FERNANDO FROTA REDÍGOLO

ARQUITETURA DE AMBIENTES DE IPTV COM SERVIÇOS DE
PRIVACIDADE

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

São Paulo
2008

FERNANDO FROTA REDÍGOLO

ARQUITETURA DE AMBIENTES DE IPTV COM SERVIÇOS DE
PRIVACIDADE

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

Área de Concentração:
Sistemas Digitais

Orientadora: Profa. Dra. Tereza Cristina
Melo de Brito Carvalho

São Paulo
2008

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 22 de agosto de 2008.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Redigolo, Fernando Frota

**Arquitetura de ambiente de IPTV com serviços de privacidade / F.F. Redigolo. -- ed.rev. -- São Paulo, 2008.
107 p.**

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

1. Redes multimídia 2. Privacidade I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

AGRADECIMENTOS

Primeiramente à professora Tereza Cristina, pela orientação, apoio, confiança e paciência, não só neste trabalho como em diversos aspectos da minha vida profissional e pessoal.

À minha esposa Carine, um agradecimento especial, pelo apoio incondicional e pelo encorajamento constante durante os altos e baixos deste trabalho. Sem seu amor, atingir a reta final desta jornada teria sido uma tarefa impossível.

Aos meus pais, Régis e Célia, e ao meu irmão Eduardo, não só por contribuir de longe com pensamentos positivos e orações nos últimos tempos, mas por toda a contribuição na minha formação ao longo da minha vida (e por entender o meu “sumiço” nos últimos meses).

Aos meus colegas do LARC, pelo apoio neste e nos outros projetos de que faço parte, para que este trabalho pudesse se tornar uma realidade. Em particular, meus agradecimentos ao Prof. Wilson, pela confiança depositada em mim desde a época do mestrado, ao Diego, pela paciência infinita em me iluminar nos detalhes do projeto, e aos outros membros dos projetos de IPTV.

Agradeço também aos colegas do IBM Thomas J. Watson Research Center , José Eduardo, pela oportunidade profissional dada, e Frank Schaffa, pelas orientações nos primórdios deste trabalho.

À Ericsson Telecomunicações do Brasil e à Ericsson Research da Suécia, pelo suporte no desenvolvimento deste trabalho.

Por fim, agradeço a todos os meus amigos que estiveram sempre por perto, mesmo nos momentos em que encontrava distante. O que seria de mim sem meus amigos! Um particular agradecimento ao André, pela camaradagem e incentivo aqui e na terra do tio Sam....as discussões regadas a sorvete certamente têm seu lugar na história deste trabalho.

RESUMO

A crescente digitalização das mídias, disponibilidade de banda larga e convergência tecnológica possibilitam o surgimento de novos serviços, como o IPTV (*Internet Protocol TeleVision*), que visa disponibilizar serviços de televisão via TCP/IP sobre uma rede de banda larga privativa. Sem os devidos cuidados, entidades ou indivíduos monitorando o tráfego deste serviço passam a ter uma maior quantidade de informações sobre os indivíduos que os utilizam, muitas vezes violando a privacidade dos mesmos em um ambiente no qual tradicionalmente não há esta preocupação, como a sala de estar ou outro ambiente doméstico. O objetivo deste trabalho é propor uma arquitetura de IPTV que apresente mecanismos capazes de garantir um nível de privacidade maior do que o existente em sistemas de IPTV tradicionais, de maneira a inviabilizar para um observador o correlacionamento entre um usuário do serviço e os conteúdos por ele assistidos.

ABSTRACT

The increase in media digitalization, broadband availability and technological convergence, allows new services, such as the IPTV (Internet Protocol Television) service, which offers television-related services over a private broadband TCP/IP network. Without proper care, entities or individuals monitoring these services' traffic obtain a large amount of information on the service users, and could violate their privacies in an environment in which traditionally there is no such preoccupation, like in a living-room or another domestic environment. The goal of this work is to propose an IPTV architecture capable of guaranteeing a higher privacy level than the existing in traditional IPTV systems, so that it is not viable for an observer to correlate a service user with the content he/she watches.

LISTA DE ILUSTRAÇÕES

Figura 1 – Classificação dos Canais (14).....	21
Figura 2 – Arquitetura de referência de um sistema de IPTV (13, 14, 15)	25
Figura 3 – Módulos do Dispositivo de Domínio	28
Figura 4 – Módulos do HDG.....	29
Figura 5 – Principais Operações em um serviço de IPTV	32
Figura 6 – Acesso ao EPG.....	34
Figura 7 – Requisição de Conteúdo	35
Figura 8 – Modelo de Comunicação e Aspectos de Privacidade (30).....	40
Figura 9 – Aparelho do IBOPE para coleta de parâmetros de audiência de TV.....	53
Figura 10 – Identificação de elementos na arquitetura utilizados na criação do perfil de um usuário	54
Figura 11 – Exemplo de Criação de Perfil de Usuário: Identificação dos Canais.....	55
Figura 12 – Exemplo de Criação de Perfil de Usuário: Correlação com Metadados.....	56
Figura 13 – Arquitetura de IPTV Modificada para ambiente de privacidade	65
Figura 14 – Exemplo de EEPG em XML, com descrição simplificada de um canal e seu conteúdo.....	70
Figura 15 – Autenticação na Arquitetura Proposta.....	73
Figura 17 – Acesso ao EEPG.....	74
Figura 17 – Comparação entre requisição de conteúdo original e proposto	76
Figura 18 –Indireção de Requisições	77
Figura 16 – Exemplo de regras de personalização automática do EEPG.....	79
Figura 17 – Janela de configuração de privacidade	82
Figura 18 – Ambiente de Testes para a solução de privacidade.....	83
Figura 19 – EPG do Microsoft Windows Vista com programação de 9/3/2008	84
Figura 20 – Aplicativo FreeGuide com programação de 9/3/2008	85
Figura 21 – Exemplo de observações de um usuário, de acordo com o gênero, desconsiderando o tráfego P2P	87
Figura 22 – Exemplo de observações de um dado usuário, de acordo com o gênero, considerando o tráfego P2P	88

LISTA DE TABELAS

Tabela 1 – Exemplo de Classificação de Canais	23
Tabela 2 – Exemplo de Criação de Perfil de Usuário: Correlação com dados do Usuário.....	57
Tabela 3 – Exemplo de Criação de Perfil de Usuário: Adição de periodicidade.....	57
Tabela 4 – Gêneros utilizados na análise	85
Tabela 5 – Relação dos requisitos funcionais atendidos pela arquitetura proposta..	89

LISTA DE ABREVIATURAS E SIGLAS

<i>ADSL</i>	<i>Asymmetric Digital Subscriber Line</i>
<i>AOL</i>	<i>America OnLine</i>
<i>API</i>	<i>Application Programming Interface</i>
<i>ARP</i>	<i>Address Resolution Protocol</i>
<i>COE</i>	<i>Council Of Europe</i>
<i>CP</i>	<i>Content Provider</i>
<i>DNS</i>	<i>Domain Name System</i>
<i>DRM</i>	<i>Digital Rights Management</i>
<i>DVD</i>	<i>Digital Versatile Disk</i>
<i>DVMRP</i>	<i>Distance Vector Multicast Routing Protocol</i>
<i>DWDM</i>	<i>Dense Wavelength Division Multiplexing</i>
<i>EPG</i>	<i>Electronic Program Guide</i>
<i>FIDIS</i>	<i>Future of IDentity in the Information Society</i>
<i>FTTH</i>	<i>Fiber To The Home</i>
<i>GMPLS</i>	<i>Generalized Multi Protocol Label Switching</i>
<i>HDG</i>	<i>Home Domain Gateway</i>
<i>HSI</i>	<i>High-Speed Internet</i>
<i>IBGE</i>	<i>Instituto Brasileiro de Geografia e Estatística</i>
<i>IBOPE</i>	<i>Instituto Brasileiro de Opinião Pública e Estatística</i>
<i>IGMP</i>	<i>Internet Group Management Protocol</i>
<i>IP</i>	<i>Internet Protocol</i>
<i>IPTV</i>	<i>Internet Protocol TeleVision</i>
<i>ISMA</i>	<i>Internet Streaming Media Alliance</i>
<i>LAN</i>	<i>Local Area Network</i>
<i>LS</i>	<i>License Server</i>
<i>MAC</i>	<i>Medium Access Control</i>
<i>MAN</i>	<i>Metropolitan Area Networks</i>
<i>MPEG2</i>	<i>Moving Picture Experts Group - 2</i>
<i>MPLS</i>	<i>Multi Protocol Label Switching</i>
<i>NAT</i>	<i>Network Address Translator</i>
<i>OECD</i>	<i>Organization for Economic Cooperation and Development</i>

<i>P2P</i>	<i>Peer-to-Peer</i>
<i>P3P</i>	<i>Platform for Privacy Preferences</i>
<i>PIM – SSM</i>	<i>Protocol Independent Multicast – Source Specific Multicast</i>
<i>PON</i>	<i>Passive Optical Network</i>
<i>PPV</i>	<i>Pay-Per-View channel</i>
<i>PREP</i>	<i>Policy and Rights Expression Platform</i>
<i>PRIME</i>	<i>Privacy and Identity Management for Europe</i>
<i>PVR</i>	<i>Personal Video Recorder</i>
<i>QoE</i>	<i>Quality of Experience</i>
<i>QoS</i>	<i>Quality of Service</i>
<i>RSO</i>	<i>Rights and Services Object</i>
<i>SDP</i>	<i>Service Distribution Provider</i>
<i>STB</i>	<i>Set-Top-Box</i>
<i>TCP</i>	<i>Transmission Control Protocol</i>
<i>TPM</i>	<i>Trusted Platform Module</i>
<i>TV</i>	<i>TeleVisão</i>
<i>VoD</i>	<i>Vídeo On-Demand</i>
<i>VoIP</i>	<i>Voice over IP</i>
<i>W3C</i>	<i>World Wide Web Consortium</i>
<i>WAN</i>	<i>Wide Area Network</i>
<i>WDM</i>	<i>Wavelength Division Multiplexing</i>
<i>xDSL</i>	família de tecnologias do tipo <i>Digital Subscriber Line</i>
<i>XML</i>	<i>eXtensible Markup Language</i>

SUMÁRIO

1	INTRODUÇÃO	12
1.1	MOTIVAÇÃO	14
1.2	OBJETIVO E ESCOPO	18
1.3	ORGANIZAÇÃO DO TEXTO	18
2	SISTEMAS DE IPTV.....	20
2.1	CARACTERIZAÇÃO	20
2.2	CANAIS IPTV	21
2.2.1	<i>Canais de Conteúdo .....</i>	<i>22</i>
2.2.2	<i>Electronic Program Guide.....</i>	<i>23</i>
2.3	ARQUITETURA DE REFERÊNCIA DE UM SISTEMA DE IPTV	24
2.3.1	<i>Rede de Transporte.....</i>	<i>25</i>
2.3.2	<i>Domínio Doméstico.....</i>	<i>26</i>
2.3.3	<i>Dispositivos do Domínio Doméstico.....</i>	<i>27</i>
2.3.4	<i>Home Domain Gateway (HDG) .....</i>	<i>28</i>
2.3.5	<i>Provedor de Conteúdo (Content Provider - CP) .....</i>	<i>30</i>
2.3.6	<i>Provedor do Serviço de Distribuição (Service Distribution Provider - SDP)...</i>	<i>30</i>
2.3.7	<i>Servidor de Licenças (License Server - LS).....</i>	<i>31</i>
2.3.8	<i>Operações .....</i>	<i>32</i>
2.4	PERSONALIZAÇÃO DE CONTEÚDO	35
2.5	CONSIDERAÇÕES FINAIS	35
3	PRIVACIDADE	37
3.1	CARACTERIZAÇÃO DE PRIVACIDADE	38
3.2	ASPECTOS DE PRIVACIDADE EM COMUNICAÇÃO DE DADOS	39
3.3	ASPECTOS JURÍDICOS DE PRIVACIDADE ON-LINE	41
3.4	SOLUÇÕES DE PRIVACIDADE.....	44
3.5	CONSIDERAÇÕES FINAIS	48
4	PRIVACIDADE EM IPTV.....	50
4.1	DESCRIÇÃO DO PROBLEMA.....	50
4.2	CRIAÇÃO DE UM PERFIL DE USO DO SERVIÇO	52

4.2.1	<i>TV tradicional</i>	52
4.2.2	<i>Ambientes de IPTV</i>	53
4.3	REQUISITOS DE PRIVACIDADE PARA AMBIENTES DE IPTV	58
4.4	ANÁLISE DE SOLUÇÕES EXISTENTES DE PRIVACIDADE SOB ÓTICA DE IPTV.....	60
4.5	CONSIDERAÇÕES FINAIS	62
5	ARQUITETURA PARA AMBIENTES DE IPTV COM SERVIÇOS DE PRIVACIDADE.....	63
5.1	VISÃO GERAL.....	63
5.2	ARQUITETURA DO SISTEMA IPTV.....	64
5.2.1	<i>Componentes da Arquitetura</i>	65
5.2.2	<i>Operações</i>	72
5.2.3	<i>Limitações</i>	80
5.3	VALIDAÇÃO DA SOLUÇÃO	81
5.3.1	<i>Implementação da Arquitetura do Sistema IPTV com Privacidade</i>	81
5.3.2	<i>Ambiente de Testes</i>	82
5.3.3	<i>Metodologia</i>	84
5.3.4	<i>Resultados</i>	86
5.4	CONSIDERAÇÕES FINAIS	88
6	CONSIDERAÇÕES FINAIS	92
6.1	ANÁLISE CRÍTICA.....	92
6.2	INOVAÇÕES E CONTRIBUIÇÕES	95
6.3	TRABALHOS FUTUROS	97
	REFERÊNCIAS.....	99

1 INTRODUÇÃO

A convergência entre dados, voz e vídeo foi inicialmente motivada por um fator tecnológico e econômico. A possibilidade tecnológica de digitalização de mídias tradicionalmente analógicas (como voz e vídeo) e sua posterior transmissão sobre uma rede TCP/IP (*Transmission Control Protocol/Internet Protocol*) aliaram-se ao menor custo de instalação e manutenção de uma rede convergente¹ quando comparada ao custo de redes distintas para dados, voz e vídeo. Dado estes fatores econômico-tecnológicos, tais redes ditas convergentes foram, inicialmente, restritas ao escopo de redes privadas de grandes empresas e de operadoras de telecomunicação, onde redes de telefonia foram substituídas por sistemas de telefonia IP e circuitos fechados de televisão foram substituídos por tecnologias de transmissão de vídeo sobre IP. Dentro deste escopo, estas tecnologias, apesar do alto custo inicial de toda nova tecnologia, refletiam-se em última instância em diminuição de custos para a empresa.

Recentemente as redes convergentes têm avançado sobre a arena dos usuários domésticos, que normalmente utilizam serviços de conexão de dados (para acesso à Internet), de voz (telefonia) e de vídeo (TV por assinatura). Tal avanço, no entanto, possui outros motivadores em relação ao contexto corporativo inicial, podendo ser mapeados não só a fatores tecnológicos e econômicos como também a fatores comportamentais (2,1,3).

Do lado comportamental, há uma mudança de paradigma de consumo de mídia por parte dos usuários. Com a crescente disponibilidade de mídias digitais (imagens, voz e vídeo) e conseqüentes serviços associados sobre a Internet (compartilhamento de imagens via Flickr², telefonia IP via Skype³ e vídeos via YouTube⁴, entre outros), há uma tendência dos usuários de exigirem cada vez mais a integração entre estas mídias, bem como o acesso às mesmas independentemente da forma e/ou do meio, seja através de seu computador, da sua TV, de seu celular e/ou de outros dispositivos pessoais (2).

---

¹ Por rede convergente, entende-se uma infra-estrutura única de rede capaz de transmitir diferentes mídias como áudio, vídeo e dados, atendendo os requisitos de Qualidade de Serviço de cada mídia.

² Site de compartilhamento de fotos – www.flickr.com.

³ Aplicativo de Telefonia IP – www.skype.com.

⁴ Site de compartilhamento de vídeos – www.youtube.com.

Do ponto de vista técnico, a evolução e a adoção de tecnologias como WDM (*Wavelength Division Multiplexing*), Ethernet óptica, ADSL (*Asymmetric Digital Subscriber Line*) e, mais recentemente, FTTH (*Fiber To The Home*) provêem uma relativa fartura de largura de banda de rede, tanto nos *backbones* de redes metropolitanas e de longa distância como nos enlaces de banda larga das redes de acesso de “última milha” (1), permitindo o uso fim-a-fim de canais de comunicação de alta velocidade e baixa latência.

Por fim, esta maior disponibilidade de serviços banda larga na “última milha” permite que as operadoras de telecomunicações e de TV a cabo ofereçam serviços do tipo *triple play*⁵ (i.e., voz, vídeo e dados). Tais serviços atendem a diversos anseios dos usuários, tais como um menor custo (quando considerado o custo individual de cada serviço), maior simplicidade (um único provedor de serviços e uma única fatura para todas as necessidades de comunicação) e serviços convergentes (por exemplo, possibilidade de acessar as mensagens do correio de voz em um *site* quando fora de casa, ou redirecioná-las para e-mails do usuário). Além de usufruir dos benefícios de economia de uma infra-estrutura compartilhada, ao atender os anseios dos usuários, a operadora passa a atrair novos usuários. Ao mesmo tempo, a operadora conta com uma redução na possibilidade de migração de clientes para concorrentes (os usuários são menos propensos a mudar para concorrentes à medida em que possuem um maior relacionamento com o provedor (3)).

Entre as novidades nesta área de serviços convergentes, destacam-se os sistemas de IPTV (*Internet Protocol TeleVision*). Um sistema de IPTV visa disponibilizar serviços de televisão via TCP/IP sobre uma rede de banda larga privativa. Ao integrar a mídia televisiva a uma conexão de dados, o usuário pode ter uma experiência diferenciada em relação ao vídeo, com serviços de valores agregados, tais como TV interativa e personalização de conteúdo.

Como é freqüente no caso de adoção de novas tecnologias, o principal foco dado às arquiteturas de IPTV em desenvolvimento está relacionado à melhor maneira de se implementar as funcionalidades básicas do serviço, legando a um segundo plano aspectos referentes à segurança do serviço e dos usuários, bem como a sua privacidade.

---

⁵ Pacote de serviços que integra acesso de banda larga à Internet, telefonia IP e transmissão de vídeo.

1.1 *Motivação*

Com a crescente digitalização das mídias e crescente dependência da Internet e de ambientes *online* para tarefas cotidianas, a monitoração do uso destes serviços pode atentar contra a privacidade dos indivíduos de diferentes maneiras. Há diversas situações cotidianas de monitoração *online* que podem impactar a privacidade dos indivíduos, tais como:

- A monitoração de e-mails de funcionários, visando evitar não só espionagem industrial como o uso indevido para atividades não pertinentes à execução de tarefas do trabalho (no caso de um uso ilícito, a empresa pode ser considerada co-responsável pelos atos do funcionário, podendo sofrer processos na justiça);
- O armazenamento e correlação de pesquisas efetuadas em mecanismos de busca de *sites* como Google e Yahoo, com o pretexto de melhorar seus mecanismos de busca, oferecer propagandas e conteúdo personalizado, projetar novos serviços;
- O armazenamento de dados cadastrais dos usuários dos provedores de serviço e *logs* de uso de serviço, visando a obtenção de estatísticas de uso, a análise de tentativas de intrusão no sistema ou a obtenção de material complementar para auxiliar a resolução de problemas.

Através destas monitorações, as empresas acabam por reunir (intencionalmente ou não) um conjunto de dados significativos sobre as pessoas, o que elas utilizam, procuram e/ou compram, muitos de caráter privativo. Há vários exemplos que ilustram como estas informações resultantes da monitoração de uso de um serviço *online* podem ser usadas contra a privacidade de indivíduos:

- Demissão por monitoração de e-mails corporativos (Brasil): como exemplos, pode-se citar o caso de um funcionário de uma empresa de importação e exportação que foi demitido por ter enviado e-mail com dados sigilosos da empresa para um funcionário de uma empresa concorrente (4). Em um caso semelhante, um funcionário da empresa HSBC Seguros foi demitido por enviar fotos de mulheres nuas com o e-mail de trabalho (5).

- Publicação de histórico de buscas da AOL (EUA): em 2006, a AOL disponibilizou dados relacionados a aproximadamente 20 milhões de pesquisas efetuadas por 650.000 usuários em seu mecanismo de busca por um período de três meses. Para não identificar os indivíduos, foram atribuídos identificadores numéricos aos mesmos, de maneira que se fosse possível correlacionar as pesquisas efetuadas por um mesmo indivíduo preservando sua privacidade. No entanto, em uma reportagem publicada no jornal New York Times (6), estes dados da AOL foram utilizados para ilustrar a facilidade de se identificar um usuário através das pesquisas por ele efetuadas, bem como que tipo de conteúdo o indivíduo procura na Internet;
- Google X Departamento de Justiça (EUA): em janeiro de 2006, o Departamento de Justiça Norte-Americano pediu que diversos *sites* de busca disponibilizassem bases de dados com milhões de registros de buscas efetuadas, para uso como evidência em um julgamento da constitucionalidade de uma lei para o controle do acesso infantil à pornografia *on-line* (7). Após a recusa do Google, o caso foi parar na justiça, com ganho de causa à Google;
- Casos CyberSLAPP (EUA). Um indivíduo ou entidade que tenha se sentido ofendido por uma publicação anônima na Internet inicia um processo na Justiça com poucas chances de vitória (uma vez que o direito de se expressar é um direito garantido pela Primeira Emenda da Constituição norte-americana). Como parte deste processo, porém, o provedor do serviço usado para a publicação das críticas recebe uma ordem judicial para identificar o usuário. Desta maneira, mesmo perdendo a causa, o criticado terá identificado o seu crítico, podendo este sofrer intimidações e/ou retaliações como resultado do processo (8);
- Prisão de dissidentes chineses (China): há diversos casos de dissidentes chineses que foram presos através da colaboração do provedor Yahoo. Em dois destes casos (9,10), eles foram presos após o Yahoo fornecer ao governo chinês dados das contas de e-mail e endereços IP utilizados por eles para enviar conteúdos contrários aos interesses do governo (de acordo com o veredicto).

