UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM

CIÊNCIA DA COMPUTAÇÃO

Sistema para a oferta de Serviços Baseados em Localização com Garantias de Privacidade ao Usuário

Filipe Nunes Ribeiro

São Carlos-SP
Maio/2009

Filipe Nunes Ribeiro

Sistema para a oferta de Serviços Baseados em Localização com Garantias de Privacidade do Usuário

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Ciências exatas e tecnologia da Universidade Federal de São Carlos como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, área de concentração: Sistemas Distribuídos e Redes.

Orientador:
Prof. Dr. Sérgio Donizetti Zorzo

São Carlos-SP
Maio/2009

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária da UFSCar

R484so

Ribeiro, Filipe Nunes.
Sistema para a oferta de serviços baseados em localização com garantias de privacidade do usuário / Filipe Nunes Ribeiro. -- São Carlos : UFSCar, 2010.
108 f.

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

1. Sistemas de recomendação. 2. Serviços baseados em localização. 3. Privacidade e personalização. I. Título.

CDD: 003.7 (20ª)

Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Programa de Pós-Graduação em Ciência da Computação

"Sistema para a Oferta de Serviços Baseados em Localização com Garantias de Privacidade ao Usuário"

FILIPE NUNES RIBEIRO

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

Membros da Banca:

Prof. Dr. Sérgio Donizetti Zorzo
(Orientador - DC/UFSCar)

Profa. Dra. Regina Borges de Araújo
(DC/UFSCar)

Prof. Dr. Arthur João Catto
(IC/UNICAMP)

Prof. Dr. Paulo Sérgio Muniz Silva
(POLI/USP)

São Carlos
Junho/2009

Dedico este trabalho à minha amada família que, em todos os momentos, sempre me apoiou incondicionalmente. Meus pais, Anderson e Julieta e minhas irmãs Débora e Maressa.

Agradecimentos

Agradeço primeiramente a Deus, que é o sustentador e mantenedor da vida, e me guiou em todos os meus passos até aqui. A Ele toda a glória!

Aos meus amados pais, Anderson e Julieta. Não tenho palavras para descrever o quanto foram importantes para a minha formação e para me tornar quem me tornei. Muito obrigado, pelo amor, incentivo e exemplo de vida que são!

Às minhas queridas irmãs, Débora e Maressa, que sempre estiveram do meu lado me apoiando e sempre dedicaram a mim um carinho especial que só elas têm.

Aos meus avós, tios e primos que mesmo com a distância nunca deixaram de me incentivar.

À UFSCar pela grande oportunidade e aprendizado.

Aos professores e funcionários do Departamento de Computação, em especial ao professor Sérgio D. Zorzo pela orientação e dedicação, e à tia Verinha e Cristina, pelos momentos de descontração.

Não poderia deixar de citar as grandes amizades feitas no departamento de computação durante o período do mestrado que foram essenciais para que eu alcançasse este objetivo. Em especial agradeço aos amigos Adriano, Thiago, Kamila, Ana Paula, Flávio, Elis, Matheus, Mariana, Claudinho.

Aos amigos da Igreja Presbiteriana de São Carlos que foram essenciais para a minha permanência nesta cidade, em especial aos amigos Adans, Marcelo, Thiago Daniel, Wesley, Natália, Flavinha, Val e Suellen.

Aos grandes amigos da república Mancebo`s House: Fil Abdalla, Murilo, Lut, Bruno, Gabriel, Baiano e Shell.

Enfim, agradeço a todos que direta ou indiretamente contribuíram para a realização deste trabalho.

Resumo

A utilização de informações de posicionamento geográfico de usuários para o oferecimento de serviços é a principal característica dos Serviços Baseados em Localização (*LBS*). Serviços como localização de restaurantes e hotéis mais próximos, previsão do tempo ou verificação das condições de tráfego nas regiões em que o usuário se encontra são apenas alguns dos serviços que podem ser encontrados sem muita dificuldade. Embora a utilização de *LBS* possa ser muito útil e oferecer diversas facilidades e benefícios, a manipulação das informações de localização por indivíduos maliciosos pode representar séria ameaça à privacidade dos usuários. A telefonia móvel tem sido o ambiente mais utilizado para a oferta de *LBS*, justificado pelo aumento do poder de processamento e pelas tecnologias de localização presentes nos dispositivos, além do grande número de potenciais usuários. Apesar da existência de algumas técnicas para o oferecimento de privacidade na execução de *LBS*, pouco interesse tem sido observado na utilização de tais técnicas no ambiente de telefonia móvel; além do mais, a maioria das técnicas propostas não apresentam resultados concretos que possam ser utilizados em um ambiente real. Este trabalho apresenta um sistema capaz de oferecer privacidade de localização para aplicações de telefonia móvel. O termo privacidade de localização indica a capacidade de evitar que terceiros tomem conhecimento sobre a localização presente ou passada do usuário. Sendo assim, é proposto aqui o Sistema Baseado em Privacidade de Localização (*SBPL*), que é capaz de oferecer controle na liberação das informações de localização e que permite a execução de *LBS* com garantias de privacidade para os usuários de telefonia móvel. O *SBPL* é composto por uma aplicação cliente, executada no dispositivo móvel, e um servidor confiável, que atua entre o dispositivo móvel e o provedor do serviço. Além disso, o sistema proposto segue as determinações dos principais guias de privacidade existentes e permite ainda ao usuário a configuração de suas preferências, o que garante a adaptação a diferentes usuários e serviços. Testes em ambientes *LBS* foram executados que evidenciaram a eficiência do *SBPL* e a possibilidade de utilização no ambiente de telefonia móvel.

Abstract

The use of geographical information about users is the main quality of Location Based Services (LBS). Services like finding nearest hotels and restaurants, weather forecasting or traffic conditions verifying are some of them that can be found without hard effort. Even though using LBS can be bring out facilities and benefits, manipulation of location information by malicious parties can represent serious threat to users' privacy. The mobile telephony has been widely used to offer LBS, mainly due to the powerful increase of mobile devices, location capabilities in the devices and the large number of potential users. Despite the existence of techniques to offer privacy in LBS execution, there is no much interest in using these techniques in the mobile telephony environment, besides, the majority of proposed techniques do not present results that can be used in a real environment. This work presents a system that offers location privacy to mobile phone applications. The expression location privacy points out the competency of avoid that third parties learn about current or past location of the user. Then, we propose the Location Privacy Based System (SBPL), that offers manners to control location information release and allows LBS execution with privacy guarantees to mobile phone users. The SBPL is composed by a client application, performed in the mobile device, and a trusted server, acting between the mobile device and the service provider. Besides, the SBPL follows the recommendations of existing privacy guidelines, and allows the user to determine his preferences, which assure adaptation to distinct users and services. Tests were performed in LBS environments that prove the efficiency of SBPL and the possibility of using it in the mobile phone environment.

Lista de Abreviaturas e Siglas

ACPL – Aplicação Cliente com Privacidade de Localização

AIC – *Adaptive-Internal Cloak*

APPEL – *A P3P Preference Exchange Language*

API – *Application Program Interface*

CDC – *Connected Device Configuration*

CLDC – *Connected Limited Device Configuration*

CoPS - *Context Privacy Service*

DM – Dispositivo Móvel

DP – Desvio Padrão

EDGE – *Enhanced Data Rates for Global Evolution*

EPC – *European Parliament and the Council*

GeoPriv – *Geographic Location/Privacy*

GPS – *Global Position System*

GPRS – *General Packet Radio Service*

HTTP – *Hypertext Transfer Protocol*

IETF – *Internet Engineering Task Force*

JME – *Java Micro Edition*

LBS – *Location Based Services*

LOC – *Location Work Group*

OECD – *Organization for Economic Co-Operation and Development*

OMA – *Open Mobile Alliance*

OpenLS – *Open Location Services Interface Standard*

PawS – *Privacy Awareness System*

P3P – *Platform for Privacy Preferences Project*

QoP – *Quality of Privacy*

MLP – *Mobile Location Protocol*

Peer-to-peer LBS – Serviço *LBS* que envolve a localização de outros usuários

Pull LBS – Serviço *LBS* no qual o usuário faz uma requisição a um provedor

Push LBS – Serviço *LBS* no qual o usuário recebe o serviço sem o envio de uma requisição a um provedor

SBPL – Sistema Baseado em Privacidade de Localização

SBPM – Servidor Baseado em Privacidade Multinível

SLIREP – *Standard Location Immediate Report*

SSLv3 – *Secure Socket Layer version 3*

TMR – Tempo Médio de Resposta

XML – *Extensible Markup Language*

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

Encontrar o restaurante ou hotel mais próximo, em um local desconhecido, sempre dependeu da busca de informações com pessoas que conheciam melhor a região. No entanto, essa situação não é mais uma regra, uma vez que, com posse de um dispositivo móvel capaz de ser localizado e com acesso à Internet, é possível obter tais informações apenas pressionando algumas teclas (RIBEIRO; ZORZO, 2009b).

Serviços que utilizam o posicionamento de um usuário-final, com base em um dispositivo capaz de ser localizado, visando algum propósito específico são chamados de serviços baseados em localização ou *LBS* (*Location Based Services*) (PERUSCO; MICHAEL, 2007). Tais serviços têm apresentado considerável crescimento tanto na diversidade de aplicações quanto no número de potenciais usuários. A possibilidade de localização de dispositivos móveis permitiu o oferecimento de diversos *LBS*, como: identificação de pontos de interesse mais próximos (por ex: hotéis, restaurantes etc); verificação das condições de tráfego ou previsão do tempo e determinação da posição geográfica de outros usuários.

Um dos mercados que têm se mostrado mais promissor para a utilização destes serviços é o de telefonia móvel, pois, além de oferecer dispositivos com maior poder de processamento, tem disponibilizado novas técnicas de localização e melhorias na comunicação com a Internet. Contudo, a manipulação de informações posicionamento geográfico de maneira indevida pode representar riscos quanto à manutenção da privacidade dos usuários, a partir do momento em que é possível associar a identidade de um usuário às suas informações pessoais (PARESCHI; RIBONI; BETTINI, 2008).

Ameaças como identificação não-autorizada de perfil e revelação de informações sobre contatos sociais (MARTUCCI et al., 2006), monitoramento das atividades de um usuário para fins maliciosos (BETTINI; WANG; JAJODIA, 2005), ou até mesmo informações de suporte em processos judiciais (BOWEN; MARTIN, 2007) representam apenas alguns dos riscos que o usuário corre se suas informações forem utilizadas inadequadamente. Warrior, McHenry e McGee (2003) levantam ainda questões concernentes à segurança dos usuários que podem surgir caso informações de localização caiam em mãos erradas.

A preocupação com relação à privacidade no que diz respeito à manipulação de informações pessoais tem levado à criação de diversos guias, limitando a forma de coleta, utilização e divulgação de dados relacionados ao usuário, não só no ambiente de execução *LBS* como em outras aplicações. Os guias de privacidade da Organização para Cooperação Econômica e Desenvolvimento (OECD, 1980) e as diretivas de proteção de dados da União Européia (EPC, 1995) se destacam na apresentação de direcionamentos concisos e rígidos quanto à manipulação e liberação de dados pessoais.

Existem três categorias de *LBS* com características distintas no que diz respeito à privacidade. Essas três categorias são denominadas *peer-to-peer, pull* e *push LBS*.

A categoria *peer-to-peer LBS* é caracterizada pela obtenção de informações de localização de outros usuários e, por isso, envolve diversos aspectos de privacidade de ordem até mesmo psicológica, presentes nas relações interpessoais. O oferecimento de privacidade para esta categoria foge do escopo do trabalho aqui proposto, visto que já há estudos aprofundados em que soluções foram propostas especificamente para essa categoria de serviços (SACRAMENTO; ENDLER; NASCIMENTO, 2005), (HONG; LANDAY, 2004).

A categoria *pull* LBS é caracterizada pela requisição direta do serviço para seu recebimento; por exemplo, o usuário solicita informações das condições de trânsito concernentes à sua atual localização.

Por fim, na categoria *push LBS*, não é necessária a solicitação direta do serviço para que ele seja oferecido; por exemplo, ao passar próximo de uma cafeteria, o usuário recebe o preço do café.

Existem algumas abordagens de privacidade que contemplam as duas últimas categorias *LBS* citadas, entretanto, não se veem soluções práticas capazes de serem aplicadas e testadas em ambientes execução *LBS* para celulares. Além do mais, o que se tem observado quando da disponibilização de aplicações *LBS*, especialmente *pull* e *push LBS*, para o usuário, é uma grande falta de interesse, por parte dos provedores, no oferecimento de políticas de privacidade que informem ao usuário o tratamento dado às suas informações pessoais, especialmente as de localização. Muito menor preocupação é notada quando se trata da utilização de técnicas de proteção à privacidade que garantam ao usuário a execução de *LBS* com mecanismos que assegurem sua privacidade.

1.1 Motivação

Nesse contexto em que pouco esforço tem sido empregado na utilização de técnicas de privacidade pelas empresas que oferecem *LBS* para celulares, o trabalho aqui apresentado buscou preencher essa lacuna e garantir condições de execução de *LBS* com privacidade para o usuário.

Apesar da necessidade do oferecimento de privacidade no ambiente de serviços baseados em localização, entende-se que as preferências de privacidade de um usuário podem ser altamente subjetivas (RIBEIRO; ZORZO, 2009b), dependendo dos mais diversos fatores como culturais e religiosos e, até mesmo, questões íntimas do usuário, como idade e saúde, dentre outros (SACRAMENTO, 2006).

Sendo assim, além do simples oferecimento de técnicas de privacidade que impeçam ou minimizem ameaças à privacidade do usuário, é necessário adaptar-se às preferências de privacidade de diferentes usuários. Além disso, alguns serviços dependem da liberação de dados com informações mais precisas para a sua execução. Dessa forma, dependendo da técnica de privacidade utilizada, pode ser que o serviço não se concretize devido à incompatibilidade das informações do usuário disponibilizadas com as informações necessárias. Então, é importante que se permita a escolha entre a execução do serviço com qualidade e a utilização de técnicas rígidas de privacidade.

Logo, a motivação para este trabalho consiste na busca da conciliação entre os benefícios oferecidos pelos serviços baseados em localização e a manutenção da privacidade do usuário, de forma que possam ser oferecidos serviços de privacidade diferenciados de acordo com as preferências dos indivíduos.

1.2 Objetivos

Os principais objetivos deste trabalho são:

- Oferecimento de garantias de privacidade ao usuário – implementar técnicas capazes de oferecer ao usuário garantias de privacidade na execução.

- Personalização - permitir a adaptação do serviço a diferentes preferências de privacidade de usuários de LBS.

- Coerência com guias de privacidade – oferecer serviços que estejam em conformidade com as normas estipuladas pelos guias de privacidade da *OECD* e da *EPC*, com relação à coleta, manipulação e liberação das informações de localização.

- Suporte a padrões de comunicação – oferecer suporte a padrões de comunicação disponibilizados para *LBS* de forma que a solução implementada possa ser utilizada e suportada por outros trabalhos que utilizam os padrões.

- Eficiência – garantir que os serviços possam ser executados com garantias de privacidade, mas sem a inserção de atraso excessivo nos tempos de resposta.

- Real aplicabilidade – oferecer um sistema que permita a aplicabilidade da solução em ambientes reais e possibilidade de utilização com *LBS* oferecidos atualmente.

1.3 Contribuições

Este trabalho apresenta um sistema capaz de oferecer garantias de privacidade aos usuários de serviços baseados em localização para celulares. Tal sistema, denominado Sistema Baseado em Privacidade de Localização (*SBPL*), atende aos objetivos descritos anteriormente.

O *SBPL* oferece suporte à execução de *LBS* das categorias *pull* e *push* com garantias de privacidade para os usuários de telefonia móvel. Além disso, assegura ao usuário a possibilidade de personalização de suas preferências, uma vez que é permitido configurar o nível de privacidade desejado.

O sistema apresentado não só foi desenvolvido em conformidade com os princípios da coleta, manipulação e liberação dos dados dispostos nos guias de privacidade citados anteriormente, como também oferece suporte ao padrão de comunicação *OpenLS* (OPENLS, 2008) para o envio de requisições aos provedores *LBS*. Sendo assim, os serviços oferecidos por provedores que disponibilizam acesso através da utilização desse padrão podem ser utilizados com garantias de privacidade por meio do *SBPL*.

Para atender às diferentes características de cada categoria de serviço suportada pelo *SBPL*, foram propostos dois diferentes modelos de execução que direcionaram o desenvolvimento do sistema com garantias de privacidade. Compõem o *SBPL* uma aplicação cliente, que deve ser executada no dispositivo móvel, e um servidor confiável, que atua como intermediário entre a aplicação cliente e o provedor.

O *SBPL* foi testado em um ambiente *LBS*, o que permitiu elucidar o impacto da utilização de técnicas de privacidade no que diz respeito ao tempo de resposta e qualidade do serviço oferecido. Dessa forma, foi possível confirmar a eficiência e real aplicabilidade do sistema.

1.4 Organização do Trabalho

Este trabalho possui 7 capítulos que desenvolvem o assunto proposto.

O capítulo 2 apresenta um estudo sobre os serviços baseados em localização. São discutidas as classificações *LBS* acompanhadas de exemplos típicos de seus serviços e apresentadas as tecnologias que permitem a localização dos dispositivos móveis.

O capítulo 3 aborda as questões de privacidade envolvidas na prestação de serviços baseados em localização e detalha as ameaças decorrentes da obtenção de informações de localização por indivíduos mal intencionados.

O capítulo 4 descreve o trabalho desenvolvido. São apresentados detalhes da arquitetura do *SBLP*, além de uma descrição mais precisa dos modelos de execução propostos e dos detalhes de implementação. Finalizando o capítulo, é apresentada uma discussão geral sobre as características do trabalho proposto.

No capítulo 5 são descritos os testes realizados que permitiram a avaliação do tempo de resposta e da qualidade dos dados obtidos com a utilização de técnicas de privacidade. Além disso, testes de escalabilidade foram executados e os resultados foram apresentados e discutidos.

No capítulo 6 são apresentados os trabalhos relacionados ao trabalho aqui descrito, ressaltando as estratégias utilizadas por cada autor para o oferecimento de privacidade e comparando-as às estratégias aqui empregadas.

Por fim, o capítulo 7 apresenta as conclusões e propõe trabalhos futuros.

2 Serviços Baseados em Localização

Serviços que utilizam informações de localização podem ser utilizados em diversos cenários, como, por exemplo: em um ambiente hospitalar para melhor controle da localização da equipe de trabalho, visando melhor atendimento a pacientes (TENTORI et al., 2005); em uma empresa de táxis para otimizar o atendimento aos clientes, enviando os taxistas mais próximos disponíveis; ou até mesmo em um supermercado para permitir a localização das mercadorias através de etiquetas de identificação por radiofrequência (*RFID*) (JUELS; RIVEST; SZYDLO, 2003). Entretanto, a telefonia móvel é um ambiente que pode ser considerado privilegiado quando se trata da quantidade de novas aplicações *LBS* disponibilizadas recentemente.

O impulso inicial dos serviços baseados em localização para celulares deu-se em 1996, quando começou-se a debater o aprimoramento do serviço de emergência norte-americano, 911. Este serviço já contava com a localização de telefonia fixa para as chamadas de emergência, e o objetivo do governo era que as empresas de telefonia móvel também fossem capazes de localizar as chamadas provenientes de dispositivos móveis. Dessa forma, seria possível a localização de pessoas caso elas não a soubessem ou não pudessem falar adequadamente em situações de perigo (WARRIOR; MCHENRY; MCGEE, 2003).

Desde então, o oferecimento de *LBS* para celulares tem apresentado considerável crescimento devido a uma série de fatores, como o desenvolvimento de novas tecnologias de localização; a redução de custos de aparelhos capazes de oferecer suporte a *LBS*; o surgimento de dispositivos móveis com maior poder de processamento; e o grande crescimento do número de usuários de tais aplicações.

Diversos *LBS* estão disponíveis para utilização por usuários de telefonia móvel. Alguns deles foram incorporados da Internet para o ambiente móvel, como o *Google Maps Mobile* (GOOGLE, 2009a), que é muito semelhante ao *Google Maps*, e disponibiliza serviços de localização de pontos de interesse mais próximos (por exemplo: restaurantes, farmácias etc), determinação de rotas entre duas localidades e informações sobre condições de tráfego.

Outros serviços facilitaram ainda mais o monitoramento dos locais frequentados por filhos, parceiros ou amigos. O antigo método de ligar para o telefone celular do “investigado” pode parecer ultrapassado em comparação com a possibilidade de

identificação de sua posição através de alguma técnica de localização para celulares, sem mesmo que ele saiba (CLARO, 2009) (VIVO, 2008).

A empresa alemã MOBILOCO (2009) oferece serviços baseados em localização para telefones celulares de usuários de todas as quatro operadoras atuantes no país. Para isso, a empresa assinou contratos com todas elas para o fornecimento das informações de localização. Dentre os serviços oferecidos por esta empresa estão a localização de amigos, a possibilidade de marcar encontros com pessoas presentes no mesmo ambiente, como em festas, além de propagandas pelo celular de preços para a entrada no cinema ou teatro, dentre outros.

Apesar da real possibilidade de faturamento com a prestação deste tipo de serviço, algumas empresas o tem fornecido sem nenhum custo para o usuário. Na verdade, deve-se arcar com os custos de comunicação, já que o serviço é provido via Internet.

Além do *Google Maps Mobile*, que oferece serviços gratuitos, existe também o *TOguide* (2009), que é um guia interativo do centro da cidade de *Turin*, na Itália. Ele permite a obtenção de informações sobre vários pontos de interesse da cidade, que são agrupados por categorias (palácios, pizzarias, hotéis, museus, teatros etc). Para alguns telefones celulares, a informação é relativa à posição atual do usuário, determinada pelo sistema de posicionamento baseado no *Cell-ID*. Outro guia turístico gratuito é o MobiEXPLORE (2009), que disponibiliza informações para passeios orientados em diversos países, como Reino Unido, Croácia e Itália.

2.1 Técnicas de Localização

Atualmente existem diversas técnicas de localização de dispositivos móveis, que diferem na precisão obtida, no ambiente no qual são utilizadas e nas características dos dispositivos.

A localização pode ser realizada de duas formas, no que diz respeito ao ambiente de utilização. Alguns casos de determinação da posição de usuários são específicos para o interior de construções (edifícios, hospitais, supermercados etc.) e por isso recebem o nome de localização interna ou *indoor*. Este tipo de localização é utilizado, geralmente, em áreas relativamente pequenas se comparadas ao posicionamento em grandes cidades, e, dessa forma, devem apresentar uma precisão elevada, pois uma informação pouco precisa não teria utilidade, uma vez que poderia não identificar um alvo.

Um exemplo de aplicação que utiliza a localização *indoor* é a busca do posicionamento de médicos e enfermeiros na área de um hospital (TENTORI et al., 2005), com o intuito de proporcionar melhor controle sobre as atividades realizadas por eles. Dessa forma, seria possível agilizar o atendimento aos pacientes, solicitando-se a presença dos médicos ou enfermeiros mais próximos.

GÖRLACH, TERPSTRA e HEINEMANN (2004) fazem um levantamento das técnicas de localização *indoor*, que são apresentadas abaixo.

Uma delas propõe a utilização de *Active Badges* (WANT et al., 1992, apud GÖRLACH; TERPSTRA; HEINEMANN, 2004), pequenos dispositivos acoplados aos usuários que, periodicamente, emitem um código único, o qual é captado por sensores instalados em toda a extensão do ambiente onde se deseja realizar a localização. Os sinais captados são encaminhados até uma estação mestre que os processa, permitindo a identificação dos usuários, e torna-os disponíveis para os clientes que desejam utilizá-los. Este sistema apresenta resolução em nível de sala.

A técnica denominada BAT (WARD; JONES; HOPPER, 1997, apud GÖRLACH; TERPSTRA; HEINEMANN, 2004) é parecida com a do trabalho citado anteriormente; no entanto, as medidas são feitas a partir de transmissores ultrassônicos, o que proporciona maior precisão, entre 8 e 14 centímetros na média.

Outro refinamento feito é o sistema de suporte à localização *Cricket (*PRIYANTHA; CHAKRABORTY; BALAKRISHNAN, 2000, apud GÖRLACH; TERPSTRA; HEINEMANN, 2004*)*, também baseado em transmissores ultrassônicos. Diferentemente das propostas anteriores, o *cricket*, dispositivo carregado pelos usuários, capta os sinais do ambiente para determinar sua localização. Desta forma, o dispositivo tem conhecimento da sua localização, mas os demais dispositivos e o restante dos componentes da rede não o têm.

Outro método de localização *indoor* é baseado na infraestrutura de rede sem-fio existente (SMAILAGIC et al., 2001, apud GÖRLACH; TERPSTRA; HEINEMANN, 2004). Através da observação da força do sinal de várias estações base, um dispositivo pode determinar sua localização. Apesar de não exigir instalação de novas estruturas, existe um custo de treinamento, no qual é determinado um mapa virtual dos sinais, permitindo a posterior localização dos dispositivos.

A localização *outdoor* por sua vez é geralmente utilizada no posicionamento em grandes áreas, como uma cidade ou país. Apesar disso, pode oferecer também uma precisão bastante elevada. Os serviços baseados em localização tratados neste trabalho frequentemente utilizam este tipo de posicionamento.

Segundo KÜPPER (2005), seria interessante para o usuário poder utilizar os dois tipos de posicionamento, *indoor* e *outdoor*, a partir do mesmo dispositivo móvel, para que fosse possível a utilização de *LBS* nos dois ambientes com reutilização de uma mesma infra-estrutura. Contudo, a grande dificuldade é a falta de uma tecnologia universal de posicionamento.

Uma das tecnologias mais conhecidas para a localização é o Sistema de Posicionamento Global ou *GPS (Global Positioning System),* que permite o posicionamento do usuário a partir das informações de satélites. Para isso, o aparelho a ser localizado capta os sinais de satélites e calcula a distância até cada um deles. A partir destas distâncias é possível determinar a posição geográfica do dispositivo.

Algumas outras abordagens foram propostas para permitir a localização de celulares com base na utilização das antenas de transmissão. Elas foram desenvolvidas inicialmente visando atender à necessidade de localização de celulares exigida pelos governos europeus e norte-americano nas chamadas de emergência. As principais tecnologias de localização para redes *GSM* de celulares são C*ellID, E-OTD, U-TDoA e A-GPS* (KÜPPER, 2005), descritas a seguir.

CellID é baseada na localização da estação base, na qual o celular está utilizando os serviços. A partir do posicionamento geográfico da estação base, supõe-se a posição aproximada do usuário. Esta técnica é por si só bastante imprecisa e pode ser também utilizada em conjunto com algumas outras informações para oferecer melhor precisão, como, por exemplo, força do sinal ou tempo de ida e volta (*RTT - Round Trip Time*) dos dados envolvidos na comunicação.

