para a validação em ambiente de execução utilizando-se uma rede *ad hoc*. O Gerente de Segurança também deverá ser integrado com os trabalhos já desenvolvidos por outros pesquisadores que contribuem para o projeto VIMOS; (Goularte 2001; Santos 2003)

(7) Dissertação de Mestrado: durante a maior parte do período de execução deste trabalho, a dissertação de mestrado estará sendo escrita, incluindo os resultados parciais que devem ser consolidados em artigos científicos;

(8) Apresentação da Dissertação: a previsão para apresentação dos resultados deste trabalho de mestrado é o mês de Dezembro.

5.5 Cronograma

O cronograma apresentado na tabela 5.1 descreve as atividades a serem realizadas no período de Março a Dezembro de 2003, no desenvolvimento dos trabalhos para a conclusão das atividades no programa de Mestrado em Ciências de Computação. Está prevista também a submissão de artigos para publicação em eventos e periódicos de relevância nas áreas de pesquisa relacionadas ao trabalho em questão.

2003										
Etapa/Mês	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
(1)	•	•	•	•	•	•	•	•		
(2)		•	•							
(3)		•	•	•						
(4)		•	•	•	•	•				
(5)				•	•	•	•	•	•	
(6)							•	•	•	
(7)			•	•	•	•	•	•	•	
(8)										•

Tabela 5.1: Cronograma de trabalho.

Referências

ABNT (2001, Agosto). NBR ISO/IEC 17799:2000 — Código de prática para a gestão da segurança da informação.

Abowd, G. D. & E. D. Mynatt (2000). Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction 7*(1), 29–58.

Abowd, G. D. & E. D. Mynatt (2002). The human experience. *IEEE Pervasive Computing 2*(1), 48–57.

Ambrósio, D. R. (2002). Alternativas de implementação de reconhecimento de padrões para agentes móveis em ambiente de segurança computacional. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Arbaugh, W. A. et al. (2001, Março). Your 802.11 wireless network has no clothes.

Baldochi, L. A. et al. (2002, Outubro). Computação ubíqua: Fundamentos e exemplos. Notas didáticas do ICMC, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Bernardes, M. C. (1999). Avaliação do uso de agentes móveis em segurança computacional. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

BSI (1998). BS 7799:1998 Revision 1 — British standard code of practice for information security management.

Cansian, A. M. (1997). *Desenvolvimento de um sistema adaptativo de detecção de intrusos em redes de computadores*. Tese de doutorado, Instituto de Física de São Carlos, São Carlos.

Cicilini, R. (1994). Desenvolvimento de um agente snmp para plataformas rodando DOS. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Dey, A. K. (2001). Understanding and using context.

Dey, A. K. & G. D. Abowd (2000, Abril). Towards a better understanding of context and context-awareness.

Faria, G. B. et al. (2001, Outubro). Uso de perfis em aplicações de televisão interativa conscientes de contexto. *Anais do VII Simpósio Brasileiro de Sistemas Multimídia e Hipermídia (*SBM*idia) 7*(1), 139–154.

Ferreira, A. B. O. (1986). *Novo Dicionário Aurélio da Língua Portuguesa*. Nova Fronteira.

Garção, A. S. et al. (2002, Janeiro). Annex to DEEPSIA's deliverable 4 - system architecture. Technical report, DEEPSIA Consortium. IST Project-1999-20483.

Goularte, R. (1998). Utilização de meta-dados no gerenciamento de acesso a servidores de vídeo. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Goularte, R. (2001, Maio). *Um Ensaio Sobre a Manipulação de Vídeo Interativo Utilizando MPEG4 e MPEG-7*. Qualificação de doutorado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Goularte, R. & E. S. Moreira (2002, Outubro). Representação de objetos de mídia em aplicações conscientes de contexto em TV interativa. *Anais do VIII Simpósio Brasileiro de Sistemas Multimídia e Hipermídia (*SBM*idia) 8*(1), 150–165.

Haartsen, J. et al. (1998, Outubro). Bluetooth: Vision, goals, and architecture. *Mobile Computing and Communications Review 2*(4), 38–45.

Haartsen, J. C. (2000, Fevereiro). The Bluetooth radio system. *IEEE Personal Communications 7*(1), 06–14.

Herrera, J. A. F. (2002). Uso de data warehousing e data mining na busca de relações e conhecimento em um ambiente de comércio eletrônico. Qualificação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Herrera, J. A. F. et al. (2002, Novembro). A model for data manipulation and ontology navigation in DEEPSIA project. *Proceedings of the First Seminar on Advanced Research in Electronic Business 1*(1), 139–145.