De maneira análoga aos serviços tradicionais de e-mail e navegação internet, novos serviços multimídia, como o IPTV, trazem consigo a preocupação com a privacidade dos assinantes do serviço. Do ponto de vista de usuários e entidades de defesa de privacidade, é esperado que os sistemas de IPTV não revelem aos provedores de serviço os hábitos de “consumo” do serviço pelos assinantes, a não ser quando explicitamente autorizados pelos usuários.

Mas o que seriam os hábitos de consumo dos usuários de um serviço de televisão? O IBOPE (Instituto Brasileiro de Opinião Pública e Estatística), em suas medições de audiência em TV, apresenta diversas variáveis mensuráveis que revelam os hábitos de um usuário de TV, tais como:

- Quais canais são assistidos;
- Quais gêneros de programa são assistidos;
- Quando os canais são assistidos e com que frequência e assiduidade eles são assistidos;
- Qual o tempo médio que o telespectador passa assistindo à televisão;
- Em que sequência estes canais são vistos;
- Em que sequência os programas são vistos;

Tradicionalmente, tais dados têm grande valor para os donos do conteúdo e provedores de serviço. A partir destes dados, é possível saber quem assiste a seus programas e a forma como cada um assiste a seus programas, identificando eventuais programas concorrentes e permitindo o direcionamento de campanhas de *marketing* para públicos-alvos desejados.

Além de donos de conteúdo e provedores de serviço, há outros interessados em conhecer os hábitos destes usuários. Alguns possuem uma motivação possivelmente justificável, tais como entidades governamentais interessadas em monitorar o consumo de conteúdos potencialmente relacionados a atividades ilegais como terrorismo ou drogas. Outros são movidos a interesses pessoais ou financeiros, tais como curiosidade sobre a vida alheia (por exemplo, vida de celebridades) ou a possibilidade de macular a reputação de uma figura pública (por

exemplo, indivíduo que assiste regularmente programas com valores políticos, religiosos ou morais contrários ao seu discurso público) .

A privacidade em um serviço de televisão está relacionada à dificuldade e/ou impossibilidade de relacionar um usuário aos seus hábitos de consumo, a não ser quando explicitamente autorizado. A questão de privacidade em sistemas de IPTV passa, portanto, pela própria questão de privacidade em sistemas de TV de uma maneira geral.

Na TV aberta, não há a preocupação com a privacidade dos telespectadores, uma vez que não é possível saber quem são e onde estão os telespectadores, ao contrário da TV paga, onde tais informações são disponíveis ao provedor do serviço como parte do contrato comercial do serviço. No entanto, tanto a TV paga como a aberta “protegem” a privacidade através de uma limitação tecnológica: por não possuírem em geral um canal de retorno, não é possível saber o que os telespectadores estão assistindo. Tal dificuldade é ilustrada pela própria metodologia do IBOPE para a medição de audiência da TV aberta e paga (11): com a autorização dos moradores, instala-se nos televisores de casas selecionadas um aparelho especializado que identifica e registra o canal sendo assistido, enviando periodicamente à central de pesquisa as informações coletadas. Dependendo da infra-estrutura da região, utiliza-se um método mais simples: a coleta de dados em um caderno preenchido pelo morador e coletado periodicamente.

A modernização da infra-estrutura de TV a cabo e o surgimento de novas tecnologias de transmissão de vídeo trouxeram consigo o advento de canais de retorno, o que possibilitou não somente o acesso à Internet via esta infra-estrutura como também o envio dos hábitos dos telespectadores de forma transparente ao usuário. Em alguns países, como nos Estados Unidos da América (EUA), as operadoras de serviços de TV por assinatura via cabo ou satélite possuem restrições em relação à coleta e à divulgação dos hábitos de TV de seus usuários, mitigando a questão de privacidade.

Sistemas de IPTV apresentam novos desafios em relação à privacidade. Dada a sua arquitetura e o uso comum de mecanismos de DRM (*Digital Rights Management*) para proteção do conteúdo e do serviço contra uso não autorizado, é possível um rastreamento dos hábitos dos usuários sem precedentes, permitindo ao provedor do serviço saber exatamente e de forma individualizada para cada assinante quando e

o quê foi consumido. Por utilizar uma rede IP, tais hábitos de coleta poderiam ser coletados por terceiros, utilizando-se de ataques conhecidos para captura de pacotes, tais como envenenamento de entradas DNS (*Domain Name System*), tabelas ARP (*Address Resolution Protocol*) e/ou tabelas de roteamento, além da utilização de *proxies* ou *middleboxes*⁶ (12).

Um outro aspecto importante refere-se aos aspectos jurídicos da privacidade em um sistema de IPTV. Evoluções tecnológicas freqüentemente provocam dúvidas em relação à correta legislação a elas aplicável (ou até mesmo se há alguma legislação aplicável). Como o serviço de IPTV permite aos usuários assistirem televisão independente da infra-estrutura física, a legislação de privacidade pode não cobrir estes usuários (por exemplo, nos EUA, a lei protege a privacidade de usuários de TV a cabo ou via satélite, mas não fica claro como ficariam os usuários que assistem TV através de um serviço de banda larga ADSL ou FTTH). Sendo assim, é necessário um sistema de IPTV que proteja a privacidade dos usuários, mantendo as características do serviço, independente do tipo de rede de acesso.

1.2 Objetivo e Escopo

Este trabalho tem como objetivo propor uma arquitetura de IPTV que apresente mecanismos capazes de garantir um nível de privacidade maior do que o existente em sistemas de IPTV tradicionais, de maneira que seja extremamente difícil para um observador obter uma visão completa do perfil de uso de um assinante (i.e., relacionar o assinante aos programas e serviços por ele consumidos).

1.3 Organização do texto

O capítulo 2 deste documento apresenta uma visão geral sobre IPTV, caracterizando o modelo a ser utilizado para o desenvolvimento do trabalho. Por sua vez, o capítulo 3 descreve os aspectos de privacidade a serem considerados no trabalho. Estes

---

⁶ Qualquer dispositivo intermediário atravessado por um fluxo de tráfego IP entre um computador de origem e um de destino, que atua na camada de rede ou camadas superiores do modelo OSI e executa funções diferentes das funções normais padronizadas de um roteador IP.

aspectos de privacidade são relacionados ao ambiente de IPTV no capítulo 4, onde se caracteriza o problema de privacidade dentro do contexto de IPTV, os requisitos necessários bem como as soluções de privacidade existentes neste contexto. O capítulo 5 apresenta a arquitetura de privacidade proposta, incluindo testes de validação. Por fim, o capítulo 6 apresenta considerações sobre contribuições e inovações da tese, bem como sobre trabalhos futuros.

2 SISTEMAS DE IPTV

Há muitas visões diferentes sobre o que é um sistema de IPTV (*Internet Protocol TeleVision*). É necessário, portanto, definir a visão utilizada neste trabalho.

Este capítulo apresenta uma caracterização de IPTV associada a uma arquitetura de referência, à descrição dos elementos de um sistema IPTV e à classificação dos dados transmitidos sobre os canais do serviço, com particular destaque para os chamados canais de conteúdo, que formam o escopo principal de um serviço de IPTV.

2.1 Caracterização

O acrônimo IPTV tem sido usado, de uma maneira geral, para qualquer transmissão de vídeo sobre uma rede TCP/IP (*Transmission Control Protocol / Internet Protocol*), tanto uma rede privativa de banda larga (por exemplo, uma rede de um provedor de serviços ou de campus acadêmico) como uma rede pública de banda variável como a Internet, não havendo um consenso quanto ao que seria um sistema de IPTV, nem a eventuais protocolos em adição ao próprio TCP/IP.

Em meados de 2007, foi formado um fórum de indústrias para definir e padronizar um ambiente de IPTV, denominado OpenIPTV Fórum (13), procurando englobar todas as soluções existentes.

Dentro do escopo deste trabalho considera-se um sistema de IPTV um **ambiente onde serviços de televisão tradicionais e personalizados são disponibilizados sobre uma rede de banda larga privativa via TCP/IP, com o uso opcional de DRM (*Digital Rights Management*) para a proteção dos direitos autorais (*copyrights*) dos donos do conteúdo**. É importante ressaltar que tal definição, derivada de (14,13,15) não procura atender o amplo espectro de soluções ditas IPTV, englobando apenas um subconjunto das soluções existentes. Em particular, a definição acima engloba o subconjunto atualmente atendido por serviços de TV por assinatura (via satélite, rádio ou redes híbridas fibra óptica – coaxial) e/ou circuitos

privativos de TV (também conhecidos por circuitos internos de TV) e exclui as soluções de vídeo sobre a Internet.

Para um melhor entendimento do sistema, é necessário conhecer, inicialmente, quais tipos de serviço serão providos via canais IPTV.

2.2 Canais IPTV

Um canal IPTV é um meio de interação entre o provedor de IPTV e o usuário final para o provimento de serviços ou conteúdo, implementado fisicamente através de uma conexão de dados entre a rede doméstica e a rede do provedor. Há três tipos de canais de IPTV (14):

- **Canais Interativos:** provêem um meio de comunicação, bidirecional, com elementos externos ao sistema de IPTV (por exemplo, servidores de e-mail e *web* espalhados na Internet ou usuários de outras operadoras de telefonia, tanto fixa como celular). O serviço de acesso à Internet e de Telefonia IP são exemplos de canais interativos;
- **Canais Auxiliares:** provêem informações (metadados) sobre o conteúdo dos canais de conteúdo, tais como a programação (EPG - *Electronic Program Guide*) e outros tipos de informações (ex.: dados do cadastro do usuário);
- **Canais de Conteúdo:** provêem as mídias do serviço de IPTV, em forma de *stream* ou *download* de conteúdo de áudio/vídeo.

A Figura 1 ilustra esta classificação dos canais.

Figura 1 – Classificação dos Canais (14).

Um serviço básico de IPTV conta com pelo menos um canal auxiliar de programação (EPG) e um ou mais canais de conteúdo, detalhados a seguir.

2.2.1 Canais de Conteúdo

Os canais de conteúdo podem ser classificados de acordo com o modelo de distribuição, o modelo de negócios e os requisitos de segurança.

Quanto ao **modelo de distribuição**, os canais podem ser classificados em (14):

- **Broadcast:** canais transmitidos na forma de um *stream* de dados. A maioria dos canais oferecidos na TV aberta e paga é deste tipo. O provedor de serviços não necessita armazenar e oferecer o conteúdo após a sua exibição, estando o usuário sujeito aos horários de distribuição do provedor;
- **Sob-Demanda:** canais oferecidos na forma de um *download* de conteúdo. O provedor de serviços armazena e disponibiliza o conteúdo para o usuário a qualquer momento, conforme desejado.

Em redes IPTV, os canais de *broadcast* são tipicamente transmitidos através de *multicast*⁷, enquanto canais sob demanda são transmitidos via *unicast*⁸ (16).

Em relação ao **modelo de negócios**, os canais podem ser classificados em (14):

- **Assinatura:** canais cujo acesso é obtido mediante o pagamento de um plano de assinatura que normalmente determina o pagamento periódico de uma tarifa (por exemplo, mensal) durante toda a duração do plano e compreende um conjunto pré-definido de canais de *broadcast* ou sob-demanda.
- **À La-Carte:** canais cujo acesso é obtido mediante um pagamento único, de forma individual para cada canal.

Por fim, quanto aos **requisitos de segurança**, as principais classificações dos canais são (14) :

⁷ Transmissão do tipo muitos-para-muitos, em que um elemento da rede transmite pacotes simultaneamente para um grupo de destinatários, utilizando uma única transmissão.

⁸ Transmissão do tipo um-para-um, em que um elemento da rede transmite pacotes para um único destinatário.

- **Abertos:** canais que não necessitam de nenhum tipo de proteção, podendo ser visualizados por qualquer usuário, pagante ou não (por exemplo, canais governamentais ou de ONGs);
- **Protegidos:** canais que exigem tanto autenticação como proteção do conteúdo para serem visualizados. Canais cuja fonte primária de receita é o próprio conteúdo do canal (ao contrário das propagandas) podem ser citados como exemplos destes canais;

Desta classificação podem ser definidos os diferentes tipos de canais comumente encontrados em TVs por assinatura, tais como os canais Básicos, *Premium*, *Pay-Per-View* (PPV) e *On-Demand* (Tabela 1), sendo os canais Básicos e Premium os serviços mais comumente utilizados.

Tabela 1 – Exemplo de Classificação de Canais

	Modelo de Distribuição	Modelo de Negócios	Requisitos de Segurança
Básico	<i>Broadcast</i>	Assinatura	Controlado
<i>Premium</i>	<i>Broadcast</i>	Assinatura	Protegido
<i>Pay-Per-View</i> (PPV)	<i>Broadcast</i>	<i>À La Carte</i>	Protegido
<i>On-Demand</i>	Sob Demanda	<i>À La Carte</i>	Protegido

2.2.2 *Electronic Program Guide*

Um *Electronic Program Guide* (EPG) é um canal auxiliar que informa aos usuários do sistema a programação dos canais de conteúdo, ou seja, que conteúdo encontra-se disponível em cada canal em um dado momento (17), tanto para canais de *broadcast* como sob-demanda. Normalmente trata-se de um guia interativo: com o controle remoto o usuário pode visualizar a programação atual e futura de cada canal.

O EPG contém informações adicionais sobre cada conteúdo, tais como duração, sinopse, atores, entre outros, de maneira a auxiliar o usuário na escolha do conteúdo a ser assistido. Além dos metadados do conteúdo, o EPG também indica

aos equipamentos de IPTV dos usuários como o conteúdo deve ser acessado (ex.: endereço IP de *multicast* para canais de *broadcast* e endereço de *download* para canais de sob demanda).

Em geral, as informações do EPG ficam todas no provedor do serviço de IPTV; quando o usuário deseja visualizar o EPG, as informações são transmitidas para o equipamento do usuário sob demanda, não exigindo muitos recursos do mesmo. Alguns sistemas mantêm um *cache* do lado do usuário com as informações dos conteúdos em exibição, de maneira a otimizar o tempo de resposta ao usuário; neste caso somente informações sobre a programação futura são requisitadas ao provedor do serviço (17).

Há também serviços que oferecem EPGs personalizados para funções específicas, tais como em um sistema de *Personal Vídeo Recorder* (PVR), onde o EPG é utilizado em conjunto com um dispositivo especializado que grava localmente o conteúdo. Neste caso, são permitidas a posterior visualização do conteúdo (como em um videocassete), a pausa e *replays* de conteúdos ao vivo ou ainda a gravação automática de conteúdo de acordo com informações do EPG, tais como atores, diretores, categorias e palavras-chaves ⁹ (17,18).

2.3 Arquitetura de referência de um sistema de IPTV

A Figura 2 apresenta uma arquitetura de referência de um sistema de IPTV, derivada de (13, 14, 15) e em conformidade com a definição de um sistema de IPTV apresentada em 2.1 . Há quatro entidades principais na arquitetura: o Provedor de Conteúdo (*Content Provider* - CP), o Provedor de IPTV, a Rede de Transporte e o Domínio Doméstico.

O Provedor de IPTV subdivide-se em outros componentes: o Provedor do Serviço de Distribuição (*Service Distribution Provider* – SDP), Servidor de Licença (*License Server* - LS), Rede de Transporte, além do *Gateway* do Domínio Doméstico (*Home Domain Gateway* - HDG).

---

⁹ O exemplo mais conhecido de PVR é o sistema da TiVo (www.tivo.com).

EPG – Electronic Program Guide

Figura 2 – Arquitetura de referência de um sistema de IPTV (13, 14, 15)

É importante ressaltar que em ambientes onde há a preocupação de proteger os conteúdos contra operações não autorizadas que poderiam significar perda de receita (ex.: cópias para revenda, compartilhamento do conteúdo entre amigos, entre outros), a arquitetura de IPTV utiliza mecanismos de DRM, que se estendem por toda a cadeia de distribuição do conteúdo, até o dispositivo do usuário que será utilizado para a sua reprodução (19). A arquitetura de referência contempla o uso de DRM, sendo explicitados, nas descrições seguintes, os módulos e elementos que implementam os mecanismos de DRM, caso o seu uso seja requisito da implementação da arquitetura..

2.3.1 Rede de Transporte

A Rede de Transporte provê a conectividade física entre os usuários e os provedores do serviço de IPTV. Ela é controlada e mantida por uma única entidade, que pode ser o próprio provedor de IPTV ou uma entidade separada (como um provedor de serviços de telecomunicações), de maneira a garantir os requisitos de QoS (*Quality of Service*) das aplicações do serviço. Ela é tipicamente composta por

três partes: uma rede principal (*core*), uma rede de borda (*edge*) e uma rede de acesso (15). A rede principal é uma rede óptica de alta capacidade, baseada em tecnologias como IP sobre DWDM (*Dense Wavelength Division Multiplexing*) e/ou MPLS/gMPLS (*Multiple Protocol Label Switching/generic MPLS*). A rede de borda interliga a rede principal à rede de acesso, sendo responsável pela distribuição de *streams* de *multicast*, através do suporte a protocolos de roteamento *multicast* como o PIM-SSM (*Protocol Independent Multicast – Source Specific Multicast*) ou DVMRP (*Distance Vector Multicast Routing Protocol*) (16). A rede de acesso representa a última milha da conexão, interligando os usuários ao serviço e podendo ser implementada por várias tecnologias, tais como PON FTTH (*Passive Optical Network Fiber to the Home*), xDSL (família de tecnologias do tipo *Digital Subscriber Line*) ou redes de TV a cabo (20).

2.3.2 Domínio Doméstico

O Domínio Doméstico representa o cliente do serviço de IPTV, sendo composto por um conjunto de dispositivos e usuários interligados através de uma rede doméstica e, quando do uso de DRM, sujeitos às políticas de uso do serviço e do conteúdo determinadas pelo provedor. Em sua forma mais simples e tradicional é representado por um ou mais dispositivos de visualização (aparelhos de TV).

A abordagem de domínio possibilita um uso adequado do conteúdo adquirido, uma vez que permite aos usuários consumir o conteúdo de IPTV em qualquer dispositivo do domínio e, ao mesmo tempo, define os limites para o consumo do conteúdo de IPTV dentro do ambiente doméstico.

O Domínio Doméstico interliga-se à Rede de Transporte através de um dispositivo especializado denominado HDG (*Home Domain Gateway*), que isola os detalhes das redes de transporte e da rede doméstica entre si. Além disso, o HDG é responsável por prover os serviços de IPTV para os dispositivos do domínio, incluindo o próprio gerenciamento do domínio (21).

2.3.3 Dispositivos do Domínio Doméstico

Os dispositivos do domínio são os elementos utilizados pelo usuário para a visualização do conteúdo do serviço de IPTV. Caso a arquitetura de IPTV utilize DRM, estes dispositivos devem obedecer às políticas definidas pelo CP (*Content Provider*) e pelo provedor de IPTV, ou seja, antes de executar qualquer operação em um conteúdo IPTV, devem verificar se a operação é permitida por estas políticas. Os dispositivos podem também distribuir o conteúdo aos outros dispositivos dentro do domínio, balanceando os interesses de proteção de direitos autorais dos provedores de conteúdo e de IPTV com os desejos dos usuários de uso adequado do serviço (22).

Para prover estas funcionalidades de controle associadas às funcionalidades de visualização do conteúdo, um dispositivo do domínio é composto por três módulos principais.

- **Trusted Environment (Ambiente Confiável):** é responsável por prover as funcionalidades de segurança para os outros módulos do dispositivo. Composto por um *hardware* de TPM (*Trusted Platform Module*)(23), ele provê o atestamento dos módulos do dispositivo, garantindo a integridade dos mesmos, bem como o armazenamento seguro de chaves e licenças de conteúdo (no caso de DRM);
- **Player (Reprodutor):** é responsável por decodificar o conteúdo, de acordo com os formatos de codificação das mídias, e exibi-lo. No caso de conteúdo criptografado, este módulo interage com o ambiente confiável para decriptá-lo;
- **Cliente IPTV:** é responsável por prover os serviços de IPTV internamente ao dispositivo. Interage com o HDG, requisitando o conteúdo dos canais. Em caso de DRM, requisita as respectivas licenças dos conteúdos e aplica as políticas de uso do conteúdo, garantindo que somente operações autorizadas por estas políticas possam ser executadas pelo *player*.

A Figura 3 apresenta a relação entre estes módulos.

Figura 3 – Módulos do Dispositivo de Domínio

No caso de ambientes sem DRM, o dispositivo pode ser resumido apenas aos módulos de Cliente IPTV e *Player*, não havendo necessidade do módulo de Ambiente Confiável. No entanto, o módulo de Ambiente Confiável é recomendado para evitar alteração indevida no dispositivo, que possa prejudicar o serviço (por exemplo, introdução de vírus e outros programas maliciosos no ambiente).

2.3.4 Home Domain Gateway (HDG)

O HDG é o ponto de entrada no domínio para os serviços IPTV, uma vez que tanto o conteúdo como as licenças do conteúdo devem passar por ele. Para prover os serviços de IPTV em um domínio, o HDG é composto por diversos módulos:

- ***Trusted Environment (Ambiente Confiável)***: módulo responsável por prover as funcionalidades de segurança para os outros módulos do próprio HDG. De maneira análoga à arquitetura dos dispositivos do domínio, ele é composto por um *hardware* de TPM (*Trusted Platform Module*)(23), que provê atestamento dos módulos e armazenamento seguro de chaves e licenças de conteúdo;
- ***Domain Manager (Gerenciador de Domínio)***: módulo responsável pelo gerenciamento do domínio, ou seja, a adição e remoção de dispositivos do domínio;

- **Content Manager (Gerenciador de Conteúdo):** módulo responsável por interagir com o provedor de IPTV para o tratamento de requisições de conteúdo e sua posterior distribuição dentro do domínio, conforme as requisições e capacidades de cada dispositivo;
- **License Manager (Gerenciador de Licença):** módulo responsável pelas funcionalidades de DRM no domínio, tais como interagir com o provedor de IPTV para solicitar as licenças de uso do conteúdo e do serviço, garantir a execução das políticas de serviço (Por exemplo, número máximo de *streams* de vídeo simultâneo no domínio) e distribuir as políticas relacionadas ao conteúdo para os dispositivos e para os módulos apropriados dentro do HDG;
- **QoS Control (Controle de Qualidade de Serviço):** módulo responsável por garantir que os requisitos de QoS definidos na política do serviço sejam obedecidos dentro do domínio.