As duas técnicas seguintes são baseadas na triangulação do sinal com base não só na antena que o celular está utilizando, mas também na comunicação observada com antenas adjacentes.

A técnica *E-OTD (Enhanced Observed Time Difference),* ou Diferença de Tempo Observado – Melhorada, é baseada na observação pelo dispositivo dos sinais emitidos por

um número de estações base e no cálculo de sua posição a partir destes. Ela é aplicada no *downlink*, ou seja, no momento em que os dados são enviados da estação base para o dispositivo móvel.

Já a U-TDoA (*Uplink Time Difference of Arrival*), ou Diferença de Tempo de Chegada no *Uplink*, é baseada na observação da recepção dos sinais provenientes do dispositivo móvel nas estações base, ou seja, durante o *uplink*.

A técnica *A-GPS* (*Assisted GPS*) mescla as funcionalidades fornecidas pelo *GPS* com informações obtidas através de procedimentos que envolvem a comunicação entre o dispositivo móvel e a rede celular. Desta forma, é possível oferecer melhor qualidade das informações de localização nas situações em que apenas a utilização de *GPS* não apresenta bons resultados, como por exemplo, no interior de construções ou quando as condições climáticas atrapalham a comunicação com o satélite.

Os métodos apresentados são característicos de redes de celulares baseados na tecnologia *GSM* (*Global System for Mobile Communications*), que é a tecnologia dominante, com cerca de um bilhão de usuários ao redor do planeta. Contudo, existem outras tecnologias de localização aplicáveis às redes de celulares que apresentam características distintas (KÜPPER, 2005).

2.2 Classificações

Algumas classificações de *LBS* são importantes para a definição dos critérios para a manutenção da privacidade. Sendo assim, são descritos a seguir dois critérios que podem ser utilizados para a divisão em categorias dos LBS. O primeiro deles considera a participação dos usuários na requisição do serviço e o segundo é baseado na identificação ou não do usuário.

2.2.1 Participação dos usuários na requisição

Os serviços baseados em localização podem ser agrupados em três categorias com base na participação do usuário na requisição do serviço, sendo estas *pull LBS, push LBS* e *peer-to-peer LBS* (MARTUCCI et al., 2006).

No *pull LBS* o usuário realiza explicitamente a requisição do serviço e envia sua informação de localização. Exemplos típicos de serviços deste tipo incluem a localização de pontos de interesset como farmácia ou restaurante mais próximo.

No *push LBS*, o usuário não envia uma requisição direta ao servidor *LBS* para que o serviço seja oferecido. Um exemplo possível é o recebimento das ofertas do dia ao se passar próximo a um supermercado que pertence a uma determinada rede.

Para o oferecimento desse serviço existem duas restrições: a primeira delas é que o usuário deve se cadastrar previamente; a segunda é que a posição do usuário deve ser calculada periodicamente para que, no momento em que ele passar por perto do ponto de notificação, sua localização seja conhecida e possa ser enviada a mensagem com as promoções para seu dispositivo móvel.

A última categoria, *peer-to-peer LBS*, engloba os serviços nos quais as requisições envolvem a localização de outros usuários. Esse tipo de serviço, em geral, ocorre entre usuários que já se conhecem previamente e têm uma relação de confiança estabelecida. Caracterizam-se por este tipo de serviço, por exemplo, encontrar amigos que estão próximos do usuário, encontrar a localização de um filho e determinar a posição geográfica dos funcionários de uma empresa.

2.2.2 Anonimato

Outra classificação com relação aos serviços baseadas em localização é apresentada por Beresford e Stajano (2003), na qual é feita uma abordagem com relação ao anonimato do usuário, que seria a possibilidade de utilização do serviço pelo usuário sem ter sua identidade revelada.

Algumas aplicações requerem a revelação da identidade do usuário, como, por exemplo, a localização de colegas durante o seu período de trabalho. Outras, no entanto, podem ser executadas de maneira completamente anônima, como, por exemplo, ao passar próximo a uma cafeteria, ser alertado com relação ao preço do café.

2.3 Considerações Finais

Este capítulo abordou o aparecimento dos serviços baseados em localização, os fatores que determinaram o seu desenvolvimento e o rápido crescimento verificado deste tipo de serviços, especialmente no ambiente de telefonia móvel, o qual já pode contar diversas aplicações. Foram descritas também as técnicas de localização para dispositivos móveis com tecnologias *GSM* e os critérios de classificação dos serviços baseados em localização.

Pode-se notar que as vantagens oferecidas pela utilização de *LBS* são diversas, tais como: maior facilidade para encontrar pontos de interesse em locais desconhecidos,

passeios turísticos direcionados pelo próprio dispositivo móvel, facilidade de obtenção de informações específicas de acordo com um posicionamento geográfico, dentre outras. Mas apesar de todos os aspectos positivos, a utilização de *LBS* deve ser cautelosa no que diz respeito à liberação de informações de localização, uma vez que, mal utilizadas, podem representar uma séria ameaça à manutenção da privacidade dos usuários. Os aspectos de privacidade envolvidos na execução de *LBS* são descritos no próximo capítulo.

3 Privacidade

A preservação da privacidade tem sido um desafio da sociedade há bastante tempo. Já em 1890, Warren & Brandeis definiram privacidade como o “direito de ser deixado só” (WARREN; BRANDEIS, 1890). Desde então, a aplicação dos conceitos de privacidade tem tomado várias conotações em diversos ambientes e situações.

Algumas tecnologias desenvolvidas, que hoje se encontram inseridas no contexto diário de grande parte da população mundial, possibilitaram facilidades de comunicação e acesso às informações, além de permitir o oferecimento de novos serviços. Em geral, a utilização desses novos serviços cria oportunidades para a obtenção de informações pessoais sobre os usuários, que poderão ser utilizadas para fins comerciais, para o oferecimento de personalização e até mesmo para fins maliciosos. A Internet figura neste contexto como um dos destaques, apresentando diversas técnicas de coleta de informações pessoais, ocasionando ameaças à manutenção da privacidade dos usuários.

Tal invasão de privacidade verificada na Internet talvez jamais tenha sido imaginada por Warren e Brandeis. No entanto, o desenvolvimento de novas tecnologias e novos serviços traz, junto com comodidade e facilidade, novos riscos e questões concernentes à privacidade. A utilização de LBS, por exemplo, resultou em novas preocupações, uma vez que informações de localização passaram a ser obtidas de usuários e manipuladas por diferentes entidades.

O processamento de quantidades cada vez maiores de dados, incluindo informações pessoais, a transmissão de dados além de fronteiras nacionais e a falta de legislação comum quanto ao tratamento das informações, levaram à criação de guias de proteção à privacidade que apresentam alguns princípios básicos para a sua manutenção.

3.1.1 Guias de privacidade

Exemplos clássicos de guias de privacidade são os guias da OECD (*Organization for Economic Co-Operation and Development*), Organização para Cooperação Econômica e Desenvolvimento (OECD, 1980), e as diretivas de proteção de dados da EPC (*European Parliament and the Council*) (EPC, 1995).

Os princípios desses guias não foram elaborados especificamente para o ambiente de serviços baseados em localização, mas alguns podem e devem ser aplicados também nestas circunstâncias.

Os guias da *OECD* declaram oito princípios para a proteção de privacidade quanto à manipulação de informações pessoais, que servem de orientação quanto à obtenção dos dados, critérios para revelação de tais dados e outras regras de manipulação de dados pessoais. Dentre os princípios, destacam-se: o princípio da limitação da coleta, o princípio da qualidade dos dados, o princípio da especificação do propósito e o princípio da limitação do uso.

O princípio da limitação da coleta estabelece que deve haver limites para a obtenção de informações pessoais e que os dados devem ser obtidos por meios justos e legais. Além disso, esse princípio determina que, sempre que possível, o sujeito cujos dados serão coletados deve estar ciente da coleta.

O princípio da qualidade dos dados diz respeito também ao propósito da coleta e determina que os dados devem ser coerentes com o propósito para o qual foram coletados. Ou seja, eles não devem conter mais informações do que aquelas necessárias para a finalidade especificada.

O princípio da especificação do propósito ressalta que os motivos para os quais os dados pessoais estão sendo coletados devem ser especificados antes da coleta, e a utilização dos dados é restrita para satisfazer os motivos da coleta ou outros que são compatíveis.

Por fim, o princípio da limitação do uso determina que os dados pessoais não devem, de maneira alguma, ser utilizados para outros propósitos que não sejam aqueles expressados anteriormente, salvo quando houver explícito consentimento do usuário ou assegurado por motivos legais.

As diretivas de proteção de dados da *EPC* também apresentam diversos princípios com relação à coleta e manipulação de informações pessoais e tratam, além destes pontos, de outros aspectos como as exceções para a liberação das informações e a transferência das informações para países não membros da União Européia.

3.1.2 Privacidade em serviços baseados em localização

Além dos princípios genéricos de proteção à privacidade do usuário que podem ser empregados em ambientes de serviços baseados em localização, existem alguns princípios específicos para a manipulação de informações de localização.

Em OMA (2002) são apresentados quatro princípios para o tratamento de dados de localização, que têm como objetivo reafirmar os princípios levantados pela *OECD*, enfatizando-os para o caso específico de dados de localização. São eles:

- Limitação da coleta: Os dados de localização de um usuário só devem ser obtidos caso a localização seja necessária para a prestação de algum serviço.

- Consentimento: Antes de cada coleta de dados de localização, uma autorização deve ser obtida. O consentimento pode ocorrer de diversas maneiras, como para cada requisição separadamente, para provedores de serviço, etc. Deve ser possível para o usuário alterar suas preferências de privacidade a qualquer momento, podendo voltar atrás em consentimentos dados anteriormente.

- Utilização e revelação dos dados: Os dados de localização devem ser utilizados e/ou revelados apenas no sentido em que foi dado o consentimento. Pseudônimos devem ser utilizados sempre que o serviço não requeira a revelação da real identidade do usuário.

- Manutenção da segurança: Os dados de localização deverão ser apagados tão logo o serviço tenha sido prestado, ou o armazenamento deverá ser feito com o consentimento do usuário.

Com relação à liberação das informações de localização para terceiros, é ressaltada a necessidade da ciência do usuário de que seus dados podem ser repassados para terceiros, e destacado o fato de que todos os terceiros também devem seguir as políticas de privacidade acordadas entre o usuário e o prestador do serviço.

Outro aspecto abordado é o que diz respeito à precisão dos dados que serão liberados, e a regra geral é que a localização liberada deverá ser de tão baixa precisão quanto possível para uma aplicação em particular. Isto é, se para a prestação de um serviço se necessita simplesmente de informações com precisão relativa à cidade na qual o usuário se encontra, não faz sentido a liberação de informações com precisão relativa à rua.

Ainda em OMA (2002) são abordadas questões específicas de revelação das informações de localização como, por exemplo, no caso entre empregador e empregado, ou no polêmico caso de pais localizarem filhos.

Além de vários aspectos semelhantes aos citados anteriormente, em EPC (2002) é apresentado outro detalhe importante para a manutenção da privacidade: a clareza na comunicação entre o provedor do serviço e o usuário. Em EPC (2006) é levantada a importância dos dados de localização para a investigação, detecção e instauração de processos por ofensas criminais, sendo por isso sugerido que a privacidade dos usuários pode ser quebrada em detrimento de um bem maior, no caso a manutenção da segurança da população.

3.1.3 Ameaças à privacidade

Uma das grandes preocupações com relação à privacidade em LBS é a possibilidade de relacionar um usuário específico à utilização de algum serviço, a alguma ação ou a qualquer outro tipo de comportamento. Por exemplo, uma requisição de busca pela clínica mais próxima de apoio a pacientes soropositivos pode ser utilizada para inferir que o usuário solicitante é portador do vírus *HIV*. Tal informação poderia ser utilizada para constrangimento público ou até mesmo extorsão.

Uma medida simples para solucionar o problema é omitir de qualquer identificação do usuário nas requisições feitas. Por exemplo, o Número de Seguro Social (*Social Security Number*) norte-americano e o número do Cadastro de Pessoa Física (*CPF*) brasileiro podem indicar a identidade de um usuário; sendo assim, se nunca estiverem presentes nas requisições, o usuário não poderá ser identificado diretamente.

No entanto, alguns elementos envolvidos durante as requisições, especialmente no caso de *LBS*, podem ocasionar a revelação da identidade do usuário. Tais elementos são chamados de quase-identificadores (*quasi-identifiers*) (BETTINI, WANG; JAJODIA, 2005), ou seja, um atributo que, sozinho ou em conjunto com outros atributos, pode ocasionar a reidentificação do usuário ao qual pertencem as informações, mesmo este não sendo identificado diretamente.

As informações de localização de usuário, por exemplo, são um potencial quase-identificador do mesmo, uma vez que, relacionadas com outras informações, podem tornar possível o descobrimento da identidade do dono de tais informações. Desse modo, mesmo

que a identificação de um usuário não seja fornecida, ameaças à sua privacidade ainda podem ocorrer por meio de identificação com base em outras informações.

O termo ameaça à privacidade é utilizado, neste trabalho, como sendo qualquer situação que pode levar, de alguma forma, à identificação do usuário e posterior invasão de privacidade do mesmo.

As ameaças à privacidade do usuário nos serviços baseados em localização são classificadas em duas categorias no trabalho aqui apresentado: ameaças do provedor e ameaças externas.

As ameaças do provedor são decorrentes da utilização das informações que fazem parte da requisição para a descoberta da identidade do usuário. Já as ameaças externas são caracterizadas por outras entidades ou indivíduos mal-intencionados que adquirem algum tipo de informação pessoal do usuário de maneira ilícita.

A diferença entre as duas ameaças é basicamente a necessidade de compartilhamento de informações. As ameaças decorrentes das informações que precisam ser compartilhadas para a execução do serviço são consideradas ameaças do provedor, mas se, por outro lado, forem baseadas em informações pessoais roubadas por entidades ou indivíduos que não deveriam ter acesso a tais informações, são consideradas ameaças externas.

As principais ameaças do provedor são: utilização de dados com precisão elevada, realização de requisições feitas solitariamente, análise do histórico de localizações e verificação das respostas enviadas em comparação com a ação do usuário. Tais ameaças são detalhadas a seguir.

Informações de localização com precisão elevada (BETTINI, WANG; JAJODIA, 2005) podem levar à identidade do usuário, uma vez que uma área muito específica pode caracterizá-lo.

A submissão de requisições solitárias (BOWEN; MARTIN 2007) pode levar à identificação de um único usuário. Uma situação exemplo seria uma requisição proveniente de um certo departamento de uma universidade específica em um domingo. Havendo conhecimento de que somente um professor sempre vai a esse departamento aos domingos, pode-se associar a requisição ao professor. A alta precisão das informações de localização ainda pode agravar esse problema, no entanto, requisições com baixa precisão e provenientes de áreas mais povoadas amenizam tal situação.

A partir de uma análise minuciosa das localizações subsequentes e dos padrões de movimentação observados, é possível criar um histórico de movimentação com base em certo dispositivo e inferir a identidade do usuário (BETTINI, WANG; JAJODIA, 2005). Suponha o cenário no qual o posicionamento do usuário deve ser obtido em curtos intervalos de tempo, com o intuito de oferecer-lhe propaganda ao se aproximar de um supermercado. A rotina de movimentação seguida por esse usuário é, por exemplo, a seguinte: deixa sua casa todos os dias em um horário determinado e, alguns minutos depois, para próximo a uma escola; por volta de meio dia, ele faz o caminho inverso. Ao verificar a repetição desse mesmo percurso, é possível primeiramente identificar um usuário e, em seguida, descobrir as localizações pelas quais ele passa. Poderia ser descoberto que o usuário sai de casa, deixa os filhos na escola, vai para o trabalho e, na hora do almoço, faz o caminho inverso, pegando os filhos na escola e voltando para casa.

Uma ameaça recentemente apresentada na literatura foi definida como ataque na sombra (*shadow attack*) **(**PARESCHI; RIBONI; BETTINI, 2008). Essa ameaça é baseada na resposta do serviço solicitado pelo usuário e no comportamento apresentado por ele depois de recebida a resposta. Para exemplificar esse ataque, os autores apresentam o cenário de um sistema "pervasivo" de um ginásio, no qual são oferecidas sugestões de exercícios aos usuários com base nos parâmetros fisiológicos de cada um (*PerGym*), ilustrado pela Figura 1.

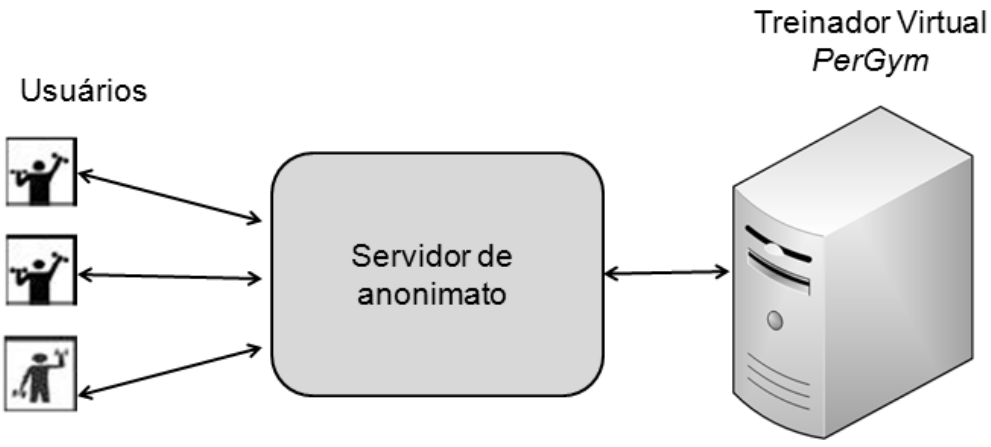


Figura 1 – Cenário de Ginásio "Pervasivo".

No cenário apresentado, os usuários portam um relógio capaz de monitorar as informações fisiológicas, sua localização e o aparelho utilizado. Esses dados são enviados para um servidor que age como treinador virtual e apresenta sugestões do próximo exercício. Para impedir que o provedor relacione os dados pessoais (fisiológicos) a

determinado usuário, o cenário também conta com um servidor intermediário (*CTA*), que elimina a identidade do usuário da requisição e utiliza um pseudônimo (apelido) para identificá-lo e, além disso, ajusta os dados de localização para que esta englobe outros usuários. Dessa forma, não é enviada ao treinador virtual a localização exata do usuário. No entanto, o *shadow attack* é feito com base na resposta do serviço enviada ao usuário. Por exemplo, se o treinador virtual sugerir o exercício *e1* apenas para o usuário *u1* através do apelido *a1* e, posteriormente, conseguir verificar qual usuário executou o exercício *e1*, ele pode inferir com grande probabilidade de acerto que o usuário de apelido *a1* é o usuário *u1*. Esse caso ocorre quando o atacante, no caso do cenário de exemplo, o treinador virtual, consegue verificar qual foi a atitude do usuário depois do recebimento da sugestão disponibilizada.

As ameaças externas são formas ilícitas de se obter as informações dos usuários por entidades que não deveriam ter tais informações. Exemplos desse caso são: a observação do tráfego na rede, aplicativos de terceiros com códigos maliciosos, etc.

A observação do tráfego na rede (CHENG; ZHANG; TAN, 2005) possibilita a captura das informações transferidas no canal de comunicação entre o dispositivo móvel e o provedor *LBS* e, dessa forma, poderiam ser obtidas informações pessoais do usuário.

Os aplicativos de terceiros instalados no dispositivo para a utilização de *LBS* podem conter trechos de código maliciosos que captem informações capazes de levar à identificação do portador do dispositivo móvel. Dados como identificadores de usuário, de dispositivo ou de hardware e informações sobre a operadora poderiam ser extraídos sem que o usuário soubesse.

Além dessas ameaças, existe ainda a possibilidade de se repassar informações pessoais a terceiros ou armazená-las por um longo período de tempo, o que, em caso de fragilidades na segurança do servidor, pode acarretar no roubo desses dados e utilização de maneira indevida.

É válido ressaltar que, independentemente da forma como as informações forem obtidas, a identidade do usuário corre o risco de ser revelada. Por exemplo, se algum atacante possui acesso ao canal de comunicação e tem acesso a todas as informações trocadas, as ameaças do provedor, descritas anteriormente, também existirão nesse caso.

A identificação de um usuário e a capacidade de associá-lo às suas respectivas informações de localização ocasionam sérios riscos quanto à manutenção de sua

privacidade. Diversas informações podem ser inferidas, tais como: descoberta da participação em reuniões religiosas ou políticas; determinação de um perfil de movimentação de usuários; oferecimento de propagandas não desejadas; e até mesmo revelação de problemas de saúde ou comportamentais, caso o usuário esteja internado em um hospital ou em uma clínica de recuperação de alcoólatras, por exemplo.

É preciso encontrar um equilíbrio na prestação dos serviços baseados em localização de tal forma que, além de oferecer um nível satisfatório de privacidade ao usuário, não o impeça de utilizar os serviços desejados.

4 Sistema Baseado em Privacidade de Localização

Beresford e Stajano (2003) definiram a expressão *privacidade de localização* como sendo a capacidade de evitar que as informações de localização dos usuários sejam reveladas para terceiros. O sistema apresentado nesta dissertação oferece garantias de privacidade para os usuários de *LBS* no ambiente de telefonia móvel. As garantias oferecidas são baseadas, principalmente, no controle da liberação dos dados de localização dos usuários e, por essa razão, o sistema foi denominado Sistema Baseado em Privacidade de Localização (*SBPL*).

Diversas empresas disponibilizam aplicativos específicos para telefones celulares que utilizam as informações de localização para oferecer serviços personalizados aos usuários. No entanto, em boa parte das áreas de *downloads* de aplicações *LBS*, não é disponibilizado nenhum documento especificando a política de privacidade aplicada aos dados pessoais coletados e, muito menos, mencionada alguma técnica utilizada em prol da manutenção da privacidade dos usuários (VIVO, 2009), (MobiEXPLORE, 2009).

Embora ocorra o fato de os usuários abrirem mão da privacidade em virtude dos benefícios disponibilizados pela utilização do serviço (HARLE; HOPPER, 2005), tal situação possivelmente não ocorreria caso fossem do conhecimento dos usuários os riscos que podem surgir em decorrência da utilização das informações de localização por indivíduos mal-intencionados.

Nesse contexto, o *SBPL* foi desenvolvido para permitir que os usuários de telefonia móvel possam ter maneiras de controlar como suas informações de localização serão utilizadas durante a utilização de *LBS*. O *SBPL* foi projetado para contar com os seguintes requisitos:

1) Personalização: É oferecida ao usuário personalização do serviço, uma vez que existe a possibilidade de configuração das preferências de privacidade e provedores *LBS* que se deseja utilizar, dentre outras características.

2) Controle de Precisão: É permitido aos usuários determinarem as situações em que suas informações de localização deverão sofrer ajuste de precisão.

3) Anonimato: os usuários podem utilizar o mecanismo do anonimato para que suas requisições sejam enviadas aos provedores juntamente com requisições semelhantes.

4) Simplicidade: Apesar de oferecer suporte à utilização de diversas técnicas de privacidade, o *SBPL* conta com um mecanismo simples de configuração de privacidade.

5) Coerência com Guias de Privacidade: O sistema proposto segue as recomendações dos principais guias de privacidade existentes, tais como: limitação da coleta dos dados (OECD 1980), utilização de informações de localização apenas em circunstâncias necessárias ao oferecimento do serviço (OMA 2002), possibilidade de o usuário a qualquer momento reverter o seu consentimento para o processamento de dados de localização (EPC 2006), etc.

6) Eficiência: Apesar da inserção de mecanismos de privacidade, a utilização de *LBS* com privacidade não deve ocasionar atrasos excessivos nos tempos de resposta observados na aplicação-cliente.

7) Interoperabilidade: O *SBPL* utiliza um padrão de comunicação para *LBS* de forma que permita o suporte a diferentes provedores e serviços.

A idéia básica do *SBPL* é permitir que o usuário tenha controle sobre suas informações pessoais. Pessoas ou entidades não-autorizadas não têm acesso a tais informações; já as entidades autorizadas terão acesso às informações, mas a liberação deverá obedecer às restrições desejadas pelos usuários.

Este capítulo apresenta a arquitetura geral de funcionamento do *SBPL*, detalhando-se a comunicação, execução e módulos envolvidos no oferecimento de *LBS* com garantias de privacidade. Além disso, são apresentados os detalhes de implementação, envolvendo tecnologias e técnicas utilizadas no desenvolvimento do sistema proposto.

4.1 Arquitetura

Esta seção apresenta a arquitetura do *SBPL* para melhor detalhamento do funcionamento do sistema de maneira geral. A arquitetura será descrita por meio de três tópicos: o modelo de comunicação, que apresenta os dispositivos e elementos de hardware envolvidos na comunicação durante o oferecimento de *LBS;* os modelos de execução diferenciados propostos para a execução dos serviços suportados pelo *SBPL*; e, por fim, a arquitetura geral do sistema.

4.1.1 Modelo de comunicação

O modelo de comunicação frequentemente verificado na utilização de *LBS* para telefonia móvel é baseado no modelo cliente-servidor, no qual o serviço é sempre oferecido diretamente pelo provedor *LBS*. Segundo esse modelo, o cliente compartilha suas informações de localização com o provedor *LBS* da forma que foram obtidas, independente da técnica utilizada ou da precisão.

Diferentemente da arquitetura cliente-servidor, predominante na maioria dos demais *LBS* disponíveis para telefonia móvel, o *SBPL* é caracterizado pela presença de um servidor confiável atuando entre o dispositivo móvel e o provedor *LBS*, como pode ser verificado na Figura 2. O servidor confiável atua como um *proxy*, de forma que todos os serviços oferecidos pelos provedores *LBS* são mediados por ele.

Figura 2 – Modelo de Comunicação SBPL.

Dessa forma, todas as informações a serem encaminhadas ao provedor *LBS* devem passar antes, impreterivelmente, pelo servidor confiável, o que permite a aplicação de técnicas que evitam a identificação do usuário pelo provedor.

A comunicação entre o dispositivo móvel e o servidor confiável é realizada através de algum canal de comunicação com a Internet disponível para o celular, podendo ser o acesso via redes sem fio comuns (*Wi-Fi*) ou algum outro canal suportado pela operadora de telefonia móvel, como GPRS, EDGE etc. Outra importante característica de comunicação no *SBPL* é a possibilidade de utilização de um canal seguro de transferência de dados entre o dispositivo móvel e o servidor confiável.

4.1.2 Modelos de Execução

O *SBPL* oferece suporte a serviços do tipo *pull* e *push LBS*, que apresentam diferentes características de execução. Sendo assim, diferentes modelos de execução foram propostos

para garantir a privacidade em cada tipo de serviço. Nos serviços em que o usuário envia uma requisição solicitando informações referentes à sua atual localização (*pull LBS*), foi definido um modelo de execução baseado em níveis de privacidade. Já nos serviços em que o usuário recebe o serviço sem o solicitar diretamente (*push LBS*), foi proposta uma técnica segundo a qual apenas as informações de localização de um usuário não são repassadas para terceiros.