IEEE (1999a). IEEE Std 802.11 (ISO/IEC 8802-11: 1999) - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specification.

IEEE (1999b). IEEE Std 802.3 CSMA/CD (Ethernet).

IEEE (2001). IEEE Std 802.11 (ISO/IEC 8802-11: 1999) - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specification

— Amendment 3: Specification for operation in additional regulatory domains.

ISO (2000, Dezembro). ISO/IEC 17799:2000 — Code of practise for information security management.

Lieira, J. F. (1995). Utilização de áudio e vídeo em sistemas gerenciadores de redes de computadores. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Milagres, F. G. et al. (2002, Novembro). Dealing with security within DEEPSIA project. *Proceedings of the 2002 WSEAS International Conference on Information Security 1*(1), 2431–2439.

Milagres, F. G. & E. S. Moreira (2001, Novembro). Detecção de intrusões com auxílio de agentes móveis. *Revista Eletrônica de Iniciação Científica 1*(2).

Milagres, F. G., E. S. Moreira, J. P. Pimentão, & P. A. C. Sousa (2002, Novembro). Security analysis of a multi-agents system in EU's DEEPSIA project. *Proceedings of the First Seminar on Advanced Research in Electronic Business 1*(1), 155–162.

Moraes, S. (1995). Voz em sistemas computacionais: projeto e implementação de módulos de processamento de voz em gerenciamento de redes. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Morishita, F. T. (1997). Uma avaliação evolutiva dos protocolos de gerenciamento da internet: SNMPv1, SNMPv2 e SNMPv3. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Morse, D. R., S. Armstrong, & A. K. Dey (2000). The what, who, where, when, and how of context awareness.

Oda, C. S. (1994). Desenvolvimento de um sistema monitor gráfico baseado em protocolo de gerenciamento SNMP. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Oliveira, F. A. (2002). Extração de informação sobre produtos comercializados em páginas brasileiras para a alimentação de catálogos eletrônicos. Qualificação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Pickett, J. P. et al. (2000). *The American Heritage Dictionary of the English Language* (4 ed.). Houghton Mifflin Company.

Power, R. (2002). CSI/FBI Computer crime and security survey. *Computer Security Issues & Trends Computer Security 8*(1), 24.

Reami, E. R. (1998). Especificação e prototipagem de um ambiente de gerenciamento de segurança apoiado por agentes móveis. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Santos, R. F. (2003, Fevereiro). Gerenciamento de informações de contexto para ambientes móveis. Qualificação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Schneier, B. (2000). *Secrets and Lies. Digital Security in a Networked World* (1 ed.). John Wiley & Sons, Inc.

Spafford, G. & S. Garfinkel (1996, Abril). *Practical UNIX & Internet Security* (2 ed.). O'Reilly & Associates.

Stajano, F. (2001). The resurrecting duckling - what next? *Proceedings of the Eighth Security Protocols Workshop – Lecture Notes in Computer Science 2133*, 204–214.

Stajano, F. (2002). *Security for Ubiquitous Computing* (1 ed.). John Wiley & Sons, Inc.

Stajano, F. & R. J. Anderson (2000). The resurrecting duckling: Security issues for ubiquitous computing. *Proceedings of the Seventh Security Protocols Workshop – Lecture Notes in Computer Science 1796*, 172–182.

Tanenbaum, A. (2002). *Computer Networks* (4 ed.). Prentice-Hall, Inc.

Tavares, D. M. (2002). Avaliação de técnicas de captura para sistemas detectores de intrusão. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Tavares, D. M. et al. (1999). ACME! (Advanced Counter-Measures Environment) - um mecanismo de captura e análise de pacotes para aplicação em detecção de assinaturas de ataque. *Anais do Primeiro Simpósio de Segurança em Informática 1*(1), 39–46.

Temple, R. & J. Regnault (2002). *Internet and Wireless Security* (1 ed.). Number 4 in BTexact Communications Technology. United Kingdom: The Institution of Electrical Engineers (IEE).

Bonifácio Jr, J. M. (1998). Sistemas de segurança distribuído: integração de firewalls com sistemas de detecção de intrusão. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Pereira Filho, S. F. (2001). Avaliação para ambientes servidores para agentes móveis. Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação, São Carlos.