A Figura 4 apresenta a relação entre os módulos do HDG.

Figura 4 – Módulos do HDG

Em uma arquitetura simples de IPTV, o HDG e o dispositivo de domínio doméstico podem ser integrados, provendo todas as funcionalidades do ambiente a um aparelho de apresentação único, tais como um *Set-Top Box* (STB) para IPTV (provê as funcionalidades do ambiente a um aparelho de TV tradicional) ou um computador com um *software* de IPTV.

2.3.5 Provedor de Conteúdo (*Content Provider* - CP)

Os Provedores de Conteúdo (*Content Providers* – CP) são as entidades que produzem e/ou são proprietárias do conteúdo (i.e., da mídia), e os fornecem para os SDP para distribuição aos usuários finais. No caso de ser necessária a proteção do conteúdo via DRM para a distribuição, os CPs podem determinar um conjunto de políticas relacionadas ao uso do conteúdo (fornecendo-as para os servidores de Licença - LS), bem como podem proteger a mídia usando mecanismos como criptografia e marca-d'água (*watermarking*¹⁰).

2.3.6 Provedor do Serviço de Distribuição (*Service Distribution Provider* - SDP)

Os Provedores do Serviço de Distribuição (*Service Distribution Providers* - SDP) são as entidades responsáveis por prover o serviço de IPTV aos Clientes.

Dados os diferentes tipos de canais e serviços, o SDP utiliza diferentes mecanismos de segurança no provimento deste serviço. As principais funções do SDP são:

- **Conversão e Encapsulamento da Mídia:** o SDP é responsável por codificar/transcodificar a mídia recebida do CP para os formatos apropriados para transmissão (ex.: MPEG-2, MPEG-4, etc.), encapsulando-os em pacotes IP (24);
- **Encriptação da Mídia:** o SDP deve garantir, através de criptografia, que o conteúdo da mídia não seja capturado por usuários não autorizados do sistema, caso o conteúdo tenha sido fornecido sem criptografia pelo CP e seja necessário o uso de DRM. As chaves do conteúdo são encaminhadas para o Servidor de Licenças (LS), que se encarrega de distribuí-las para os clientes;
- **Distribuição da Mídia:** o SDP utiliza a rede de transporte, descrita anteriormente para distribuir a mídia aos clientes, por meio de *streams* de

---

¹⁰ Técnica de inserção de informações relacionadas a *copyright* em uma mídia digital, que permita identificar o autor e/ou dono do conteúdo, bem como o comprador do conteúdo, possibilitando o rastreamento de cópias não-autorizadas.

multicast ou tráfego *unicast* conforme o tipo de canal (*Broadcast* ou sob Demanda);

- **Geração de Políticas:** o SDP gera as políticas de uso do conteúdo (conforme as políticas definidas pelos CPs), bem como as políticas de uso do serviço, no caso de conteúdo protegido via DRM. Estas políticas são também encaminhadas para o Servidor de Licenças (LS) para posterior distribuição;
- **Controle de QoS:** o SDP deve definir políticas de QoS para o conteúdo e para o serviço, que devem ser obedecidas tanto na rede de transporte quanto na rede doméstica dos clientes. Estas políticas também são enviadas para o Servidor de Licenças (LS) para posterior distribuição;
- **Cobrança:** o SDP pode ser responsável pela própria cobrança dos serviços de IPTV.

2.3.7 Servidor de Licenças (*License Server - LS*)

O Servidor de Licenças é a entidade do lado do provedor de serviços responsável pelas funcionalidades de proteção de conteúdo via DRM. O LS agrega as políticas e chaves relacionadas aos conteúdos (definidas pelo SDP e pelo CP) e as distribui para os clientes, usando a rede de transporte, na forma de um RSO (*Rights and Services Object*).

O RSO é uma coleção de permissões associadas a um conteúdo protegido, formadas a partir das políticas do CP e do SDP, juntamente com a chave de criptografia simétrica deste conteúdo.

As principais funções do LS são:

- **Criação de um RSO:** para a criação de um RSO, o LS recebe do CP e do SDP as chaves e as políticas referentes ao conteúdo, efetua uma composição das políticas (resolvendo eventuais conflitos de permissões) e cria o RSO contendo esta política composta, além das referidas chaves. Em particular, o RSO contém um atributo para relacioná-lo de forma unívoca ao conteúdo a ser protegido;

- **Distribuição de RSOs:** o LS encarrega-se de distribuir os RSOs para os HDGs das redes domésticas autorizadas a assistir o conteúdo/serviço;
- **Autoridade de Referência para Tempo:** quando houver políticas que determinem restrições baseadas em tempo, o HDG e/ou dispositivo do cliente devem se ajustar ao relógio do LS para o cumprimento das políticas (por exemplo, o conteúdo pode ser visualizado no máximo 3 vezes ou somente pode ser visualizado durante a próxima semana).

2.3.8 Operações

Dentro da arquitetura apresentada pode-se definir quatro operações básicas entre o HDG e o provedor de IPTV: o registro inicial do HDG, a autenticação periódica para uso do serviço, o acesso à programação no EPG e, por fim, a requisição de conteúdo. A Figura 5 ilustra estas principais operações.

Figura 5 – Principais Operações em um serviço de IPTV

2.3.8.1 Registro do HDG

Após a contratação do serviço de IPTV, o HDG deve ser registrado junto ao provedor. Este registro, efetuado normalmente uma única vez (quando o HDG é inicializado pela primeira vez após a instalação no Domínio Doméstico), é necessário para que o provedor possa associar o HDG ao contrato do usuário, permitindo a tarifação e controle do serviço.

Durante a inicialização são definidos também os parâmetros para o uso do serviço, tais como:

- **Parâmetros de Autenticação:** utilizados para a comprovação do uso do serviço por um usuário autorizado. Como exemplos de possíveis parâmetros de autenticação pode-se citar o uso login/senha ou o uso de um par de chaves assimétricas;
- **Parâmetros de DRM:** utilizados para a proteção do conteúdo contra uso não autorizado. Os principais parâmetros de DRM definidos nesta fase são o par de chaves assimétricas associadas ao usuário com o qual o servidor de licenças irá distribuir os RSOs associados aos conteúdos.

2.3.8.2 Autenticação

Um aspecto essencial de um serviço de IPTV é que somente usuários autorizados possam ter acesso aos conteúdos (em geral, usuários que tenham pago a assinatura, ou usuários de uma determinada comunidade). Desta maneira, é importante autenticar os usuários antes do acesso ao conteúdo.

A autenticação é feita de forma periódica, de acordo com o modelo de negócios do provedor (por exemplo, se a cobrança do serviço é proporcional aos dias corridos de acesso ao serviço, uma única autenticação diária poderia ser suficiente). Os parâmetros usados na autenticação são os definidos durante a etapa de registro do HDG.

2.3.8.3 Acesso ao EPG

Conforme visto em 2.2.2, as informações do EPG ficam no provedor de serviço, sendo transmitidas para o HDG conforme necessário, uma vez que o HDG normalmente possui limitações de armazenamento. Para visualizar a programação de um ou mais canais é necessário, portanto, o envio de uma requisição ao SDP, com a identificação dos canais, o horário inicial e a duração da programação que se deseja visualizar. A Figura 6 ilustra este processo.

Figura 6 – Acesso ao EPG

2.3.8.4 Requisição de Conteúdo

Uma vez que o usuário decide que conteúdo deseja assistir, o HDG deverá requisitá-lo ao SDP. Caso o conteúdo esteja protegido por DRM, o HDG deverá solicitar ao LS o respectivo RSO do conteúdo, que é enviado usando a chave pública do usuário, definida durante a etapa de registro do HDG. Uma vez de posse do RSO, o HDG emite uma requisição para a transmissão do conteúdo (via *multicast* ou *unicast*, dependendo do tipo do canal). A Figura 7 ilustra o processo de requisição do conteúdo com os passos adicionais para conteúdos protegidos por DRM.

Figura 7 – Requisição de Conteúdo

2.4 Personalização de Conteúdo

Um aspecto que diferencia as plataformas de IPTV de sistemas tradicionais é o aspecto de personalização. Enquanto que em um sistema de TV tradicional o mesmo conteúdo é enviado para todos os usuários do serviço dentro de uma área geográfica (conteúdo regionalizado), em um ambiente de IPTV conteúdos diferenciados podem ser enviados para grupos de usuários distintos, de acordo com critérios variados, tais como faixa etária ou sexo, através de grupos de *multicast* distintos. Tal possibilidade é altamente desejada para propagandas dirigidas, onde diferentes categorias de usuários recebem intervalos comerciais diferenciados de acordo com seu perfil.

Para tal personalização é necessário classificar o usuário de acordo com as variáveis a serem usadas para a personalização e, através de regras explicitadas no EPG, o HDG poderá, então, selecionar os grupos de *multicast* apropriados de acordo com esta classificação. Em última instância, seria possível até mesmo utilizar canais de *unicast* para conteúdos individualizados por assinante.

2.5 Considerações Finais

Através de uma rede TCP/IP privativa e de banda larga, um ambiente de IPTV disponibiliza serviços de televisão, tais como canais de conteúdo e EPG, com funcionalidades inovadoras, tais como a personalização de conteúdo. Dada a

preocupação com direitos autorais de conteúdos, pode ser adotado o uso de mecanismos de DRM para a proteção de determinados conteúdos (não sendo o uso de DRM uma premissa básica do IPTV). Uma arquitetura para IPTV deve, portanto, contemplar não só os aspectos de transmissão de vídeo como também aspectos de personalização e uso de DRM.

No entanto, ao utilizar como base uma rede TCP/IP e ao contemplar aspectos de personalização e uso de DRM, há uma preocupação com a privacidade dos usuários, uma vez que se torna possível o rastreamento dos hábitos de consumo de conteúdo dos usuários, utilizando-se técnicas e ferramentas ao alcance de qualquer indivíduo conectado ao sistema. Uma análise mais aprofundada sobre privacidade e sobre o problema de privacidade em ambientes de IPTV faz-se necessária, sendo o objetivo dos capítulos posteriores.

3 PRIVACIDADE

De acordo com (25), há referências à privacidade na Bíblia, na Grécia Antiga e nas antigas culturas chinesas e hebraicas. Em particular, Aristóteles já distinguia entre a esfera pública da atividade política e a esfera privada, associada com a família e a vida doméstica (26).

No entanto, a visão de privacidade como um direito fundamental do indivíduo é bem mais recente: no século XVIII começam a aparecer mecanismos de proteção à privacidade com caráter jurídico, tais como o *Ato de Acesso aos Registros Públicos* na Suécia (1776) e a *Declaração Universal dos Direitos do Homem e do Cidadão* na França (1858).

Um marco no direito à privacidade no mundo moderno é a *Declaração Universal dos Direitos do Homem*, proclamada pela Assembléia Geral das Nações Unidas em Dezembro de 1948 definida como um “ideal comum a ser atingido por todos os povos e todas as nações”. Ela prevê em seu artigo XII:

“Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.”

Após a experiência na 2ª Guerra Mundial, onde a revelação de questões de foro pessoal, como raça, religião ou orientação sexual poderia significar a diferença entre a vida e a morte, os europeus evoluíram na proteção do direito à privacidade. Em 1950, a Convenção Européia de Direitos Humanos ratifica a Declaração de Direitos Humanos e, em seu artigo 8º, determina que “*Todos têm o direito de respeito à sua vida privada e familiar, seu lar e sua correspondência*”. Indo um passo adiante, a Convenção cria a Comissão Européia de Direitos Humanos e a Corte Européia de Direitos Humanos, para garantir que a Convenção seja seguida e para punir eventuais abusos por parte de um governo contra seus cidadãos.

Apesar de considerado um direito, há diferentes visões sobre o que é privacidade e como devem ser as leis e regulamentações necessárias para atingir o ideal das Nações Unidas. Tais leis e regulamentações refletem-se nos mecanismos necessários para garantir a privacidade.

3.1 Caracterização de Privacidade

A definição de privacidade é bastante difícil, dadas as diferentes visões de diferentes grupos sociais e dos diferentes contextos, tais como juristas, filósofos, antropólogos, entre outros. Há diversas tentativas de definições na literatura da área, e uma discussão bastante extensa pode ser encontrada em (26). Destas, algumas definições se destacam, tais como:

- Em (27), os autores refletem sobre o direito de privacidade como o “direito de ficar sozinho” e discutem que o direito à propriedade compreende não só bens tangíveis como também intangíveis, como as emoções, pensamentos e sentimentos. Discutem ainda sobre a necessidade de proteger a disseminação pública de detalhes privativos da vida de um indivíduo (considerada a “personalidade inviolável”);
- Em (28), a privacidade é definida como “o direito das pessoas de escolher livremente sob quais circunstâncias e em que extensão elas irão expor a si mesmas, suas atitudes e comportamentos a outros”;
- Em (29), a privacidade de dado indivíduo é caracterizada sobre três pilares: do sigilo (ninguém tem informação sobre o indivíduo), anonimato (ninguém conhece no indivíduo) e solidão (ninguém tem acesso físico ao indivíduo)

Nas definições apresentadas é possível observar que em todas há um conceito implícito e comum, o do controle sobre a informação relacionada ao indivíduo. Desta maneira, em muitas situações o conceito de privacidade confunde-se com o conceito de proteção de dados privativos e com o próprio conceito de sigilo.

No entanto, a privacidade de um indivíduo vai além do controle de suas informações privativas. Por exemplo, em (25), a privacidade de um indivíduo é dividida em quatro diferentes aspectos:

- Privacidade da Informação: relacionada à coleta e manuseio de dados pessoais, tais como informações financeiras e registros médicos;
- Privacidade Corporal: relacionada à proteção física do indivíduo contra procedimentos como testes de drogas e revista íntima;

- Privacidade da Comunicação: relacionada à segurança e privacidade de cartas, e-mails, telefones e outras formas de comunicação;
- Privacidade Territorial: relacionada ao estabelecimento de um espaço físico privativo, livre de intrusão, tal como um ambiente doméstico, um espaço em um ambiente de trabalho e até mesmo em um ambiente público (situação bastante discutida em relação à atuação de repórteres e fotógrafos de celebridades).

Dado o escopo deste trabalho, as referências à privacidade compreenderão o controle das informações relacionadas ao indivíduo (ou seja, a privacidade da informação) e das informações associada à privacidade de suas comunicações, salvo quando explicitamente especificado o tipo de privacidade.

3.2 Aspectos de Privacidade em Comunicação de Dados

Utilizando a taxonomia de (30), os diferentes aspectos de privacidade podem ser caracterizados em função de um modelo simples, onde **sujeitos** (entidades tais como pessoas físicas, jurídicas ou computadores) se comunicam através de uma **rede de comunicação**, assumindo papéis de **remetentes** ou **destinatários** dependendo do sentido da comunicação. Neste cenário, **um atacante** é um indivíduo ou entidade com capacidade de monitorar e/ou controlar a comunicação, bem como estações e equipamentos (e.g. roteadores) da rede, visando atentar contra a privacidade dos sujeitos.

Figura 8 – Modelo de Comunicação e Aspectos de Privacidade (30).

A **anonimidade** de um sujeito pode então ser definida como o estado de ser não-identificável dentro de um conjunto de sujeitos, denominado conjunto de anonimidade. (todos os possíveis sujeitos).

Dentro deste modelo define-se a **não-relacionabilidade de dois ou mais itens de interesse**: dentro de um sistema contendo diversos itens, o conhecimento do relacionamento entre estes itens de interesse que um atacante obtenha após observá-los não deve ser nem maior nem menor em relação ao conhecimento que ele tinha antes de observá-los. Considerando-se como itens de interesse um dado remetente e um dado destinatário, pode-se dizer que eles não estão relacionados caso não se consiga inferir nenhuma informação sobre eles após a observação de todas as mensagens trocadas na rede de comunicação bem como dos próprios itens considerados.

A **anonimidade** pode ser definida em termos da **não-relacionabilidade**: se considerarmos os itens de interesse como as mensagens trocadas no sistema, pode-se definir a anonimidade como a não-relacionabilidade entre um sujeito e as mensagens que ele envia ou recebe. Não sendo possível identificar o sujeito

diretamente ou por suas mensagens, há uma certa melhoria na privacidade do indivíduo. No entanto, caso o conteúdo das mensagens possua caráter pessoal, a privacidade do indivíduo é afetada, mesmo não sendo possível identificá-lo. Deve-se, portanto, considerar não somente o relacionamento entre sujeitos e mensagens como também as próprias mensagens.

Dois conceitos aparecem relacionados às mensagens. O **sigilo de uma mensagem** implica que somente os sujeitos relacionados a esta mensagem conseguem visualizar seu conteúdo. Já a **não-observabilidade de uma mensagem** é o estado em que sujeitos não relacionados ao item de interesse não podem distinguir se este item existe ou não. Em particular, a **não-observabilidade** de uma comunicação implica que não é possível distinguir se dois sujeitos estão se comunicando, enquanto que em uma **comunicação em sigilo** pode-se até saber que dois sujeitos estão se comunicando, porém não se pode saber o teor da comunicação.

Desta maneira, em um sistema voltado à privacidade existem diversos aspectos que devem ser considerados, tais como a não-identificação dos sujeitos em comunicação (anonimato), a não-identificação da comunicação entre os sujeitos (não-relacionabilidade entre os sujeitos e/ou a não-observabilidade das mensagens) e o sigilo do conteúdo da comunicação. É importante ressaltar que tais aspectos não são mutuamente exclusivos, e a abordagem a ser considerada é dependente do problema..

3.3 Aspectos Jurídicos de Privacidade On-line

Além de atender preocupações individuais, as tecnologias relacionadas à privacidade refletem as necessidades de uma legislação, na medida em que estas tecnologias visam garantir o cumprimento desta legislação como de detectar o seu não-cumprimento.

Na legislação brasileira a questão de privacidade é tratada diretamente na Constituição Federal de 1988 em seu Artigo 5º (31):

“Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

...

X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

...

XII: é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

O Código Civil Brasileiro trata a questão da privacidade em seu Artigo 21 (32):

"A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

O Código de Defesa do Consumidor em seu artigo 43 protege também os dados pessoais de usuários que porventura estejam em um cadastro de um prestador de serviço (33,34):

"(i) os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão;

(ii) a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor;

(iii) direito do consumidor providenciar correção de seus dados (5 dias para o arquivista comunicar a alteração);

(iv) os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público"

Vale observar que tanto no artigo 5º, inciso X como no Artigo 21 não há referência ao tipo de ambiente no qual deve haver a privacidade, uma vez que esta é considerada uma característica intrínseca da pessoa, e não do ambiente no qual ela se encontra inserida.

A Europa, por sua vez, apresenta uma legislação bastante rígida e abrangente em relação à proteção da privacidade de seus indivíduos, incluindo mecanismos para a regulamentação e proteção da privacidade. Seguindo a Convenção Européia de Direitos Humanos, os países europeus criaram legislações para proteger os direitos dos cidadãos. No entanto, a questão da privacidade só começou de fato a ser tratada com leis específicas nos anos 70 (25).

A evolução da tecnologia e, em particular, dos mecanismos de processamento e comunicação de dados, em conjunto com a disparidade das legislações de privacidade entre os países europeus, provocaram uma preocupação maior com a

privacidade, em particular com os dados privativos dos indivíduos serem transferidos para países com um nível de proteção menor. Desta maneira, dois tratados foram definidos nos anos 80, que tiveram uma influência grande nas legislações modernas sobre privacidade (25): o *Guia para a Proteção da Privacidade e Fluxo de Dados Pessoas entre Fronteiras* (1980) da Organização para Cooperação e Desenvolvimento Econômico (*Organization for Economic Cooperation and Development* – OECD) e a *Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais* (1981) do Conselho da Europa (*Council of Europe* – COE).

Os tratados do COE e da OECD são equivalentes, ao definirem regras para o manuseio das informações pessoais em formato eletrônico, incluindo as fases de coleta, armazenamento e transmissão/disseminação de conteúdo. De uma maneira geral, elas requerem que os dados sejam obtidos de maneira justa e legal, usados somente para o propósito original, contenham apenas os dados relevantes ao propósito, estejam atualizados e disponíveis para o indivíduo, sejam mantidos de forma segura e sejam destruídos depois de utilizado. Ambas procuram regulamentar também o aspecto da transferência dos dados entre fronteiras, facilitando a transferência entre países signatários e restringindo a transferência para países que não se comprometeram com os princípios dos tratados. Requerem, ainda, que as legislações dos signatários sejam adaptadas para se adequar aos princípios dos tratados.

Em 1995, o Parlamento da União Européia instituiu a Diretiva da União Européia de Proteção de Dados 95/46/EC (35), com o intuito de compatibilizar as legislações de privacidade entre seus países membros com os objetivos de integração da União. Além de ratificar e explicitar os pontos dos tratados do COE e da OECD, introduz como um dos pontos chave que os dados só podem ser exportados para um país fora da União Européia se este oferecer proteção de dados adequada (36).