4.1.2.1 Modelo de Execução para *Pull LBS*

Encontrar o restaurante mais próximo, solicitar informações de previsão do tempo ou de condições de tráfego na atual localização têm em comum a característica de que o usuário sempre solicita a informação diretamente, característica inerente ao *pull LBS*.

A execução de serviços do tipo *pull* ocorre, em geral, da seguinte maneira: o dispositivo móvel obtém sua localização e envia uma requisição contendo o tipo de serviço desejado e a localização para o provedor que, por sua vez, processa a requisição e envia a resposta com as informações úteis para o usuário.

Essas características de execução estão sujeitas a uma série de ameaças à privacidade do usuário descritas anteriormente, tais como: possibilidade de obtenção de informações através da observação do tráfego, envio de dados com precisão elevada, requisições feitas solitariamente, etc.

No entanto, as ameaças existentes podem não representar riscos tão grandes para o usuário, dependendo de sua avaliação pessoal. Dessa forma, podem existir usuários com diferentes restrições de privacidade.

A elevada subjetividade da privacidade de um usuário dificulta a obtenção de suas preferências de forma automatizada. Isso ocorre pelo fato de que, independente do ambiente, cada usuário pode possuir uma visão distinta de quais informações liberadas a seu respeito podem interferir na sua privacidade. No ambiente Web, por exemplo, o armazenamento de informações de navegação em *cookies*[1] pode caracterizar extrema invasão de privacidade para um usuário, enquanto para outro não haveria problema em ter tais tipos de informações armazenadas.

[1] *Cookies* são dados trocados entre o computador do usuário e o servidor web, que são armazenados em arquivos de texto e podem conter informações pessoais como algumas páginas visitadas.

A mesma situação também é verificada no ambiente de execução *LBS*. Um usuário pode não encontrar problemas ao liberar suas informações de localização com precisão elevada se, por exemplo, confia no provedor *LBS*, enquanto outro usuário jamais permitiria a liberação de tais informações. Isso ocorre porque as preferências de privacidade de um usuário dependem de uma série de fatores como: conhecimentos sobre a tecnologia utilizada, confiança no provedor que oferece o serviço, experiências negativas com outros tipos de tecnologia, dentre outros.

Visando oferecer diferentes garantias de privacidade para a utilização de *pull LBS*, é apresentado um modelo de execução baseado em níveis que oferece garantias distintas de privacidade. Dessa forma, é possível atender a diferentes usuários com diferentes preferências de privacidade e, além disso, permitir a utilização de serviços que têm diferentes restrições de precisão de dados.

A idéia básica do funcionamento do modelo de execução baseado em níveis é a seguinte:

Cinco níveis de privacidade foram definidos, baseados no controle da coleta e armazenamento de dados e na utilização das seguintes técnicas de proteção de privacidade: canal seguro de comunicação, ajuste de precisão e técnicas de obtenção de conjunto de anonimato. A seguir são detalhadas as características de cada nível e as ameaças à privacidade combatidas.

Nível Mínimo (0): Controle da coleta e armazenamento de dados – Tal controle está diretamente ligado aos princípios da limitação da coleta e da limitação do uso, propostos no guia de privacidade da *OECD*. Estes determinam que somente os dados necessários para o oferecimento do serviço devem ser coletados e que, uma vez coletados, sejam utilizados apenas para o objetivo para o qual foram obtidos, não devendo ser armazenados por maior período do que o do oferecimento do serviço.

A execução de *pull LBS* com nível mínimo garante que apenas as informações necessárias para o oferecimento do serviço serão coletadas. Dados como números do aparelho, informações sobre a operadora ou sobre hardware do dispositivo não são coletados. Além disso, as informações coletadas são utilizadas apenas durante a execução do serviço e não serão armazenadas por período maior de tempo, salvo com explícito consentimento do usuário e apenas em situações necessárias.

O controle da coleta e do armazenamento impede que informações subsequentes possam ser analisadas, uma vez que não serão armazenadas após a execução do serviço. Sendo assim, mesmo que o servidor confiável seja invadido por eventuais falhas de segurança, não serão obtidos históricos de movimentação de usuários. O controle característico do nível mínimo também está presente nos demais níveis.

Nível Baixo (1): Canal seguro de comunicação – Qualquer tipo de comunicação em rede está sujeita à ação de indivíduos maliciosos que tentam capturar o tráfego e obter informações que, de alguma maneira, podem se tornar valiosas. Existe uma série de *sniffers*[2] capazes de interceptar informações confidenciais transmitidas através das redes de comunicação. O êxito de "curiosos" que desejam roubar informações através da observação do tráfego em redes de telefonia celular é um pouco dificultado em virtude do aparato de hardware necessário e das frágeis técnicas criptográficas utilizadas. No entanto, mesmo assim, com os recursos necessários, ainda é possível ocorrer o roubo de informações.

O nível baixo de execução de *pull LBS* conta com suporte a um canal seguro de comunicação entre o dispositivo móvel e o servidor confiável, de forma que dificulte ainda mais o roubo de informações pessoais através da observação do tráfego na rede. Assim como ocorre com o nível mínimo, o canal seguro de dados, presente no nível baixo, também está presente nos níveis seguintes.

Nível Médio (2): Ajuste de Precisão – A questão da precisão ou, mais especificamente, do ajuste de precisão, é muito importante no oferecimento de melhores garantias de privacidade aos usuários LBS. A capacidade de fazer com que as informações de localização com alta precisão representem áreas diferentes ou maiores do que a área dada inicialmente é fundamental para evitar a identificação dos usuários.

O nível médio oferece suporte ao ajuste de precisão por meio da alteração da posição original do usuário, com base em um deslocamento aleatório para qualquer direção, cuja distância é determinada pelo usuário através de um coeficiente de ajuste de precisão. Dessa forma, ao se requisitar um serviço com esse nível de privacidade, o provedor *LBS* não terá acesso à localização exata do usuário. A utilização dessa técnica impede que o usuário seja identificado devido à alta precisão de suas informações de localização, e dificulta a

[2] *Sniffers* são programas utilizados para o monitoramento do tráfego de redes através da interceptação e armazenamento dos dados trafegados na rede.

identificação nos casos de requisições solitárias, porque, mesmo que a requisição tenha sido enviada ao provedor solitariamente, ela não contém informações tão precisas sobre o usuário.

A técnica de ajuste de precisão também é utilizada nos níveis com maiores garantias de privacidade para a aplicação das técnicas de cada nível.

Nível Alto (3): Anonimato – O conjunto de anonimato é definido como o conjunto de indivíduos dentro do qual a ação de um usuário não pode ser identificada (PFITZMANN; KOHNTOPP, 2001). Tratando-se de requisições a um determinado tipo de serviço, o conjunto de anonimato é obtido através do envio de requisições do mesmo tipo, provenientes de usuários diferentes, para um fornecedor do serviço. Dessa maneira, a associação entre um usuário e sua respectiva requisição torna-se cada vez mais difícil, de forma proporcional ao tamanho do conjunto de anonimato.

O nível alto de privacidade busca oferecer o anonimato através da técnica de ocultação de informações espaciais e temporais, também chamada de generalização. A técnica utilizada funciona da seguinte forma: quando o usuário realiza uma requisição, suas coordenadas de localização são armazenadas de alguma forma, e então se aguarda alguns instantes para verificar a chegada de outra requisição do mesmo tipo, proveniente de uma área próxima. Caso isso ocorra antes de um tempo limite, é calculada uma nova área que englobe todas as requisições próximas e, só então, as requisições são enviadas ao provedor.

A utilização dessa técnica não garante o conjunto de anonimato, uma vez que nem sempre será possível agrupar requisições em uma mesma área antes de encaminhá-las ao provedor *LBS*. No entanto, em regiões povoadas e com grande utilização de *LBS*, espera-se que o conjunto de anonimato possa ser obtido em boa parte das requisições solicitadas. O modelo sugere a espera de até 5 segundos por requisições provenientes da mesma área, a princípio. Caso nenhuma requisição próxima seja recebida, é calculada uma nova área dentro da qual a posição inicial do usuário é englobada e, só então, a requisição será encaminhada ao provedor *LBS* escolhido pelo usuário.

Nos casos em que não é possível compor um conjunto de anonimato, as informações de localização do usuário sofrerão uma generalização, representando uma área maior do que a área dada inicialmente. Isso dificulta ainda mais a identificação do usuário, se comparado com o nível médio, uma vez que, no nível garantido, ao invés de ser passada uma localização em formato de ponto, é passada uma área.

Nível Garantido (4): Anonimato – O nível garantido utilizou a técnica de envio de requisições falsas para obtenção do conjunto de anonimato. Essa técnica funciona da seguinte maneira: ao receber uma requisição *LBS*, o servidor ajusta a localização do usuário seguindo a técnica de ajuste de precisão. Além disso, o servidor calcula outras quatro localizações a partir da posição inicial do usuário e monta outras quatro requisições com base nas novas coordenadas. Por fim, as cinco requisições resultantes são "embaralhadas" e enviadas ao provedor *LBS*. A utilização dessa técnica garante o anonimato, uma vez que sempre haverá, no mínimo, mais quatro requisições provenientes da mesma região da requisição original.

Sendo assim, o nível garantido é o que oferece maior dificuldade quanto à possibilidade de identificação do usuário. O caso de requisição solitária não irá mais ocorrer, uma vez que sempre existirão requisições do mesmo tipo em regiões próximas. Os casos de *shadow attacks* também serão dificultados, pois, para o provedor, existirão vários usuários requisitando o serviço, e não será possível, na maioria dos casos, ter certeza se uma requisição é verdadeira ou não.

A Tabela 1 apresenta os níveis de privacidade que foram definidos e quais as características (técnicas ou controle de coleta e armazenamento) que foram aplicadas em cada nível. Os níveis Mínimo, Baixo, Médio, Alto e Garantido são representados pelos números 0, 1, 2, 3 e 4, respectivamente. Cada 'ν' indica as características de privacidade que são garantidas pelo nível em questão e cada '-' indica aquelas que não o são.

	Anonimato	Precisão	Canal Seguro	Coleta	Armazenamento
0	-	-	-	ν	ν
1	-	-	ν	ν	ν
2	-	ν	ν	ν	ν
3	ν / -	ν	ν	ν	ν
4	ν	ν	ν	ν	ν

Tabela 1 – Níveis de privacidade oferecidos e funcionalidades suportadas.

Desse modo, os níveis de privacidade oferecidos para a execução de *pull LBS* são de forma resumida: o nível Mínimo (0), que conta apenas com o controle de coleta e armazenamento; o nível Baixo (1), que além do controle do nível 0, utiliza o canal seguro de transmissão de dados; o nível Médio (2), que utiliza a técnica do ajuste de precisão de informações de localização além dos itens anteriores; o nível Alto (3), que aplica a técnica de ocultação de informações espaciais e temporais para a obtenção do conjunto de

anonimato, sendo que, nem sempre será possível garanti-lo, por isso a presença das duas opções 'ν / -' na coluna anonimato deste nível na tabela; e, por fim, o nível Garantido (4), que assegura a presença do anonimato ao utilizar a técnica de envio de requisições falsas.

O modelo de execução de *pull LBS* proposto visa o oferecimento de personalização ao usuário por meio da possibilidade de escolha do nível de privacidade e do coeficiente de ajuste de precisão em função do provedor utilizado. Dessa forma, o usuário pode escolher diferentes níveis de privacidade para provedores distintos. Essa possibilidade permite ao usuário controlar, de maneira seletiva, para quem suas informações serão liberadas e com quais garantias de privacidade. Além disso, é possível abrir mão da privacidade nos casos em que o serviço exija dados com maior precisão. É válido ressaltar que o modelo também propõe a utilização de uma configuração genérica de privacidade que é aplicada a todos os provedores que não possuem configurações específicas.

O modelo de execução proposto também trata do aspecto do armazenamento das informações de privacidade. O nível de privacidade desejado e o coeficiente de ajuste de precisão a serem utilizados nos serviços serão armazenados no próprio dispositivo móvel. Essa opção foi feita em virtude do desejo de reduzir a sobrecarga do servidor. Caso as preferências de privacidade fossem armazenadas no servidor, seria necessária a autenticação do usuário toda vez que algum serviço fosse ser utilizado além da necessidade de recuperar as informações pessoais. Ao armazenar tais informações no próprio dispositivo, a aplicação cliente é responsável por obtê-las e encaminhar as requisições com as respectivas preferências.

As preferências genéricas armazenadas possuem valores-padrão para as configurações de privacidade que são: 500 metros para o coeficiente de ajuste de precisão e nível de privacidade médio.

De maneira geral, o modelo de execução para *pull LBS* buscou oferecer garantias de privacidade ao usuário e, ao mesmo tempo, permitir que o usuário possa configurar suas preferências de privacidade para a liberação das informações de localização.

4.1.2.2 Modelo de Execução para *Push LBS*

Em serviços do tipo *push LBS* o usuário não realiza uma requisição diretamente mas, em geral, está cadastrado de alguma forma para que o serviço seja recebido. Um dos mais

característicos serviços dessa categoria de *LBS* é o recebimento de propagandas ao se passar próximo a algum tipo de estabelecimento.

Notificações sobre as ofertas do dia de uma rede de supermercados, informações sobre o preço da entrada do cinema ou sobre oportunidade de compra das últimas entradas para o teatro são apenas algumas das utilidades que podem ser obtidas através da utilização do *push LBS*.

Para o oferecimento desse tipo de serviço é necessária a constante atualização do posicionamento geográfico do usuário e a verificação da proximidade de algum dos pontos dos quais se deseja receber notificações. Em geral, o usuário cadastra-se em algum provedor e o dispositivo móvel de tempos em tempos encaminha sua localização.

Se o fornecimento de apenas uma informação de localização já pode representar ameaças à privacidade do usuário, a realização de várias aferições subsequentes pode agravar ainda mais tal situação. Com base na análise do histórico de várias informações de localização dos usuários é possível determinar facilmente suas rotas e locais preferencialmente freqüentados.

Visando oferecer privacidade para esse tipo de aplicações, é apresentado um novo modelo de execução para os serviços *push* denominado modelo de execução desvinculado do provedor. O objetivo básico do modelo é evitar que as informações de localização sejam encaminhadas a diferentes provedores e, para isso, o processamento de verificação de proximidade dos pontos em que se deseja receber notificações deve ser realizado no dispositivo móvel, sempre que possível.

Para que as informações de localização não sejam repassadas a diferentes provedores, é necessário que estes se registrem no servidor confiável e especifiquem as coordenadas geográficas dos pontos onde as notificações devem ser enviadas e as informações que devem ser encaminhadas aos usuários no momento em que passarem próximo a um dos pontos. As coordenadas geográficas dos locais de que se deseja receber algum tipo de notificação foram, neste trabalho, denominadas pontos de notificação.

O servidor confiável deve manter o controle de todas as empresas cadastradas e fazer a mediação com o dispositivo móvel, permitindo que o usuário possa escolher as empresas das quais deseja receber notificações e, além disso, garantir que essas serão enviadas quando o usuário estiver próximo ao local.

Esse modelo pode ser considerado desvinculado do provedor porque as informações de localização do usuário nunca serão encaminhadas até ele. Para isso, leva-se em consideração que o próprio dispositivo móvel é capaz de obter sua própria localização, independente da tecnologia utilizada. Dessa forma, o próprio dispositivo móvel pode verificar a proximidade dos pontos de notificação e informar ao servidor confiável que, em seguida, retorna a notificação.

Os passos para a prestação deste serviço segundo o modelo proposto são ilustrados pela Figura 3. Primeiramente, como apresentado no passo 1, o provedor *LBS* ou algum servidor da empresa que pretende fornecer o serviço deverá abastecer o servidor confiável com os dados de localização dos pontos comerciais e de informações das notificações. Diversos provedores diferentes poderão se cadastrar e, regularmente, atualizar as informações de notificações a serem encaminhadas aos usuários.

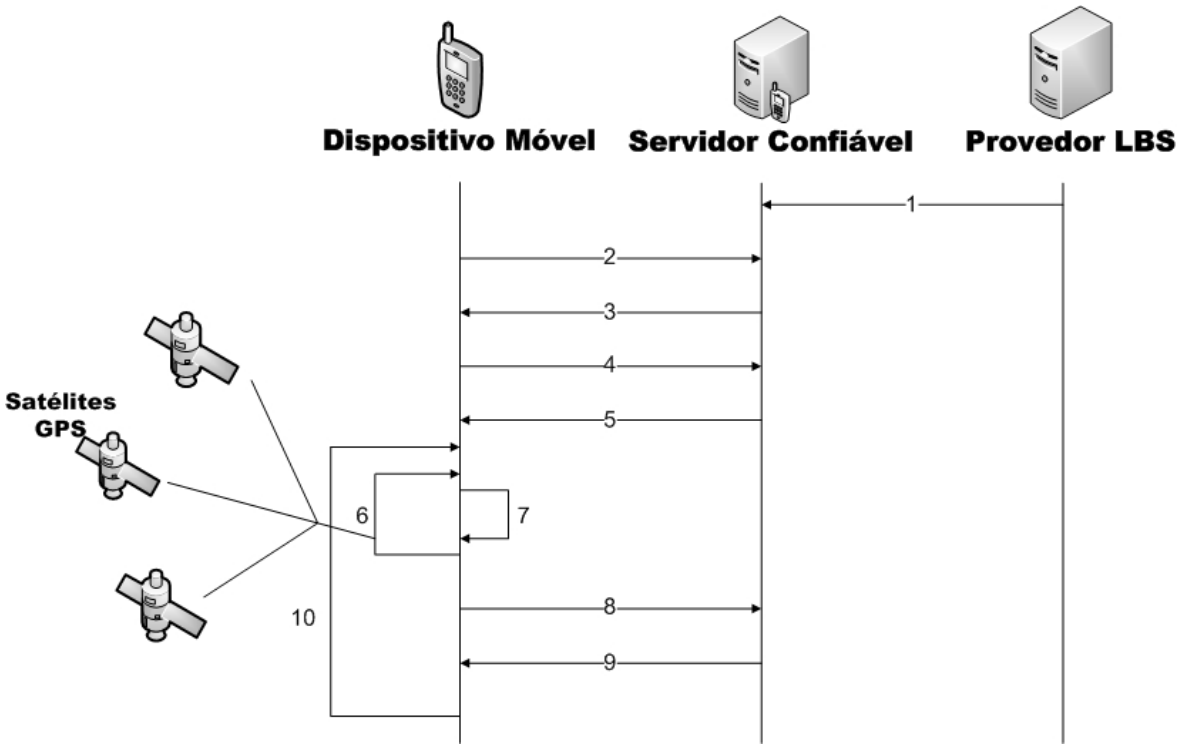


Figura 3 – Execução do *push LBS* segundo o modelo proposto.

Em seguida, no passo 2, o usuário, portando seu dispositivo móvel, acessa o servidor confiável e requisita a lista dos serviços disponíveis, que é retornada no passo 3. Com base na lista, o usuário pode então escolher quais notificações deseja receber e, no passo 4, enviar ao servidor o código daquelas que foram escolhidas. No passo 5, o servidor confiável envia para o dispositivo móvel os pontos de notificação, que são armazenados localmente.

Depois de realizada as operações descritas anteriormente, o dispositivo móvel entra em um *loop*, ilustrado pelos passos 6 e 7, para a verificação da aproximação de algum ponto escolhido, que funciona da seguinte maneira: no passo 6 é feita a verificação da localização do usuário (por exemplo: por satélites *GPS*) e comparada, no passo 7, com os pontos escolhidos. Caso o dispositivo não esteja próximo a nenhum ponto, é esperado um tempo que varia de acordo com a proximidade e velocidade de deslocamento e, então, se calcula novamente a localização e a compara com as posições, e assim sucessivamente, até que se esteja próximo a algum ponto. Nessa situação, o dispositivo móvel envia o código do ponto próximo ao servidor confiável, verificado no passo 8, e espera a resposta com a notificação, dada pelo passo 9. Por fim, no passo 10, o dispositivo retorna para o loop dos passos 6 e 7 para verificar a aproximação de outros pontos escolhidos.

No modelo de execução comumente utilizado para a execução dessa categoria de serviços, o usuário deve concordar que suas informações de localização sejam obtidas de tempos em tempos e repassadas ao provedor *LBS*, já que este deverá controlar o posicionamento do usuário. No entanto, no modelo de execução aqui proposto, as informações de localização do usuário serão manipuladas apenas pelo dispositivo móvel. Nem mesmo o servidor confiável terá acesso a estas informações, exceto no momento em que o dispositivo informa que está próximo a determinado ponto, contudo essa informação não será armazenada pelo servidor confiável, uma vez que este realiza controle de coleta e armazenamento.

Dessa forma, com o novo modelo de execução não é possível inferir a identidade do usuário, ainda mais considerando que os serviços executados com base nesse modelo também realizam controle da coleta e armazenamento dos dados além de utilizarem o canal seguro de comunicação.

4.1.3 Arquitetura Geral do Sistema

Para oferecer suporte à execução de *LBS* com garantias de privacidade, de acordo com os modelos de execução propostos, o *SBPL* possui a arquitetura geral apresentada na Figura 4, com uma aplicação cliente, específica para o dispositivo móvel, e uma aplicação servidor.

A aplicação cliente presente no dispositivo móvel possui cinco módulos: o módulo de comunicação cuja funcionalidade é a execução das atividades relacionadas à transmissão e recepção dos dados, oferecendo suporte à transmissão comum e segura; o módulo de *push*

LBS que é responsável pela execução em paralelo da determinação da localização e comparação com pontos de notificação; o módulo de localização, que oferece suporte à busca das coordenadas geográficas dos usuários; o módulo de gerência dos dados de privacidade, que permite a manipulação, armazenamento e recuperação das preferências de privacidade dos usuários; e, por fim, o módulo de controle, responsável pela coordenação e interação entre os demais módulos, pela execução do *pull LBS* e pela interface gráfica de maneira geral. Os dados de privacidade são armazenados localmente no dispositivo móvel e a comunicação com o servidor confiável é processada por algum canal de comunicação disponível para acesso à Internet, pelo dispositivo móvel.

Já o servidor confiável possui seis módulos: o módulo de controle, que atua de maneira similar ao módulo de controle presente na aplicação cliente, no que diz respeito à coordenação dos demais módulos; o módulo de comunicação com o provedor *LBS*, que oferece suporte tanto para a solicitação de serviços quanto para a atualização das informações oferecidas no *push LBS*; o módulo de interface de comunicação, que trata da construção e interpretação dos dados utilizados na requisição de serviços e na recepção de mensagens de atualização de *push LBS* provenientes dos provedores; o módulo *Push LBS*, que permite a o armazenamento e recuperação das informações desse tipo de serviço; o módulo de níveis de privacidade, que é o principal módulo do servidor confiável, sendo responsável pelo oferecimento das características de privacidade, de acordo com cada nível de uma requisição *pull LBS*; e, por fim, o módulo de comunicação com o dispositivo móvel, que oferece suporte à comunicação comum e segura com o dispositivo móvel (*DM*).

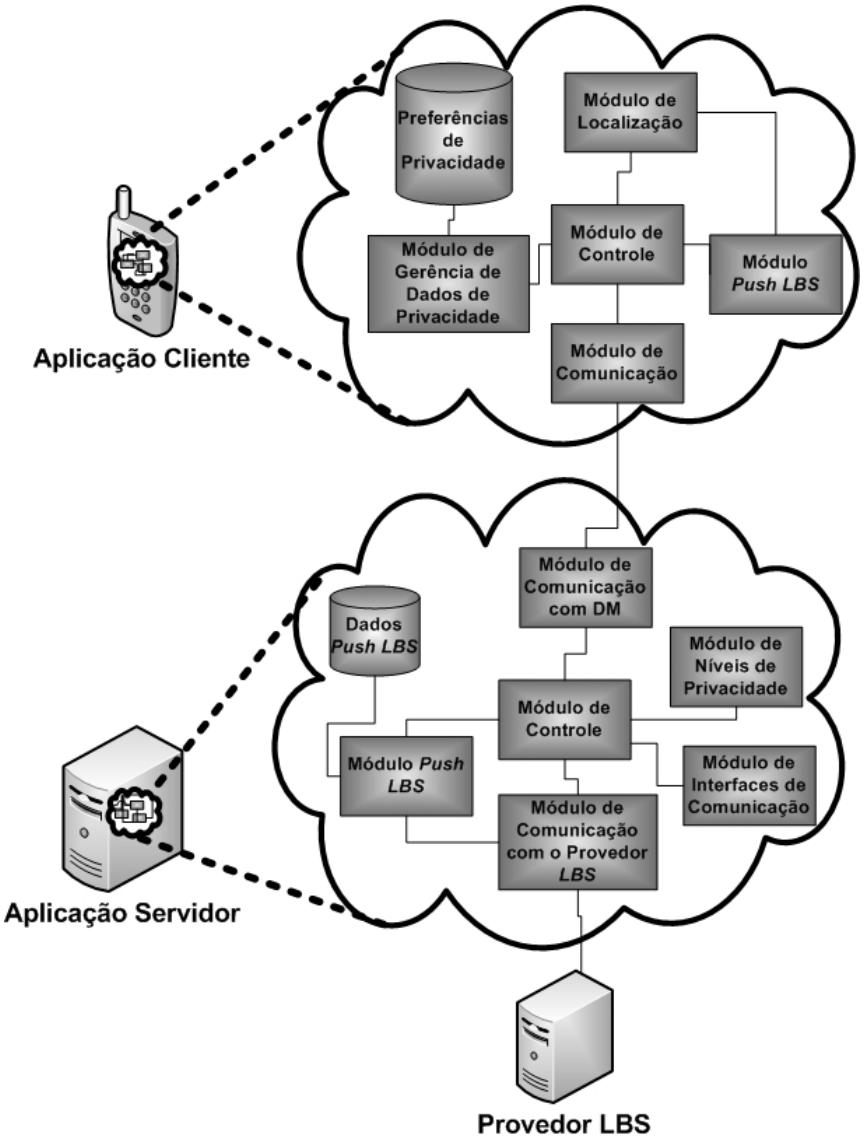


Figura 4 – Módulos do *SBPL*

O *SBPL* foi implementado com base na arquitetura descrita acima. A seção seguinte apresenta os detalhes envolvidos no desenvolvimento de cada módulo.