Santa Eulália, L. A. et al. (2002, Setembro). Using ontologies for intelligent information retrieval in an e-commerce application case study. *Proceedings of the Fourth European Conference on Product and Process Modelling in the Building and Related Industries 1*(1), 277–284.

Truong, K. N., G. D. Abowd, & J. A. Brotherton (2001, Outubro). Who, what, when, where, how: Design issues of capture & access applications. *Proceedings of Ubiquitous Computing (UBICOMP) 2201*, 209–224.

Vaughan-Nichols, S. J. (2002, Novembro). Bull market for IEEE 802.11 WLAN chisets. *IEEE Computer 35*(11), 17–19.

W3C (2000). eXtensible Markup Language (xml) 1.0. http://www.w3.org/TR/REC-xml.

Weiser, M. (1991, Setembro). The computer for the twenty-first century. *Scientific American 265*(3), 94–10.

Weiser, M. (1993). Some computer science issues in ubiquitous computing. *Communications of the ACM 36*(7), 75–84.

APÊNDICE

A

Projeto VIMOS
Vídeo, Mobilidade e Segurança

Com o objetivo de fornecer suporte a aplicações de vídeo em ambiente de redes sem fio e de forma segura, o projeto VIMOS foi formado, incluindo em sua equipe pesquisadores pertencentes a instituições como UNICAMP, ICMC - USP, UFRJ, UERJ, UNIFACS e IBMEC. A principal motivação do VIMOS são os novos desafios relacionados às atuais redes de comutação de pacotes e transmissão de vídeo. A transmissão de mídia contínua corresponde a grande parte do tráfego nestas redes. No entanto, o transporte deste tipo de mídia requer a garantia da qualidade do serviço oferecido ao usuário, através de protocolos e mecanismos de QoS (*Quality of Service*).

Outra característica relevante dessas redes é a mobilidade, que proporciona a ubiqüidade computacional, resultando em transparência na disseminação da informação. No entanto, esta característica traz consigo problemas relacionados ao volume de tráfego gerado e ao nível de qualidade de serviços exigido. Em contrapartida, a apresentação do vídeo no cliente móvel pode ser afetada pela natureza *ad hoc* do acesso à rede. Como possível solução deste problema, pode-se usar aplicações conscientes de contexto de forma a melhorar a interação, tanto do usuário com o sistema quanto deste com a rede, o que, por sua vez, incrementa a complexidade do problema de modelagem e avaliação da rede.

Diante de todos esses desafios, o projeto VIMOS se propõe a estudar, propor e avaliar modelos de caracterização e ferramentas de geração de tráfego. Através desta abordagem, pretende-se alcançar os seguintes objetivos:

- Criar um ambiente de pesquisa em transporte de vídeo em redes móveis;

- Assegurar a formação e o aperfeiçoamento dos participantes do projeto;
- Realizar estudos comparativos e avaliações, tanto qualitativas quanto quantitativas, de modelos, mecanismos, arquiteturas, serviços e protocolos relacionados aos temas abordados;
- Desenvolver aplicações de transmissão de vídeo que utilizem as características de mobilidade, consciência de contexto, qualidade de serviço e segurança;
- Prototipar os resultados obtidos na pesquisa em sistemas de TV Interativa.

Em relação aos resultados e impactos esperados, podem ser exemplificados a formação de recursos humanos para a nova sociedade de informação como avanços para a pesquisa de redes de computadores no Brasil, benefícios para provedores de serviços Internet tais como vídeo sob demanda, educação à distância, comércio móvel, tele-medicina, e, potencialmente, inovativos modelos de negócios para a área em questão.

O Laboratório Intermídia, através de seus pesquisadores, pretende especificar um ambiente de testes, definir uma metodologia e implementar experimentações utilizando protocolos de transmissão de vídeo (MPEG-4 e MPEG-7) que permitem adaptações dinâmicas de fluxo dependentes do contexto de aplicações e das condições da rede. Deste modo, as principais tarefas que deverão ser executadas são as seguintes:

- Apresentação de uma proposta para a modelagem do ambiente interativo consciente de contexto, utilizando a linguagem UML (*Unified Modelling Language*);
- Implementação de ferramentas de controle dinâmico do ambiente de modo que a transmissão responda a variações de parâmetros como carga do servidor, da rede ou suporte do cliente de recepção, entre outros;
- Definição de perfis de segurança para as aplicações e clientes inseridos no ambiente VIMOS para controle de requisitos de segurança.