Tal diretiva foi posteriormente complementada pela Diretiva da União Européia de Privacidade em Comunicações Eletrônicas 2002/58/EC (37), que define a necessidade do consentimento do usuário para a interceptação ou vigilância de suas comunicações eletrônicas e para o envio de *spams*, bem como a necessidade de apagar, anonimizar ou ter o consentimento explícito do usuário em relação ao armazenamento de metadados relacionados ao tráfego do usuário (tanto dados

necessários para o propósito de transmissão de dados como dados relativos à localização de usuários) para fins de serviços de valor agregado (38).

Por sua vez, nos Estados Unidos da América (EUA) utiliza-se uma abordagem diferente sobre a questão da privacidade em relação à abordagem adotada nos países Europeus. Nos EUA, a questão da privacidade é tratada de forma setorial, com legislações, regulamentações e auto-regulamentações específicas por setor. Dentre os exemplos podem-se citar:

- *Video Privacy Protection Act* (1988): protege contra exposição não-autorizada os registros pessoais de aluguéis de fitas de videocassete e similares (39);
- *Cable Television Consumer Protection and Competition Act* (1992): determina as situações em que os dados pessoais dos usuários em um serviço de TV a cabo (ou similares) podem ser monitorados, armazenados e expostos com e sem a autorização do usuário (40);

É possível perceber portanto que as diferentes legislações também tratam de forma diferenciada a questão da privacidade. Enquanto a **legislação brasileira** trata a privacidade de forma bastante genérica, independente de onde ela é considerada e sem entrar em detalhes do tratamento dos dados, a **legislação norte-americana** trata a questão de privacidade de forma exclusiva ao setor considerado, porém com detalhes do tratamento dos dados. Por sua vez, as **diretivas européias** tratam a questão de forma genérica, à semelhança do tratamento brasileiro, porém define regras bastante extensas sobre como estes dados devem ser manuseados. De comum, todos eles tratam do controle dos dados privativos.

3.4 Soluções de Privacidade

Conforme (41), as soluções para proteção da privacidade utilizam 4 técnicas principais:

- **T1 - Agentes de anonimização intermediários:** técnica onde se utilizam um ou mais elementos intermediando a comunicação entre remetente e destinatários e trabalhando com a privacidade em nível de conexão TCP/IP. Estes agentes substituem dados da conexão do remetente (ex. endereço IP,

porta TCP) por seus próprios dados, de maneira a evitar a correlação entre um usuário e seus dados de conexão. Tais agentes podem também alterar o tráfego para evitar análises de padrões de tráfego (todos os pacotes saem do agente a uma taxa constante, independente da taxa com que foram recebidos);

- **T2 - Agentes de anonimização intermediários com filtros de aplicação:** técnica onde se utilizam um ou mais elementos intermediando a comunicação entre remetente e destinatários e trabalhando com a privacidade em nível de aplicação. Técnica similar à T1, porém os agentes analisam os dados das aplicações, sendo capazes de alterar e até mesmo eliminar cabeçalhos e outras informações do protocolo de aplicação capazes de identificar o usuário;
- **T3 - Agentes de pseudônimos:** técnica onde um agente cria para um usuário um conjunto de identidades especiais para usos, denominadas pseudônimos. Cada pseudônimo deve ser usado para apenas um único serviço (ex.: acesso a um servidor *web* específico ou envio de mensagens a um determinado remetente), minimizando a possibilidade de construção de perfis com dados de diferentes serviços. O agente fica, então, responsável pelo gerenciamento destes pseudônimos, bem como para o mapeamento do pseudônimo apropriado para cada uso;
- **T4 - Agentes de negociação:** técnica onde um remetente, antes de enviar um conjunto de dados para um destinatário, deve consultar antes um agente (tipicamente um *middleware*) para verificar se estes dados podem ser revelados de acordo com um conjunto de regras de privacidade definidas junto ao agente (políticas de privacidade).

Pode-se verificar que a maioria das soluções trata a questão da **privacidade** como uma **questão de anonimato**. Algumas soluções são bastante conhecidas, podendo-se citar:

- As redes do tipo **DC-Net** (*Dining Cryptographers Network*), baseadas no problema do Jantar dos Criptógrafos (*Dining Cryptographers* (42)) visam garantir o anonimato do remetente e do destinatário da comunicação. Para proteger o destinatário, uma rede DC-Net utiliza *broadcasts* na rede, com os dados encriptados de forma que somente o destinatário possa decriptá-los. Já

para o anonimato do remetente, a comunicação é feita em rodadas onde, a cada rodada, um pacote deve percorrer todos os elementos da rede, que devem individualmente alterar *bits* específicos de uma máscara no pacote que sinaliza se alguém está transmitindo, se ninguém está transmitindo ou se dois elementos estão transmitindo simultaneamente (colisão). Uma vez que todos os elementos alteraram os respectivos *bits* da máscara, o pacote deve se propagar novamente para todos os elementos da rede para que todos verifiquem se há algo transmitido na mensagem. Desta maneira, as redes do tipo DC-Net operam de forma mais adequada em topologias de anel (onde um pacote passa de forma determinística por todos os elementos da rede), com o uso do *broadcast* ajudando a mascarar análises de tráfego simples (seria necessária a análise em pontos distintos da rede para se poder descobrir o remetente). Apresenta, porém, uma latência grande (cada transmissão necessita de duas voltas no anel para se concretizar), inviabilizando seu uso em redes sensíveis a tempo como as redes de IPTV.

- Um **Anonimizador** é uma entidade confiável que fica entre o remetente e o destinatário, que provê a comunicação de forma anônima. É tipicamente implementado através de um roteador ou *proxy* que emprega uma combinação das técnicas T1 e T2, analisando o tráfego enviado e removendo cabeçalhos e campos que possam identificar o remetente (ex.: serviço *Anonymizer* (43)). A principal desvantagem de um Anonimizador é o fato de que ele tem acesso ao conteúdo da comunicação, sendo um ponto de vulnerabilidade na anonimidade dos usuários caso seja controlado por um atacante. Além disso, como toda a comunicação trafega pelo mesmo Anonimizador, ele é vulnerável a análises de tráfego que correlacionam o tráfego de entrada com o tráfego de saída, independente de haver ou não criptografia no conteúdo.

Há diversas redes *overlay* que estendem a idéia do anonimizador, provendo um conjunto de entidades confiáveis (que formam a rede *overlay*) para prover a comunicação de forma anônima. Redes do tipo Mix-Net (44) baseiam-se na idéia de uma cadeia de computadores confiáveis (denominados *Mixes*). Para prover o anonimato, cada *Mix* utiliza várias técnicas: cada *Mix* reordena o tráfego recebido (para eliminar possíveis correlações entre pacotes de entrada e saída), provê uma

taxa de envio de mensagens constante, com mensagens do mesmo tamanho, independente da taxa de recebimento da mensagem (através do envio de tráfego espúrio para os outros *Mixes*, inserção de atrasos nos pacotes recebidos e de *padding* nas próprias mensagens). Para proteger o conteúdo das mensagens, utiliza várias camadas de criptografia: o remetente A escolhe uma seqüência de *Mixes* $M_1, M_2, \dots, M_i$, e encapsula a mensagem X a ser enviada para o destinatário B com as chaves públicas K_j de B e dos *Mixes* escolhidos:

$$K_1 (K_2 (\dots (K_i (K_B (X)))))$$

Desta maneira, as redes do tipo Mix-Net apresentam um custo muito alto para o uso em redes sensíveis a atrasos, dado o uso extensivo de criptografia assimétrica, os reordenamentos de mensagens e atrasos inseridos, que acabam por afetar a latência e o *jitter* na rede. Tais características derivam de sua premissa original, de proteger a privacidade no tráfego de e-mail.

Outras redes *overlay* anonimizadoras utilizam-se de variações sobre a idéia das redes Mix-Nets. Por exemplo, as redes de *Onion Routing* (45,46) utilizam a idéia de uma cadeia de computadores confiáveis, denominados roteadores *Onion* (*Onion routers*), para prover a privacidade do remetente e do destinatário, utilizando várias camadas de criptografia. Apresentam as seguintes diferenças em relação a redes Mix-Nets:

- Utilizam-se criptografia assimétrica fim-a-fim (entre remetente e destinatário) e criptografia simétrica entre os roteadores;
- As rotas entre os *Onion routers* são escolhidas pelos próprios roteadores de forma dinâmica (cada pacote pode ir por uma rota diferente, com comprimentos diferentes);
- A rede visa suportar tráfego interativo (ex.: telnet e SSH – *Secure Shell*) e tráfego *web*. Desta maneira, o atraso nos roteadores *Onion* é restrito, e eles não reordenam as mensagens nem inserem atrasos aleatórios no fluxo.

Há outras redes *overlay* de anonimidade que utilizam técnicas de *broadcast*, tais como a P^5 (47) e a Herbivore (48). No caso da P^5 , uma entidade confiável envia um *broadcast* para todas as outras entidades confiáveis da rede com taxa constante (enviando tráfego espúrio quando não houver dados a serem transmitidos). Já a

Herbivore baseia-se no conceito das DC-Nets, agrupando os usuários em grupos de *broadcast* menores para melhorar a eficiência da mesma.

A técnica do tipo T3 pode apresentar um potencial interessante para a questão da anonimidade sem introduzir o *overhead* da comunicação. Soluções como o P3P (*Platform for Privacy Preferences*) (49) criam, a partir da identidade do usuário, diversos pseudônimos, cada qual para ser usado em serviços diferentes, evitando-se assim a correlação entre os serviços.

Por fim, soluções do tipo T4 de negociação de privacidade, como o P3P, são necessárias para se atender aos requisitos legais como os existentes na Europa, fornecendo ao usuário os meios de controlar as suas informações junto aos provedores de serviços.

3.5 Considerações Finais

O conceito de privacidade é uma questão antiga, intrinsecamente relacionado à associação entre um indivíduo e um conjunto de informações (ditas privativas) que revelam detalhes de suas vidas, cuja exposição nem sempre é desejada. Diferentes indivíduos e mesmo diferentes países têm visões distintas do que é uma informação privativa e de como deve ser feito a proteção destas informações contra exposição indevida.

Há diferentes maneiras de se enxergar o conceito de privacidade em uma rede de comunicação de dados. A privacidade pode ser determinada tanto pela anonimidade (não se sabe quem é o indivíduo), pela não-relacionabilidade (tem-se informações privativas, mas não é possível relacioná-las a um indivíduo), pelo sigilo (não se consegue obter informações privativas) e pela não-observabilidade (não se consegue distinguir quais informações são privativas no conjunto de informações observadas).

Ao se utilizar um serviço *online*, é comum se pensar na privacidade somente em relação a informações pessoais, como data de nascimento ou número de carteira de identidade. No entanto, a forma como um indivíduo utiliza um serviço constitui um

conjunto de informações significativas, que pode revelar detalhes privativos sobre este indivíduo (ex.: quando ele utiliza o serviço, o que ele procura, entre outros).

Sendo assim, é necessária a análise dos aspectos de privacidade dentro do contexto de um serviço. Os capítulos seguintes tratam a questão de privacidade dentro do escopo do serviço de IPTV, com a análise de problemas, definição de requisitos e uma proposta para o tratamento da privacidade neste serviço de forma apropriada.

4 PRIVACIDADE EM IPTV

O entendimento da questão da privacidade em ambientes de TV tradicionais é fundamental para se entender as questões de privacidade dentro do contexto de IPTV. De posse da análise da privacidade em ambientes de TV tradicional e das ameaças à privacidade específicas no contexto de IPTV, define-se um conjunto de requisitos que uma solução de privacidade para IPTV deve atender. Tais requisitos serão utilizados como base para a análise das soluções de privacidade vistas em 3.4, verificando-se a adequação das mesmas dentro do contexto de IPTV.

4.1 *Descrição do Problema*

A forma como os usuários utilizam um serviço de IPTV (ex.: quando e quais canais os usuários assistem) constituem um conjunto de informações importantes sobre estes usuários. Para um provedor de IPTV, a capacidade de monitorar o uso de todos os canais e seus usuários permite não só categorizar o público alvo de cada programa de forma mais precisa (desejado para a venda de espaço de propaganda nos programas), mas também identificar as preferências de cada usuário. A identificação das preferências dos usuários pode ser uma característica desejada para o provimento de serviços personalizados; porém ao mesmo tempo permite oferecer propagandas altamente personalizadas a seus usuários, o que nem sempre é desejável (ex.: uma propaganda intrusiva voltada aos filhos do assinante, chamando-os pelos seus próprios nomes e incitando-os a comprar certos produtos).

É importante destacar que na TV tradicional (aberta e por assinatura), a associação entre usuários e hábitos de uso do serviço só é permitida com a autorização do usuário, seja devido a restrições tecnológicas (nem toda tecnologia de transmissão possui um canal de retorno para relatórios de uso) como restrições legais estabelecidas através de legislações próprias de cada país (como exemplo, a legislação norte-americana *Cable Television Consumer Protection and Competition Act*, de 1992 (40), que trata da privacidade no contexto de TVs a cabo). Sendo assim, os usuários de um serviço de TV, de uma maneira geral, não estão

acostumados a terem seu comportamento monitorado dentro de suas próprias residências.

Por sua vez, em um sistema de IPTV, tem-se uma facilidade tecnológica muito maior para se monitorar os hábitos de consumo de um usuário. Por exemplo, os hábitos de consumo do usuário podem ser monitorados por alguém espionando o tráfego. Dada as características de controle e gerenciamento da rede de transporte do serviço de IPTV (necessárias para garantir a qualidade do serviço), é razoável supor que qualquer monitoração seja proveniente do provedor de IPTV (ou do provedor da rede de transporte, se diferente do provedor de IPTV). No entanto, é possível também a monitoração indireta por usuários maliciosos do serviço, que podem utilizar diversas técnicas para captura do tráfego desejado, caso não haja proteção adequada na rede de transporte (ex.: ataques de envenenamento de rotas¹¹, envenenamento de serviços de nomes¹², cópia de tráfego *multicast*, entre outros).

Entende-se, por **privacidade em sistemas de IPTV**, a **impossibilidade de criação de um perfil de usuário**, ou seja, a **impossibilidade de relacionar um usuário a seus hábitos de consumo** (serviços e conteúdos assumidos) **a partir da monitoração do tráfego do usuário em um dado ponto da rede de transporte**. Desta caracterização, define-se um **sistema de IPTV com mecanismos de privacidade parcial** como sendo um **sistema onde somente perfis parciais de usuário podem ser criados a partir da referida monitoração**. Tais definições **vão ao encontro da abordagem de não-relacionabilidade apresentada em 3.2**.

Para um melhor entendimento destas definições é necessário um entendimento de como um usuário pode ser identificado e como pode ser criado um perfil de usuário em uma arquitetura de IPTV.

---

¹¹ Ataque que insere rotas falsas em um roteador, visando redirecionar um determinado tráfego para uma máquina que não faz parte do fluxo normal daquele tráfego (por exemplo, para captura de pacotes).

¹² Ataque que insere um mapeamento falso em um serviço de nomes como DNS (*Domain Name System*), com o intuito de redirecionar o tráfego para uma máquina inválida (por exemplo, *sites* falsos de bancos que capturam senhas dos usuários).

4.2 Criação de um Perfil de Uso do Serviço

Um perfil de uso do serviço caracteriza-se pela identificação de um usuário e pela correlação entre esta identificação, a forma como ele consome o serviço e eventuais dados complementares (por exemplo, dados cadastrais do usuário). Para um melhor entendimento da criação de um perfil de uso em um ambiente de IPTV, é necessário verificar como se caracteriza o perfil de uso em um ambiente de TV tradicional.

4.2.1 TV tradicional

Conforme mencionando anteriormente, na TV aberta não há a preocupação com a privacidade dos telespectadores, até mesmo por uma questão tecnológica: por não possuir um canal de retorno, não é possível saber o que os usuários estão assistindo (na verdade não é possível saber nem quem são e onde estão os telespectadores). Para determinar a audiência da TV, o IBOPE (Instituto Brasileiro de Opinião Pública e Estatística) utiliza um método com diferentes passos, cujos principais são:

- **Escolha da Amostra:** os usuários são selecionados conforme métodos estatísticos de amostragem, utilizando-se dados do censo demográfico brasileiro feito pelo IBGE (Instituto Brasileiro de Geografia e Estatística) e dos estudos sócio-demográficos e de consumo realizados pelo próprio IBOPE (50);
- **Coleta Automatizada:** utiliza-se, para a coleta, um aparelho desenvolvido pelo IBOPE denominado *peoplemeter*. Cada usuário que liga a televisão deve se identificar no *peoplemeter*, que se encarrega de coletar os dados periodicamente, e enviá-los de forma *on-line* (via sinais de rádio) ou em lote no final do dia (via linha telefônica) para a Central do IBOPE, para validação e processamento.

Figura 9 – Aparelho do IBOPE para coleta de parâmetros de audiência de TV

- **Processamento:** Os dados enviados pelos diversos *peoplemeters* são validados e correlacionados com a programação dos canais assistidos, de maneira a se definir a audiência de cada programa.

Os serviços de TV por assinatura apresentam limitações semelhantes às da TV aberta, uma vez que nem todas as tecnologias e infra-estrutura destes serviços oferecem o canal de retorno. Mesmo os mecanismos de proteção existentes prescindem do uso de um canal de retorno: o provedor efetua um *broadcast* com os parâmetros de segurança associados a cada *Set-Top Box* (STB), que indicam quais canais cada STB têm permissão de exibir e os parâmetros necessários para a visualização dos canais protegidos. Sendo assim, a questão de privacidade é análoga a das TVs abertas (novamente, como ilustração, o IBOPE utiliza para a medição de audiência em TVs por assinatura da mesma metodologia de medição de audiência em TVs abertas), apesar dos provedores terem as informações relacionadas aos usuários do serviço.

4.2.2 Ambientes de IPTV

Diferentemente do caso da TV aberta, que exige equipamentos próprios para a monitoração do uso do serviço, em um serviço de IPTV tal monitoração poderia ser efetuada pelos HDGs (*Home Domain Gateways* - 2.3.4) ou mesmo via rede de transporte (2.3.1), através da simples monitoração do tráfego IP de um usuário escolhido.

A Figura 10 ilustra quais os principais tráfegos e identificadores dentro da arquitetura que, ao serem monitorados, permitem a criação do perfil de uso do serviço de um dado usuário.

Figura 10 – Identificação de elementos na arquitetura utilizados na criação do perfil de um usuário

Há diversas maneiras de se identificar o usuário em um serviço de IPTV:

- **Identificadores de conexão:** identificadores necessários para a comunicação entre o usuário e o provedor de serviço, tais como o endereço IP e endereço MAC do HDG;
- **Identificadores de serviços IPTV:** identificadores necessários para ambientes de serviços diferenciados de acordo com o usuário, tais como diferentes pacotes de canais ou conteúdos personalizados. Em geral são relacionados a mecanismos de autenticação do usuário (ex.: senha).
- **Identificadores de DRM:** identificadores associados aos mecanismos de DRM, tais como chaves dos usuários.

Tais identificadores por si só não revelam quem é o usuário do serviço, devendo ser relacionado com dados cadastrais para tanto. No entanto, é possível, mesmo sem uma identificação completa do usuário, monitorar o seu uso (ex.: monitorar os

hábitos do usuário com IP 10.20.30.40 ou do HDG com endereço MAC AA:BB:CC:11:22:33).

Para o uso anônimo de um serviço de IPTV, seria necessário que estes identificadores fossem todos variáveis, de maneira que não se pudesse relacionar os conteúdos a um identificador fixo. Tal característica exigiria uma arquitetura extremamente complexa e de difícil gerenciamento.

Dado que o usuário é passível de identificação, a criação do perfil de uso do serviço é feita de forma análoga à executada na TV aberta. Para a criação de um perfil de usuário assume-se que todo o tráfego de um usuário com o provedor de serviço esteja sendo monitorado e que haja algum identificador fixo associado ao usuário (por exemplo, #123956).

Como passo inicial, identificam-se os canais assistidos pelo usuário (Figura 11), de forma análoga à coleta efetuada pelo *peoplemeter* em 4.2.1.

Figura 11 – Exemplo de Criação de Perfil de Usuário: Identificação dos Canais

Os canais são identificados facilmente através da transmissão *multicast* e do EPG. (*Electronic Program Guide* - 2.2.2) Cada canal de *broadcast* na prática é um *stream* de *multicast*, com um endereço de *multicast* IP próprio, e somente os usuários que requisitam acesso ao canal fazem parte do grupo de *multicast*. Como o protocolo utilizado para o *multicast*, o IGMP (*Internet Group Management Protocol*) versão 3 (51) não possui mecanismos de segurança padronizados, um atacante espionando a rede poderia observar as requisições de IGMP (*IGMP join*) para associar um determinado usuário a uma determinada sessão de *multicast*. Além disso, há

diversos equipamentos de rede (muitos de baixo custo) que implementam uma funcionalidade chamada *IGMP snooping* que, através da monitoração dos mesmos pacotes de *IGMP join*, determinam para quais portas do equipamento o tráfego *multicast* deve ser redirecionado. Desta maneira, é possível para um espião saber se um determinado usuário participa de uma dada sessão de *multicast*, caso ele tenha acesso ao equipamento da rede de transporte conectado à última milha do usuário monitorado.

Caso um dos canais assistidos esteja protegido por mecanismos de DRM, por si só o fato do usuário participar de um grupo de *multicast* não indica que ele assistiu ao canal. Para tanto deverá ser efetuado um passo extra, de correlacionar os conteúdos vistos com o respectivo histórico de requisição de licenças por parte do usuário. É importante ressaltar que o LS (*License Server* - 2.3.7) sabe sempre quais HDGs têm permissão de decriptar cada conteúdo.

Uma vez identificadas as sessões de *multicast* do usuário, o EPG, por sua vez, faz o mapeamento entre os identificadores do canal (número ou nome do canal) com os identificadores de conexão (endereço IP de *multicast*).