4.2 Implementação do Sistema

O *SBPL* é constituído de duas aplicações, a Aplicação Cliente com Privacidade de Localização (*ACPL*), para o dispositivo móvel, e o Servidor Baseado em Privacidade Multinível (*SBPM*), para o servidor confiável. O *SBPM* possui esse nome devido ao modelo de execução de níveis oferecido para suporte à privacidade de *pull LBS*, embora o servidor também ofereça suporte ao *push LBS.*

De maneira geral, o *SBPM* é responsável por oferecer suporte para a disponibilização de níveis de privacidade e gerenciamento das informações necessárias para a execução de

push LBS. O servidor é capaz de garantir que uma requisição proveniente do dispositivo móvel será executada com o nível de privacidade solicitado e com o valor de ajuste de precisão determinado. Além disso, o *SBPM* gerencia a comunicação com os provedores *LBS* e se mantém atualizado sobre o status dos serviços e provedores aos quais oferece suporte.

A *ACPL* tem como principais objetivos: realizar a comunicação com o módulo servidor, organizar e armazenar as preferências de privacidade dos usuários e sincronizá-las com os serviços disponíveis no servidor, além de fazer a verificação de proximidade dos pontos de notificação.

Para o desenvolvimento da *ACPL* foi utilizada a linguagem *JME* (*Java Micro Edition)* por diversos fatores, como: a existência de bibliotecas bem documentadas, o fato de ser uma linguagem de código-fonte aberto e, principalmente, a sua portabilidade.

Existem duas plataformas para desenvolvimento *Java* no que diz respeito a dispositivos móveis. A plataforma *CDC* (*Connected Device Configuration*), para dispositivos com maior poder de processamento, como *Palms* e *SmartPhones*, e a plataforma *CLDC* (*Connected Limited Device Configuration*), que possui bibliotecas mais simples, tendo o foco em dispositivos com menor poder de processamento. A maioria dos celulares oferece suporte apenas à plataforma *CLDC,* por isso, o desenvolvimento foi neste ambiente, visando o atendimento ao maior número possível de usuários.

A linguagem *Java* também foi utilizada no servidor confiável para o desenvolvimento de suas funcionalidades e os motivos da escolha são os mesmos apresentados anteriormente, além da existência de bibliotecas eficientes no auxílio à manipulação de documentos *XML,* que foram constantemente utilizadas no desenvolvimento.

4.2.1 Aplicação Cliente - ACPL

A aplicação presente no cliente, desenvolvida com API Java para dispositivos móveis, foi testada em pelo menos dois aparelhos de fabricantes diferentes, nos quais funcionou sem necessidade de adaptações. Os aparelhos testados foram um *Nokia N95* e um *HTC TYTNII*. A seguir é apresentado um detalhamento de cada módulo desenvolvido na Aplicação Cliente com Privacidade de Localização.

4.2.1.1 Módulo de Localização

A localização do dispositivo móvel implementada no desenvolvimento deste trabalho foi realizada através da *API Java Location* (LOYTANA, 2006), que garante a localização do dispositivo através de uma interface de alto nível. Essa *API* é caracterizada pela definição de dois objetos principais que auxiliam na obtenção da posição geográfica do dispositivo: o primeiro é o critério de localização, que permite a determinação de alguns critérios para a busca da posição geográfica do dispositivo, tais como precisão e consumo de bateria; o segundo é o provedor de localização, que pode ser implementado de maneira diferente para cada celular, dependendo da técnica de localização escolhida pelo fabricante.

A utilização da *API Java Location* permite que as coordenadas geográficas sejam obtidas através de diferentes técnicas de localização, dependendo da solução utilizada pela empresa fabricante do dispositivo móvel.

Uma das possibilidades para o suporte a outra técnica de localização é a realização de contato com as operadoras para que informações baseadas na triangulação do sinal das antenas sejam disponibilizadas. No entanto, deveria ser discutida e definida uma interface de comunicação, além de questões como custos do serviço e precisão oferecida. Uma boa solução para a interface de comunicação seria a utilização do protocolo de localização móvel (MLP 2002), descrito no Apêndice I, pelo fato de ser um padrão e oferecer suporte à solicitação de informações de posicionamento geográfico em diversos formatos.

4.2.1.2 Módulo Push LBS

O módulo *push LBS* tem como principal objetivo cuidar da verificação constante da localização do usuário e consequente comparação com a localização dos pontos de notificação.

Para isso, a *ACPL* possui uma *thread,* executando em paralelo, que obtém as informações de localização e compara com os pontos de notificação previamente escolhidos pelos usuários. Caso se verifique que o dispositivo se encontra próximo a algum ponto de notificação, é feita uma consulta ao *SBPM* sobre a mensagem a ser exibida ao usuário.

A implementação desse serviço levou em consideração alguns aspectos essenciais para o bom funcionamento, tais como o consumo de bateria devido às constantes aferições de localização e o envio de mensagens repetidas para o cliente.

O cálculo constante da posição do usuário pode acarretar um consumo excessivo de energia, especialmente em casos em que se utiliza um receptor *GPS*. Dessa forma, quanto mais frequentemente for atualizada a localização, maior será o consumo e menor será o tempo de uso da bateria.

Visando atenuar essa situação, a aplicação cliente oferece a possibilidade de determinação da freqüência de atualização das informações de localização, que pode ser realizada tantas vezes quanto possível ou de maneira controlada, para evitar o consumo excessivo de bateria. Para isso, foram definidos dois critérios para a obtenção da localização, o melhor-esforço e o econômico.

O critério do melhor-esforço executa a função de localização sempre que possível; dessa forma, os intervalos de tempo da localização variam de acordo com a disponibilidade do serviço. Por exemplo, nos casos em que se utiliza a localização através do *GPS*, o tempo para determinar a posição geográfica do dispositivo depende das restrições do receptor *GPS* (condições de tempo, nível de "visibilidade" com os satélites, proximidade de construções etc.).

A localização, segundo o critério econômico, segue a seguinte determinação: se o usuário está distante de todos os pontos nos quais ele deve receber a mensagem, então a busca da posição é feita em intervalos de tempo maiores, mas caso o usuário esteja perto de alguns dos locais ou se aproximando de algum deles, as aferições serão feitas em intervalos de tempo mais curtos.

A eficiência desse critério consiste na capacidade de fazer que a localização seja aferida com o maior intervalo de tempo possível, mas de forma controlada, para que não se passe por um ponto de notificação sem que a mensagem seja recebida.

Para o cálculo de um tempo estimado para a localização seguinte foram considerados aspectos como a distância do ponto de notificação mais próximo, a velocidade de movimentação e a disponibilidade do serviço de localização. Se o usuário estiver próximo a um ponto de notificação e se movendo em direção a ele com velocidade constante, a aferição da localização é realizada com pequeno intervalo de tempo. Caso o usuário esteja

parado, o intervalo para a determinação da localização será determinado conforme a distância do ponto de notificação mais próximo.

A utilização desses algoritmos não é muito eficiente nos casos em que o usuário fica parado por muito tempo, pois o tempo de aferição da localização deverá ser proporcional à distância do ponto de notificação mais próximo. Por exemplo, supondo-se que um usuário esteja parado no seu ambiente de trabalho e o ponto de notificação mais próximo esteja a cinco quilômetros de distância, o algoritmo para cálculo do tempo estimado para a localização não poderá determinar espera muito longa, pois caso o usuário saia a qualquer momento de carro, por exemplo, poderá passar próximo ao local e perder a notificação.

Entende-se que o mais viável seria a ativação da localização apenas nos momentos em que se deseja receber a notificação, contudo pode ser bastante inconveniente para o usuário ter de informar à aplicação quando começar a verificar os pontos de notificação. Uma hipótese viável é a possibilidade de determinação de tempos determinados de ativação, por exemplo, todos os dias, das dezoito às dezenove horas, caso esse seja o horário em que o usuário saia do trabalho e vá para casa.

No entanto, não é possível a implementação de tempos específicos de ativação de uma aplicação utilizando-se *JavaME/CLDC*. Sendo assim, a *ACPL* implementa apenas o algoritmo para o cálculo de tempo estimado para a localização e a possibilidade de iniciar ou cancelar a execução do serviço *push LBS*.

Outra restrição que existe na implementação do *push LBS* é a prevenção do envio de mensagens repetidas, isto é, se o usuário já recebeu a mensagem para um determinado ponto de notificação, a mensagem não deve ser enviada novamente até que tenha tido o conteúdo alterado pelo provedor.

Essa verificação também é realizada pela aplicação cliente e ocorre como é ilustrado na Figura 51. Primeiramente, o *SBPM* armazena o *timestamp* toda vez que recebe a alteração de alguma mensagem de notificação para determinada empresa. A *ACPL* executa os passos de determinação da localização e comparação com os pontos de notificação desejados. Quando é verificada a proximidade de algum ponto de notificação, a *ACPL* solicita a notificação ao ponto de notificação. O *SBPM* deve responder com a mensagem de notificação e o *timestamp* referente à última atualização da mensagem.

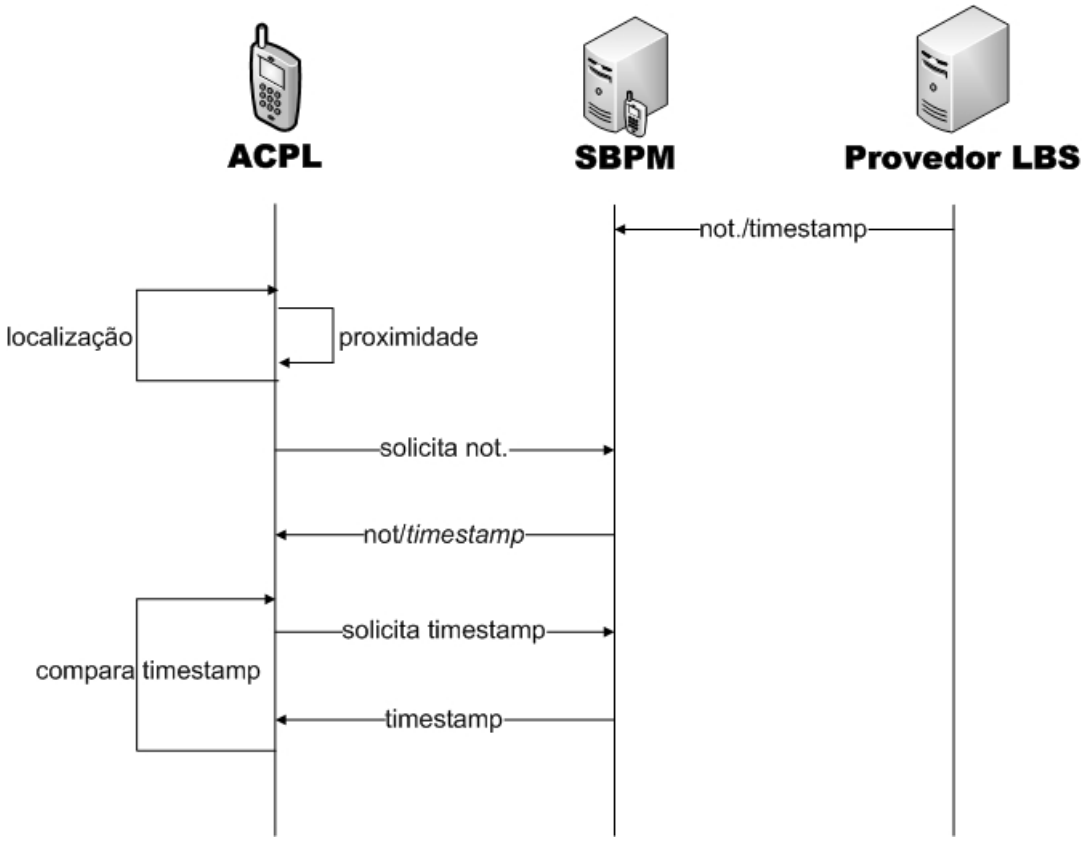


Figura 5 – Passos para a prevenção do envio de notificações repetidas

A partir de então, a *ACPL* solicita, de tempos em tempos, o *timestamp* referente à última atualização feita pelo provedor e verifica se é maior do que o *timestamp* da última mensagem recebida. Enquanto o *timestamp* for igual, a *ACPL* não deve enviar mensagem para os pontos de notificação já recebidos, uma vez que a mensagem ainda não foi atualizada no *SBPM*. É válido ressaltar que a *ACPL* continua realizando, em paralelo, a verificação de proximidade dos demais pontos de notificação.

O cálculo da distância entre as duas coordenadas geográficas apresenta algumas dificuldades. Tal cálculo seria razoavelmente simples levando-se em consideração um plano cartesiano comum com coordenadas *X* e *Y*, no entanto, ao se tratar de posicionamento geográfico, a operação não é trivial. Tal dificuldade é explicada pelo fato de a superfície terrestre não ser plana e as coordenadas de latitude e longitude serem fornecidas no formato de graus, minutos e segundos, sendo que cada grau nem sempre corresponde a um valor fixo em outras medidas, como quilômetros ou milhas.

A medida de um grau de latitude é equivalente a um arco no qual o comprimento é aproximadamente o mesmo em qualquer local sobre a superfície terrestre, cerca de cento e dez quilômetros. No entanto, os graus de longitude resultam em arcos cujo comprimento

varia de acordo com o local, partindo de cento e dez quilômetros no Equador até zero nos pólos.

Sendo assim, é necessária a utilização de alguma equação que permita o cálculo de forma precisa da distância. Uma das equações comumente aplicada para tal situação (Fórmula 1) é a utilização da lei dos cossenos para trigonometria esférica, na qual é calculada a distância entre dois pontos dados por (*lat1, lon1*) e (*lat2, lon2*). A letra '*R*' presente na fórmula indica o raio aproximado da terra.

$$a = \sin(lat1) * \sin(lat2)$$

$$b = \cos(lat1) * \cos(lat2) * \cos(lon2 - lon1)$$

$$c = \arccos(a + b)$$

$$d = R * c$$

Fórmula 1 – Lei dos cossenos

Apesar de ser usada frequentemente para o cálculo da distância entre dois pontos sobre a superfície de uma esfera, a lei dos cossenos para trigonometria esférica ocasiona erros altos para o cálculo de distâncias curtas. Como será constantemente necessário o cálculo de distâncias curtas para a verificação da proximidade de pontos de interesse, foi utilizada a fórmula de *Haversine* (SINNOTT, 1984), apresentada abaixo, como base para o cálculo da distância entre dois pontos.

$$\Delta lat = lat2 - lat1$$
$$\Delta lon = lon2 - lon1$$

$$b = \sin^2\left(\frac{\Delta lat}{2}\right) + \cos(lat1) * \cos(lat2) * \sin^2\left(\frac{\Delta lon}{2}\right)$$

$$c = 2 * \arcsin\left(\min\left(1, \sqrt{b}\right)\right)$$

$$d = R * c$$

Fórmula 2 – Fórmula de Haversine

Por motivos de eficiência de programação, é indicada a substituição da quarta linha apresentada na fórmula de *Haversine* por outra com a função arco-tangente2, como pode ser observado na Fórmula 3. Tal substituição não implica em redução relevante na qualidade dos dados retornados como cálculo.

$$c = 2 * \arctan 2\left(\sqrt{b}, \sqrt{(1-b)}\right)$$

Fórmula 3 – Função a ser utilizada na fórmula de Haversine

A aplicação da fórmula de *Haversine* é suficientemente precisa, ocasionando erros com valores abaixo de 0,3 %, em geral. Isto é, em um cálculo de deslocamento de um quilômetro, o erro máximo obtido seria, em geral, abaixo de três metros. Na Fórmula 2, os campos 'c', 'R' e 'd' indicam respectivamente: a distância do círculo máximo (*great circle*) entre as duas coordenadas (dado em radianos); o raio da terra; e, por fim, a distância entre os dois pontos iniciais. O resultado d é a mesma distância dada na unidade do raio da terra que é caracterizado por R. Para aplicação da fórmula neste trabalho, o raio utilizado foi dado em 6367 km, como sugerido por (*GIS FAQ*, 2009).

4.2.1.3 Módulo de Comunicação

O módulo de comunicação presente na *ACPL* é responsável pela comunicação com o *SBPM* e oferece suporte tanto à comunicação segura quanto não-segura.

Para a implementação do canal seguro de dados como garantia de privacidade foi utilizado o protocolo *SSLv3* (*Secure Socket Layer version 3*) (DIERKS; RESCORLA, 2006), que oferece mecanismos para a troca de mensagens criptografadas pela rede.

O protocolo *SSL* utiliza duas técnicas de criptografia para o oferecimento do canal seguro de dados, sendo que, inicialmente, utiliza-se a criptografia de chave pública para a troca de uma chave única negociada entre o cliente e o servidor para que, em seguida, a comunicação prossiga com a utilização de criptografia simétrica (MENEZES, OORSCHOT e VANSTONE, 1996).

A realização da comunicação segue basicamente os seguintes passos: primeiramente o cliente envia a solicitação de conexão com o servidor e, caso o servidor suporte o acesso seguro, será então feita a negociação do algoritmo a ser utilizado para a realização da criptografia sobre os dados e da chave simétrica. Posteriormente, se necessário à aplicação que implementa o protocolo seguro, é realizada a autenticação dos lados envolvidos na comunicação e, por fim, ocorre a troca das informações úteis.

Uma das vantagens da utilização do *SSL* é a sua adaptação ao modelo *ISO/OSI*, que propõe o uso de camadas para a realização da comunicação em rede, sendo que o *SSL* se encaixa entre a camada de transporte e a camada de aplicação. Dessa forma, a adaptação

para a utilização de técnicas criptográficas durante a troca de informações é feita de maneira facilitada.

Ambas as formas de comunicação foram implementadas com o auxílio da biblioteca de *sockets* disponibilizada pela *API Java* para dispositivos móveis. A Figura 6 apresenta o código comparativo com a realização da conexão segura e não-segura. A conexão com o servidor é feita através da chamada do método *open* da classe *Connector* (linhas 11 e 14). A diferença entre a conexão segura e a não-segura está na *String*, contendo o endereço de conexão. Na conexão baseada em *SSL*, a *String* contém "*ssl://*" antes do endereço IP do servidor e da porta de conexão (linha 13); já na conexão comum a *String* de endereço contém "*socket://*" antes dos demais dados. O restante da programação se realizará da mesma forma nos dois casos.

```
 6 StreamConnection conexaoComum = null;
 7 SecureConnection conexaoSSL = null;
 8 try {
 9     //CONEXÃO COMUM
10     String enderecoComum = "socket://" + Server_IP + ":" + Server_Port;
11     conexaoComum = (StreamConnection) Connector.open(enderecoComum);
12     //CONEXÃO SSL
13     String enderecoSSL = "ssl://" + Server_IP + ":" + Server_Port;
14     conexaoSSL = (SecureConnection) Connector.open(enderecoSSL);
15
16 } catch (IOException ex) {
17     ex.printStackTrace();
18 }
```

Figura 6 – Código comparativo entre conexão segura (*SSL*) e comum em *JavaMe*.

A opção pela utilização de *sockets* foi devido ao fato da simplicidade de implementação da comunicação com base nessa biblioteca em comparação com outras como, por exemplo, através de *HTTP* (*Hypertext Transfer Protocol*) e *HTTP* seguro.

4.2.1.4 Módulo de Gerência dos dados de Privacidade

O módulo de gerência dos dados de privacidade oferece suporte à manipulação, armazenamento e recuperação das preferências de privacidade dos usuários e das informações sobre as empresas das quais se deseja receber informações de notificação. Os dados necessários para a utilização dos serviços são: preferências de privacidade genéricas, preferências de privacidade específica e empresas das quais se deseja receber notificações.

Para o armazenamento das informações destacadas acima, foi utilizado o armazenamento em formato de registros suportado pela linguagem *JavaME*. Sendo assim, utilizou-se o objeto *RecordStore* capaz de executar tal tarefa.

As informações são todas armazenadas em um único arquivo inicializado durante a primeira execução da aplicação cliente. A partir de então, todas as vezes que o aplicativo for inicializado, os dados serão carregados em memória e alterados, caso sejam reconfigurados pelo usuário e, no término da execução do aplicativo serão regravados no registro, substituindo os valores iniciais. Dessa forma, a execução não é custosa, uma vez que o acesso aos registros não será realizado constantemente e os dados carregados na memória do dispositivo não são em grande quantidade.

O armazenamento é realizado conforme detalhado a seguir: primeiramente, as preferências genéricas de privacidade são armazenadas no início do arquivo através de dois inteiros que representam o nível de privacidade e o coeficiente de ajuste de precisão, respectivamente; em seguida são armazenadas as preferências de privacidade específicas (exceções), sendo que os dados de cada registro são três inteiros, indicando o código do provedor, o nível de privacidade desejado e o coeficiente de ajuste de precisão, respectivamente; por fim, os códigos das empresas das quais se deseja receber notificações são armazenados.

4.2.1.5 Módulo de Controle

O módulo de controle possui três funcionalidades principais: oferecimento do acesso à execução dos serviços e configurações de preferências de privacidade por meio de uma interface gráfica; gerência da execução dos demais módulos e controle do serviço *LBS*.

A gerência da execução consiste em inicializar os serviços oferecidos pelos módulos e coordenar os casos em que é necessária a relação entre eles. Por exemplo, o módulo de execução *push LBS*, enquanto executando, ao detectar a aproximação de um ponto de notificação, necessita fazer uma requisição da mensagem a ser exibida para o usuário mas, para isso, deve solicitar ao módulo de controle que a requisição seja efetuada.

O controle de execução do serviço *pull LBS* é feito da seguinte maneira: a partir do momento em que o usuário solicita a execução de um serviço deste tipo, por meio da interface gráfica, o módulo de controle aciona o módulo de comunicação para que a requisição seja enviada ao servidor com o nível de privacidade e ajuste de precisão

desejado. A partir de então, aguarda-se a resposta e, quando ela for retornada, exibe-se o resultado na tela do dispositivo.

Um importante papel a ser executado pelo módulo de controle é a determinação da utilização ou não do canal seguro de transmissão. Para isso, quando o usuário fizer uma requisição de *pull LBS*, deve ser verificado qual é o nível de privacidade desejado para tal serviço. Caso seja o nível 0, a comunicação será não-segura, mas caso seja nível 1 ou superior, o canal de comunicação deverá contar com técnicas de criptografia. As demais técnicas de privacidade são todas implementadas e aplicadas no servidor. O módulo de controle não obtém nenhuma informação pessoal do usuário para a execução de *pull LBS*, conforme determinado pelo controle de coleta e armazenamento realizado em todos os níveis de privacidade.

Por fim, a funcionalidade que trata da interface entre o usuário e o *SBPL* é bastante importante, pois deve oferecer recursos que permitam ao usuário utilizar o sistema de forma clara e eficiente. A seguir, são apresentadas algumas telas da aplicação cliente.

A *ACPL* possui um menu principal que possibilita o acesso aos serviços e configurações oferecidos, através das opções que podem ser observadas na Figura 7: “Serviços de Solicitação”, para a utilização dos serviços do tipo *pull LBS*; “Serviços de Notificação”, para a realização do cadastro em serviços de notificação (*push LBS*) e início da execução dos serviços; “Configurações”, para a configuração das preferências de privacidade; e, por fim, a opção “Sair”.

Figura 7 – Menu principal do *ACPL*

Ao selecionar o item “Serviços de Notificação”, é exibido outro menu, ilustrado pela Figura 8a, que permite a execução de diversas ações: “Iniciar” o serviço de notificação, ou seja, fazer com que o dispositivo passe a aferir sua localização e comparar com a localização dos pontos de notificação; “Iniciar em Backgroud” inicia a execução do serviço

mas em segundo plano, de forma que permita a utilização de outras aplicações; a opção “Meus Serviços” permite a visualização dos serviços de notificação cadastrados e ainda a exclusão destes serviços; e o item “Opções” permite a configuração das características do serviço, como, por exemplo, a frequência com que a localização será obtida, o que interfere na duração da bateria; por fim, a “Ajuda” exibe um texto descrevendo as principais características desse tipo de serviço e as opções de configuração.

O item “Adicionar Serviço” permite a escolha de novos serviços de notificação que são classificados por categoria e subcategoria. As Figura 8b, 8c e 8d apresentam os passos para o cadastramento em um novo serviço de notificação. Na execução dos passos apresentada, é realizado o cadastro para o recebimento de informações ao se aproximar do Teatro Municipal, que faz parte da categoria Lazer e da Subcategoria Teatro.

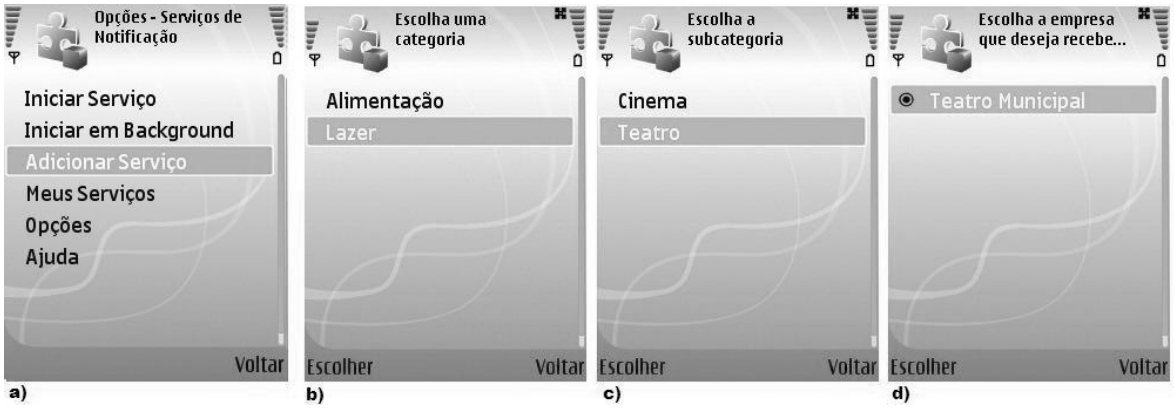


Figura 8 – Interface gráfica dos serviços de notificação.

Já a opção “Configurações”, presente no menu inicial, oferece os mecanismos que auxiliam nas configurações de privacidade para o usuário. Como já mencionado, o usuário pode configurar o nível desejado (Mínimo, Baixo, Médio, Alto ou Garantido) de forma genérica ou específica. Isto é, haverá sempre a configuração básica escolhida para todos os serviços, mas é possível também adicionar exceções aos serviços nos quais se deseja ter menores ou maiores garantias de privacidade.

A Figura 9 detalha as opções de configurações oferecidas pela aplicação cliente. Na Figura 9a são apresentadas as opções de escolha de configuração (genéricas ou exceções), conforme discutido acima.

Figura 9 – Interface gráfica para a configuração de privacidade.

Caso a primeira opção seja escolhida, será exibida uma tela com as opções de configuração apresentadas na Figura 9b, permitindo a determinação do nível de privacidade genérico e do coeficiente de ajuste de precisão genérico dado em metros. Caso seja escolhida a opção “Exceções”, uma tela com a lista de provedores será exibida, como verificado na Figura 9c. Após a escolha do provedor ao qual se deseja adicionar a exceção a ser feita, a tela da Figura 9b é novamente mostrada para a configuração, desta feita, para um único provedor. No caso da escolha da opção “Ajuda”, será exibido um texto explicando o funcionamento das configurações de privacidade, apresentando as principais características de cada nível oferecido. É válido ressaltar que as configurações específicas sempre serão seguidas prioritariamente, em detrimento das configurações genéricas.