Como infra-estrutura tecnológica para desenvolvimento dos projetos, deverão ser utilizados os padrões MPEG-4 (para transporte), MPEG-7 (para descrição de objetos de mídia e metadados) e MPEG-J (para inserção de funções interativas) da família de padrões MPEG (*Moving Picture Expert Group*). O ambiente de testes será composto por servidor de vídeo MPEG-4 baseado em tecnologia ENVIVIO [1] e o acesso a este ambiente será feito através de PDAs e *notebooks* capazes de acessar redes sem fio IEEE 802.11 e *Bluetooth*.

[1] Veja http://www.envivio.com

APÊNDICE

B

Projetos de Pesquisa do Grupo Intermídia

O grupo de pesquisas do Laboratório Intermídia no Instituto de Ciências Matemáticas e de Computação (ICMC) [1] da Universidade de São Paulo (USP) vem desenvolvendo projetos em duas frentes importantes na área da computação: Segurança de Redes de Computadores e Sistemas Multimídia Distribuídos.

Tendo iniciado seus trabalhos no início da década de 1990 com projetos relacionados ao gerenciamento de redes de computadores (Oda 1994; Cicilini 1994; Lieira 1995; Moraes 1995; Morishita 1997), o grupo de pesquisas já desenvolveu pesquisas na área de segurança computacional com sistemas detectores de intrusões com suporte de redes neurais para o reconhecimento de padrões de ataques (Bonifácio Jr 1998; Cansian 1997; Tavares et al. 1999) e aplicando a tecnologia de agentes móveis para o gerenciamento da segurança (Reami 1998) e verificação de anomalias. (Bernardes 1999; Milagres & Moreira 2001) Também foram desenvolvidas pesquisas sobre ambientes servidores para agentes móveis (Pereira Filho 2001) e ferramentas que conferem inteligência a tais agentes (Ambrósio 2002) bem como estudos para implementação de sistemas detectores de intrusão em dispositivos de segmentação de redes (*switches*). (Tavares 2002)

A segunda frente de trabalho desenvolve pesquisas em sistemas multimídia distribuídos aplicando estudos em padrões para a representação de informações e metadados na identificação de fluxos de mídia contínua e técnicas adequadas para transmissão e distribuição de vídeo na Internet. (Goularte

[1] Veja http://www.icmc.usp.br/

1998) Estudos com padrões de transmissão de vídeo com controle qualidade de serviço e informações de contexto em multimídia são também temas de pesquisas desenvolvidas no Intermídia, que aplica os resultados destas em projetos de televisão interativa e multimídia distribuída. (Faria et al. 2001; Goularte 2001; Goularte & Moreira 2002)

A partir do segundo semestre de 2001, o Laboratório Intermídia, juntamente com o NUMA (Núcleo de Manufatura Avançada)[2] e financiados pelo CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico)[3] (CNPq-680263/01-2), passou a integrar a iniciativa brasileira de cooperação com o projeto internacional DEEPSIA (*Dynamic on-linE IntErnet Purchasing System based on Intelligent Agents*) [4].

O projeto DEEPSIA foi estabelecido por um consórcio entre diversas instituições e empresas européias com o apoio da *Information Society Technologies* (IST)[5], tendo como objetivo principal promover o ingresso das Pequenas e Médias Empresas (PMEs) no comércio eletrônico, utilizando uma solução centrada no comprador e tratando as PMEs não somente como fornecedoras de produtos, mas também como consumidoras de bens e serviços. (Garção et al. 2002) A participação em tal projeto motivou o grupo a instituir uma nova frente de trabalho relacionada ao estudo e ao desenvolvimento de soluções otimizadas para sistemas de Comércio Eletrônico, com a aplicação de técnicas apropriadas para as tarefas de busca, classificação, armazenamento e extração de informações sobre produtos.

Os principais projetos correlatos que estão em fase de conclusão de desenvolvimento pelo grupo são segurança para o sistema multi-Agentes DEEPSIA (Milagres et al. 2002; Milagres, Moreira, Pimentão, & Sousa 2002), mineração de dados nas informações do catálogo (Herrera 2002), implementação de técnicas de extração de informações de produtos em páginas da Web brasileira para inclusão em catálogos eletrônicos (Oliveira 2002) e navegação em ontologias visando facilitar a interação do usuário com a ontologia dos produtos (Herrera et al. 2002; Santa Eulália et al. 2002).

[2]Veja http://www.numa.org.br/
[3]Veja http://www.cnpq.br/
[4]Veja http://www.deepsia.com/br/
[5]Veja http://www.cordis.lu/ist/