Os dados dos canais assistidos são, então, sobrepostos com os metadados do conteúdo, tais como os contidos no EPG (Figura 12). Dado que o EPG contém a programação do canal, em particular ele indica qual é o conteúdo em exibição em um dado momento do *stream* de *multicast* (Figura 12 – setas vermelhas)

Figura 12 – Exemplo de Criação de Perfil de Usuário: Correlação com Metadados

Podem haver metadados que não são distribuídos no EPG, por não apresentarem utilidade prática para os usuários do serviço ou por sua distribuição não ser conveniente, tais como identificadores dos intervalos comerciais (Figura 12 – setas verdes) ou granularidade maior em relação ao conteúdo (Figura 12 – setas azuis).

Estes dados monitorados mais os metadados pertinentes são correlacionados com os dados dos usuários, formando um perfil específico de um determinado período de monitoração (Tabela 2).

Tabela 2 – Exemplo de Criação de Perfil de Usuário: Correlação com dados do Usuário

Assinante #123956	Hábitos dia 24/6/2007
Sr. Luiz da Silva End. CPF, RG Renda / Histórico de Crédito Filhos	1) Assistiu Novela canal 5 até o fim • com troca de canais nos intervalos 2) Assistiu Noticiário Esportivo canal 2 parcialmente • sem troca de canais nos intervalos • parada após notícias Palmeiras 3) Assistiu Noticiário Geral canal 3 parcialmente • não se pode inferir comportamento nos intervalos • parada após bloco de notícias políticas

Por fim, a repetição deste processo por vários períodos e correlação entre eles completa o perfil do usuário, agregando a periodicidade de seus hábitos de consumo (Tabela 3).

Tabela 3 – Exemplo de Criação de Perfil de Usuário: Adição de periodicidade

Assinante #123956	Hábitos Semanais
Sr. Luiz da Silva End. CPF, RG Renda / Histórico de Crédito Filhos	1) Assistiu Novela canal 5 até o fim – 100% • com troca de canais nos intervalos – 100% 2) Assistiu Noticiário Esportivo canal 2 parcialmente - 60% • sem troca de canais nos intervalos – 40% • parada após notícias Palmeiras – 60% 3) Assistiu Noticiário Geral canal 3 parcialmente – 60% • parada após bloco de notícias políticas - não se pode inferir

É importante ressaltar que, na rede de IPTV, qualquer espião teria acesso tanto aos dados de uso do serviço como aos metadados da programação, podendo fazer quase todos os passos de correlação descritos (só não teria acesso aos dados cadastrais do usuário, uma vez que tais dados são tipicamente obtidos como parte de uma transação comercial e/ou contratual)

4.3 Requisitos de Privacidade para Ambientes de IPTV

Um ambiente de IPTV deve proteger não somente os direitos dos provedores de conteúdo como também os direitos dos consumidores, em particular a privacidade do usuário no uso do serviço. Desta maneira, deseja-se garantir a privacidade do destinatário do serviço (o consumidor dos *streams* de vídeo), principalmente dos seus hábitos de consumo:

- Quais canais são assistidos;
- Quais gêneros de programa são assistidos;
- Quando os canais são assistidos e com que frequência e periodicidade eles são assistidos;
- Tempo médio que o telespectador passa assistindo à televisão;
- Em que sequência estes canais são vistos;
- Em que sequência os programas são vistos;

Para tanto, o ambiente de IPTV deverá atender diversos requisitos específicos de privacidade, muitos derivados de ambientes de multimídia e/ou de DRM (52).

Em relação ao próprio serviço de IPTV, são definidos os seguintes requisitos de privacidade:

- S1 – Os mecanismos de privacidade deverão ser aplicáveis ao conteúdo de canais de *broadcast*;

- S2 – Os mecanismos de privacidade deverão ser aplicáveis tanto para canais básicos como para canais *premium* (conforme classificação de canais descritas em 2.2.1);
- S3 – Os mecanismos de privacidade não devem impactar a QoE (*Quality of Experience*) do serviço ou apresentar um impacto mínimo no QoE do usuário;
- S4 – Os mecanismos de privacidade deverão apresentar robustez contra monitoração não-autorizada de tráfego de um usuário;
- S5 – A ativação dos mecanismos de privacidade deverá ser decidida pelo usuário, podendo ser ativados por tipo de conteúdo.

Os mecanismos de privacidade devem levar em consideração os aspectos de privacidade associados aos mecanismos de DRM, quando eles forem utilizados na arquitetura. Sendo assim, os seguintes requisitos devem ser atendidos para arquiteturas que façam uso de DRM:

- D1 – Os mecanismos de privacidade devem manter a proteção do conteúdo provida pelos mecanismos de DRM contra acessos não autorizados;
- D2 – Não deverá ser possível correlacionar um usuário a todas as licenças por ele recebidas (em outras palavras, relacionar o usuário a todo o conteúdo que ele teria condições de assistir).

Os mecanismos de privacidade devem, também, levar em consideração os mecanismos de personalização do IPTV, de acordo com os seguintes requisitos:

- P1 – Personalização do conteúdo deverá ser permitido;
- P2 – Sistema deve suportar criação de EPGs personalizados;
- P3 – O usuário poderá definir algumas categorias às quais ele pertence (tais como faixa etária, faixa de renda, entre outras), visando uma melhor personalização do conteúdo e/ou EPG;
- P4 – Os aspectos de personalização (de conteúdo e EPG) não poderão ser derivados via monitoração de tráfego;
- P5 – O sistema não deve disponibilizar os aspectos de personalização a terceiros, a não ser mediante aprovação do usuário.

Conforme visto anteriormente, estatísticas de uso podem ser necessárias em alguns casos, como a monitoração de audiência ou para personalização de conteúdo. Sendo assim, a coleta de estatísticas deve atender a alguns requisitos:

- E1 – O sistema deve permitir a coleta de estatísticas de uso, porém o controle desta coleta deve ser do usuário (i.e., coleta só deve ser permitida mediante autorização do usuário);
- E2 – A autorização para a coleta de estatísticas de uso não implica em autorização para a divulgação das estatísticas, devendo estas serem, também, explicitamente autorizadas;
- E3 – A solução não deve invalidar o uso de mecanismos tradicionais de monitoração de uso do serviço, utilizando aparelhos externos.

4.4 *Análise de Soluções Existentes de Privacidade sob Ótica de IPTV*

Trabalhos relacionados à privacidade concentram-se, em sua maioria, nos aspectos de anonimidade de remetente e destinatário, bem como no sigilo das mensagens. A maioria destes trabalhos tende a privilegiar tráfegos IP genéricos (tais como (45,46)) ou tráfegos de aplicações específicas (em particular anonimidade no tráfego *web*, tais como (43,53)). Dadas estas características do tipo de tráfego atendido, tais arquiteturas não atendem as especificidades de um tráfego multimídia sensível a atrasos e *jitter*, como é o caso do tráfego de *streams* de vídeo IPTV (requisito S3). Um exemplo são as técnicas de anonimidade através de agentes de anonimização intermediário, que provêem privacidade em detrimento do desempenho da comunicação (através do roteamento das mensagens por um ou mais destes agentes).

Há também projetos de anonimidade de escopo mais amplo, como os projetos PRIME (*Privacy and Identity Management for Europe*) (54) e FIDIS (*Future of Identity in the Information Society*) (55), que visam alcançar a privacidade através do gerenciamento de identidade do mundo *on-line* de forma casada com a do mundo *offline*. Tanto estes projetos como outros projetos que utilizam técnicas de

pseudônimo, enquanto interessante por não introduzirem *overhead* na comunicação não se apresentam como viáveis dentro do contexto do IPTV, uma vez que eles consideram somente um dos tipos de identificação possíveis neste contexto, conforme visto em 4.2 (estes projetos consideram apenas a identificação do indivíduo, deixando de lado identificadores associados à conexão e ao uso opcional de DRM).

Há trabalhos cujo foco se aproxima mais da necessidade da aplicação de IPTV, tais como os trabalhos de privacidade em sistemas de DRM. Em (36) define-se uma arquitetura para o gerenciamento de privacidade (*Privacy Rights Management*) associada ao sistema de DRM. Tal arquitetura, porém, tem o foco definido no controle do perfil dos usuários, visando atender os requisitos da Diretiva 95/46/EC da União Européia, através da extensão da linguagem de descrições de direitos ORDL (*Open Rights Description Language*) para especificação dos parâmetros de privacidade em conjunto com as próprias permissões do conteúdo. Ela não trata, no entanto, os aspectos de privacidade e robustez contra análise de tráfego.

Uma classe interessante de trabalhos de privacidade são os baseados em modelos de PKI diferenciados do modelo de certificados X.509 tradicionais, que são formalmente associados a um indivíduo. A arquitetura de SPKI (56,57) associa um certificado de autorização a uma chave pública apenas, e não a uma chave pública e uma identificação, como no caso dos certificados X.509. Tal arquitetura é estendida em (58) com algumas técnicas de anonimidade. Certificados criptografados (com apenas alguns campos visíveis) são propostos em (59), em conjunto com os mecanismos de validação do certificado. O trabalho apresentado em (60) baseia-se na integração do modelo de SPKI com o modelo de DRM, especificamente para o modelo de distribuição de áudio e vídeo. No entanto, tais técnicas se aplicariam somente à anonimidade dos identificadores de serviço IPTV e DRM, restando ainda a necessidade de se anonimizar identificadores de conexão como endereços IP e MAC (4.2).

Os requisitos E1 e P5 implicam na utilização de um mecanismo de negociação de privacidade, tal como o P3P (*Platform for Privacy Preferences*) (49), para a indicação dos dados válidos para divulgação. Há propostas para se estender o padrão P3P (originalmente para navegação *web*) para suportar as características específicas de ambientes DRM. Em (52) apresentam-se os requisitos para tal extensão e (61)

propõe-se uma arquitetura denominada PREP (*Policy and Rights Expression Platform*), para atender estes requisitos em aplicações baseadas em *web*.

Para um ambiente de IPTV é necessário, portanto, uma solução que combine diferentes técnicas e atente às particularidades do ambiente do tipo de serviço, QoE e aspectos de tráfego do conteúdo.

4.5 Considerações Finais

Em um ambiente de IPTV, a questão de privacidade é mais crítica do que em um ambiente tradicional, uma vez que o ambiente facilita a monitoração dos hábitos de consumo de um usuário, permitindo a criação de um perfil completo do uso do serviço pelo usuário.

Há diferentes maneiras de um provedor de IPTV identificar os usuários a partir de seus tráfegos na rede, tais como através de endereços de rede e autenticação do serviço. Além disso, em sistemas que utilizam DRM, o levantamento das preferências dos usuários é ainda mais facilitado, uma vez que os usuários podem ser identificados por chaves criptográficas assimétricas e suas preferências através do histórico de requisição de licenças de conteúdo.

Dada a facilidade de criação de um perfil de uso do serviço e da inadequação dos mecanismos tradicionais de privacidade dentro de um ambiente de IPTV, é necessária uma arquitetura que proteja a privacidade dos usuários, atentando para as particularidades do ambiente. O capítulo seguinte apresenta uma proposta de arquitetura com estas características e discute suas vantagens e desvantagens.

5 ARQUITETURA PARA AMBIENTES DE IPTV COM SERVIÇOS DE PRIVACIDADE

A arquitetura proposta neste trabalho visa oferecer um serviço de IPTV com mecanismos de privacidade para conteúdo em canais básicos e *premium* (2.2.1), permitindo a personalização da programação do conteúdo.

5.1 Visão Geral

Conforme visto, os mecanismos de privacidade tradicionais não atendem os requisitos descritos anteriormente para sistemas IPTV, principalmente em função da dificuldade de se anonimizar o usuário e dos requisitos de desempenho inerente ao tráfego multimídia. Dada estas dificuldades, uma solução para a questão de privacidade exige tanto uma abordagem alternativa às técnicas usuais de anonimato como a utilização de mecanismos que minimizem o impacto no tráfego dos serviços IPTV em consequência das técnicas de privacidade utilizadas. Sendo assim, este trabalho propõe a combinação de técnicas de P2P (*Peer-to-Peer*) e de *caching* para atender os requisitos descritos em 4.3, e *para* prover a privacidade com baixo impacto nos serviços prestados pelo sistema IPTV.

Nesta proposta utiliza-se do lado do usuário um HDG (*Home Domain Gateway*) com capacidade de armazenamento, para *caching* do conteúdo. Uma vez recebido, o conteúdo pode ficar armazenado no HDG; um HDG de um outro assinante “vizinho” pode requisitar este conteúdo via P2P, ao invés de requisitá-lo diretamente ao SDP (*Service Distribution Provider*). Desta maneira, forma-se uma rede P2P de *caching* entre os HDGs e uma via alternativa para a requisição de conteúdo.

A capacidade de armazenamento é utilizada, também, para a personalização do conteúdo, de maneira análoga à utilizada em mecanismos de PVR (*Personal Video Recorder*): uma vez armazenado o conteúdo, o usuário poderá assisti-lo quando desejado (funcionalidade conhecida também como *timeshifting*).

Dada esta via alternativa para a requisição de conteúdo, o trabalho propõe uma abordagem alternativa para a questão da privacidade: ao invés de procurar

anonimizar o usuário, procura-se invalidar a criação do perfil de uso do serviço. Para tanto o HDG efetua parte das requisições através da rede P2P de forma aparentemente aleatória, balanceando as requisições entre P2P e *multicast*.

Por fim, caso o ambiente utilize-se de DRM (*Digital Rights Management*), a arquitetura proposta contempla a modificação da forma de distribuição de licenças e chaves em relação à forma associada à arquitetura de referência descrita no capítulo 2. Para tanto, propõe-se estender o EPG (*Electronic Program Guide*) com os parâmetros de DRM, constituindo-se um EPG estendido (*Extended EPG – EEPG*). O EEPG contém não somente os metadados do conteúdo, mas também as licenças de cada conteúdo, criptografadas com chaves de sessão alteradas periodicamente (e recebidas durante o processo de autenticação no provedor de serviço). Este EEPG pode ser transmitido via *multicast* para todos os assinantes do serviço, sendo armazenado no HDG e localmente personalizado de acordo com as preferências do usuário definidas no próprio HDG.

Na próxima seção, é descrita a arquitetura modificada para sistemas de IPTV com o objetivo de atender os requisitos de privacidade relacionados em 4.3.

5.2 Arquitetura do Sistema IPTV

A arquitetura do ambiente de IPTV com serviços de privacidade é semelhante à descrita em 2.3 em relação aos seus componentes básicos. Uma alteração significativa refere-se aos limites do ambiente do provedor e do domínio doméstico: o controle do HDG deixa de ser exclusivo do provedor de IPTV para ser compartilhado com o domínio doméstico (Figura 13). Uma outra alteração é a inclusão de nós de *cache* na rede de transporte, para otimização dos mecanismos de privacidade e provimento de funcionalidade de *timeshifting*.

Figura 13 – Arquitetura de IPTV Modificada para ambiente de privacidade

Além destas alterações na arquitetura, a solução de privacidade, exige mudanças nos elementos do sistema, bem como em algumas operações particulares. A Figura 13 ilustra algumas destas diferenças nas operações, tais como a mudança na distribuição dos parâmetros de DRM na forma de RSOs (*Rights and Service Objects*) embutidos no EEPG.

5.2.1 Componentes da Arquitetura

A solução de privacidade proposta exige a alteração em alguns componentes-chaves do sistema. Alterações significativas no HDG acabam por definir uma rede P2P dentro da rede de transporte do provedor, que exige também alterações para a otimização do acesso, via nós de *cache*. Por fim, o EPG deve ser estendido para refletir as alterações na arquitetura e para prover a privacidade no caso de ambientes com DRM.

5.2.1.1 HDG com armazenamento

A utilização de um HDG com capacidade de armazenamento é essencial para a privacidade do usuário. A viabilidade de tal dispositivo pode ser facilmente comprovada pela miríade de soluções multimídia existentes com discos rígidos internos, tais como reprodutores de MP3, filmadoras, gravadores de DVD (*Digital Versatile Disc*) domésticos, PVRs (*Personal Video Recorders*) e consoles de vídeo-games. É possível encontrar dispositivos com até 500 GB e capacidade de expansão (ex.: PVR da Sony, modelo DHG-HDD500), sendo mais comumente encontrados equipamentos com capacidade entre 80 e 160 GB¹³.

Um outro aspecto importante é que o controle do HDG não deve ser exclusivo do provedor, uma vez que não seria possível saber quais processos são executados pelo provedor no HDG. O modelo assumido aqui é o de um HDG modular, onde a parte de privacidade e o *caching* ficam sob controle do usuário, e um módulo complementar é responsável pela comunicação com o provedor. A viabilidade deste modelo pode ser vislumbrada ao se considerar o HDG como um dispositivo que o usuário adquire em lojas, de acordo com as características que lhe forem mais convenientes, e que o módulo de comunicação com o provedor seja um cartão fornecido pelo próprio. Tal modelo é similar aos sistemas de TV a cabo existentes nos Estados Unidos, onde há um padrão para o cartão do provedor, denominado CableCARD (62).

Vale ressaltar que os mecanismos de privacidade dentro do HDG deverão, também, ser executados dentro do ambiente confiável existente no mesmo, conforme visto em 2.3.4. Este ambiente confiável deve garantir que alterações no HDG possam impactar a privacidade do usuário (por exemplo, um processo que registre as ações do usuário, análogo a um *keylogger*¹⁴ em computadores pessoais).

---

¹³ A capacidade de armazenamento é impactada, também, por aspectos de portabilidade e tamanho dos dispositivos, uma vez que discos rígidos de dimensões físicas menores possuem menor capacidade.

¹⁴ Um *keylogger* é um processo malicioso que, quando em execução, captura a sequência de teclas pressionadas pelo usuário no teclado, enviando-as para um atacante quando apropriado. Desta maneira é possível identificar *sites* acessados, senhas digitadas, e-mails escritos, entre outros.

5.2.1.2 Rede P2P

Há vários estudos que incorporam, na arquitetura de um sistema de IPTV, uma rede P2P, de maneira a prover funcionalidades adicionais ao serviço, tais como *caching* na rede e *timeshifting* de conteúdo, utilizando-se para tanto os próprios HDGs ou outros elementos na rede de transporte (65,66,63,64).

Com certos cuidados, uma rede P2P contribui para o aspecto de privacidade ao oferecer uma via alternativa para a requisição e transmissão do conteúdo: além da transmissão normal, via *multicast*, o usuário poderia também requisitar ao vizinho um conteúdo, independente do vizinho tê-lo ou não em *cache*. Tal mecanismo atende ao requisito S4, uma vez que, ao se utilizar um protocolo P2P criptografado, é possível obter a não-relacionabilidade entre usuário e conteúdo: qualquer monitoração do tráfego do usuário indicaria apenas um tráfego P2P entre diversos HDGs, sem contudo indicar o conteúdo.

Dentre os trabalhos na área, utilizou-se como base o trabalho de (67), no qual uma rede P2P baseada em BitTorrent foi incorporada ao ambiente de IPTV para prover a funcionalidade de *timeshifting*. Em (67) os HDGs registram em uma *Distributed Hash Table* (DHT) os conteúdos que possuem em seus respectivos *caches*. Para efetuar o *download* de um conteúdo, um HDG procura na DHT outros HDGs que possuam o conteúdo desejado, requisitando o conteúdo diretamente aos nós relacionados na DHT. Além dos HDGs, nós de *caching* na rede de transporte do provedor participam da rede P2P para melhorar o desempenho do *timeshifting*, atuando de forma análoga aos HDGs para prover o conteúdo.

O presente trabalho baseia-se em (67), introduzindo diferenças importantes. Uma delas diz respeito à forma de utilização da DHT: a utilização da DHT em (67) permite correlacionar o usuário aos seus hábitos de consumo, uma vez que cada usuário registra na DHT o que eles possuem em *cache*. Sendo assim, neste trabalho, a DHT é utilizada de forma diferenciada, apenas para a localização de HDGs, e não do conteúdo armazenado em cada dispositivo.

Uma outra diferença importante é no conceito de **indireção de requisições**. No protocolo BitTorrent e em (67), um *peer* requisita os blocos de conteúdo diretamente aos *peers* que os possuam. Na arquitetura proposta, as requisições são feitas para

outros HDGs, independente deles possuírem ou não os conteúdos desejados. Os HDGs que receberem tais requisições, se não possuírem o conteúdo desejado, efetuam o que se denomina uma indireção da requisição: podem novamente encaminhar a requisição para outros nós na rede, independente deles possuírem o conteúdo, ou então podem obter o conteúdo desejado via requisições aos nós de *cache* e a outros HDGs, repassando o conteúdo ao requisitante original. Desta maneira, o trabalho proposto utiliza-se do protocolo BitTorrent modificado para suportar a indireção da requisição. O conceito de indireção de requisições encontra-se definido em mais detalhes em 5.2.2.4.

Por fim, em (67) o protocolo BitTorrent é usado sem modificações. No caso do sistema IPTV com privacidade aqui proposto, além das modificações necessárias para a indireção de pedidos, o protocolo BitTorrent deve ser usado de forma encriptada via protocolo *Message Stream Encryption* (MSE), que foi desenvolvido especialmente para uso em redes P2P (68).

5.2.1.3 Nós de Cache

Em (67), a rede de transporte conta com nós que armazenam parte do conteúdo já transmitido para otimizar o mecanismo de *timeshifting*. Ao se procurar um conteúdo, a DHT retorna uma lista contendo tanto HDGs como nós de *cache*, de forma indistinta.

Na presente proposta, os nós de *cache* da rede do provedor possuem um caráter diferenciado dos HDGs na rede P2P. Diferentemente dos HDGs, que estão associados a usuários (e, portanto, passíveis de questões de privacidade destes usuários), os nós de *cache* estão associados aos provedores (da rede de transporte ou ao SDP), não havendo portanto a necessidade de se proteger a privacidade destes nós e seus respectivos conteúdos no contexto da proposta. Sendo assim, eles devem registrar na DHT seus conteúdos e atuam tanto para otimizar o acesso (um *cache* na rede) como para limitar o mecanismo de indireção (há pelo menos um nó na rede de transporte contendo o conteúdo, evitando-se *loop* infinito nas requisições).