O penúltimo item do menu principal, além da opção “Sair”, é o serviço “Minhas coordenadas” que exibe, na tela, as coordenadas geográficas do usuário e o tempo gasto para a determinação das mesmas.

Dessa forma, a interface gráfica da *ACPL* permite aos usuários configurar as preferências de privacidade genéricas e específicas e escolher as empresas das quais se deseja receber notificação, além de oferecer o acesso aos serviços do tipo *pull* e *push LBS.*

4.2.2 Aplicação Servidor

O Servidor Baseado em Privacidade Multinível foi implementado com base nos seis módulos descritos na Figura 4. A seguir os detalhes de cada módulo são apresentados separadamente.

4.2.2.1 Módulo de Níveis de Privacidade

O módulo de níveis de privacidade é responsável por oferecer as características de privacidade (controle da coleta e armazenamento, canal seguro de comunicação, ajuste de precisão e técnicas de anonimato) referentes ao nível solicitado pelo usuário, no momento da requisição *pull LBS.*

O nível Mínimo de privacidade não necessitou de implementação de algum tipo diferenciado de técnica de proteção à privacidade, no entanto, este nível garante o controle da coleta e do armazenamento de dados pessoais dos usuários. Esse controle, realizado pelo *SBPM*, consiste em evitar qualquer tipo de armazenamento das informações pessoais dos usuários, por períodos superiores ao necessário para o oferecimento do serviço.

O nível Baixo garante a utilização de um canal seguro de comunicação entre o dispositivo móvel e o servidor confiável, além do controle verificado no nível Mínimo. Na prática, a implementação dessa técnica não foi realizada pelo módulo de níveis de privacidade, mas sim pelo módulo de comunicação. Portanto, o detalhamento da implementação dessa técnica é realizado no módulo de comunicação.

Os níveis mais elevados contaram com a implementação de técnicas específicas de privacidade para atender ao modelo de execução para *pull LBS*. A seguir são apresentados os detalhes de implementação das técnicas utilizadas

4.2.2.1.1 Nível Médio

O nível Médio oferece ao usuário a possibilidade de ajuste de precisão de suas informações de localização com base em um deslocamento aleatório, segundo o modelo de execução *pull*. A implementação do ajuste de precisão foi realizado de forma similar à apresentada por Ribeiro e Zorzo (2008). O ajuste é calculado baseado no deslocamento aleatório da localização original para qualquer direção dentro de um raio, como pode ser verificado na Figura 10.

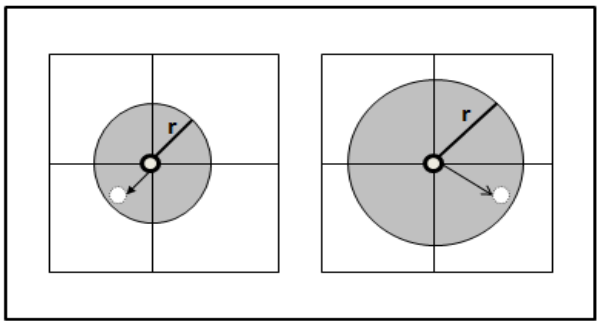


Figura 10 - Ajuste de precisão das informações de localização

A técnica funciona da seguinte maneira: dada uma posição inicial, apresentada na Figura 10 pelo círculo menor central, e um raio de deslocamento, caracterizado pela reta ‘r’, ocorrerá um deslocamento aleatório para qualquer parte do círculo maior. Por exemplo, supondo que ‘r’ é igual a 500 metros, a nova localização calculada por esta técnica poderá estar em qualquer um dos pontos internos à circunferência resultante com uma área de 785000 m^2 ou 0.785 km^2. O coeficiente de ajuste de precisão pode ser definido pelo usuário de acordo com sua preferência.

O cálculo da nova posição geográfica também apresenta os mesmo problemas do cálculo da distância entre dois pontos. Para solucionar tal situação, foi utilizada a fórmula abaixo que é baseada no triângulo esférico formado pelo ponto inicial, ponto final e o polo norte (SMART, 1977). Desse triângulo já são conhecidos dois lados - o lado entre o ponto inicial e o polo norte e o lado referente à distância de deslocamento - além do ângulo formado por estes dois lados, caracterizado pela direção de deslocamento fornecida. A partir dessas informações e da utilização de relações entre os ângulos e lados específicos da trigonometria esférica, são derivados os outros dados e o ponto final, que será utilizado no ajuste de precisão (WILLIAMS, 2009).

$$lat2 = \arcsin\left(\sin(lat) * \cos(d/R) + \cos(lat1) * \sin(d/R) * \cos(\theta)\right)$$

$$dlon = \arctan 2\left(\sin(\theta) * \sin(d/R) * \cos(lat1), \cos(d/R) - \sin(lat1) * \sin(lat2)\right)$$

$$lon2 = \mathrm{mod}\left(lon1 - dlon + pi, 2 * pi\right) - pi$$

Fórmula 4 – Fórmula para o cálculo do deslocamento

A fórmula é caracterizada pelos seguintes elementos: θ representa a direção de deslocamento; *lat1* e *lon1* são coordenadas do ponto inicial; e ‘*d/R*’ caracteriza a chamada distância angular, na qual ‘*d*’ é a distância desejada de ajuste e ‘*R*’ o raio da terra. Além disso, a função do módulo aplicada na terceira linha tem como objetivo tratar os casos nos quais os pontos estão em meridianos opostos. A latitude e longitude do ponto final calculado são dadas por *lat2* e *lon2*, respectivamente.

Esta fórmula é válida apenas para os casos em que a distância calculada é inferior a um quarto da circunferência da terra, o que é adequado às necessidades do sistema proposto, uma vez que os cálculos de ajuste de precisão terão a distância sempre inferior a poucos quilômetros. O código utilizado que implementa o ajuste de precisão é apresentado na Figura 11.

No trecho de código entre as linhas 11 e 22, é calculada a direção de deslocamento que deverá ser utilizada no ajuste. Primeiramente, as linhas 11 a 13 calculam aleatoriamente a direção em graus, minutos e segundos, que é, em seguida, convertida para *double*, como pode ser verificado na linha 14. Por fim, entre as linhas 19 e 22, é definido aleatoriamente se a direção será positiva ou negativa. Dessa forma, o deslocamento poderá ser realizado para qualquer direção a partir do ponto inicial, como ilustrado na Figura 10. A linha 24 calcula o valor do deslocamento aleatório (*dAleatorio*), que será entre 0 e o valor máximo que foi definido pelo usuário no coeficiente de ajuste de precisão. Em seguida, das linhas 28 a 35, é calculado o novo ponto com a informação de localização ajustada.

```
 8 private Point accuracyAdjustment(double lat, double lon, int distance) {
 9     double earthRadius = 6371; //KM
10     //SORTEAR ALEATOREAMENTE A DIREÇÃO DO DESLOCAMENTO (Graus, minutos e segundos)
11     int degrees = (int) (Math.random() * 180);
12     int minutes = (int) (Math.random() * 60);
13     int seconds = (int) (Math.random() * 60);
14
15     //CONVERTER A DIREÇÃO DE DESLOCAMENTO PARA DOUBLE
16     double direction = degrees + (double) minutes / 60 + (double) seconds / 3600;
17     //NÚMERO ALEATÓRIO PARA VERIFICAR SE SERÁ POSITIVA OU NEGATIVA A DIREÇÃO
18     //DE DESLOCAMENTO
19     double numAleatorio = Math.random();
20     if (numAleatorio > 0.5) {
21         direction = direction * (-1);
22     }
23     //CALCULA O VALOR DE DESLOCAMENTO ALEATÓRIO
24     int dAleatorio = (int) (Math.random() * distance);
25     //TRUNCA A DISTÂNCIA PARA APENAS DUAS CASAS DECIMAIS
26     double d = truncate(dAleatorio * 0.001, 3);
27     //CÁLCULO DA LATITUDE E LONGITUDE COM O DESLOCAMENTO EM UMA DIREÇÃO
28     double lat1 = Math.toRadians(lat);
29     double lon1 = Math.toRadians(lon);
30     double brng = Math.toRadians(direction);
31     double lat2 = Math.asin(Math.sin(lat1) * Math.cos(d / earthRadius) +
32             Math.cos(lat1) * Math.sin(d / earthRadius) * Math.cos(brng));
33     double lon2 = Math.atan2(Math.sin(brng) * Math.sin(d / earthRadius) * Math.cos(lat1),
34             Math.cos(d / earthRadius) - Math.sin(lat1) * Math.sin(lat2));
35     lon2 = (lon1 - lon2 + Math.PI) % (2 * Math.PI) - Math.PI;
36     //RETORNA O NOVO PONTO EM GRAUS
37     return new Point(Math.toDegrees(lat2), Math.toDegrees(lon2));
38 }
```

Figura 11 – Código do ajuste de precisão

Com base na implementção da técnica de ajuste de precisão apresentada na Figura 11, foi possível a manipulação com a eficiência e a qualidade desejada das coordenadas geográficas, sendo importante ressaltar que o tempo de execução desse trecho de código não acrescentou atraso excessivo, como detalhado nos resultados.

4.2.2.1.2 Nível Alto

Para atender ao modelo de execução de *pull LBS* para ao nível Alto, foi implementada uma técnica de ocultação de informações espaciais e temporais similar à apresentada por Gruteser e Grunwald (2003).

A Figura 12 detalha o funcionamento dessa técnica. Na etapa 1, o servidor recebe uma requisição LBS proveniente do dispositivo móvel 1 (DM1), contendo o tipo de serviço solicitado (por ex: busca por restaurantes próximos) e a localização do usuário (representado pelo círculo escuro). Em seguida, na etapa 2, o *DM2* também envia uma requisição *LBS* ao servidor. O servidor verifica a proximidade das duas requisições e então ajusta as informações geográficas em latitude e longitude para que englobe a posição dos usuários do *DM1* e *DM2*. Posteriormente, o servidor envia as duas requisições contendo o serviço e a área que engloba as duas localizações (representada pelo círculo claro). As requisições são "embaralhadas" e enviadas, não necessariamente na ordem que chegaram, de forma análoga às *MixZones* (BERESFORD; STAJANO, 2003), como verificado nas etapas 4 e 5. Finalmente, na etapa 6, o provedor *LBS* processa as requisições e, posteriormente, retorna os resultados ao servidor confiável, que os encaminhará aos dispositivos móveis.

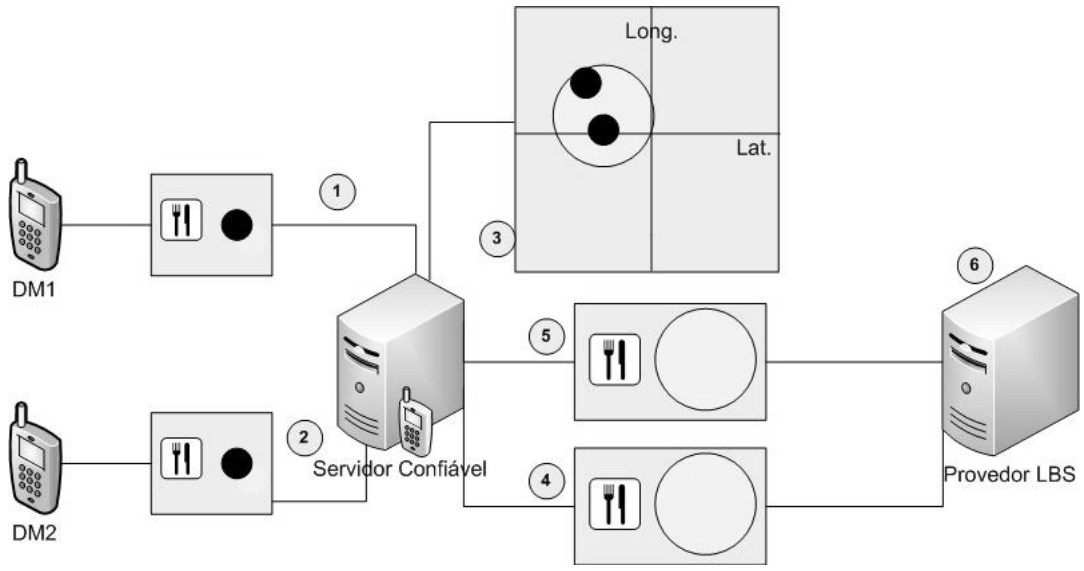


Figura 12 - Ocultação de informações espaciais e temporais.

Para tratar desse nível foi criada a classe *AnonymitySetRegion* que é responsável por armazenar as informações da região de conjunto de anonimato e as requisições pendentes dessa área (*PendingRequest*). Além dessas, a classe *ASRManager* é responsável por

receber todas as requisições como nível de privacidade ‘3’ e verificar se alguma delas pode ser agrupada em uma região de conjunto de anonimato (*AnonymitySetRegion)*. Caso a resposta seja positiva, ela é inserida na região correspondente como uma nova requisição pendente (*PendingRequest*) dessa área. Caso contrário é calculada uma nova região de conjunto de anonimato para essa nova requisição, que irá aguardar cinco segundos pela chegada de novas requisições provenientes da região calculada.

Esse nível de privacidade requer o controle de centenas, possivelmente milhares de requisições simultaneamente. Dessa forma, alguma técnica que reduza o número de comparações necessárias para encontrar a região de conjunto de anonimato de uma nova requisição deve ser utilizada. Imagine se, por exemplo, em determinado momento houvesse duzentas mil regiões de conjunto de anonimato e que, ao chegar uma nova requisição, comparações com cada uma das regiões devessem ser efetuadas.

O custo computacional despendido para tal situação seria muito grande, podendo até mesmo ocasionar a má qualidade da execução do serviço, caso o tempo de espera de uma região de anonimato não fosse suficiente para que uma nova requisição fosse agrupada à região. Por exemplo, supondo que, ao chegar uma nova requisição, exista uma região de conjunto de anonimato recentemente calculada em que a requisição possa ser encaixada. Entretanto, o tempo de espera da região até enviar as requisições pendentes não é suficiente para que a nova requisição também seja adicionada como uma nova requisição pendente. Por fim, a requisição poderia acabar sendo enviada solitariamente em função da falta de eficiência na busca de regiões de conjunto de anonimato.

Um primeiro esforço em otimizar a pesquisa foi o agrupamento de regiões de conjunto de anonimato em regiões maiores, como bairros e cidades. Para isso foi criada a classe *AnonymitySetSuperRegion* que é composta por várias *AnonymitySetRegion*. Dessa forma, ao receber uma nova requisição, a classe *ASRManager* compara primeiramente a qual *AnonymitySetSuperRegion* a requisição pertence e, depois de encontrar a super-região é então feita a busca nas regiões que a compõem. Desse modo, o número de comparações é diminuído consideravelmente e a possibilidade de não encontrar uma região de conjunto de anonimato é reduzida.

4.2.2.1.3 Nível Garantido

O nível Garantido sempre assegura a existência de um conjunto de anonimato no envio de uma requisição ao provedor *LBS*. Para isso, é utilizada a técnica de envio de

requisições falsas, ilustrada pela Figura 13. A mesma técnica utilizada no nível Médio para o ajuste de precisão foi utilizada no nível Garantido para o cálculo de uma nova posição para o usuário e das quatro novas posições falsas. Na Figura 13, o círculo interno central representa a localização original do usuário, e o outro círculo branco indica a posição ajustada do usuário, e os demais círculos escuros determinam a localização utilizada nas quatro requisições falsas.

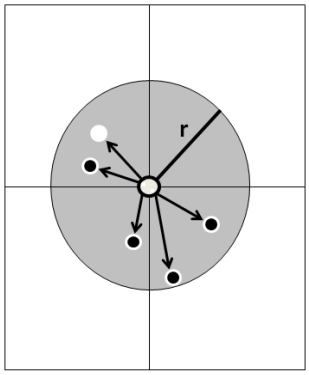


Figura 13 – Envio de requisições falsas.

Desta forma, a área interna ao círculo caracterizado pelo raio ‘r’ conterá cinco requisições enviadas em ordem aleatória ao provedor.

4.2.2.2 Módulo de Interfaces de Comunicação

O módulo de interfaces de comunicação possui funcionalidade muito importante para a concretização dos serviços, uma vez que é responsável por manipular as informações que devem ser trocadas com o provedor.

A comunicação com o provedor exige a representação de diversas informações. No caso de requisições de um serviço do tipo *pull LBS* ao provedor, por exemplo, é necessário encapsular dados como o tipo do serviço solicitado e a localização do usuário. Já nas respostas das requisições *pull*, deve-se oferecer suporte à representação da localização de pontos de interesse, endereços, mapas, dentre outros.

Da mesma maneira, para o abastecimento do servidor confiável com dados para execução de *push LBS*, deve ser possível o encapsulamento de várias informações. Dados como nome da empresa, coordenadas geográficas de todos os pontos de alerta ao usuário e conteúdo das notificações devem ser fornecidos ao servidor confiável para a execução do serviço.

Para a utilização de serviços do tipo *pull*, o *SBPM* implementou o suporte ao padrão de comunicação chamado *OpenLS* (*Open Location Services Interface Standard*) (OPENLS, 2008), ou padrão aberto para interfaces de serviços de localização, que oferece uma interface para a utilização de diversos serviços baseados em localização.

O *OpenLS*, detalhado no Apêndice I, foi desenvolvido pelo Consórcio Geoespacial Aberto (*Open Geospatial Consortium*) e apresenta a definição de documentos *XML* projetados para representar os dados necessários nas transações com provedores LBS. O *XML* oferece campos como o '*<gml:pos>*', para a representação da posição, e '*<xls:POIProperty name =“keyword” value =“restaurant”>*', que indica o nome do ponto de interesse, no caso, restaurante.

Apesar da existência de padrões para este tipo de comunicação, a utilização dos mesmos ainda não é uma realidade na prática. Diversos *LBS* oferecem a aplicação cliente para o dispositivo móvel, restringindo o acesso aos serviços apenas àqueles usuários que instalam essa aplicação em seu dispositivo móvel. O *SBPL* oferece suporte aos provedores que utilizam o padrão *OpenLS* para o oferecimento de *pull LBS*, considerando-se que a utilização de padrões é de fundamental importância para interoperabilidade entre diferentes dispositivos e serviços.

Já para o suporte aos serviços do tipo *push*, seguindo o modelo de execução, foi proposta uma representação baseada em um documento *XML* padrão que permite a representação das informações necessárias. Foi criado um schema[3] *XML* que definiu os campos do documento *XML*. A raiz do documento é o campo '*Company*', que representa a empresa que deseja fornecer o serviço. A princípio, o documento é caracterizado pela descrição da empresa ('*CompanyDescription*'), como pode ser observado na Figura 14, que apresenta uma extração da primeira parte do schema *XML* proposto.

Os primeiros três campos definidos para a descrição da empresa são obrigatórios e deverão ocorrer apenas uma vez em todos os casos (*minOccurs*="1" *maxOccurs*="1"). O primeiro, '*CompanyName'*, indica o nome da empresa, enquanto o segundo representa um código que é específico para cada uma ('*CompanyCode*') e, por fim, o campo '*Category'* indica a categoria das notificações que serão enviadas ao cliente. A seguir, vem o campo

[3] *XML Schema Definition* (*XSD*) é um documento que descreve a estrutura de um documento *XML* de forma geral, determinando dados como campos, atributos, organização hierárquica de elementos, número de ocorrência dos campos definidos, valores pré-definidos, etc. O esquema proposto pode ser consultado em http://www.dc.ufscar.br/~filipe_ribeiro/pushService/pushService.xsd.

‘*SubCategory*’ que, em conjunto com o campo ‘*Category*’, permite a indicação da categoria do serviço em uma hierarquia simples.

Além desses três campos, a descrição da empresa ainda conta com o campo de ‘*Locality’*, que indica as localidades das lojas pertencentes à empresa nas quais o usuário, ao passar próximo, deverá receber a notificação. Esse campo deverá ocorrer pelo menos uma vez para cada empresa. Ele é composto por outros cinco campos que são: ‘*CityName*’, para indicar a cidade; ‘*Latitude’* e ‘*Longitude’*, para a indicação das coordenadas geográficas e ‘*Address*’ e ‘*Phone*’, para a inserção dos campos de endereço e telefone, respectivamente.

```
- <element name="CompanyDescription">
  - <complexType>
    - <sequence>
        <element name="CompanyName" type="string" minOccurs="1" maxOccurs="1" />
        <element name="CompanyCode" type="integer" minOccurs="1" maxOccurs="1" />
        <element name="Category" type="string" minOccurs="1" maxOccurs="1" />
        <element name="Subcategory" type="string" minOccurs="0" maxOccurs="1" />
      - <element name="Locality" minOccurs="1">
        - <complexType>
            <element name="CityName" type="string" />
          - <sequence>
              <element name="latitude" type="double" minOccurs="1" maxOccurs="1" />
              <element name="longitude" type="double" minOccurs="1" maxOccurs="1" />
              <element name="address" type="string" minOccurs="1" maxOccurs="1" />
              <element name="phone" type="string" minOccurs="1" maxOccurs="1" />
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
```

Figura 14 – Primeiro fragmento do *schema* XML.

Além da descrição da empresa, é necessário que o servidor confiável também tenha acesso à notificação que deverá ser enviada ao usuário. Para isso foi definido o campo ‘*Notification*’, que pode ser visualizado no segundo fragmento do *schema XML*, apresentado na Figura 15.

```
- <element name="Notification">
  - <complexType>
    - <sequence>
        <element name="initMessage" type="string" minOccurs="1" maxOccurs="1" />
      - <element name="product" maxOccurs="unbounded">
        - <complexType>
          - <sequence>
              <element name="productName" type="string" minOccurs="1" maxOccurs="1" />
              <element name="description" type="string" minOccurs="1" maxOccurs="1" />
              <element name="price" type="string" minOccurs="1" maxOccurs="1" />
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
```

Figura 15 – Segundo fragmento do *schema XML*.

Este campo é composto por uma mensagem inicial (‘*initMessage*’) seguida de produtos (‘*product*’) que podem estar ou não presentes na requisição. O campo produto é caracterizado por três outros campos, ‘*productName*’, ‘*description*’ e ‘*price*’, que indicam o nome do produto, sua descrição e seu preço, respectivamente.

Com base nessas definições, é possível construir documentos *XML* que representem as informações necessárias para que seja oferecido *push LBS* com privacidade. Os documentos a seguir apresentam exemplos de utilização do documento *XML* proposto, sendo o primeiro para o caso de um supermercado que envia as promoções, como ilustrado pela Figura 16, e o segundo para um teatro que envia convites mais baratos para ocupar os últimos lugares de uma peça, apresentado na Figura 17.

```
<?xml version="1.0" encoding="UTF-8"?>
<ns1:Company  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:ns1='http://www.dc.ufscar.br/~filipe_ribeiro/pushService'
   xsi:schemaLocation='http://www.dc.ufscar.br/~filipe_ribeiro/pushService pushService.xsd'>
    <ns1:CompanyDescription>
        <ns1:CompanyName>Supermercado do Joaquim</ns1:CompanyName>
        <ns1:CompanyCode>1</ns1:CompanyCode>
        <ns1:Category>Alimentação</ns1:Category>
        <ns1:Subcategory>Supermercado</ns1:Subcategory>>
        <ns1:Locality>
            <ns1:CityName>São Carlos</ns1:CityName>
            <ns1:latitude>-22.001236</ns1:latitude>
            <ns1:longitude>-47.892119</ns1:longitude>
            <ns1:address>Av. São Carlos, 3803 Cidade Jardim - São Carlos - SP CEP- 13.566-330</ns1:address>
            <ns1:phone>(16) 3361-2957</ns1:phone>
        </ns1:Locality>
    </ns1:CompanyDescription>
    <ns1:Notification>
        <ns1:initMessage>Ofertas do dia</ns1:initMessage>
        <ns1:Product>
            <ns1:productName>Batata</ns1:productName>
            <ns1:description>KG</ns1:description>
            <ns1:price>R$ 0,89</ns1:price>
        </ns1:Product>
        <ns1:Product>
            <ns1:productName>Contra-filé</ns1:productName>
            <ns1:description>KG</ns1:description>
            <ns1:price>R$ 7,43</ns1:price>
        </ns1:Product>
        <ns1:Product>
            <ns1:productName>Panetone do Ze</ns1:productName>
            <ns1:description>Unidade - 500 gramas</ns1:description>
            <ns1:price>R$ 9,80</ns1:price>
        </ns1:Product>
    </ns1:Notification>
</ns1:Company>
```

Figura 16 – Exemplo de utilização do *XML* proposto – caso supermercado.

Nos documentos apresentados é possível verificar a utilização dos campos ‘Category’ e ‘*SubCategory*’ que podem receber valores diferentes, dependendo da classificação desejada. No exemplo do supermercado, foi utilizado como categoria “Alimentação” e subcategoria “Supermercado”. Já no caso do Teatro, foi utilizado “Lazer” e “Teatro” para a classificação de categoria e subcategoria, respectivamente.

```
<ns1:Company  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:ns1='http://www.dc.ufscar.br/~filipe_ribeiro/pushService'
   xsi:schemaLocation='http://www.dc.ufscar.br/~filipe_ribeiro/pushService pushService.xsd'>
<ns1:CompanyDescription>
        <ns1:CompanyName>Teatro Central</ns1:CompanyName>
        <ns1:CompanyCode>2</ns1:CompanyCode>
        <ns1:Category>Lazer</ns1:Category>
        <ns1:Subcategory>Teatro</ns1:Subcategory>>
        <ns1:Locality>
            <ns1:CityName>São Carlos</ns1:CityName>
            <ns1:latitude>-22.017151</ns1:latitude>
            <ns1:longitude>-47.893835</ns1:longitude>
            <ns1:address>Rua 7 de Setembro, 1735 Centro - São Carlos - SP CEP- 13.560-180</ns1:address>
            <ns1:phone>(16) 3371-4339</ns1:phone>
        </ns1:Locality>
    </ns1:CompanyDescription>
    <ns1:Notification>
        <ns1:initMessage>Promoção das últimas entradas para a apresentação:</ns1:initMessage>
        <ns1:Product>
            <ns1:productName>To be or not to be</ns1:productName>
            <ns1:description>Baseada na obra de Shakespeare</ns1:description>
            <ns1:price>R$ 15,00</ns1:price>
        </ns1:Product>
    </ns1:Notification>
</ns1:Company>
```

Figura 17 – Exemplo de utilização do XML proposto - caso teatro.

Com a utilização do padrão de comunicação *OpenLS* e com o documento *XML* proposto, o módulo de interfaces de comunicação permite que o *SBPM* se comunique com os provedores para o oferecimento de *pull* e *push LBS*, respectivamente. A vantagem de se utilizar *XML*, para este tipo de comunicação, é a facilidade que existe para que novos provedores possam se adaptar ao serviço, bastando para isso implementar a comunicação, seguindo-se os modelos propostos.

4.2.2.3 Módulo de Comunicação com Provedor

O módulo de comunicação com o provedor é responsável por oferecer o canal de comunicação sobre o qual são trocadas as informações apresentadas no módulo de interfaces de comunicação. A comunicação entre o provedor e o *SBPM* apresenta características diferentes para cada tipo de serviço. No caso de *pull LBS*, o *SBPM* envia requisições para o provedor *LBS* e, no caso de *push LBS*, é o provedor que envia dados para o *SBPM*. Dessa forma, o servidor deverá atuar de forma diferente para cada caso, como apresentado na Figura 18.

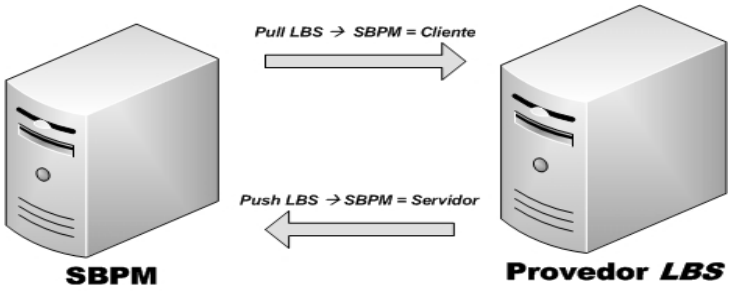


Figura 18 – Comunicação do *SBPM* com o Provedor *LBS*

Além de ser o servidor da aplicação cliente do dispositivo móvel, o *SBPM* oferece suporte à execução de um cliente para a comunicação com o provedor no suporte ao *pull LBS* e, também, à execução de um servidor para a recepção dos dados provenientes dos provedores nos casos de *push LBS*.

4.2.2.4 Módulo *Push LBS*

O módulo *push LBS* trata do armazenamento e recuperação dos dados necessários para a execução de *push LBS.* O modelo de execução para este serviço propõe que o servidor confiável deve armazenar as informações referentes às notificações envolvidas, que são: as localizações dos pontos de notificação e as mensagens a serem enviadas para o cliente, quando este passar próximo a algum ponto de notificação.

O *SBPM* implementa essa restrição do modelo de execução no módulo *push LBS*, de forma que, no momento em que o provedor abastece o *SBPM* com tais informações, elas são repassadas para esse módulo que gerencia a manipulação e armazenamento. A princípio, a implementação foi baseada na manutenção dessas informações em memória. Sendo assim, o *SBPM* mantém os registros de todos os provedores cadastrados e suas respectivas localizações e mensagens de notificação em memória.

Conforme mencionado na descrição do módulo *push LBS* da aplicação cliente, a verificação do recebimento de mensagens repetidas para um mesmo ponto de notificação fica a cargo do próprio dispositivo móvel. Se a *ACPL* já recebeu a notificação para determinado ponto, a própria aplicação verifica de, tempos em tempos, se a mensagem de notificação para aquele ponto já foi alterada. A verificação é feita através do *timestamp* que é armazenado pelo *SBPM* toda vez que alguma empresa altera sua mensagem de notificação. Quando a *ACPL* verifica que o usuário está próximo a um ponto de notificação e solicita o envio da mensagem correspondente, o *SBPM* envia, juntamente com esta, o *timestamp* da última atualização da mensagem. Assim, para a *ACPL* verificar se a

mensagem de notificação já foi alterada, basta solicitar o *timestamp* da última atualização da empresa e comparar com o *timestamp* da última mensagem recebida.

4.2.2.5 Módulo de Comunicação com DM (Dispositivo Móvel)

O Módulo de comunicação com o dispositivo móvel oferece suporte tanto à comunicação segura quanto à não-segura e, da mesma forma que ocorre no dispositivo móvel, o canal seguro de dados é suportado através do *SSLv3*.

Para a implementação desse protocolo no *SBPM*, foi utilizada a Extensão Java para *Socket* Seguro (*JSSE – Java Secure Socket Extension*) (JSSE, 2002), a qual oferece uma série de mecanismos já implementados que facilitam a implantação do canal seguro, como: manipulação de chaves criptográficas, suporte a *HTTP* encapsulado em *SSL* (*HTTPS*), além de controle de todas as etapas envolvidas durante o processo de negociação (algoritmos e chaves).

A adaptação de um *socket* seguro ao código é simples, uma vez que a única diferença está presente apenas na inicialização do mesmo. A Figura 19 apresenta um código com a inicialização de um *socket* comum (*socketComum*) e um *socket* baseado em comunicação segura (*socketSSL*), ambos em Java.

```
 8 ServerSocket socketComum = null;
 9 SSLServerSocket socketSSL = null;
10 try {
11     //INICIALIZAÇÃO SOCKET COMUM
12     socketComum = new ServerSocket(PORTA);
13     //INICIALIZAÇÃO SOCKET SSL
14     KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
15     KeyStore ks = KeyStore.getInstance("JKS");
16     char[] passphrase = "meupassword".toCharArray();
17     ks.load(new FileInputStream("certificado"), passphrase);
18     kmf.init(ks, passphrase);
19     SSLContext context = SSLContext.getInstance("SSLv3");
20     context.init(kmf.getKeyManagers(), null, null);
21     SSLServerSocketFactory ssf = context.getServerSocketFactory();
22     socketSSL = (SSLServerSocket) (ssf.createServerSocket(PORTA));
23 } catch (Exception e) {
24     e.printStackTrace();
25 }
```

Figura 19 – Código de comparação entre *socket* comum e *socket SSL*.

Enquanto para o *socket* comum é necessária apenas a inicialização, o *socket* com *SSL* é criado por uma "fábrica" de *sockets SSL* (linha 22) apenas depois da inicialização do objeto que irá manipular as chaves (linha 14), da definição do arquivo contendo o certificado

(linha 17) e da determinação do protocolo de comunicação (*SSLv3* – linha 19). Após a criação do *socket* seguro, todo o restante do código manipulador dos *sockets* será idêntico para os dois casos. No entanto, além da inserção do código extra para a utilização do *socket* seguro, é necessária a criação e manipulação dos certificados manualmente.

O *SBPM* possui duas *threads* principais aguardando conexões, sendo que uma recebe conexões seguras e a outra conexões não-seguras, ambas provenientes da *ACPL*.

4.2.2.6 Módulo de Controle

O módulo de controle possui atuação semelhante ao módulo de controle da *ACPL*, no que se refere à coordenação do relacionamento entre os demais módulos. É necessário que as tarefas de cada módulo sejam gerenciadas e interligadas para a execução do serviço de maneira eficiente, especialmente nos casos em que um módulo depende de tarefas realizadas por outro módulo. Esse módulo é responsável por comandar a execução do *SBPM* de maneira geral. É válido ressaltar que a aplicação servidor não possui um módulo específico para *Pull LBS*, já que, para execução desse tipo de serviço, as requisições são recebidas no módulo de comunicação e encaminhadas para o módulo de níveis de privacidade, onde serão tratadas.

4.3 Considerações finais

Esta seção apresenta algumas discussões com relação ao sistema proposto, no que diz respeito à arquitetura de servidor confiável escolhida, aos aspectos de privacidade tratados e aos custos que podem ser inseridos em decorrência da cobrança pelo oferecimento dos serviços.

4.3.1 Servidor Confiável Centralizado

A abordagem utilizada para a implementação do *SBPL* caracterizada por um servidor confiável foi embasada no fato de que a utilização de *LBS*, em geral, está vinculada ao oferecimento dos serviços por diversos provedores *LBS*, o que faz com que as informações pessoais, em especial informações de localização, sejam repassadas a diversas entidades diferentes.

Conforme levantado por Youssef, Atluri e Adam (2005), quando um cliente confia em várias entidades diferentes, torna-se difícil controlar como os dados são tratados por cada uma das entidades e como alguma entidade será responsabilizada por eventuais problemas. Desse modo, é proposta a limitação do número de entidades confiáveis para uma única

entidade, especialmente no caso de *LBS*, pois, assim, técnicas de privacidade e controle de acesso poderão ser assegurados pela entidade confiável.

No entanto, a utilização de uma única entidade confiável, especialmente como no *SBPL*, no qual existe um único servidor intermediário, duas questões principais podem ser levantadas: concentração de dados e escalabilidade.

O problema da concentração de dados diz respeito ao armazenamento de informações de diversos usuários em um único local. Essa situação poderia ocasionar a perda dos dados, caso houvesse algum problema de ordem física, como, por exemplo, problemas lógicos no hardware de armazenamento e danos à estrutura de hardware ou, ainda, roubo de informações pessoais de usuários, caso o servidor fosse invadido devido a brechas de segurança. Entretanto, segundo os modelos propostos, as informações pessoais de usuários não serão mantidas no servidor; tanto as informações de preferências de privacidade quanto as informações de localização serão utilizadas apenas para o oferecimento do serviço e não serão armazenadas por mais tempo.

Outro problema que surge diz respeito à escalabilidade do sistema proposto, uma vez que um único servidor com certeza apresentará limites quanto à carga de requisições suportadas. E ainda, o servidor único seria um ponto de falha, de forma que, caso haja alguma falha, a execução do *SBPL* seria inviabilizada. Entretanto, com relação à carga de requisições suportadas por um único nó, foi verificado, através de testes detalhados posteriormente, que o volume de tráfego suportado foi elevado, considerando-se um único nó. E, para solucionar o problema do ponto de falha e da necessidade de carga disponível superior à suportada, poderia ser realizada uma abordagem distribuída, com possibilidade de distribuição de carga em tempo de execução, de maneira que a característica de um servidor confiável centralizado não seja perdida e continue existindo apenas uma única entidade confiável.

4.3.2 Privacidade

O *SBPL* oferece garantias de privacidade para a execução de *pull* e *push LBS*. No caso do *push LBS*, o modelo de execução desvinculado do provedor implementado impede que as informações de localização sejam encaminhadas para outras entidades, sendo manipuladas apenas pelo dispositivo móvel. Assim, as ameaças para a utilização desse serviço são suprimidas. Uma das principais preocupações quanto à utilização de *push LBS* é a aferição de várias localizações do usuário de maneira subsequente e compartilhamento

de tais informações com provedores. A avaliação da movimentação do usuário representa grande risco à manutenção da privacidade do usuário, pois, além da possibilidade de determinar os locais frequentados, permite a caracterização de toda uma rotina de movimentação. A utilização de *push LBS* com o modelo implementado pelo *SBPL* garante a privacidade do usuário para esse tipo de serviço.

Já para a execução de *pull LBS*, o modelo de execução baseado em níveis possibilita a configuração das preferências de privacidade, como apresentado na Tabela 1, o que permite a adequação das necessidades de cada usuário. O próprio usuário pode configurar o nível de privacidade que deseja e a medida, em metros, a ser utilizada no ajuste de precisão.

Ambas as características possuem valores-padrão para as requisições, sendo 'médio' o nível de privacidade padrão e 500 metros a medida padrão utilizada no ajuste de precisão. É permitido ao usuário tanto modificar as configurações utilizadas como padrão quanto adicionar exceções específicas, alterando o nível de privacidade e a medida do ajuste de precisão para determinado provedor *LBS*.

A utilização das técnicas de privacidade para *pull LBS* dificulta consideravelmente a possibilidade de identificação de um usuário, especialmente nos níveis Médio, Alto e Garantido, uma vez que suas informações de localização não serão repassadas a nenhum terceiro (provedor *LBS*, atacante espionando a rede, etc) com precisão elevada. Além disso, o conjunto de anonimato implementado nos níveis Alto e Garantido dificulta ainda mais o relacionamento de uma requisição a um usuário específico.

O *SBPL* oferece diversas garantias de privacidade para a execução de *pull LBS*, no entanto não é possível assegurar a total privacidade do usuário em virtude de dois aspectos: o primeiro deles é a avaliação diferenciada e subjetiva sobre o que seria uma real invasão de privacidade para cada usuário; o segundo é a possibilidade de se burlar as técnicas de privacidade utilizadas, como detalhado a seguir.

Suponha que um usuário solicite ao provedor *LBS* informações sobre o hotel mais próximo de sua atual localização, e a resposta seja um único hotel para esse usuário. Se o provedor estiver atuando como um atacante e tiver como descobrir que o usuário realmente seguiu o direcionamento dado pela resposta, ele poderá inferir a identidade do usuário. A possibilidade de ataque na sombra (*shadow attack*) é remota no ambiente de telefonia móvel, devido à amplitude de tal ambiente se comparado com o cenário do ginásio

“pervasivo” apresentado previamente. No entanto, não se pode garantir que um ataque desse tipo nunca irá acontecer.

Embora o *SBPL* esteja sujeito a alguns ataques, como o descrito anteriormente, tais ataques têm muito mais dificuldades de obter êxito se comparados à utilização de *pull LBS* sem o *SBPL*.

Sabemos, também, que o *SBPL* não é capaz de oferecer privacidade para todos os serviços. Alguns serviços podem exigir o envio da identificação do usuário, como, por exemplo, a solicitação de um táxi. Outros necessitam da indicação da posição exata do usuário como, por exemplo, a determinação de rotas entre dois locais. Por fim, os serviços de navegação dirigida exigem a aferição da localização, sempre que possível, para a exibição da rota a ser seguida. Assim, caso sejam aplicadas técnicas de privacidade, especialmente o ajuste de precisão, a navegação dirigida poderia ser dificultada, apresentando percursos inconsistentes.

No entanto, o *SBPL* permite que tais serviços sejam utilizados, uma vez que existe a possibilidade de utilização sem as técnicas de privacidade que os inviabilizam. Dessa forma, este pode ser considerado um ponto forte do *SBPL*, pois, em geral, os trabalhos de proteção à privacidade recorrem a técnicas que inviabilizariam a utilização de determinados serviços. Desse modo, consideramos o trabalho aqui apresentado como uma boa solução para a utilização de *LBS* no ambiente de telefonia móvel com garantias de privacidade.

4.3.3 Custos

Outro aspecto importante a ser observado para a execução do sistema proposto em um ambiente real é o que diz respeito aos custos envolvidos durante o oferecimento dos serviços. Dois elementos principais podem acarretar custos ao usuário, que são a utilização do canal de comunicação com a Internet e as cobranças que, eventualmente, podem ocorrer em decorrência do oferecimento do serviço pelo provedor *LBS*.

Existem atualmente várias tecnologias de acesso à Internet via dispositivo móvel, como, por exemplo, *GPRS (General Packet Radio Service)* e *EDGE* (*Enhanced Data GSM Environment*). Ambos os serviços visam prover comunicação baseada em pacotes que permita acesso a Internet. A tecnologia *GPRS* promete taxas de 56 até 114 kbps e conexão contínua à Internet, mas outras tecnologias foram desenvolvidas com o objetivo de prover

acesso com maior velocidade, como *AMR (Adaptive Multi-Rate Codec), EDGE* e outras (HALONEN, 2003).

Este tipo de serviço é, em geral, tarifado pelas operadoras de telefonia móvel e tem apresentado queda razoável nos custos, mas a tendência é que, com a implantação das redes de telefonia móvel *3G*, o acesso seja disponibilizado com melhor qualidade e com preços mais atraentes para o consumidor. Principalmente levando-se em consideração que o celular tem se tornado um meio muito utilizado para acesso à Internet para diversas finalidades, como por exemplo, acesso *Web.*

O segundo custo mencionado diz respeito à cobrança feita pelos provedores em função da prestação do serviço. Embora haja uma série de serviços baseados em localização oferecidos gratuitamente, existe a possibilidade de que determinados provedores só permitam o acesso a determinado tipo de serviço com garantias de que ele poderá ser cobrado.

Como o anonimato do usuário – inclusive para o servidor confiável – é uma das principais características do sistema proposto, a identificação das requisições feitas por determinado usuário e posterior cobrança pela utilização dos serviços não é abordada inicialmente. No entanto, é possível que o sistema se adapte a este tipo de situação de modo semelhante ao modelo proposto por *Martucci et al.* (2006), de forma que o provedor *LBS* realize a cobrança à entidade vinculada ao servidor confiável. Tal cobrança é calculada com base no número de respostas decorrentes das requisições solicitadas pelo servidor confiável. O servidor confiável por sua vez deve ser capaz de verificar quais são as requisições que devem ser cobradas e identificar qual usuário fez cada requisição, para que possa repassar a cobrança ao usuário.

Para o oferecimento de suporte à realização de cobranças, o sistema proposto deve lidar com duas questões principais: permitir o cadastramento do usuário no servidor confiável de forma que ele possa ser cobrado de alguma maneira e, principalmente, a definição de regras claras entre o provedor *LBS* e o servidor confiável concernentes à cobrança, oferecimento e disponibilidade do serviço.

Sem dúvida, a possibilidade de realização de cobranças ao usuário permite o relacionamento de um usuário e suas respectivas requisições *LBS*, no entanto essa verificação pode ser realizada apenas pelo servidor confiável. Sendo assim, não existe a preocupação de que o provedor *LBS* determine quais requisições foram feitas pelo usuário.

Tal situação pode ocorrer apenas no servidor confiável que deve ser controlado por uma entidade confiável e que, em nenhuma situação, irá compartilhar essas informações.

5 Resultados

Para verificar a real aplicabilidade do sistema proposto, foram realizados testes práticos que permitiram a avaliação de aspectos como tempo de resposta das requisições, qualidade dos dados e escalabilidade. A seguir é descrito, primeiramente, o estudo de caso implementado e, em seguida, os resultados obtidos em cada avaliação.

5.1 Estudo de Caso

Foram implementados dois serviços do tipo *pull* para testar a aplicação do sistema em um ambiente de execução *LBS*. Primeiro, o serviço de busca por pontos de interesse que, baseado na localização do usuário e em uma palavra-chave de pesquisa (por ex: pizzaria, hotel, restaurante), permite a busca por pontos de interesse próximos à atual localização do usuário. O segundo serviço foi denominado "Meu Local" e exibe um mapa com a localização do usuário. As telas de execução dos serviços implementados na aplicação cliente são apresentadas na Figura 20.

Figura 20 – Tela de execução do serviço "Meu Local" e busca por Pontos de Interesse

Os dados de pontos de interesse e mapas foram fornecidos pela *Navteq*[4]e *TeleAtlas*[5], empresas de suporte ao oferecimento de serviços baseados em localização. No entanto, todos os dados foram acessados por meio de um serviço oferecido pela *deCarta*[6], chamado *deCarta Mobile Server*, que nada mais é do que uma interface para acesso aos dados

[4] http://www.navteq.com/
[5] http://www.teleatlas.com/index.htm
[6] http://www.decarta.com

oferecidos pela *Navteq* e *TeleAtlas*, com a utilização do *OpenLS*, padrão para comunicação em LBS descrito anteriormente.

A *ACPL* desenvolvida utilizou a técnica de localização baseada no Sistema de Posicionamento Global (*GPS*) oferecida pelo aparelho utilizado nos testes, contudo outras técnicas de localização poderiam ser utilizadas, dependendo das técnicas implementadas pelo dispositivo móvel ou do suporte à localização oferecido pelas operadoras de telefonia.

O *GPS* foi escolhido em virtude da possibilidade de obtenção das coordenadas geográficas do dispositivo, sem necessidade de contato com nenhuma outra entidade como a operadora de telefonia móvel. Em geral, as operadoras oferecem o serviço de localização através de triangulação do sinal das antenas, no entanto a disponibilização dessas informações para acesso, via aplicações presentes no dispositivo móvel, não é alcançada de forma trivial.

O dispositivo móvel utilizado no estudo de caso foi um celular *N95* do fabricante *Nokia* com suporte a Java, acesso à localização via *GPS* e acesso à Internet via *Wi-Fi* ou *GPRS*. Já o *SBPM* possuía as seguintes configurações: processador *Intel Pentium Dual Core* (3000 *MHZ*), 4 *MB* de memória *Cache* e 2 *GB* de memória *RAM*, Sistema Operacional *Windows XP* e plataforma Java *JDK 1.6u2*.

Todas as execuções realizadas no celular que necessitaram de acesso à Internet foram executadas de duas maneiras: através do acesso a redes *Wi-Fi* e com o acesso *GPRS* oferecido pela operadora de telefonia móvel. Apesar do reconhecimento de que o acesso à banda larga via celular é uma tendência e a comunicação via rede provavelmente não será uma restrição à eficiência de aplicações futuras, os testes também utilizaram o acesso *GPRS* devido ao fato de essa tecnologia ainda ser amplamente utilizada.

Dessa forma, a arquitetura geral de execução do estudo de caso, ilustrada pela Figura 21, contou com um celular *Nokia N95* para a execução da aplicação cliente e, como provedor *LBS*, o servidor da *deCarta* que oferece suporte à *LBS* através do *OpenLS*, sendo que a comunicação entre a *APCL* e o *SBPM* foi realizada por meio de pontos de acesso (*Wi-Fi*) ou da antenas de telefonia móvel (*GPRS*).

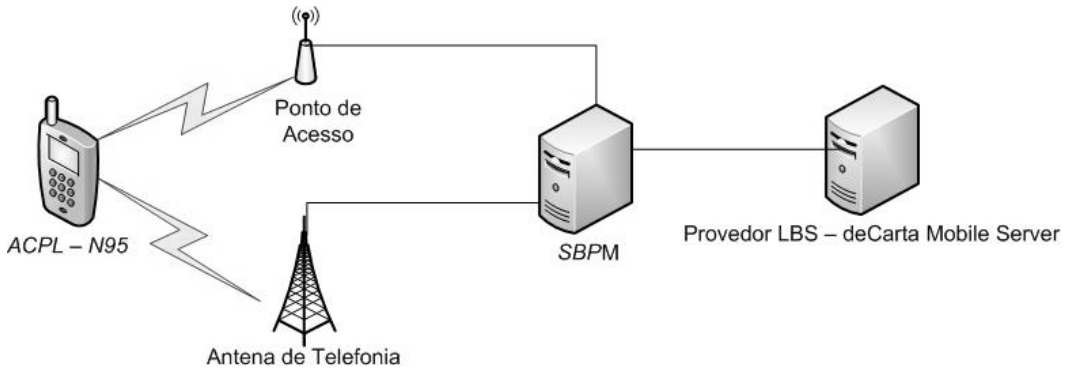


Figura 21 – Arquitetura de execução do Estudo de Caso.

A seguir, são detalhados os testes realizados com base no estudo de caso implementado e apresentados os resultados.

5.2 Tempos de resposta

O primeiro teste realizado tinha como principal objetivo avaliar o tempo de resposta observado durante as requisições a partir de um dispositivo móvel. Em um primeiro momento foram realizadas requisições com dez localidades pré-definidas, a partir da *ACPL*. Para cada localidade foram feitas requisições de busca por pontos de interesse e "Meu Local", e com todos os níveis oferecidos. Além disso, cada requisição foi realizada dez vezes para evitar que interferências na comunicação influenciassem os resultados.

A não-utilização da localização através do *GPS* para o cálculo dos tempos médio de resposta se explica pelo fato de a função de localização através de *GPS* apresentar variação de tempo muito grande. Questões como condições climáticas e baixas condições de visibilidade do receptor, isto é, caso o receptor esteja entre construções, por exemplo, e não tenha bom contato com os satélites, podem atrasar ou até mesmo impossibilitar a determinação da localização.

A Tabela 2 e a Tabela 3 explicitam os resultados dos tempos médios de resposta (*TMR*) e do desvio padrão (*DP*) observados durante a execução dos dois serviços para cada nível. As colunas apresentam o *TMR* e o *DP* observado, em segundos, para cada serviço, e as linhas especificam o nível de privacidade aplicado, do nível Mínimo até o Garantido, indicados pelos números de 0 a 4. O alto valor do tempo de resposta do nível Alto (3) de privacidade se deve ao fato da espera de cinco segundos para a composição do conjunto de anonimato, atraso que não deve ser verificado, caso o número de usuários do serviço aumente. A Tabela 2 destaca os resultados feitos através da comunicação com redes *Wi-Fi*

e na Tabela 3, são apresentados os resultados com a utilização de *GPRS* para a comunicação.

Técnica / Tipo de Serviço	**Pontos de Interesse**		**Meu Local**	
	TMR (s)	**DP** (s)	**TMR** (s)	**DP** (s)
0	1,12	0,32	2,87	0,23
1	2,02	0,17	3,11	0,27
2	2,39	0,40	3,39	0,34
3	6,02	0,36	8,56	0,55
4	2,47	0,87	3,67	0,29

Tabela 2 – Tempo Médio de Resposta com *Wi-Fi*

Técnica / Tipo de Serviço	**Pontos de Interesse**		**Meu Local**	
	TMR (s)	**DP** (s)	**TMR** (s)	**DP** (s)
0	1,57	0,21	3,32	0,57
1	2,91	0,38	4,39	0,46
2	3,15	0,33	4,79	0,63
3	8,34	0,87	10,26	1,01
4	3,24	0,27	5,29	0,71

Tabela 3 – Tempo Médio de Resposta com GPRS

Os tempos de resposta podem ser considerados aceitáveis, se comparados com o tempo gasto com a determinação da localização através do receptor *GPS* embutido no celular. Mesmo sabendo que o tempo de localização, utilizando essa técnica, sofre variação excessiva, foi feito um levantamento do tempo médio gasto em tal procedimento que foi de aproximadamente 22 segundos na primeira vez.

Outro importante fator de comparação foram os resultados da execução do serviço com a utilização de *GPS*. Experimentos que tiveram a localização aferida pelo dispositivo móvel também foram realizados e verificou-se o tempo gasto com o acesso ao servidor

confiável e a espera do retorno das requisições representou, em média, apenas 27,59% do tempo total da requisição.

5.3 Escalabilidade

Os experimentos apresentados anteriormente foram efetuados apenas para a verificação do tempo de resposta observado no dispositivo móvel, em comparação com o tempo gasto na determinação da localização. Sendo assim, não são conclusivos no que diz respeito à utilização do servidor com sobrecarga de requisições. Visando uma avaliação concreta da capacidade do servidor com relação ao número de requisições recebidas simultaneamente e o tempo de resposta verificado com sobrecarga, alguns testes de escalabilidade foram efetuados.

Para a execução desses testes foi criada uma aplicação que pudesse ser executada em computadores, de forma a simular o comportamento da aplicação cliente presente no dispositivo móvel. A aplicação desenvolvida para o teste era capaz de efetuar requisições de todos os níveis e tipos de serviço ao servidor confiável, de maneira concorrente, baseado na utilização de *threads*. Cada *thread* era responsável por fazer requisições de um único tipo de serviço durante um tempo pré-determinado. Para um cálculo de tempo de resposta exato, cada *thread* se conectava ao servidor, requisitava o serviço, aguardava a resposta e, assim que esta chegasse, marcava o tempo de resposta da requisição, fechava o fluxo da conexão e começava a execução do início novamente.