5.2.1.4 Extended EPG (EEPG)

O EPG Estendido (*Extended EPG* – EEPG) visa obter a privacidade relacionada aos mecanismos de DRM. No EEPG, os metadados do conteúdo (contidos no EPG) são acrescidos das informações das licenças de cada conteúdo, incluindo as respectivas chaves de conteúdo. Os dados relativos à licença e à chave do conteúdo são criptografados no EEPG, utilizando-se chaves de sessão diferentes para cada pacote de assinatura com cobrança diferenciada, refletindo os canais básicos e *premium* (requisito S2). Os assinantes do serviço devem autenticar-se periodicamente junto ao SDP, para obter as chaves de sessão (5.2.2.2).

O EEPG utilizado na proposta é descrito na linguagem de marcação XML (*eXtensible Markup Language*), sendo baseado no EPG simplificado de (67) e na especificação de XMLTV (69). No EEPG propõe-se estender a descrição de cada canal que utiliza DRM com a adição de uma *tag* denominada <DRM>, contendo duas outras *tags*:

- <sig> : indica o pacote de assinatura ao qual o canal pertence;
- <license> : contém as políticas de uso e chaves relacionadas aos conteúdos do canal, na forma de um RSO (*Rights and Services Object*), representadas através de uma codificação Base64.

A Figura 14 apresenta um exemplo de um EEPG, mostrando os metadados relativos a um canal e a um conteúdo deste canal, juntamente com os parâmetros de DRM do canal.

```

<root version="1.1">
  <channel>
    <name>Globo</name>
    <description>Rede Globo de Televisão</description>
    <multicastAddress value="224.123.111.201"/>
    <port value="1234"/>
    <DRM>
      <sig type=01 />
      <license>
        VhCgQzUE6Rn+GOZKCX/AQkYRedHKaDN6/ppJvnAMQ1Gkvr
        WVfAxI67Et+7NXNd31uSXMWoHLpUGouPJZK3rQmoW6kcCp
        ...
        cr63g23veeizxtxcfp7jFDaAIvLy7pNgOGFvcep7/2SfDT
        IH22J1CJEVb6szAIlWLxZIJz4rwFU7GojhBXPu8DW/Uj
      </license>
    </DRM>
    <contents>
      <content id=0A94527>
        <name>SPTV</name>
        <description>Noticias Regionais</description>
        <genre value="notícias" />
        <date>
          <startTime value="2008-02-13 14:01:00 -0200" />
          <endTime value="2008-02-13 14:29:59 -0200" />
        </date>
        <RemovalDate value="2008-12-31 23:59:59 -0200" />
      </content>
      <content id=07891FG> ... </content>
      <content id=T0L91FA> ... </content>
      ...
      <content id=78HTX67> ... </content>
    </contents>
  </channel>
  <channel> ... </channel>
  <channel> ... </channel>
  ...
  <channel> ... </channel>
</root>

```

Figura 14 – Exemplo de EEPG em XML, com descrição simplificada de um canal e seu conteúdo.

No exemplo, pode-se visualizar junto à descrição do canal (de nome “Globo” no exemplo) tanto os parâmetros de conexão (endereço de *multicast* e porta) como os parâmetros de DRM (pacote de assinatura e RSO em Base 64). Para se ter acesso ao conteúdo deste canal é necessário obter, na autenticação, as chaves de sessão

relativas ao tipo do pacote de assinatura tipo 01 (que tem significado apenas para o SDP, podendo ser, por exemplo, um pacote básico de assinatura), para a partir dela obter as licenças e chaves dos conteúdos contidas no EEPG.

Para atender os requisitos P2 (personalização do EPG) e P4 (monitoração de tráfego não pode revelar aspectos de personalização), a personalização do EEPG deverá ser feita localmente no HDG, conforme instruções do usuário, exigindo o armazenamento do EEPG localmente no HDG previamente à sua utilização.

Um EEPG não exige um espaço significativo de armazenamento, uma vez que os metadados como título e descrição do conteúdo são curtos (para exibição na tela em forma concomitante com o conteúdo). Para uma estimativa, pode-se considerar um canal com um grande número de programas, tais como um canal que exhibe programas de 30 minutos (ex. seriados ou programas infantis) durante 24 horas. Este canal apresentará 48 entradas no EPG. Assumindo que cada entrada (licença e metadados) consuma 1 KB, teríamos 48 KB ocupados no EPG por este canal. Em um serviço com 500 canais, este EPG consumiria aproximadamente 23,5 MB sem compressão. Na prática, porém este espaço acaba sendo menor, uma vez que é comum haver programas que se repetem ao longo da programação (ex.: o mesmo filme ou episódio de um seriado é exibido de manhã e à noite)

Tal EEPG também não necessitaria de muita banda para transmissão. Assumindo uma taxa de transferência de 256 Kbps (uma taxa básica de banda larga), a transmissão deste EEPG completo sem compressão demoraria aproximadamente 12,5 minutos, ou 1,5 segundos por canal. Apesar deste valor de tempo poder parecer excessivo, ele ainda é passível de otimização (através de compressão ou através do envio de forma parcial, conforme o usuário for navegando na programação) ou ainda diminuído em função da disponibilidade de banda do usuário (por exemplo, para uma banda de 1 Mbps, as informações de cada canal do EEPG poderiam ser transmitidos em aproximadamente 400 ms).

É importante ressaltar que a programação dos canais de uma maneira geral é definida de forma antecipada. Sendo assim, poder-se-ia aproveitar a capacidade ociosa da rede para a transmissão e *caching* dos EEPGs, tais como o período da madrugada, atendendo também o requisito S3 de não impactar a QoE (*Quality of Experience*) do serviço. Esta abordagem (*download* de EPG completo) é análoga à

utilizada em sistemas do tipo *Media Center*¹⁵ (que transformam um computador pessoal em uma central multimídia para domínios domésticos) para as funcionalidades de visualização de canais de TV tradicionais (aberta, TV por assinatura) e PVR.

5.2.2 Operações

Além de alterações nos elementos que compõem a arquitetura, são necessárias também alterações nas interações entre estes elementos. A arquitetura proposta apresenta as mesmas operações básicas descritas em 2.3.8, porém com alterações relacionadas à melhoria da privacidade.

5.2.2.1 Registro do HDG

Como parte do registro do HDG, um par de chaves assimétricas é gerado para o HDG e um certificado com a chave pública do HDG é emitido pelo SDP. O HDG recebe, também, um certificado com a chave pública do SDP.

O processo de registro utiliza uma abordagem tradicional: um par de chaves assimétricas é gerado no HDG. A seguir, uma página *web* especial é acessada no SDP, onde se preenche os dados do assinante para a cobrança (ex.: nome, endereço, CPF, cartão de crédito, entre outros). Estes dados são então enviados para o SDP via formulário *web*, juntamente com os dados do HDG (ex. □: endereço MAC, marca e modelo do HDG, entre outros), e a chave pública gerada, sendo recebido como resposta o certificado do HDG, assinado pelo SDP, bem como o certificado do próprio SDP.

Dada a possibilidade de se rastrear usuários baseados na utilização de par de chaves públicas/privadas, o uso de criptografia assimétrica é restrito na arquitetura, sendo utilizado apenas para a autenticação periódica do HDG junto ao provedor e conseqüente proteção das chaves de sessão do EEPG durante a autenticação.

---

¹⁵ Exemplos de sistemas do tipo *Media Center*: Microsoft Windows XP Media Center Edition, Microsoft Windows Vista Premium/Ultimate, MythTV (www.mythtv.org) e Freevo (www.freevo.org).

5.2.2.2 Autenticação do Serviço

Periodicamente o usuário deverá se autenticar no provedor. Além de comprovar sua identidade ao provedor, a autenticação no provedor visa obter as chaves de sessão necessárias para o acesso aos parâmetros de DRM no EEPG (licenças e chaves do conteúdo). As chaves de sessão são passadas do SDP para o HDG durante a autenticação, utilizando-se de um canal seguro estabelecido com o uso dos pares de chaves públicas/privadas do HDG e do SDP (as chaves públicas foram trocadas entre os pares durante o registro do HDG). A Figura 15 ilustra o processo de autenticação na arquitetura proposta.

Figura 15 – Autenticação na Arquitetura Proposta

Desta maneira, não é possível relacionar um usuário às chaves DRM do conteúdo: através do histórico de autenticação um observador só consegue inferir se o usuário tem acesso a todos os conteúdos relacionados à sua assinatura (uma vez que recebeu as chaves de sessão na autenticação) ou a nenhum destes conteúdos (não recebeu nenhuma das chaves de sessão).

Uma periodicidade razoável para a autenticação no provedor e para novas chaves de sessão seria uma periodicidade diária. Tal periodicidade é compatível com os sistemas de tarifação normalmente utilizados em serviços pagos, que costumam utilizar uma granularidade de dias para a cobrança proporcional de serviços, em casos de revogações de direitos de acesso dos usuários (ex.: usuário cancelou a assinatura ou saiu da comunidade com acesso ao serviço à qual ele pertencia).

Nestes casos, o usuário deixaria de ter acesso ao serviço e seus conteúdos a partir do dia posterior à revogação, sendo a cobrança efetuada de forma proporcional aos dias utilizados.

5.2.2.3 Acesso ao EEPG

Conforme mencionado anteriormente, o EEPG pode ser distribuído via *multicast*, utilizando-se a capacidade ociosa da rede (ex.: madrugada). Sendo assim, o acesso ao EEPG é feito simplesmente através de uma operação de *join* na sessão de *multicast* responsável pelo EEPG (via protocolo IGMP – *Internet Group Management Protocol*). O EEPG também pode ser distribuído via *multicast* para nós de *cache*, de maneira que HDGs que porventura estiverem desligados durante a madrugada possam, posteriormente, obter o EEPG diretamente dos *caches*, de forma análoga à requisição de conteúdo.

Como o EEPG contém os RSOs de todos os conteúdos do período de validade das chaves de sessão obtidas na autenticação, o LS deverá passar estes RSOs para o SDP, que irá encriptá-los com as chaves de sessão apropriadas e distribuir o EEPG assim formado via *multicast* para o HDG (Figura 16)

Figura 16 – Acesso ao EEPG

A monitoração do tráfego *multicast* do EEPG não revela nenhuma informação complementar, uma vez que todos os usuários recebem a mesma cópia do EEPG (ou seja, a mesma programação e os mesmos RSOs) e qualquer personalização do EEPG é feita localmente no HDG (P2, P4).

5.2.2.4 Requisição do Conteúdo

Na arquitetura de um sistema de IPTV tradicional, a única maneira do usuário receber um conteúdo de um canal de *broadcast* é através da requisição ao SDP desejado e posterior recebimento via *multicast*, permitindo a inferência do perfil do usuário facilmente via monitoração do tráfego. Ainda, no caso de uso de DRM, é possível inferir o perfil do usuário pelas requisições de RSOs ao LS, uma vez que para cada conteúdo protegido é necessário obter-se inicialmente o respectivo RSO (que é encriptado com a chave pública do usuário).

Através da rede P2P, o HDG conta com uma alternativa para a requisição do conteúdo de broadcast (S1): ele pode requisitar o conteúdo a outros HDGs, que podem então responder com as partes do conteúdo, i.e, o conteúdo desejado não precisa estar necessariamente todo armazenado em um único nó, i.e, em um único HDG ou nó da rede P2P, mas suas partes podem estar distribuídas em diferentes nós

Dada estas duas possibilidades para requisição do conteúdo, a escolha se dá através de uma distribuição estatística binominal, utilizando um parâmetro denominado no trabalho como **sensibilidade** do mecanismo de privacidade (indicado por **s**). Esta sensibilidade é um valor entre 0 e 1 que indica para o HDG a probabilidade de se escolher a rede P2P para a privacidade do conteúdo. Dado que diferentes usuários podem utilizar diferentes parâmetros de sensibilidade, a utilização do P2P tende a ser diferente para usuários com as mesmas configurações de privacidade (ex.: que desejam a privacidade apenas para determinados gêneros de conteúdos), contribuindo para a unicidade do padrão de tráfego e aumentando a dificuldade na análise do mesmo.

Na Figura 17 é possível observar as diferenças na requisição do conteúdo da arquitetura original e da arquitetura proposta. É importante ressaltar que na arquitetura proposta os eventuais RSOs de conteúdos já foram obtidos previamente no EEPG, não sendo necessário requisitá-los a cada conteúdo a ser exibido.

Figura 17 – Comparação entre requisição de conteúdo original e proposto

Um outro aspecto importante é que para que o uso da rede P2P contribua para a privacidade dos usuários, as requisições não devem ser feitas somente para aqueles que possuem o conteúdo em *cache* (pois isto indicaria para o nó requisitado os interesses do requisitante). De maneira análoga, um HDG que deseje privacidade não deve divulgar o conteúdo de seu *cache*.

Desta maneira, define-se o conceito de **indireção de requisições**: as requisições podem ser feitas para outros HDGs, independente deles possuírem ou não os conteúdos desejados; caso o HDGs requisitado não possua o conteúdo desejado, ele encaminha a requisição para outros nós na rede, atuando como *supernodes* na P2P (Figura 18). É possível utilizar-se múltiplos níveis de indireção para uma melhor unicidade no tráfego de requisições.

Figura 18 –Indireção de Requisições

Para se obter um conteúdo de forma privativa na rede P2P utiliza-se a seguinte lógica:

- Um HDG requisitante procura por outros HDGs e envia a requisição para eles, independente do conteúdo do mesmo;
- Caso o HDG requisitado possua o conteúdo em seu *cache*, ele simplesmente devolve o conteúdo pedido. Caso o HDG requisitado não possua o conteúdo, há uma indireção na requisição; o HDG deve efetuar uma das seguintes opções:
  - a) Acessar o conteúdo por *multicast*, caso possível;
  - b) Procurar um nó na rede P2P que possua o conteúdo, requisitá-lo e repassá-lo (tipicamente existem nós de *cache* e HDGs que não estão com mecanismos de privacidade habilitado e, portanto, publicam na DHT os conteúdos que possuem);
  - c) Requisitar o conteúdo a outro HDG da rede, independente se ele possui ou não o conteúdo.

A presença de nós de *cache* visa limitar e otimizar as indireções, ao disponibilizar na rede P2P nós com o conteúdo registrado na DHT (e portanto localizáveis sempre que o HDG decidir pela opção *b* acima).

Com esta lógica, nenhum dos HDGs na rede P2P realmente pode inferir algo sobre os conteúdos requisitados: as requisições são enviadas independente do requisitado possuir o conteúdo. Os nós requisitados (tanto HDGs como nós de *cache*) também não podem inferir nada sobre o requisitante, uma vez que pode ser uma requisição indireta.

Para se evitar um *loop* infinito nas indireções, na requisição inicial o HDG requisitante adiciona um contador regressivo que é diminuído cada vez que há uma indireção. Quando zerado, o contador indica ao HDG requisitado que ele deve procurar o conteúdo em nós de *cache* ou em outros HDGs, sem indireções. A presença de um contador zerado na requisição por si só é um indicativo da utilização de mecanismos de privacidade, sinalizando aos nós requisitados que qualquer inferência sobre o requisitante pode ser inválida. Além disso, o valor inicial do contador varia de acordo com o usuário: cada usuário pode definir o número máximo de indireções que achar razoável (parâmetro **Max_i**), sendo o contador inicializado com um valor entre 0 e Max_i.

Ao distribuir o tráfego de requisição de conteúdo, a monitoração do tráfego do usuário fica mais complexa (S4): enquanto que o conteúdo pode ser facilmente identificado no fluxo de *multicast*, através deste mecanismo somente parte do conteúdo é recebido via *multicast*, e mesmo o conteúdo recebido via *multicast* pode não ser mais destinado ao HDG requisitante, mas a outros HDGs. Além disto, parte do conteúdo é recebido via P2P encriptado, inviabilizando ao observador inferir o conteúdo requisitado via monitoração do tráfego (lembrando que o HDG pode receber diferentes porções do conteúdo de diferentes HDGs, de maneira a distribuir mais ainda o acesso).

5.2.2.5 Personalização do EEPG

Há dois tipos de personalização possível: manual e automática. Na personalização manual o usuário define exatamente quais canais deseja assistir, bem como quais

tipos de conteúdo o usuário deseja assistir. A personalização automática, por sua vez, visa ressaltar determinados aspectos da programação de acordo com as categorias a que o usuário pertence, por exemplo, ressaltando na programação filmes diferentes, dependendo da faixa etária, faixa de renda ou gênero do usuário (P3).

Para a personalização automática do EEPG, o usuário deverá definir estas categorias na configuração do HDG. O EEPG deve também incluir algumas regras de personalização, de maneira que o HDG possa efetuar a personalização localmente. A Figura 19 apresenta um exemplo de regras de personalização de um EEPG (descritas pela *tag* `<personalization>`) na qual são sugeridos conteúdos específicos para grupos baseados em faixa etária (de 12 a 17 anos e de 18 a 25 anos), gênero do usuário (indivíduos do sexo masculino) e renda (de 1000 a 3000 reais); os conteúdos são apenas identificados por seu identificador único, uma vez que já foram descritos anteriormente no EEPG (como no exemplo da Figura 14).

```
...
<personalization>
  <age range="12-17">
    <content id=0A94527>
      ...
    </age>
  <age range="18-25">
    <content id=07891FG>
      ...
    </age>
  <genre value="Male">
    <content id=T0L91FA>
      ...
    </genre>
  <income range="1k-3k">
    <content id=78HTX67>
      ...
    </income>
</personalization>
...
```

Figura 19 – Exemplo de regras de personalização automática do EEPG

5.2.2.6 Configuração do HDG

Há diversas configurações possíveis no HDG.

- a) **Categorização do Usuário:** o usuário poderá definir no HDG algumas variáveis usadas para a personalização do EEPG e/ou do conteúdo (P3), tais como faixa etária, gênero do usuário e renda;
- b) **Personalização do EEPG:** o usuário deverá definir se deseja a personalização manual e/ou automática; no caso da personalização manual ele deverá definir os canais e conteúdos desejados, enquanto que no caso da personalização automática o sistema deverá se utilizar das categorias definidas no item anterior (5.2.2.5);
- c) **Personalização do conteúdo:** o usuário deverá definir quais conteúdos deseja assistir posteriormente, para armazenamento no HDG. Poderá definir também categorias de conteúdo que deseja que sejam armazenadas (E1, E2);
- d) **Estatísticas:** o usuário deverá definir se deseja que sejam coletadas estatísticas de uso, bem como se autoriza que estas estatísticas sejam divulgadas;
- e) **Privacidade:** o usuário poderá definir quais canais e quais categorias de conteúdo ele deseja que sejam acessadas no modo privativo, ou seja, variando o acesso entre requisição via *Multicast* e P2P (S5). Além disso, poderá definir os parâmetros de privacidade: a sensibilidade **s** e o número máximo de indireções **Max_i**. Por fim, poderá definir também se deseja a divulgação do seu EEPG personalizado (P4), estatísticas coletadas e histórico de navegação.

5.2.3 Limitações

Enquanto que a arquitetura proposta engloba arquiteturas de IPTV baseadas em *multicast* (podendo ou não utilizar DRM), os mecanismos de privacidade da arquitetura não se aplicam a todos os tipos de conteúdo, uma vez que alguns

conteúdos não são apropriados para armazenamento em *cache* ou para o atraso causado pelo uso do P2P em detrimento do *multicast*. Entre os exemplos podem-se citar conteúdos ao vivo, tais como eventos ou noticiários, ou conteúdos em que possa haver alguma interação envolvendo o próprio usuário (ex.: usuário conversa via telefone com o apresentador do programa). Tais conteúdos, no entanto, podem ser mantidos em *cache* uma vez passado o horário de sua exibição, possivelmente com uma ressalva indicando que é versão gravada, e não uma versão ao vivo.

5.3 Validação da solução

Para a validação da solução foram implementados os principais mecanismos da proposta sobre uma implementação de IPTV existente (67), de maneira a se determinar a eficácia da solução em relação à privacidade. Escolheu-se para a validação a análise do perfil do usuário de acordo com os gêneros por ele assistidos.

5.3.1 Implementação da Arquitetura do Sistema IPTV com Privacidade

A implementação da arquitetura utiliza a linguagem Java, versão 5 (70,71) e do ambiente de desenvolvimento Eclipse (72). A implementação baseia-se nas bibliotecas em Java de IPTV de (67), definidas nos conjuntos de pacotes `br.usp.larc.iptv.*`, e ferramentas de terceiros. Dentre estas, destacam-se o aplicativo de visualização de vídeos VLC (73,74) e as bibliotecas em Java para BitTorrent (75) e para integração entre o Java e o VLC (JVLC (76)).

Definiu-se na implementação um pacote em java denominado `br.usp.larc.iptv.privacy`, contendo os mecanismos de EEPG e de requisição de conteúdo. Foram necessárias alterações no código das bibliotecas de `br.usp.larc.iptv` originais, de maneira a integrar o código de privacidade às mesmas.

Na implementação, os mecanismos de privacidade na requisição de conteúdos são utilizados de acordo com os seus gêneros. Para tanto, definiu-se uma janela para a configuração dos gêneros que requerem os mecanismos de privacidade (Figura 20). Nesta janela o botão inferior determina se o sistema deve ser utilizado no modo

tradicional (implementação de IPTV original – botão em estado *PrivacyMode OFF*) ou se deve utilizar os mecanismos de privacidade de acordo com o gênero do conteúdo (botão em estado *PrivacyMode ON*).

Figura 20 – Janela de configuração de privacidade

O mecanismo de privacidade é iniciado através de um arquivo de configuração, que indica os gêneros privativos, o estado inicial (*PrivacyMode ON / OFF*) e a sensibilidade do mecanismo de privacidade.

Para a validação, optou-se por utilizar uma cópia local do EEPG, assumindo-se que ela tenha sido previamente distribuída para o HDG.