O número de *threads* durante a execução deveria ser sempre múltiplo de dez, uma vez que foram testados dois serviços para cinco níveis de privacidade. Um aspecto importante a ser definido nesse momento do teste foi a determinação do número de computadores que deveriam executar e a quantidade de *threads* executando em cada computador. Para a determinação de um valor ideal a ser utilizado nos testes, foram executados testes iniciais com dois, quatro, e seis computadores e com número variável de threads de cinquenta a cento e cinquenta. Definiu-se que o número ideal de *threads* realizando requisições deveria ser cem, devido ao fato de que, com quantidade inferior de *threads*, o total de requisições realizadas não era o melhor possível; já com quantidade superior, o tempo de resposta acabava sendo prejudicado por questões de controle local, como troca de contexto entre *threads* e outras questões de escalonamento. Com relação ao número de computadores clientes executando a aplicação de teste, chegou-se à conclusão de que a quantidade ideal

seria quatro, uma vez que, com dois, o número de requisições não foi expressivo e, com seis o número de requisições perdidas foi bem alto.

Uma vez definidos os valores para os números de computadores e de *threads* ideais para a execução dos testes, outro importante aspecto precisou ser tratado. A utilização do *deCarta Mobile Server* como provedor *LBS* não poderia ser feita de maneira indiscriminada, uma vez que a conta criada para os testes possuía restrições quanto ao número de requisições diárias.

Para solucionar tal problema, foi utilizada a seguinte estratégia: para cada nível e serviço foram realizadas duas mil requisições ao servidor confiável. Do total de requisições, metade retornava a resposta real com uma consulta ao provedor *LBS*, enquanto a outra metade retornava valores pré-definidos armazenados na memória do servidor confiável. Dessa forma, foi calculado o coeficiente de aumento a ser inserido nos tempos médios finais calculados com os testes. Por exemplo, ao tomar como base uma requisição de ponto de interesse mais próximo com o nível médio de privacidade, verificou-se que o tempo de resposta cuja consulta foi repassada ao provedor *LBS* foi de 2000 milissegundos e o tempo de resposta da mesma requisição, sem que fosse consultado o provedor *LBS*, foi de 1500 milissegundos, logo o coeficiente de aumento foi de 500 milissegundos.

Definidos todos os parâmetros a serem utilizados nos testes de escalabilidade, seguiu-se então à execução dos mesmos. Cada aplicação teste foi executada em cada um dos quatro computadores simultaneamente e tiveram duração de cinco minutos. Os testes foram executados sem interferências externas de rede que pudessem ocasionar atrasos resultantes de tráfego indesejado e, além disso, foram repetidos por três vezes para evitar alguma outra possível interferência externa.

Como resultado dos testes, o servidor recebeu em média aproximadamente quinhentas requisições por segundo, sendo que a perda resultante da sobrecarga foi inferior a 0,005 por cento do total de requisições submetidas. A Tabela 4 apresenta os resultados do tempo médio de resposta (*TMR*) e do desvio padrão (*DP*), ambos em segundos, para cada nível de privacidade e para cada um dos serviços testados. Pode ser verificado que, mesmo com desvio padrão considerável, o tempo de resposta observado com o elevado número de requisições é satisfatório, se considerarmos esse tempo como espera de uma aplicação para dispositivos móveis.

Nível de Privacidade / Tipo de Serviço	Busca por pontos de Interesse		"Meu Local"	
	TMR (s)	**DP** (s)	**TMR** (s)	**DP** (s)
Nível 0	0,757	0,358	1,275	0,384
Nível 1	2,376	0,845	2,698	0,862
Nível 2	2,508	0,690	2,861	0,813
Nível 3	8,443	0,918	8,744	1,426
Nível 4	3,763	1,032	4,011	0,973

Tabela 4 – Tempo de Resposta com alta carga no servidor

Com o teste de escalabilidade foi possível comprovar que o *SBPL* se comporta de maneira adequada, mesmo com carga razoável de requisições simultâneas (quinhentas requisições por segundo), apresentando, em geral, resultados melhores do que os tempos de resposta obtidos pelos testes com dispositivo móvel em baixa carga do servidor confiável, como verificado nas Tabelas 2 e 3. Apesar do bom resultado apresentado pelo *SBPL,* caso seja necessário o suporte a cargas superiores às taxas máximas de requisições por segundo obtidas nos testes, novas soluções devem ser planejadas como, por exemplo, a utilização de servidores diferentes para o oferecimento de cada nível de privacidade, o que já reduziria bastante a sobrecarga. Ou, ainda, poderia ser desenvolvida uma abordagem completamente distribuída capaz de realizar balanceamento de carga entre servidores dinamicamente, de acordo com a disponibilidade de cada um.

5.4 Qualidade dos dados

O teste descrito a seguir foi realizado com o intuito de verificar a qualidade dos dados recuperados com a utilização do ajuste de precisão. A idéia básica era verificar se os dados retornados como resposta a uma requisição com informações de localização ajustadas eram semelhantes aos dados retornados de requisições sem o ajuste de precisão. Os testes foram realizados para os dois serviços, localização de pontos de interesse e 'Meu Local'.

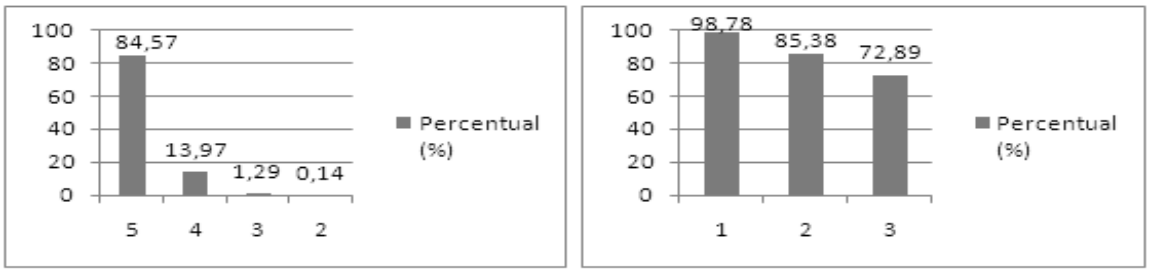
A primeira etapa, que avaliou a qualidade dos pontos de interesse com ajuste de precisão, foi realizada da seguinte maneira: dada uma localização geográfica, foi realizada uma requisição dos cinco restaurantes mais próximos; estes resultados foram comparados a dez requisições com ajustes de precisão sobre o mesmo ponto.

Como a comparação de um único ponto ou de alguns pontos escolhidos aleatoriamente não seria suficiente para um resultado expressivo, foi utilizada a seguinte metodologia para

busca de pontos a serem avaliados. Foram escolhidos dez cidades com maiores quantidades de pontos de interesse. Para cada ponto central, escolhido em cada cidade, foram calculados oitenta e quatro pontos equidistantes entre si que cobriam uma área de dezoito quilômetros quadrados ao redor do ponto de origem. Só então as comparações foram realizadas para cada ponto separadamente. Dessa forma, as requisições feitas para cada ponto foram comparadas a dez requisições ajustadas, totalizando 850 comparações por cidade e 8500 comparações ao todo.

O primeiro aspecto avaliado foi o percentual de respostas iguais presentes nas requisições. Como pode ser observado na Figura 22a, verificou-se que, em quase 85% das respostas, todos os cinco pontos de interesse retornados eram iguais; em seguida, aproximadamente 14% das requisições obtiveram quatro respostas iguais; e pouco mais de 1% das requisições tiveram apenas três resultados iguais.

Outro aspecto avaliado foi a igualdade dos pontos de interesse mais próximos, ilustrado pela Figura 22b. Verificou-se que, em 98,78% das requisições, o ponto mais próximo retornado foi igual; em 85,38%, os dois pontos de interesse mais próximos foram iguais e, em 72,89%, os três primeiros foram iguais.



a) Quantidade de Respostas Iguais b) Pontos mais próximos iguais

Figura 22 - Gráficos comparativos da qualidade dos pontos de interesse com ajuste de precisão

A segunda etapa de avaliação foi a verificação da qualidade dos mapas indicando o local do usuário. Como essa avaliação é bastante subjetiva e depende de análise visual, foram selecionadas trinta localidades com o objetivo de verificar se os mapas retornados continham o local exato da localização, mesmo com um ajuste de precisão. Verificou-se que, com um ajuste da ordem de cento e cinquenta metros, todos os mapas retornados continham o local exato da solicitação. No entanto, ao se aumentar o ajuste de precisão para a ordem de quinhentos metros, o número de mapas que continham a real localização do usuário caiu para treze, ou seja, 43% do total de requisições.

Com os testes realizados, pôde-se verificar que o *SBPL* apresentou bons resultados de tempo de resposta ao oferecer *pull LBS* com garantias de privacidade, mesmo com carga de

aproximadamente quinhentas requisições por segundo submetidas ao *SBPM*. No entanto, caso seja necessário suporte a maiores volumes de carga, deve-se utilizar uma arquitetura distribuída.

Foi verificado também que, além do oferecimento de serviços com bom tempo de resposta, a qualidade verificada nas respostas retornadas que sofreram ajuste de precisão pode ser considerada boa, uma vez que, na maioria dos casos, coincidiu com a resposta sem o ajuste de precisão.

6 Trabalhos Relacionados

Diversos trabalhos foram desenvolvidos visando atenuar as ameaças à privacidade inerentes às aplicações de serviços baseados em localização. Apresentamos, neste capítulo, a descrição de alguns deles: *CoPS*, trabalhos baseados em políticas, outros que empregam o anonimato, *Trusted Server Model*, *LP-Proxy*, *QoP* e, por fim, o *Geopriv*. Tais trabalhos, dentre aqueles presentes na literatura, têm um relacionamento mais estreito com a proposta apresentada nesta dissertação.

6.1 CoPS

Os *LBS* baseados na determinação da localização de outras pessoas (*peer-to-peer*) são caracterizados por peculiaridades no que diz respeito à privacidade dos usuários. Nesses tipos de serviço o usuário, em geral, está de acordo com a liberação de suas informações de localização para um grupo de pessoas conhecidas previamente e que não representam, a princípio, nenhuma ameaça de segurança.

Mesmo considerando que os usuários se conheçam pessoalmente, importantes questões de privacidade de ordem social e psicológica podem vir à tona (SACRAMENTO, 2006). Por exemplo, imagine que, no ambiente de uma faculdade, o professor possa ter acesso à localização de seus alunos orientandos de mestrado e descubra que, durante uma palestra importante do grupo de pesquisa, um deles estava na cantina, que fica em um departamento próximo. Essa situação poderia gerar um constrangimento muito grande entre os dois envolvidos e, até mesmo, prejudicar a relação de confiança que poderia haver antes do ocorrido. Essa é apenas uma das situações que podem ocorrer, caso a liberação de localização de um usuário seja passada para outra pessoa em um momento inoportuno.

Alguns trabalhos descritos na literatura propuseram técnicas que permitem maior controle na liberação das informações de localização para os solicitantes (*requesters*), usuários que solicitam informações de localização de outros.

Sacramento, Endler e Nascimento (2005) apresentam o *CoPS* (*Context Privacy Service*), um serviço que permite aos usuários compartilhar suas informações de contexto, especialmente dados de localização, com as pessoas desejadas, no momento certo e com precisão esperada. Para isso, o serviço proposto conta com a arquitetura de execução geral exibida na Figura 23 (SACRAMENTO; ENDLER; NASCIMENTO, 2005), que funciona da seguinte maneira: inicialmente, o indivíduo que deseja compartilhar suas informações de contexto deve definir as políticas de liberação dos dados (1); paralelamente, o serviço de contexto irá coletar as informações de contexto do indivíduo periodicamente (2); o solicitante pode requisitar o acesso às informações do indivíduo (4), mas deve autenticar-se no *CoPS*, previamente (3), e esperar a verificação das preferências de privacidade do indivíduo cujas informações coletadas dizem respeito (5).

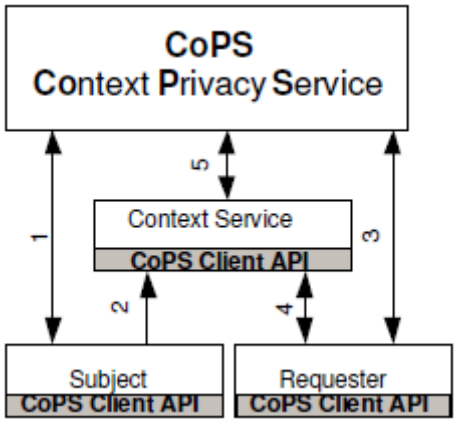


Figura 23 – Arquitetura Geral do CoPS

O *CoPS*, que também é descrito na tese de doutorado de Sacramento (2006), segue um modelo que permite atender às necessidades de privacidade de organizações e indivíduos de maneira hierárquica, sendo para isso definidas políticas com precedências diferentes. Dessa forma, a política da organização tem maior precedência sobre as demais. Por exemplo, caso o administrador do sistema defina, na política da organização, que a localização de todos os usuários poderá ser revelada em casos de emergência (por exemplo, invasão do prédio por grupos terroristas ou em casos de incêndios), a localização será revelada mesmo que a política de um usuário proíba a localização para qualquer outro solicitante naquele momento.

Outro aspecto definido no modelo seguido pelo *CoPS*, que visa impedir a criação de situações constrangedoras entre usuários de *peer-to-peer*, é a possibilidade da negação aceitável, uma forma de se rejeitar a liberação da informação solicitada sem que o solicitante saiba diretamente que ela foi rejeitada. Para isso, além das opções de liberar e negar acesso, existe também a opção não-disponível que pode ser enviada como resposta ao solicitante.

Para a representação das regras de privacidade foram definidos vários campos, de forma a abranger a maior quantidade de restrições possível. Dentre os campos que compõem as regras destacam-se:

Subject, que indica o usuário cujas informações de contexto são tratadas na regra. *Requester*, para representar o usuário que solicita informações de contexto do *subject*. *Precision*, para indicar a precisão característica das informações de contexto a serem liberadas. *Temporal Restriction*, que permite a representação das restrições concernentes à data e hora para a liberação das informações. Por fim, o campo *Result*, que indica o resultado a ser aplicado a uma solicitação de liberação que se encaixe nas regras acima. Os valores para esse campo podem ser: "*Not Available*", "*Ask me*", "*Grant*" e "*Deny*". Tais valores indicam respectivamente: não disponível; solicitar autorização direta do usuário, autorizar e negar a liberação da informação solicitada.

É importante ressaltar que o solicitante pode ser um grupo de usuários ao invés de um usuário específico. Dessa forma, a seguinte regra poderia ser definida por um professor de uma universidade: minha localização não estará disponível no período das doze às catorze horas durante a semana, para meus alunos orientados de mestrado.

Um trabalho parecido com o *CoPS* é a *Confab* ou *ContextFabric*, que é uma infra-estrutura projetada com o intuito de simplificar a criação de aplicações ubíquas sensíveis à privacidade (HONG;LANDAY, 2004). Os autores apresentam uma arquitetura e um conjunto de técnicas que permitem aos desenvolvedores construírem aplicações sensíveis à privacidade para um grupo de usuários. Os problemas abordados no desenvolvimento da *Confab* são parecidos com os discutidos por Sacramento (2006) e a principal diferença entre os trabalhos é o mecanismo de coleta de informações de contexto. No *CoPS* a coleta é realizada através da *MoCA (Mobile Collaboration Architecture)*, uma arquitetura específica de provisão de contexto *(*SACRAMENTO et al. 2005*)*, já a coleta de

informações de contexto na *Confab* é feita dentro da mesma arquitetura de software (SACRAMENTO, 2006).

O *CoPS* poderia ser utilizado para o oferecimento de p*eer-to-peer LBS* para os usuários de telefonia móvel, com algumas adaptações no provedor de informações de contexto, uma vez que a arquitetura *MoCA* oferece suporte à determinação da localização, inicialmente, apenas com base nos pontos de acesso sem fio. Dessa forma, o *CoPS* e o *SBPL* podem ser considerados complementares no que diz respeito ao oferecimento de serviços baseados em localização com garantias de privacidade, abrangendo, juntos, considerável parte dos *LBS* disponíveis.

Além de poder ser considerado complementar ao *CoPS*, o *SBPL* utilizou parte do embasamento teórico apresentado por Sacramento (2006) para a definição dos requisitos de privacidade que direcionaram a proposta e desenvolvimento durante a realização do trabalho.

6.2 Políticas

O trabalho de Myles, Friday e Davies (2003), que apresenta o *LocServ*, questiona o controle da liberação das informações de localização através do questionamento direto ao usuário durante cada requisição. Desta forma, sua privacidade não seria invadida, uma vez que ele teria total controle sobre as informações que seriam liberadas. No entanto, este método pode tornar-se bastante inoportuno, exigindo a atenção do usuário com frequência exagerada.

O *LocServ* busca tratar destes dois requisitos conflitantes dos sistemas baseados em localização – a necessidade dos usuários em controlar sua privacidade de localização e a necessidade de minimizar a demanda de atenção do usuário. Para isto, é proposto um mecanismo automatizado para controle da liberação das informações pessoais baseado na arquitetura apresentada na Figura 24 adaptada de Myles, Friday e Davies (2003).

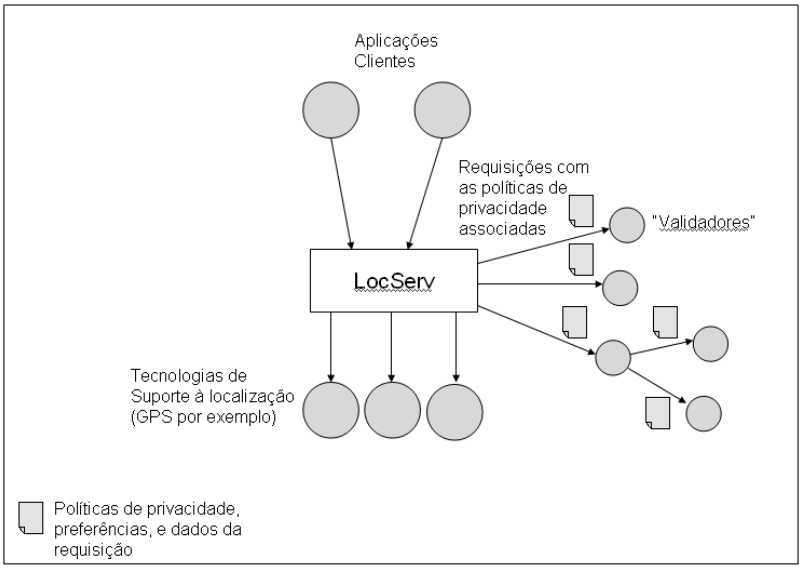


Figura 24- Arquitetura do *LocServ.*

Segundo proposto pelos autores desse trabalho, os usuários devem se inscrever em um ou mais servidores de localização e registrar seus requisitos de privacidade em cada um. Estes requisitos são chamados no sistema de *validators*, ou validadores, devido ao fato de verificarem se a liberação dos dados poderá ser executada ou não. Cada requisição das informações de localização de um usuário feita ao *LocServ* deve ser acompanhada das políticas de privacidade implementadas pela aplicação interessada nos dados. Os *validators,* por sua vez, terão a responsabilidade de determinar se as políticas de privacidade estão de acordo com as preferências do usuário e permitir a liberação dos dados ou impor algum tipo de restrição especial, tal como redução da precisão dos dados de localização.

Para a representação das políticas de privacidade pelas entidades que requisitam a localização do usuário, é proposta a utilização de um esquema semelhante ao padrão *P3P (Platform for Privacy Preferences Project)* (CRANOR et al., 2001) para a *Web.* Obviamente, no contexto de serviços baseados em localização, são necessários acréscimos de termos e algumas adaptações para a devida adequação.

Já para permitir a representação das preferências de privacidade dos usuários e uma possível checagem entre tais preferências e as políticas apresentadas pelos provedores do serviço, é sugerida a utilização da *APPEL (A P3P Preference Exchange Language),* linguagem de troca de preferências *P3P* (CRANOR; LANGHEINRICH; MARCHIORI, 2002).

O trabalho apresentado por LANGHEINRICH (2002), chamado de sistema consciente de privacidade (*pawS - Privacy Awareness System*), é caracterizado por um esquema parecido com o *LocServ*. Nesta proposta, quando um usuário entra em um ambiente onde suas informações estão sendo solicitadas, um aviso de privacidade (*privacy beacon*) anuncia a coleta de dados de cada serviço e suas respectivas políticas de privacidade. Em seguida, um *proxy* de privacidade checa estas políticas com as preferências de privacidade predefinidas. Se estiverem de acordo, o serviço poderá coletar informações, caso contrário, o sistema notifica o usuário que poderá, ou não, permitir a coleta.

Estas técnicas são chamadas por alguns autores de políticas (GÖRLACH; TERPSTRA; HEINEMANN, 2004), pois atuam basicamente através da comparação entre as preferências de privacidade dos usuários e as políticas que os provedores declaram aplicar no tratamento dos dados de localização. Dessa forma, não é possível garantir que o provedor, que requisita as informações, realmente aplique as políticas no tratamento dos dados. Uma forma de assegurar que a privacidade realmente seja respeitada nesses casos é a definição de uma legislação rigorosa que reprima provedores que não aplicam as políticas informadas, além de um criterioso processo de fiscalização.

Pode-se dizer que o *LocServ* possui aspectos semelhantes ao sistema proposto, no que diz respeito à possibilidade de definição das preferências de privacidade dos usuários e posterior verificação das mesmas. No entanto, os *validators* atuam no momento da liberação das informações de localização apenas. No *SBPL*, as preferências de privacidade dos usuários são determinadas em níveis, e cada nível corresponde à aplicação de diferentes técnicas de privacidade.

Resumindo a diferença entre os trabalhos baseados em políticas e o *SBPL*, pode-se considerar que as políticas partem do princípio que diversos serviços podem solicitar a localização do usuário, sendo necessária a automação da liberação das informações (*push LBS*) e, além disso, não tratam claramente dos serviços do tipo *pull LBS*. O *SBPL* aqui apresentado implementa um modelo de execução baseado em níveis de privacidade para os serviços *pull LBS* e um novo modelo desvinculado do provedor para os serviços *push* LBS.

6.3 Anonimato

Diversos trabalhos buscaram, no oferecimento de anonimato, os meios para a obtenção de garantias de privacidade, seja através da ocultação, do envio de requisições falsas ou da utilização de *Mix-Zones*.

6.3.1 Ocultação

A primeira abordagem que visa a obtenção do conjunto de anonimato é baseada na ocultação de informações. Segundo esta abordagem, duas técnicas são utilizadas para garantir que a requisição de um usuário sempre esteja inserida em um conjunto de anonimato, ocultação espacial e ocultação temporal.

A utilização das duas técnicas ocorre da seguinte maneira: no momento em que o usuário realiza uma requisição, é feita a verificação da existência de outras requisições provenientes da mesma região; em caso da não-existência de um conjunto de anonimato, é realizada a redução da precisão das informações de localização (ocultação espacial). Caso o conjunto de anonimato ainda não tenha sido obtido, é inserido um atraso na resposta da requisição para aguardar o recebimento de outras solicitações da área ajustada (ocultação temporal). Só então, as requisições são encaminhadas ao provedor *LBS*. Essa abordagem utiliza o conceito de *k-anonymity*, permitindo a utilização de conjuntos de anonimato de tamanho variado.

No trabalho de Gruteser e Grunwald (2003), esta técnica é utilizada com a proposta de um *middleware* capaz de identificar as localizações e verificar quais ações tomar mediante as condições verificadas. Tais ações consistem em determinar se as informações devem ter sua precisão reduzida ou se é necessário esperar um tempo até que outras requisições próximas àquela localização sejam realizadas.

Gruteser e Grunwald apresentaram também um estudo de caso, no qual se utilizou uma simulação baseada nos volumes de tráfego de algumas cidades, envolvendo desde grandes avenidas com um volume intenso de tráfego até ruas com pequena movimentação de veículos. Além disso, a simulação colocou a restrição de que o tamanho do conjunto de anonimato deveria ser de, no mínimo, cinco usuários.

Como esperado, nos locais onde o fluxo de automóveis era mais elevado, o conjunto de anonimato mínimo esperado foi obtido com maior facilidade, necessitando-se esperar menor tempo para a realização de requisições no mesmo local. Já em locais onde o volume

de tráfego era menor, a obtenção do conjunto de anonimato foi dificultado, acarretando algumas vezes a inserção de elevado atraso na resposta da requisição.

Tanto Gruteser e Grunwald (2003) como Mokbel, Chow e Aref (2006), utilizam um algoritmo baseado em uma *quadTree*, para realizar a ocultação das informações espaciais, cada trabalho com suas peculiaridades. A idéia básica do algoritmo é que cada localização pode ser dividida em quatro novos quadrantes, e isso pode acontecer recursivamente em cada quadrante, como pode ser visto na Figura 25. Cada ponto indica um usuário presente naquele quadrante.

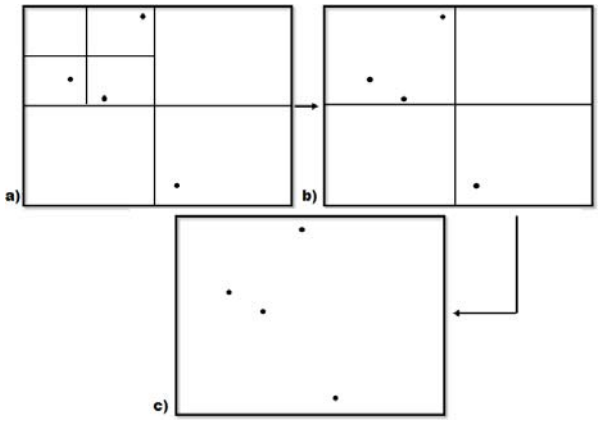


Figura 25 - QuadTree utilizada na ocultação das informações espaciais

Suponha que o usuário posicionado mais à esquerda realize uma requisição, e que o conjunto de anonimato requerido seja de dois usuários. O algoritmo de ocultação com intervalo adaptável *AIC (Adaptive-interval cloak*) (GRUTESER; GRUNWALD, 2003) busca primeiro o quadrante mais interno, ilustrado pela Figura 25a. Ao se realizar o ajuste de precisão, como verificado na Figura 25b, é utilizada a área correspondente ao quadrante anterior que envolve três usuários. Caso o conjunto de anonimato ainda não tivesse sido obtido, o ajuste de precisão seria feito para o quadrante mais externo novamente, englobando a área total apresentada na Figura 25c.

Kalnis (2007) apresenta algumas alternativas que buscam a maior rapidez no cálculo da área do conjunto de anonimato e, ainda, a obtenção de uma área inferior à área calculada pelos trabalhos anteriores, já que o *AIC* utiliza, para cada redução da precisão, um aumento em quatro vezes o tamanho da área original. Caso as requisições sejam feitas em períodos e locais em que não existem outros usuários próximos realizando requisições, seria difícil calcular uma área razoável para o conjunto de anonimato utilizando-se o *AIC*.