5.3.2 Ambiente de Testes

Para a validação da solução um ambiente de testes foi montado em máquinas virtuais, utilizando uma arquitetura simplificada, com 3 diferentes HDGs, separados do provedor pela rede de transporte. O próprio SDP faz o papel de *cache* na arquitetura.

Figura 21 – Ambiente de Testes para a solução de privacidade

Utilizou-se também nos testes uma versão modificada do HDG. A versão original do HDG de (67) é uma versão interativa, na qual o usuário seleciona os conteúdos através de cliques de *mouse*, que são visualizados após a transferência para o HDG. Para a execução de forma automatizada dos testes, bem como para garantir a capacidade de reprodução dos testes, optou-se por criar um HDG modificado, que opera essencialmente com arquivos de entrada e saída em substituição à interação do usuário. Esta versão modificada utiliza um arquivo de entrada que descreve as requisições de conteúdo efetuadas por um usuário, sem o mecanismo de privacidade. Também em função da automatização as requisições do HDG são automaticamente correlacionadas, registrando-se em arquivos de saída as requisições de conteúdo efetuadas pelo usuário após a aplicação dos mecanismos de privacidade. Por fim, dada a diferença entre o número absoluto de requisições visíveis na rede através de *multicast* e P2P (no *multicast* há uma requisição por conteúdo, enquanto que na implementação de P2P utilizada há requisições para cada bloco, representando 1 minuto de conteúdo), optou-se por registrar apenas uma requisição por conteúdo, independente dela ser executada via *multicast* ou P2P (facilitando a análise posterior).

5.3.3 Metodologia

Para a análise do perfil de usuários utilizou-se a programação real de uma operadora de TV a cabo da cidade de São Paulo (TVA), referentes a um período de cinco dias, entre 5 e 9 de março de 2008. Estas informações da programação foram inicialmente obtidas através do EPG do Windows Vista (Figura 22).

Figura 22 – EPG do Microsoft Windows Vista com programação de 9/3/2008

Através da ferramenta MceEpg2XmlTv (77), o EPG do Windows Vista foi convertido para o formato XMLTV e importado pela ferramenta FreeGuide (78), que permite a criação de arquivos com roteiros personalizados (Figura 23). Através do FreeGuide, apresentou-se a referida programação para diferentes indivíduos, requisitando-se que eles definissem na própria aplicação quais programas assistiriam. Tais definições foram utilizadas para a criação dos arquivos de entrada para a automatização do HDG, onde os conteúdos foram associados a gêneros distintos, conforme descritos na Tabela 4.

Figura 23 – Aplicativo FreeGuide com programação de 9/3/2008

Tabela 4 – Gêneros utilizados na análise

Desenhos	Documentários
Educacionais	Entrevistas
Filmes	Notícias
Novelas	Reality Shows
Seriados	Shows
Talk Shows	Variedades

Para comparar a distribuição dos gêneros dos conteúdos que cada usuário requisitou (obtida por meio do FreeGuide) com a distribuição esperada quando a escolha é feita ao acaso utilizou-se o teste Qui-quadrado¹⁶. Repetiu-se, então, o

¹⁶ O teste Qui-quadrado é um teste estatístico de aderência que permite inferir se um conjunto de dados distribuídos em categorias segue um modelo de distribuição probabilística ao acaso ou se apresenta alguma tendência específica para uma ou mais categorias (79).

procedimento com os mecanismos de privacidade habilitados, e novamente aplicou-se o teste estatístico. Os resultados das duas condições, com e sem o mecanismo de privacidade, foram então comparados com o intuito de verificar se as tendências observadas se mantiveram ou se alteraram. O nível de significância adotado foi de 5%.

Para cada indivíduo, foi ativado o mecanismo de privacidade de forma seletiva, para os 2 gêneros com maior número de observações. Procurou-se utilizar diferentes valores de sensibilidade, escolhidos de forma arbitrária, de maneira a se verificar o efeito da mesma na análise final: utilizou-se os valores de 0,25 (probabilidade maior de uso de *multicast*), 0,75 (probabilidade maior de uso de P2P) e 0,5 (probabilidade igual entre *multicast* e P2P). Foi feito também um experimento extra, onde o mecanismo de privacidade foi utilizado para todos os gêneros, com sensibilidade igual a 0,5, para se verificar se havia alguma diferença entre aplicar o mecanismo para apenas alguns gêneros ou para todos os gêneros.

5.3.4 Resultados

A análise das requisições dos usuários sem os mecanismos de privacidade com o teste do Qui-Quadrado revelou que todos eles apresentavam algum tipo de tendência em relação aos gêneros assistidos. Ao se aplicar o mecanismo de privacidade para os 2 gêneros com maior número de observações, com parâmetro de sensibilidade igual a 0,25 e 0,5, bem como para todos os gêneros (com sensibilidade igual a 0,5) foi possível observar que, apesar dos testes estatísticos ainda indicarem que havia uma tendência nos gêneros observados (ou seja, a distribuição entre os gêneros era significativamente diferente da distribuição homogênea), as tendências observadas se alteravam: os principais gêneros ainda podiam ser vislumbrados, porém outros gêneros passaram a ser considerados significativos. No entanto, para sensibilidade igual a 0,75, não se pode mais observar uma tendência clara entre os gêneros.

A Figura 24 ilustra estes resultados, através das observações obtidas de um dado usuário, considerando-se apenas as requisições via *multicast*. Neste exemplo, pode-se ver que, para as requisições sem o uso do mecanismo de privacidade, há uma

clara tendência no gênero *Seriados*, seguida por *Filmes* e *Desenhos*. Ao se aplicar o mecanismo com sensibilidade pode-se ver que, para uma sensibilidade igual a 0,75, não se pode inferir uma tendência clara entre os gêneros. Isto não acontece com os outros experimentos, onde ainda se pode distinguir a tendência em *Seriados*, apesar das tendências em *Filmes* e *Desenhos* começarem a ficar menos clara (com 0,5 a quantidade de observações em *Noticiários* e *Documentários* é equivalente à de *Filmes* e *Desenhos*).

Figura 24 – Exemplo de observações de um usuário, de acordo com o gênero, desconsiderando o tráfego P2P

Ao se considerar apenas o tráfego de *multicast* um observador pode ainda inferir um determinado perfil de usuário, ainda que possivelmente falso. No entanto, a própria presença significativa de requisições P2P é um indicativo para o observador que parte do conteúdo está sendo mascarada por mecanismos de privacidade. Isto pode ser observado na Figura 25, que ilustra as observações do mesmo usuário vistas na Figura 24, porém com a inclusão de requisições P2P observadas. Nesta figura pode-se ver observar que o número de requisições P2P equipara-se ou ultrapassa os gêneros mais assistidos.

Figura 25 – Exemplo de observações de um dado usuário, de acordo com o gênero, considerando o tráfego P2P

Um outro resultado obtido foi de que a aplicação de P2P para todo o tráfego não traz benefícios ou até mesmo é pior do que aplicar para apenas determinadas categorias. A Figura 24 ilustra também esta situação: ao se utilizar o P2P com probabilidade 0,5 para todo o tráfego (identificado na figura por $s=0,5$ (*all*)), os três gêneros com maior número de observações são os mesmos gêneros obtidos sem o uso de nenhum mecanismo de privacidade, ainda que em quantidades absolutas diferentes. Além disso, pode-se visualizar na Figura 25 que o uso de P2P neste exemplo foi bastante alto (53% das requisições), equivalente ao uso com sensibilidade igual a 0,75, e com resultados piores do que na aplicação do mecanismo de privacidade para com sensibilidade de 0,25 (que efetuou apenas 26% das requisições via P2P).

5.4 Considerações Finais

A arquitetura proposta neste trabalho visa oferecer um serviço de IPTV com mecanismos de privacidade para conteúdo em canais básicos e *premium* (2.2.1), que tradicionalmente utilizam-se de *multicast*. Partindo como base de uma arquitetura de IPTV que utiliza P2P para *timeshifting*, este trabalho define uma

arquitetura híbrida, que mescla requisições via *multicast* com requisições via P2P, de maneira a inviabilizar possíveis análises de tráfego. A utilização do P2P é feita de forma seletiva, de acordo com regras que definem quando se utilizam os mecanismos de privacidade (por exemplo, para determinados gêneros de conteúdo), bem como de forma balanceada, através de um parâmetro de sensibilidade que balanceia a proporção entre requisições via P2P e *multicast*. Aproveita-se ainda a presença de *caches* na rede de transporte e nos próprios HDGs, da arquitetura original para a otimização do tráfego P2P.

A Tabela 5 mostra como a Arquitetura Proposta para Ambientes de IPTV com Serviços de Privacidade atende os requisitos funcionais relacionados em 4.3.

Tabela 5 – Relação dos requisitos funcionais atendidos pela arquitetura proposta

Requisitos	Funções usadas no atendimento a requisitos
S1 - Mecanismos de privacidade aplicáveis ao conteúdo de canais de <i>broadcast</i>	Os canais de broadcast caracterizam-se na arquitetura de referência pela transmissão para um conjunto de usuário, ao invés do fluxo individualizado de canais sob-demanda. A arquitetura proposta baseia-se no fato do conteúdo ser transmitido para vários usuários, e armazenadas em cache, para tratar da privacidade deste tipo de tráfego, variando entre P2P e <i>multicast</i> .
S2 - Mecanismos de privacidade aplicáveis a canais básicos e <i>premium</i>	A arquitetura permite distinguir diferentes tipos de canais, através da <i>tag</i> <sig> no EEPG e conseqüentes trocas de chaves durante a autenticação do HDG.
S3 - Mecanismos de privacidade devem ou apresentar um impacto mínimo no QoE do usuário	A arquitetura utiliza-se de <i>caches</i> na rede de transporte para minimizar o impacto do uso de P2P. Além disso, o P2P é usado apenas quando necessário, de acordo com os requisitos de privacidade do usuário (no caso da implementação testada, baseada em gêneros de conteúdo).
S4 – Robustez contra monitoração de tráfego não	A monitoração do tráfego gera um perfil falso do usuário, quando se considera apenas o tráfego

autorizada	<i>multicast</i> . Não é possível utilizar o tráfego P2P para a criação do perfil, uma vez que ele se encontra encriptado.
S5 – Ativação seletiva dos mecanismos de privacidade	Para cada conteúdo desejado, a arquitetura verifica se é um conteúdo em que se deseja privacidade, para poder decidir a forma de requisição.
D1 – Proteção do conteúdo via DRM deve ser mantida	Conteúdo é protegido através de criptografia simétrica, utilizando chaves de sessão trocadas periodicamente.
D2 – Impossibilidade de correlacionamento entre usuário e histórico de requisição de licenças	Usuário sempre recebe pelo EEPG todas as licenças a que tem direito, não havendo mais a operação de requisição de licenças.
P1 – Possibilidade de personalização do conteúdo	A personalização do conteúdo é possível através do uso de tráfego P2P encriptado e com indireções.
P2 – Possibilidade de personalização do EPG	Suportado através de caching do EEPG e do uso de regras locais e automatizadas
P3 – Categorização do usuário para suporte a personalização automática	Foram definidas classes em Java para suportar a categorização do usuário.
P4 – Impossibilidade de inferir aspectos de personalização via monitoração de tráfego	Para a personalização de conteúdo, utiliza-se o P2P encriptado e com indireções para evitar a inferência via monitoração. Para o caso de personalizações de EEPG, elas são efetuadas localmente, no HDG, não havendo tráfego específico de personalização do EEPG.
P5 – Controle de exportação de configurações de personalização	A arquitetura atual não permite a exportação via rede das configurações de personalização (ficam todas locais ao HDG).
E1 – Controle de coleta de	A implementação atual permite a coleta de dados de

estatísticas pelos usuários	dia, horário e categoria dos conteúdos requisitados (tal funcionalidade foi utilizada para os testes estatísticos).
E2 – Controle de divulgação de estatísticas	A arquitetura atual não permite a exportação via rede das estatísticas, ficando elas locais no HDG.
E3 – Possibilidade de monitoração de estatísticas via mecanismos tradicionais	Com os mecanismos de privacidade desabilitados, a solução equivale-se à da arquitetura de IPTV de referência, permitindo o uso de mecanismos tradicionais de monitoração.

A validação da arquitetura em relação à proteção da privacidade foi feita através de análises estatísticas comparando o perfil do uso de diferentes indivíduos sem os mecanismos de privacidade habilitados com os mecanismos habilitados (e diferentes parâmetros de sensibilidade). Os resultados mostraram que a utilização de um parâmetro de sensibilidade alto de forma seletiva (apenas para determinados conteúdos) apresenta-se como a melhor opção para invalidar o perfil de usuários criados a partir da monitoração de tráfego na rede.

Em relação ao desempenho da solução, o principal problema é relacionado à transferência do bloco inicial de conteúdo: somente após receber o primeiro bloco de conteúdo o HDG inicia a reprodução do vídeo. Uma vez transferido o primeiro bloco, no entanto, os outros blocos podem ser transferidos em paralelo, aproveitando-se a banda disponível na rede de transporte. Sendo assim, após a transferência do primeiro bloco, eventuais atrasos causados pela indireção de requisições são mitigados pela transferência em paralelo dos blocos. Deve-se, no entanto, definir um valor baixo para o número máximo de indireções Max_i , para que a soma dos atrasos causados pelas diferentes indireções não se torne significativo.

Após a validação da arquitetura, deve-se proceder a uma análise crítica da mesma. O capítulo a seguir apresenta esta análise, destacando-se as contribuições, inovações e evoluções futuras do trabalho.

6 CONSIDERAÇÕES FINAIS

A maioria dos estudos em sistemas de IPTV é voltada para a eficiência na distribuição do conteúdo e para a proteção do conteúdo via DRM (*Digital Rights Management*), garantindo direitos autorais e prevenindo contra fraudes. Apesar de haver uma certa preocupação com a privacidade em sistemas DRM e em sistemas baseados em certificados, não se encontram trabalhos específicos de privacidade em ambientes de IPTV, independente do uso de DRM. O presente trabalho propõe uma arquitetura de IPTV com mecanismos capazes de aumentar a privacidade dos usuários do sistema.

6.1 Análise Crítica

A solução proposta por este trabalho permite que se tenha um grau de privacidade maior no uso do serviço de IPTV em relação às arquiteturas tradicionais.

A abordagem escolhida para oferecer privacidade aos usuários difere das abordagens tradicionais de privacidade. Conforme pôde ser visto em 4.4, a maioria das soluções para proteção de privacidade na comunicação de dados (referente ao uso de serviços *online*) baseiam-se no anonimato do usuário do serviço, tarefa de extrema complexidade no ambiente de IPTV, dada as particularidades da aplicação. Dada esta dificuldade, a abordagem deste trabalho segue um caminho alternativo, o da não-relacionabilidade, com o objetivo de invalidar possíveis monitorações de tráfego do usuário: um observador pode monitorar um dado usuário e seu respectivo tráfego, porém ele não poderia saber se este tráfego está de fato sendo consumido pelo usuário, se está sendo armazenado em algum *cache* ou retransmitido para outros usuários. Em outras palavras, através da monitoração não se pode ter certeza de quem consome o conteúdo.

Os mecanismos de privacidade foram definidos considerando-se conteúdos distribuídos via *multicast* (canais básicos e *premium*), que podem alternativamente ser distribuídos via P2P. No entanto, conforme visto em 5.2.3, alguns conteúdos não são adequados para a distribuição via P2P, especialmente no caso de conteúdo ao

vivo. A proporção destes programas na programação geral tende, porém, a ser pequena, em função da logística maior para a produção deste tipo de programa.

Através do valor de sensibilidade do mecanismo de privacidade é possível ajustar o HDG para um uso maior ou menor de P2P, assim como é possível ajustá-lo para permitir um número maior de indireções. Esta parametrização traz uma flexibilidade grande à arquitetura, permitindo que cada usuário defina o que achar razoável em função da privacidade e eventuais contrapartidas (ex.: atraso maior devido a um número grande de indireções).

O uso do BitTorrent como protocolo base de P2P visa aproveitar-se da escalabilidade demonstrada pelo mesmo na distribuição de conteúdo na Internet, especialmente em casos em que há um conjunto relativamente pequeno de conteúdos compartilhados por um grande número de usuários, como no caso do serviço de IPTV (centenas de conteúdos sendo compartilhados pelos assinantes do serviço).

A arquitetura permite uma implantação de forma incremental em uma rede de IPTV como a descrita em (67). Para tanto o HDG deve apenas distinguir quais nós suportam o mecanismo de indireção. Isto pode ser facilmente obtido se os nós, ao se registrarem na DHT, registrarem também uma versão do protocolo P2P implementado (os nós que não registrarem a versão são tratados como nós originais de (67)).

A arquitetura proposta exige o suporte do SDP (*Service Distribution Provider*), tanto para a disponibilização de nós de *cache* na rede de transporte como para a criação e distribuição do EEPG (*Extended Electronic Program Guide*) contendo as licenças. Tal dependência pode ser um entrave, uma vez que com a arquitetura parte dos usuários contam com mecanismos que os protegem contra monitorações do provedor. No entanto, a arquitetura proposta não força a utilização dos mecanismos de privacidade para todos os usuários, podendo cada usuário decidir se deseja ou não utilizá-los e mesmo quanto se deseja utilizá-los (através dos parâmetros dos mecanismos de privacidade). O provedor poderia, por exemplo, oferecer algum incentivo para os usuários que permitirem a monitoração.

Há também outros aspectos da arquitetura que são atraentes para o provedor, tal como a possibilidade de se utilizar a capacidade ociosa da rede para a distribuição

de conteúdo (ex.: EEPG), a utilização conjunta de mecanismos para a melhoria de desempenho da rede (ex.: mecanismos de *caching*) e de *timeshifting* via P2P (*Peer-to-Peer*) e a não exclusão de aspectos de personalização de conteúdo.

A arquitetura pode também vir a enfrentar a oposição de entidades que trabalham com dados de audiência, como o IBOPE (Instituto Brasileiro de Opinião Pública e Estatística), no caso brasileiro, ou departamentos de marketing de redes de televisão, pelo receio de não ser mais possível realizar o levantamento e a comparação de dados de audiência. No entanto, não há nada na arquitetura que inviabilize os métodos tradicionais de medição de audiência através de equipamentos na casa dos usuários. Tais entidades poderiam ainda se beneficiar de parcerias com o SDP dentro do escopo proposto: mediante autorização do usuário, a medição poderia ser feita diretamente no HDG (*Home Domain Gateway*), sem a necessidade de aparelhos adicionais (e logística de distribuição e manutenção destes aparelhos adicionais), utilizando-se ainda a própria infra-estrutura de comunicação do SDP para o retorno dos dados.

Uma possível crítica à solução proposta seria o maior custo do HDG devido ao armazenamento necessário. Dado que tal HDG viabiliza o suporte a funcionalidades adicionais (além dos aspectos de privacidade, ele poderia por exemplo ser utilizado como um PVR – *Personal Video Recorder*), o custo maior acaba sendo justificado pelo valor agregado destas funcionalidades.

É importante ressaltar que, apesar do foco específico, pode-se estender o uso dos mecanismos de privacidade para redes de distribuição de conteúdo genéricas (CDN – *Content Distribution Networks*). Para tanto, a CDN deverá contar com pelo menos alguns servidores capazes de manter o cache de conteúdo, atuando de forma análoga aos nós de cache da arquitetura proposta como pontos finais das requisições dos clientes (análogos aos HDGs). A arquitetura também não se restringe somente a *multicast* IP e o protocolo P2P proposto para a obtenção do conteúdo; sendo assim, seria possível utilizar outros protocolos na distribuição do conteúdo (e.g., *multicast* em nível de aplicação), permitindo uma maior aplicabilidade dos conteúdos para CDNs genéricas.

6.2 Inovações e Contribuições

Ao focar o **problema de privacidade em um ambiente específico (IPTV)** ao invés de um ambiente mais genérico, a arquitetura deste trabalho destaca-se com contribuições significativas.

Uma inovação importante do trabalho é a **abordagem diferenciada para a privacidade**, que objetiva a **não-relacionabilidade** através do próprio tráfego da aplicação, ao contrário da abordagem tradicional de anonimidade. Tal idéia é particularmente útil em situações onde é necessário identificar o usuário, porém deseja-se um certo grau de privacidade (por exemplo: serviços comerciais onde a identificação é necessária para fins de cobrança).

O conceito do EEPG, que integra o EPG com parâmetros de DRM criptografados apresenta uma forma diferenciada de distribuição de chaves e licenças, que se aproveita da capacidade ociosa da rede ao mesmo tempo em que permite a personalização da programação e evita o rastreamento das chaves existentes em aplicações DRM tradicionais.

A arquitetura proposta utiliza também protocolos P2P (em particular do BitTorrent) de forma inovadora para a privacidade, através do conceito de indireção. Normalmente no uso do BitTorrent um usuário consulta um *tracker* ou DHT (*Distributed Hash Table*) para saber quais *peers* possuem e compartilham o conteúdo desejado, acessando-os diretamente para requisitar blocos deste conteúdo. Na arquitetura proposta altera-se este comportamento: a consulta à DHT simplesmente revela quem participa da rede P2P de privacidade; ao se requisitar o conteúdo a um determinado *peer* não se sabe se o requisitado possui o conteúdo (ele pode pedir para outro *peer* ou para um servidor de *cache*) nem se o requisitante é quem irá consumi-lo (ele pode estar efetuando a requisição para retransmissão). Apesar de ser utilizada dentro do contexto de IPTV, tal abordagem não utiliza nenhuma particularidade de IPTV, e poderia ser utilizada para novos protocolos P2P voltados à privacidade dos usuários, em particular, dentro do contexto de redes de distribuição de conteúdo (CDNs – *Content Delivery Networks*) baseadas em P2P, que possuem características semelhantes às redes de IPTV.

Uma outra contribuição do trabalho é a parametrização da operação do mecanismo de privacidade, através dos conceitos de sensibilidade e número máximo de indireções. Como a decisão de utilizar P2P ou multicast é baseada não só em um conjunto de regras (ex.: privacidade para determinados gêneros) como também em um modelo probabilístico binomial, aumenta-se a unicidade do padrão de tráfego de cada indivíduo, dificultando a análise do tráfego ao se utilizar diferentes parâmetros. Além disso, a parametrização permite que se ajustem os mecanismos de privacidade de acordo com o que cada usuário achar razoável em termos tanto da privacidade como de eventuais atrasos causados por um grande número de indireções.

Destaca-se também como contribuição o tratamento da própria questão de privacidade dentro do contexto de IPTV, uma preocupação que começa agora a aparecer em conjunto com as primeiras implementações comerciais e nas quais as soluções de privacidade existentes não são aplicáveis (pois visam tráfegos genéricos ou aplicações tradicionais como e-mail, *web* e *download* de conteúdo multimídia, sem a preocupação com atrasos e *jitter* do tráfego inerentes ao IPTV).

Da preocupação com os atrasos na rede deriva uma **arquitetura inovadora**, que **combina aspectos de *caching* com P2P para prover privacidade aos usuários**. Ao se basear em mecanismos de melhoria de desempenho de IPTV com *timeshifting* (ao invés de se basear em uso anônimo), consegue-se uma solução de privacidade mais adequada às necessidades de aplicações de *streaming* em ambientes controlados de rede e, ao mesmo tempo, não excluindo funcionalidades da arquitetura tradicional. Tal solução também é passível de generalização para distribuição de conteúdos diversos em redes CDN.

Resumindo, o principal objetivo deste trabalho foi prover uma solução de privacidade para sistemas IPTV usando a abordagem de **não-relacionabilidade** entre o tráfego consumido por um usuário e o próprio usuário, ao contrário da abordagem tradicional de anonimidade. Isto ajuda a evitar situações indesejadas no próprio serviço de IPTV, tais como propagandas personalizadas, como também fora do serviço de IPTV, tais como vazamento do perfil de uso para profissionais da mídia (jornais, revistas, blogs), spammers, entidades governamentais, entre outros.

Dentro deste contexto, as principais inovações e contribuições deste trabalho foram:

- Uma abordagem diferenciada para a questão da privacidade, baseada na não-relacionabilidade;
- Uma solução baseada em redes P2P com caching como infra-estrutura básica da rede de transporte de sistemas IPTV com serviços de privacidade, sem deixar de lado a transmissão via *multicast*.
- O conceito de indireção para evitar que a correlação entre a origem de uma requisição de conteúdo e o conteúdo requisitado;
- Uma solução de privacidade com operação parametrizável (a sensibilidade e o número máximo de indireções), de forma a balancear as necessidades de diferentes usuários em relação à privacidade e, ao mesmo tempo, dificultar a análise de padrões de tráfego;
- Tratamento do problema de privacidade quando do uso de DRM, através do conceito de EEPG;
- Uma arquitetura passível de generalização para uso em redes CDN.

6.3 Trabalhos Futuros

Este trabalho teve por foco a privacidade nos canais de *broadcast*. Uma evolução natural do trabalho seria a complementação da arquitetura, contemplando aspectos não tratados aqui, tais como canais de vídeo sob demanda, *pay-per-view* e dispositivos *offline* (dispositivos temporariamente não conectados na rede de transporte como, por exemplo, um computador portátil, telefone celular ou reprodutor de mídia). Tais aspectos exigem uma adequação da arquitetura nos aspectos de eventuais limitações dos próprios dispositivos (ex.: de armazenamento e/ou conectividade) e da infra-estrutura (ex.: presença ou não de nós de cache), bem como nos aspectos de DRM (ex.: distribuição de chaves).

Um outro ponto de evolução do trabalho seria um estudo mais aprofundado dos parâmetros relacionados ao mecanismo de privacidade, utilizando-se diferentes sensibilidades no mecanismo de privacidade e diferentes valores máximos de indireção para se detectar possíveis parâmetros ótimos de utilização, tanto do ponto

de vista de privacidade como da relação custo X benefício entre os mecanismos de privacidade e aspectos de desempenho e carga na rede.

Apesar do foco em IPTV, tal solução poderia ser utilizada como base para serviços de distribuição de conteúdos diversos (não somente de áudio/vídeo) em outros ambientes de rede em que possa haver a necessidade de privacidade, tais como redes acadêmicas, tradicionalmente mais abertas que uma rede de propósito específico como a de um provedor de IPTV. Nestes ambientes seria interessante avaliar o comportamento da arquitetura face à competição com outros tipos de tráfegos.

Por fim, a abordagem utilizada no mecanismo de P2P para a privacidade pode formar o embrião de futuras redes *overlay* P2P com privacidade: os nós com o mecanismo de privacidade habilitado formariam um cluster de nós “privativos” para a comunicação com nós tradicionais de forma a se obter a não-relacionabilidade.

REFERÊNCIAS

- 1 KIM, K. On the evolution of PON-based FTTH solutions. **Information Sciences**, v. 149, n. 1-3, p. 21-30, 2003.
- 2 FUCHS, H.; FARBER, N. ISMA interoperability and conformance. **IEEE Multimedia**, v. 12, n. 2, p. 96, 2005.
- 3 CHERRY, S. The battle for broadband [Internet protocol television]. **IEEE Spectrum**, v. 42, n. 1, p. 24, 2005.
- 4 EMPRESA tem direito de vasculhar micro de empregado, diz TRT. **Folha de São Paulo**, 1 Mar. 2006. Disponível em: <<http://www1.folha.uol.com.br/folha/informatica/ult124u19709.shtml>>. Acesso em: 27 Fev. 2008.
- 5 JUSTIÇA permite que empresas monitorem e-mails de funcionários. **Folha de São Paulo**, 16 mai. 2005. Disponível em: <<http://www1.folha.uol.com.br/folha/dinheiro/ult91u96305.shtml>>. Acesso em: 27 Fev. 2008.
- 6 BARBARO, M.; ZELLER, T. A face is exposed for AOL searcher no. 4417749. **New York Times**, 9 ago. 2006. Disponível em: <<http://www.nytimes.com/2006/08/09/technology/09aol.html>>. Acesso em: 27 Fev. 2008.
- 7 ELECTRONIC FRONTIER FOUNDATION. **Google v. DoJ Subpoena**. 2006. Disponível em: <http://www.eff.org/Privacy/search/google_doj_decision.pdf>. Acesso em: 27 Fev. 2008.
- 8 ELECTRONIC FRONTIER FOUNDATION. **CyberSLAPP / John Doe cases**. Disponível em: <<http://www.eff.org/Privacy/Anonymity/cyberslapp.php>>. Acesso em: 27 Fev. 2008.
- 9 BRITISH BROADCASTING CORPORATION. Yahoo 'helped jail China writer'. **BBC**, 2005. Disponível em: <<http://news.bbc.co.uk/1/hi/world/asia-pacific/4221538.stm>>. Acesso em: 27 Fev. 2008.

10 CHA, A.; DIAZ, S. Advocates Sue Yahoo In Chinese Torture Case. **The Washington Post**, 2007. Disponível em: <<http://www.washingtonpost.com/wp-dyn/content/article/2007/04/18/AR2007041802510.html?hpid=moreheadlines>>. Acesso em: 27 Fev. 2008.

11 INSTITUTO BRASILEIRO DE OPINIÃO PÚBLICA E ESTATÍSTICA. **Metodologia de pesquisas de audiência de TV**. 2004. Disponível em: <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortallBOPE&pub=T&db=caldb&comp=pesquisa_leitura&nivel=Metodologia&docid=330AEB5AA888144183256EE40054E25C>. Acesso em: 27 Fev. 2008.

12 CARPENTER, B.; BRIM, S. **RFC 3234 - middleboxes: taxonomy and issues**. [S.l.: s.n.], 2002. Disponível em: <<http://www.faqs.org/rfcs/rfc3234.html>>. Acesso em: 27 Fev. 2008.

13 OPEN IPTV FORUM. **Open IPTV Forum - functional architecture - v.1.1**. 2008. Disponível em: <http://www.openiptvforum.org/docs/OpenIPTV-%20Functional%20Architecture-V1_1-2008-01-15_APPROVED.pdf>. Acesso em: 27 Fev. 2008.

14 LABORATÓRIO DE ARQUITETURA E REDES DE COMPUTADORES DA UNIVERSIDADE DE SÃO PAULO. **Relatório técnico 1 - projeto IPTV**. São Paulo: Escola Politécnica, Universidade de São Paulo, 2007.

15 KIM, J.Y. et al. NGN architecture for IPTV service without effect on conversational services. In: THE 8TH INTERNATIONAL CONFERENCE ADVANCED COMMUNICATION TECHNOLOGY, 2006. **Proceedings of ICACT 2006**. [S.l.: s.n.], 2006. p. 5.

16 LAO, L. et al. A comparative study of multicast protocols: top, bottom, or in the middle ? In: EIGHTH IEEE GLOBAL INTERNET SYMPOSIUM (GI 2005), 2005, Miami. **Proceedings of the Eighth IEEE Global Internet Symposium**. Miami: The IEEE Communications Society Internet Technical Committee, 2005. Disponível em: <http://www.cs.ucla.edu/NRL/OverProbe/papers/csd_tr_040054.pdf>. Acesso em: 27 Fev. 2008.

17 SIMPSON, W.; GREENFIELD, H. **IPTV and internet video: expanding the reach of television broadcasting (NAB executive technology briefings)**. Burlington, MA, USA: Focal Press, 2007.

18 IBRAHIM, K.F. **Newnes guide to television and video technology**. 4th Ed. Oxford: Newnes, 2007.

- 19 SIMPSON, W. **Video over IP: a practical guide to technology and applications**. Burlington: Focal Press, 2006.
- 20 LEE, Y.K.; LEE, D. Broadband access in Korea: experience and future perspective. **IEEE Communications Magazine**, v. 41, n. 12, p. 30-36, 2003.
- 22 LEE, S.; CHO, C.; HAN, I. FTTH residential gateway and IP tuner for IPTV service. In: CCNC 2006 - CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE, 2006, Las Vegas. **Proceedings of the 3rd IEEE CCNC**. Las Vegas: [s.n.], 2006.
- 21 POPESCU, B. et al. A DRM security architecture for home networks. In: ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT, 2004, Washington, DC. **Proceedings of the 4th ACM workshop on Digital Rights Management**. Washington, DC: ACM Press, 2004. p. 1-10.
- 23 TRUSTED COMPUTING GROUP. **Trusted platform module (TPM) specifications**.2007 Disponível em: <<https://www.trustedcomputinggroup.org/specs/TPM/>>. Acesso em: 27 Fev. 2008.
- 24 FARMER, J.O. **The basics of video**.2005 Disponível em: <<http://www.ftthcouncil.com/documents/458441.pdf>>. Acesso em: 27 Fev. 2008.
- 25 BANISAR, D. **Privacy and human rights**.2000 Disponível em: <<http://www.gilc.org/privacy/survey/>>. Acesso em: 27 Fev. 2008.
- 26 DECEW, J. Privacy. 2006. **The Stanford Encyclopedia of Philosophy (Fall 2006 Edition)**. [S.l.: s.n.], 2006. Disponível em: <<http://plato.stanford.edu/archives/fall2006/entries/privacy>>. Acesso em: 27 Fev. 2008.
- 27 WARREN, S.; BRANDEIS, L. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890.
- 28 WESTIN, A. **Privacy and freedom**. New York: Atheneum New York, 1967. Disponível em: <<http://www.faculty.piercelaw.edu/roy/06PrivacyLaw/Reading%208-22.doc>>. Acesso em: 27 Fev. 2008.

29 GAVISON, R. Privacy and the limits of law. **The Yale Law Journal**, v. 89, n. 3, p. 421-471, 1980.

30 PFITZMANN, A.; HANSEN, M. **Anonymity, unlinkability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology**.2007 Disponível em: <http://dud.inf.tu-dresden.de/Anon_Terminology.shtml>. Acesso em: 27 Fev. 2008.

31 BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 27 Fev. 2008.

32 BRASIL. **Código civil brasileiro (Lei No 10.406)**. Brasília: Senado Federal, 2002. Disponível em: <<http://www.planalto.gov.br/CCIVIL/leis/2002/L10406.htm>>. Acesso em: 27 Fev. 2008.

33 **Código de Defesa do Consumidor (Lei No 8.078)**. Brasília: Senado Federal, 1990. Disponível em: <<http://www.mj.gov.br/DPDC/servicos/legislacao/cdc.htm>>. Acesso em: 27 Fev. 2008.

34 PINHEIRO, P. **E-mail corporativo**.2007 Disponível em: <http://www.pppadvogados.com.br/paginas_unicas.asp?PaginaUnicaTipoID=6&intePaginaUnicaID=63>. Acesso em: 27 Fev. 2008.

35 EUROPEAN PARLIAMENT. **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**. Brussels: [s.n.], 1995. Disponível em: <http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf>. Acesso em: 27 Fev. 2008.

36 KORBA, L.; KENNY, S. Towards Meeting the Privacy Challenge: Adapting DRM. In: ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT, 2002. **Proceedings of the ACM Workshop on Digital Rights Management** . [S.l.: s.n.], 2002.

37 EUROPEAN PARLIAMENT. **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)**. Brussels: [s.n.], 1995. Disponível em: <

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT>. Acesso em: 27 Fev. 2008.

38 ANDERSSON, C. **Enhancing privacy for mobile networks: examples of anonymity solutions and their analysis**. Karlstad: Division for Information Technology, Department of Computer Science, Karlstads Universitet, 2005.

39 UNITED STATES OF AMERICA. **Video privacy protection act (18 U.S.C. § 2710)**. [S.l.: s.n.], 1988. Disponível em: <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html>. Acesso em: 27 Fev. 2008.

40 UNITED STATES OF AMERICA. **Cable television consumer protection and competition act (47 U.S.C. § 551)**. [S.l.: s.n.], 1992. Disponível em: <http://www4.law.cornell.edu/uscode/search/display.html?terms=551&url=/uscode/html/uscode47/usc_sec_47_00000551----000-.html>. Acesso em: 27 Fev. 2008.

41 RAO, J.; ROHATGI, P. Can pseudonymity really guarantee privacy? In: 9TH USENIX SYMPOSIUM, 2000, Denver. **Proceedings of the 9th Usenix Symposium**. Denver: [s.n.], 2000. Disponível em: <<http://www.freehaven.net/anonbib/cache/rao-pseudonymity.pdf>>. Acesso em: 27 Fev. 2008.

42 CHAUM, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. **Journal of Cryptology**, v. 1, n. 1, p. 65-75, 1988.

43 BOYAN, J. The Anonymizer: protecting user privacy on the web. **Computer-Mediated Communication Magazine**, v. 4, n. 9, 1997.

44 CHAUM, D. Untraceable electronic mail, return addresses, and digital pseudonyms. **Communications of the ACM**, v. 24, n. 2, p. 84-88, 1981.

45 GOLDSCHLAG, D.; REED, M.; SYVERSON, P. Onion routing for anonymous and private internet connections. **Communications of the ACM**, v. 42, n. 2, p. 39-41, 1999.

46 DINGLEDINE, R.; MATHEWSON, N.; SYVERSON, P. Tor: the second-generation onion router. In: 13TH USENIX SECURITY SYMPOSIUM, 2004, San Diego. **Proceedings of the 13th USENIX Security Symposium**. San Diego: [s.n.], 2004.

- 47 SHERWOOD, R.; BHATTACHARJEE, B.; SRINIVASAN, A. P5: A protocol for scalable anonymous communication. **Journal of Computer Security**, v. 13, n. 6, p. 839-876, 2005.
- 48 GOEL, S. et al. **Herbivore: a scalable and efficient protocol for anonymous communication**. [S.l.: s.n.], 2003. Disponível em: <<http://ecommons.library.cornell.edu/handle/1813/5606>>. Acesso em: 27 Fev. 2008.
- 49 CRANOR, L. **Web privacy with P3P**. Sebastopol: O'Reilly, 2002.
- 50 INSTITUTO BRASILEIRO DE OPINIÃO PÚBLICA E ESTATÍSTICA. **Metodologia target group index**.2004 Disponível em: <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&db=caldb&comp=pesquisa_leitura&nivel=Metodologia&docid=7289EBCFC218136C83256EE6006A16A7>. Acesso em: 27 Fev. 2008.
- 51 CAIN, B. et al. **RFC 3376 - Internet group management protocol version 3**. [S.l.: s.n.], 2002. Disponível em: <<http://www.faqs.org/rfcs/rfc3376.html>>. Acesso em: 27 Fev. 2008.
- 52 VORA, P. et al. Privacy and digital rights management. In: W3C WORKSHOP ON DIGITAL RIGHTS MANAGEMENT, 2001, Sophia-Antipolis. **Proceedings of the W3C Workshop on Digital Rights Management**. Sophia-Antipolis: [s.n.], 2001. Disponível em: <<http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html>>. Acesso em: 27 Fev. 2008.
- 53 REITER, M.; RUBIN, A. Crowds: anonymity for web transactions. **ACM Transactions on Information and System Security**, v. 1, n. 1, p. 66-92, 1998.
- 54 PRIME. **PRIME - privacy and identity management for Europe**.2007 Disponível em: <<https://www.prime-project.eu/>>. Acesso em: 27 Fev. 2008.
- 55 FIDIS. **FIDIS - future of identity in the information society**.2007 Disponível em: <<http://www.fidis.net>>. Acesso em: 27 Fev. 2008.
- 57 ELLISON, C. **RFC2692: SPKI requirements**. [S.l.: s.n.], 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2692.txt>>. Acesso em: 27 Fev. 2008.

56 ELLISON, C. et al. **RFC2693: SPKI certificate theory**. [S.l.: s.n.], 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2693.txt>>. Acesso em: 27 Fev. 2008.

58 AURA, T.; ELLISON, C. **Privacy and accountability in certificate systems**. [S.l.]: Helsinki University of Technology, 2000.

59 PERSIANO, P.; VISCONTI, I. User privacy issues regarding certificates and the TLS protocol: the design and implementation of the SPSL protocol. In: 7TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2000, Athens. **Proceedings of the 7th ACM conference on Computer and communications security**. Athens: ACM Press, 2000. p. 53-62.

60 CONRADO, C. et al. Privacy in an identity-based DRM system. In: 14TH INTERNATIONAL WORKSHOP ON DATABASE AND EXPERT SYSTEMS APPLICATIONS, 2003. **Proceedings of the 14th International Workshop on Database and Expert Systems Applications**. [S.l.: s.n.], 2003. Disponível em: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1232053>. Acesso em: 27 Fev. 2008.

61 ERICKSON, J. et al. Principles for standardization and interoperability in web-based digital rights management. In: W3C WORKSHOP ON DIGITAL RIGHTS MANAGEMENT, 2001, Sophia-Antipolis. **Proceedings of the W3C Workshop on Digital Rights Management**. Sophia-Antipolis: [s.n.], 2001.

62 CABLELABS. **CableCARD primer**.2006 Disponível em: <http://www.opencable.com/primer/cablecard_primer.html>. Acesso em: 27 Fev. 2008.

63 HUANG, Y. ET AL. Challenges of P2P streaming technologies for IPTV services. **Proc. of IPTV Workshop, International World Wide Web Conference**, 2006.

64 SILVERSTON, T.; FOURMAUX, O. Measuring p2p iptv systems. **Proc. of NOSSDAV**, 2007.

65 CHEN, Y.F. ET AL. When is P2P Technology Beneficial for IPTV Services. **Proceedings of the 17th International Workshop on Network and Operating System Support for Digital Audio and Video, May**, 2007.

66 HEI, X. ET AL. A measurement study of a large-scale P2P IPTV system. **IEEE Transactions on Multimedia**, 2007.

67 GALLO, D. **Arquitetura de IPTV com visualização deslocada no tempo** . 2008. Exame de Qualificação (Mestrado) - Universidade de São Paulo. 2008

68 AZUREUS PROJECT. **Message Stream Encryption**. Disponível em: <http://www.azureuswiki.com/index.php/Message_Stream_Encryption>. Acesso em: 27 Fev. 2008.

69 XMLTV PROJECT. **XMLTV File Format**.2008 Disponível em: <<http://xmltv.org/wiki/xmltvfileformat.html>>. Acesso em: 27 Fev. 2008.

70 ARNOLD, K.; GOSLING, J.; HOLMES, D. **The Java programming language**. 4th ed. Stoughton: Prentice Hall PTR, 2005.

65 GOSLING, J. et al. **The Java language specification**. 3rd Ed. Stoughton: Prentice Hall PTR, 2000.

72 ECLIPSE FOUNDATION. **Eclipse.org homepage**.2008 Disponível em: <<http://www.eclipse.org>>. Acesso em: 27 Fev. 2008.

73 VIDEOLAN PROJECT. **VideoLAN - VLC media player**.2008 Disponível em: <<http://www.videolan.org>>. Acesso em: 27 Fev. 2008.

74 FALLON, H. ET AL. **VLC user guide**.2003 Disponível em: <<http://www.videolan.org/doc/vlc-user-guide/en/vlc-user-guide-en.html>>. Acesso em: 27 Fev. 2008.

75 **Java bittorrent API**.2008 Disponível em: <<http://sourceforge.net/projects/bitext/>>. Acesso em: 27 Fev. 2008.

76 VLC PROJECT. **JVLC Java multimedia library**.2008 Disponível em: <<http://trac.videolan.org/jvlc/>>. Acesso em: 27 Fev. 2008.

77 GB-PVR GROUP. **GBPVR Documentation Wiki - Utility - MceEpg2XmlTv**. Disponível em: <<http://gbpvr.com/pmwiki/pmwiki.php/Utility/MceEpg2XmlTv>>. Acesso em: 27 Fev. 2008.

78 FREEGUIDE PROJECT. **FreeGuide - your TV Guide**. Disponível em: <<http://freeguide-tv.sourceforge.net/>>. Acesso em: 27 Fev. 2008.

79 MAGALHÃES, M.N.; DE LIMA, A.C.P. **Noções de probabilidade e estatística.** 4a Edição. São Paulo: Edusp, 2002.