O *SBPL* utiliza uma técnica baseada nas técnicas de ocultação espacial e temporal para o oferecimento do nível Alto de privacidade. No entanto a utilização de técnicas desse tipo pode ocasionar atraso excessivo no tempo de resposta, caso existam dificuldades em compor o conjunto de anonimato. Esse atraso pode até mesmo inviabilizar a utilização de alguns serviços como, por exemplo, a busca por restaurantes próximos. Para solucionar tal situação, o *SBPL* realiza a ocultação de informações espaciais e temporais, contudo o tempo máximo de espera por novas requisições provenientes da mesma área é de, no máximo, cinco segundos.

6.3.2 Requisições Falsas

Uma alternativa para tentar evitar a identificação dos usuários, quando é feita uma requisição solitária ou quando não existe um conjunto de anonimato razoável, é a utilização de informações falsas aos provedores *LBS*. Segundo esse mecanismo, cada usuário, ao realizar a requisição, envia não só sua localização atual, mas uma série de localizações reais nas quais ele poderia estar, sendo que apenas uma destas é sua localização exata (CHENG; ZHANG; TAN, 2005) e (KIDO; YANAGISAWA; SATOH, 2005).

A Figura 26 esquematiza o funcionamento desta técnica. O dispositivo móvel, no momento da realização da requisição, envia uma mensagem com várias informações sobre localização, sendo que apenas uma delas é a correta. O provedor, por sua vez, processa a requisição e, na mensagem de retorno, inclui a resposta da requisição para todas as localizações. No momento em que a resposta chega ao dispositivo móvel, verifica-se quais são as informações relevantes que devem ser utilizadas pela aplicação e as restantes são descartadas. É válido ressaltar que todas as informações de localização enviadas ao provedor *LBS* contêm posições reais, que são armazenadas no dispositivo móvel com o decorrer do tempo.

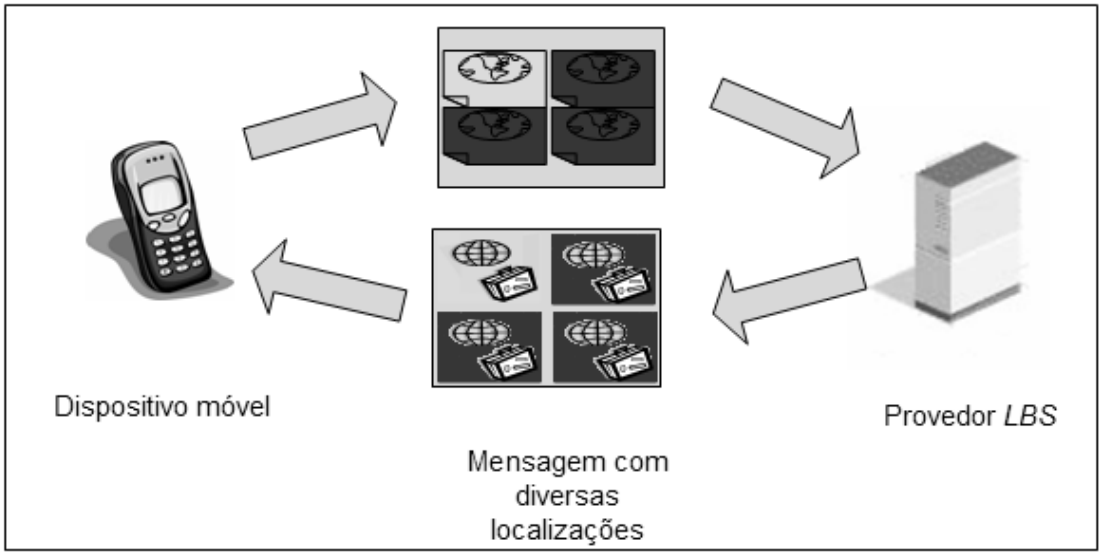


Figura 26 - Esquema das requisições falsas

Apesar de esta solução realmente prover o anonimato na maioria dos casos, já que o servidor de localização não poderá definir exatamente qual é a localização do usuário, elas ocasionam aumento nos custos de comunicação, uma vez que as requisições, ao invés de conterem apenas uma localização, irão conter várias. Além disso, o custo envolvido na resposta dos provedores *LBS* será aumentado, já que deverão ser buscadas respostas para cada uma das localizações enviadas pelos clientes.

A utilização de várias informações de localização não garante a não-identificação dos usuários, no caso em que são feitas várias requisições seguidas. A identificação poderá ocorrer a partir do momento em que o provedor consegue identificar um padrão de movimentação.

Considere a situação em que o usuário realiza a primeira requisição com quatro localizações e, alguns minutos depois, realiza uma nova requisição com outras quatro localizações. Se três das quatro localizações mais recentes são totalmente distintas das informações antigas, o provedor pode considerar que estas são as informações falsas, já que, em um período muito curto de tempo, o usuário não poderia se mover para locais tão discrepantes. Dessa forma, as posições reais do usuário poderiam ser identificadas.

Kido, Yanagisawa e Satoh (2005) propõem um algoritmo que soluciona esse problema, sendo que, em requisições consequentes, todas as localizações submetidas seguirão padrões de movimentação, evitando a possibilidade de identificação dos usuários pela eliminação de informações discrepantes. São propostas também algumas alternativas

para a diminuição dos tamanhos das mensagens, tanto da requisição quanto da resposta. Para diminuir o tamanho das requisições é proposta uma maneira de agrupar as localizações enviadas, utilizando-se um relacionamento entre as coordenadas. Já para diminuir os tamanhos dos custos de resposta, são propostos alguns artifícios como a utilização de abreviaturas nas mensagens de resposta.

O *SBPL* utiliza um esquema parecido com o das técnicas de envio de requisições falsas para o oferecimento do nível Garantido de privacidade. Contudo, no modelo utilizado, ao invés do envio de várias informações de localização em uma única requisição, a posição exata é encaminhada ao servidor confiável que calcula cinco novas posições, baseado no ajuste de precisão do *SBPL*. Posteriormente, o servidor confiável envia cinco requisições embaralhadas ao provedor *LBS*, das quais apenas uma será encaminhada ao usuário. Além de reduzir o custo de implementação na aplicação cliente, esta técnica minimiza consideravelmente a possibilidade de identificação do usuário, devido a dois fatores. O primeiro é que as informações de localização são enviadas em requisições diferentes, o que já impede a dedução direta do provedor de que tais dados foram originados de um mesmo usuário. O segundo aspecto é que as informações falsas são todas calculadas com base na posição original do usuário. Sendo assim, as informações não conterão dados tão discrepantes, como poderá ocorrer com frequência nos demais casos apresentados de envio de requisições falsas.

6.3.3 Mix-Zones

O trabalho descrito por Beresford e Stajano (2003) foi baseado na idéia de *mix* criada por Chaum (1981). Uma rede de *mixes* é uma rede de armazenamento e encaminhamento de pacotes que oferece suporte ao anonimato. Ela é composta de uma sequência de *mixes*, que são nodos responsáveis por realizar o encaminhamento de pacotes, de forma a não permitir que um observador relacione um pacote que chega aos pacotes de saída. Além disso, a técnica é acompanhada de vários níveis de criptografia assimétrica, o que dificulta ainda mais a identificação dos remetentes e emissores das mensagens.

Análogo à idéia das redes *Mix*, foi introduzido o conceito de *Mix-Zones*, que são regiões espaciais de tamanho máximo, nas quais existem usuários que não estão registrados em nenhum dos serviços de localização. Em contraste, existe o conceito também de *Application-Zones*, que são regiões onde os usuários estão registrados em serviços de localização. Enquanto os usuários percorrem as *Mix-Zones*, seus pseudônimos

são trocados constantemente, permitindo que haja uma mistura entre as identificações dos usuários. Dessa forma, quando os usuários atingirem uma *Application Zone*, torna-se difícil identificá-los, já que eles podem ter obtido vários pseudônimos diferentes.

A troca constante de pseudônimos não garante que os usuários não serão identificados, pois, em casos onde as *Mix-Zones* tenham um tamanho muito grande, ou se o conjunto de anonimato for pequeno, a partir do rastreamento das localizações, pode-se inferir que um conjunto de pseudônimos pertenceu a um mesmo usuário. Além disso, o grau de complexidade inerente à modelagem e implementação das *Mix Zones* em ambientes reais de execução *LBS* é bastante elevado (BHASKAR; AHAMED, 2007).

A única característica presente na abordagem das *Mix-Zones* que pode ser observada no *SBPL* é a reordenação das mensagens a serem encaminhadas aos provedores *LBS* que ocorre no servidor confiável, tanto no nível Alto quanto no nível Garantido de privacidade.

6.4 Trusted Server Model

O trabalho proposto por Martucci et al. (2006) apresenta um modelo para o aumento da privacidade em serviços baseados em localização, com base na idéia de que o provedor de telecomunicações ou operadora de telefonia celular atue como um servidor confiável.São apresentados protocolos para a comunicação entre as entidades envolvidas durante a prestação do serviço, abrangendo os serviços do tipo *pull*, *push*, e *peer-to-peer*. Além disso, é proposto também um protocolo de subscrição aos *LBS*.

A comunicação, tanto entre o dispositivo móvel e o servidor confiável, quanto entre o servidor confiável e o provedor *LBS*, é realizada com a utilização de técnicas criptográficas para evitar que atacantes maliciosos, que têm acesso ao meio, possam captar a comunicação e, consequentemente interceptar a localização dos usuários e os serviços que este está utilizando.

O modelo de servidor confiável tem o foco no modelo de execução e comunicação envolvidos na execução *LBS* e não trata das preferências de privacidade do usuário como, por exemplo, a precisão com a qual o usuário deseja que seus dados sejam liberados.

O *SBPL*, assim como o modelo descrito nesta seção, é caracterizado pela presença de um servidor confiável e pela utilização do canal seguro de comunicação entre o dispositivo móvel e o servidor confiável. No entanto, o modelo de execução dos serviços no *SBPL* é

bastante diferenciado, tanto no que diz respeito à participação da operadora de telefonia celular, quanto nas técnicas de privacidade utilizadas.

6.5 LP-Proxy

O *LP-Proxy* (RIBEIRO e ZORZO, 2008) é um *proxy* localizado entre o dispositivo móvel e o provedor *LBS*, que oferece garantias de privacidade através do ajuste de precisão e do canal seguro de dados. Segundo esta proposta, todas as requisições de serviços baseados em localização provenientes do celular passam pelo *LP-Proxy* e sofrem o ajuste de precisão para diminuir a possibilidade de identificação dos usuários pelos provedores *LBS*.

O *LP-Proxy* oferece suporte apenas aos serviços do tipo *pull LBS* e com apenas o mecanismo de ajuste de precisão. O *SBPL* possui o mesmo modelo de arquitetura e execução do *LP-Proxy*, mas permitiu a utilização de níveis no suporte à privacidade em serviços *pull LBS* e criou um novo modelo para a execução de aplicações *LBS* nas quais o usuário não realiza a requisição diretamente (*push LBS*).

6.6 QoP – Quality of Privacy

Outra abordagem é a utilização da qualidade de privacidade (*QoP – Quality of Privacy*) (TENTORI et al., 2005) de forma análoga à qualidade de serviço (*QoS – Quality of Service*), em redes de computadores, para garantir a manutenção da privacidade de usuários que utilizam serviços baseados em localização.

Para esclarecer essa analogia, será utilizado um exemplo similar àquele apresentado pelos autores do trabalho. Suponha que dois médicos estejam discutindo algo sobre uma imagem de raio-X de um paciente, através de uma vídeo-conferência. Ao se utilizar qualidade de serviço, um usuário pode solicitar certo comportamento da rede na realização da aplicação, como reserva de recursos para certos serviços. Para isso, os médicos expressariam suas necessidades qualitativamente, como, por exemplo, conferência com qualidade de *DVD*. E a rede, por sua vez, utilizaria parâmetros quantitativos como largura de banda, atraso, dentre outros parâmetros inerentes à comunicação via rede.

Com base na qualidade de privacidade, os serviços baseados em localização poderiam ser tratados de maneira similar. Por exemplo, o usuário pode definir, de maneira qualitativa, sua restrição de privacidade como, por exemplo, fazer *login* no sistema de maneira anônima. Esta restrição deve ser então mapeada para valores quantitativos de

cinco elementos contextuais: localização, identidade, acesso, atividade e persistência para que a privacidade desejada pelo usuário seja garantida.

Essa abordagem implica em mudanças dos valores dos elementos contextuais, dependendo do ambiente de execução e das necessidades de cada usuário, o que implica na adaptação de uma ontologia proposta pelos autores.

6.7 Geopriv

O grupo de trabalho *GeoPriv (Geographic Location/Privacy)* (CUELLAR et al., 2004), vinculado à *IETF (Internet Engineering Task Force)*, tem como objetivo tratar das aplicações que envolvam troca de informações de localização. O grupo propõe que a obtenção e transferência de tais informações para os serviços de localização sejam realizadas com segurança e garantia da privacidade dos indivíduos envolvidos.

A base da abordagem deste grupo de trabalho para obter a privacidade é a criação de objetos de localização (*LO - Location Objects*), que conterão as informações de localização dos usuários e outros campos, incluindo: identificação ou pseudônimo do usuário, informações de tempo, regras de privacidade etc.

Além disso, são definidos diversos papéis envolvidos durante a execução dos serviços baseados em localização, como o criador das regras (*Rule Maker*), que é o indivíduo que tem autorização para determinar as regras de privacidade para um potencial alvo de localização.

Nesse modelo, também é definido o provedor de acesso (*AP - Access Provider)*, domínio que provê o acesso inicial à rede, que pode ser, por exemplo, a operadora de telefonia e, ainda, o mantenedor das regras (*Rule Holder*), que armazena as regras de privacidade para receber, filtrar e distribuir objetos de localização.

Apesar de uma série de definições dos papéis e requisitos de privacidade que, inclusive, se assemelham em parte com o *SBPL*, o *Geopriv* não trata da gerência na liberação das informações nem dos tipos de regras de privacidade utilizadas para controlar a liberação (MYLES; FRIDAY; DAVIES, 2003).

6.8 Observações Finais

Os trabalhos relacionados apresentam diversas soluções que visam tratar do problema da privacidade na execução de LBS. Alguns deles abordam as questões envolvidas na

liberação de informações de localização para outros usuários e apresentam soluções que levam em consideração as restrições necessárias para esse tipo de serviço. Os trabalhos focados em soluções de privacidade para *peer-to-peer LBS* abrangem uma categoria com restrições diferentes de privacidade das tratadas no trabalho aqui apresentado. Desta forma, o *SBPL* pode ser considerado complementar a estes trabalhos, uma vez que busca o oferecimento de privacidade para aplicações do tipo *pull e push LBS* executadas em telefones celulares.

Outros trabalhos ofereceram técnicas capazes de minimizar as ameaças à privacidade do usuário, baseados no anonimato, na utilização de políticas ou na implementação de qualidade de privacidade. Foram também investigados trabalhos que apresentaram modelos de execução *LBS* que tratavam principalmente de questões técnicas de comunicação, características do ambiente de execução e das entidades envolvidas em tais serviços.

Embora grande esforço tenha sido empregado na busca de soluções que ofereçam privacidade em *LBS*, os trabalhos relacionados que se aplicam aos casos de *pull e push LBS* não apresentam resultados concretos na forma de um possível sistema que permita a utilização em ambientes práticos. Alguns deles, apresentam abordagens para a utilização em redes de telefonia móvel, como o *Geopriv*, o *LocServ* e as *Mix Zones*, entretanto não apresentaram soluções técnicas para serem executadas em ambientes reais.

O trabalho aqui descrito buscou oferecer garantias de privacidade para os usuários de telefonia móvel em geral. Foi proposto e implementado um novo modelo de níveis de privacidade para a utilização de serviços *pull LBS*. A possibilidade de configuração das preferências de privacidade garante aos usuários duas vantagens: a primeira delas é a possibilidade de escolher o nível de privacidade que se encaixa no seu perfil, uma vez que, como já discutido anteriormente, diversos fatores podem influenciar nas preferências de privacidade dos indivíduos; a segunda vantagem é a possibilidade de utilização de serviços que seriam inviabilizados devido à utilização de técnicas de privacidade, isto é, caso o usuário deseje utilizar um serviço que exija elevada precisão ele pode abrir mão de sua privacidade e utilizar o serviço.

Desta forma, o usuário não fica desprotegido aos ataques de indivíduos maliciosos que tentam roubar informações pessoais e, ao mesmo tempo, não é obrigado a abrir mão de serviços aos quais deseja ter acesso e que exijam informações mais precisas.

Além disso, o trabalho aqui descrito apresentou um novo mecanismo de execução de *push LBS*, que garante total privacidade ao usuário. Diferentemente das outras abordagens, como *Mix-Zones* e *LocServ*, o novo modelo de execução garante que as informações de localização do usuário serão manipuladas apenas pelo dispositivo móvel e não serão armazenadas ou repassadas aos provedores *LBS*.

7 Conclusões e Trabalhos Futuros

A utilização de serviços baseados em localização está se tornando comum no cotidiano das pessoas, especialmente dos portadores de telefones celulares com capacidade de localização. No entanto, questões de privacidade vêm à tona quando se trata da manipulação de informações de localização.

A questão da manutenção da privacidade dos usuários na execução de *LBS* tem sido amplamente estudada e grande esforço tem sido empregado na busca de soluções que a possam garantir.

Um fato a ser notado é que diferentes categorias *LBS* apresentam diferentes restrições de privacidade. Alguns trabalhos apresentam soluções específicas para aplicações *peer-to-peer LBS* que envolvem uma série de restrições distintas das demais aplicações *LBS*. No entanto, pouco se vê de resultados concretos e práticos que viabilizem a utilização de *pull e push LBS*, com garantias de privacidade para o ambiente de telefonia móvel.

Este trabalho apresenta um sistema que permite a execução de *pull* e *push LBS* com garantias de privacidade para o ambiente de telefonia móvel, denominado Sistema Baseado em Privacidade de Localização (*SBPL*). Como os dois serviços atendidos apresentam características de execução diferenciadas e, consequentemente, requisitos de privacidade distintos, este trabalho apresenta um modelo de execução diferenciado para cada serviço.

O modelo de execução *pull LBS* é caracterizado por um mecanismo de níveis que oferece diferentes garantias de privacidade com base na utilização de técnicas como anonimato, ajuste de precisão, canal seguro de dados, dentre outros. Desta forma, pretendeu-se atender a diferentes serviços e restrições de usuários. A possibilidade de escolher o nível de privacidade desejado e as medidas a serem utilizadas no ajuste de precisão garante ao usuário um ambiente personalizado, podendo ser determinadas as preferências de privacidade e a maneira como seus dados serão tratados

Já o modelo de execução *push LBS* foi planejado de forma que não permita que as informações de localização dos usuários sejam disponibilizadas para os provedores do serviço. Isso foi conseguido através de um modelo de execução desvinculado do provedor *LBS*.

O *SBPL* segue as recomendações dos guias de privacidade da *OECD* e da *EPC*, no que se refere à coleta, manipulação e liberação dos dados pessoais dos usuários, especialmente

dados de localização. Além disso, considerando-se que a interoperabilidade é facilitada pela utilização de padrões, o *SBPL* oferece suporte à realização de requisições aos provedores *LBS* por meio do padrão de comunicação *OpenLS*.

Também foram realizados testes em um ambiente de execução *LBS* que comprovaram a eficiência do *SBPL*, apresentando tempos de resposta satisfatórios e dados com boa qualidade, mesmo ao se realizar operações de privacidade sobre as informações de localização. Dessa forma, pôde-se confirmar a possibilidade de utilização do sistema em ambientes reais.

Em suma, o *SBPL* oferece um ambiente confiável para a execução de serviços baseados em localização para celulares, que permite a adequação às preferências de privacidade dos usuários, atende aos princípios dos guias de privacidade com relação às informações pessoais e ainda conta com serviços de qualidade, mesmo com a utilização de técnicas de proteção à privacidade.

É válido ressaltar três aspectos quanto ao desenvolvimento deste trabalho: o primeiro é que o *SBPL* não oferece garantias totais de privacidade, uma vez que tal situação é praticamente impossível dado o alto grau de subjetividade envolvido na determinação das preferências de privacidade de um usuário e, além disso, alguns ataques podem permitir a identificação do usuário, embora sejam muito pouco viáveis de ocorrer; em segundo lugar, temos consciência de que nem todos os *LBS* oferecidos são suportados pelos modelos de execução propostos; e, ainda, reconhecemos também o fato de que, apesar de propormos uma solução que insere privacidade em *LBS* para telefonia móvel, a solução não será aplicada em grande parte dos serviços, caso não haja interesse dos provedores em oferecer o serviço com a utilização dos padrões de comunicação propostos.

No entanto, acreditamos que existe, sim, um ganho considerável com a proposta do *SBPL*, pois a possibilidade de se oferecer os serviços com garantias de privacidade pode ser um primeiro passo para que usuários e, principalmente, empresas fornecedoras dos serviços percebam os riscos envolvidos na utilização de *LBS* e busquem soluções alternativas que realmente tenham foco na privacidade e bem estar do usuário.

Dentre os trabalhos futuros, destacam-se: a utilização de outras formas de comunicação com provedores LBS, uma vez que o padrão *OpenLS* não é utilizado por todos os provedores *LBS*, e a incorporação de novas técnicas de proteção à privacidade, para que seja possível o oferecimento de novos serviços com garantias de privacidade.

Referências Bibliográficas

BHASKAR, P.; AHAMED, S. I. **Privacy in Pervasive Computing and Open Issues**. In: SECOND INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY (ARES), 2007, Vienna, Áustria. **Proceedings…** pp 147-154.

BELLOTTI, V.; SELLEN, A. **Design for Privacy in Ubiquitous Computing Environments**, In: 3RD EUROPEAN CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK (ECSCW), 1993, Milão, Itália. **Proceedings…** pp. 77-92

BERESFORD, A. R.; STAJANO, F. J. **Location Privacy in Pervasive Computing**. IEEE PERVASIVE COMPUTING, vol. 2 , No. 1, pp 46-55 , 2003.

BETTINI, C.; WANG, X. S.; JAJODIA, S. **Protecting Privacy Against Location-Based Personal Identification.** In: SECOND VLDB WORKSHOP SECURE DATA MANAGEMENT *(SDM)*, 2005, Trondheim, Noruega. **Proceedings…** pp. 185-199.

BOWEN, C. L. III; MARTIN, T. L. **A Survey of Location Privacy and a Approach for Solitary Users.** In: 40TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 2007, Havaii, EUA. **Proceedings…** p 163c.

CAS, J. **Privacy in pervasive computing environments - a contradiction in terms?.** TECHNOLOGY AND SOCIETY MAGAZINE, IEEE Magazine. Vol. 24, No. 1, pp 24-33, 2005.

CHAUM, D. **Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms**. COMMUNICATIONS OF ACM. Vol. 24, No. 2, pp. 84–88, 1981.

CHENG, H. S.; ZHANG, D.; TAN, J. G. **Protection of Privacy in Pervasive Computing Environments**, In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING. 2005, Nevada, USA. **Proceedings...** pp. 242-247.

CLARO, **Claro Localizador.** 2009. Disponível em:
<http://www.claroideias.com.br/portal/site/CIdeias/menuitem.587907fcfbb28d7d7a709520648051a0/&idlocal=56> Acesso em: 29/04/2009.

CRANOR, L.; LANGHEINRICH, M.; MRCHIORI, M.; PRESLER-MARSHALL, M.; REAGLE, J. **P3P - The Platform for Privacy Preferences 1.0 (P3P1.0) Specification**. WORLD WIDE WEB CONSORTIUM, 2001. Disponível em:
<www.w3.org/TR/2001/WD-P3P-20010928> Acesso em: 21/04/2009.

CRANOR, L.; LANGHEINRICH, M.; MARCHIORI, M. **A P3P Preference Exchange Language 1.0 (Appel 1.0)**, working draft, WORLD WIDE WEB CONSORTIUM, 2002. Disponível em: <www.w3.org/TR/P3P-preferences>. Acesso em: 21/04/2009.

CUELLAR, J.R.; MORRIS, J.B.; MULLIGAN, D.K; PETERSON, P., POLK, J. **IETF Geopriv Requirements**. RFC (REQUEST FOR COMMENTS) 3693. 2004. Disponível em: < http://www.ietf.org/rfc/rfc3693.txt>. Acesso em: 18/02/2009

DIERKS, T.; RESCORLA, E. **The Transport Layer Security (TLS) Protocol.** RFC (REQUEST FOR COMMENTS) 4346. 2006. Disponível em: http://www.ietf.org/rfc/rfc4346.txt Acesso em: 29/04/2009.

EPC - European Parliament and the Council, **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**. 1995. Official Journal. L 281, vol. 23/11/1995, pp. 31-50. Disponível em:

<http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett> Acesso em: 18/02/2009.

EPC - European Parliament and the Council, **Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector**. 2002 Official Journal L No.201. Disponível em: <http://www.etsi.org/public-interest/Documents/Directives/Standardization/Data Privacy Directive.pdf> Acesso em: 18/02/2009.

EPC. European Parliament and the Council, **Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/ec**. 2006. Official Journal L No.105, 13
Disponível em:
<http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf> Acesso em: 18/02/2008>. Acesso em: 18/02/2009.

GAYAL, S.; MANICKAM, A. V. **Comparative analysis Of GSM and CDMA technologies "A Security Perspective".** Disponível em: <http://citeseer.ist.psu.edu/cache/papers/cs/26850/http:zSzzSzsangram.8k.comzSzgsmcdma.pdf/comparative-analysis-of-gsm.pdf>. Acesso em: 21/02/2009.

GIS FAQ - **Geographic Information Systems FAQ.** Disponível em: http://www.faqs.org/faqs/geography/infosystems-faq>. Acesso em: 29/04/2009

GETTING I. A. **The Global Positioning System**. IEEE Spectrum, Vol.30, No. 12 pp. 36-38, December 1993.

GOOGLE. **Google Maps Mobile**. Disponível em: <http://www.google.com/gmm>. Acesso: 20/04/2009.

GOOGLE. Política de Privacidade do Google Maps Mobile. Disponível em: http://www.google.com.br/mobile/privacy.html Acesso em: 21/02/2009.

GOOGLE. **Google Maps**. Disponível em: <http://maps.google.com/> Acessado em: 21/02/2009.

GÖRLACH, A.; TERPSTRA, W. W.; HEINEMANN, A. **Survey on Location Privacy in Pervasive Computing**. In: THE FIRST WORKSHOP ON SECURITY AND PRIVACY AT THE CONFERENCE ON PERVASIVE COMPUTING (SPPC), 2004, Vienna, Austria. **Proceedings…** pp. 23-34.

GRUTESER, M.; GRUNWALD, D. **Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking**. In: THE FIRST INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS AND SERVICES (MobiSys), 2003, California, USA. **Proceedings…** pp 31–42.

HALONEN, T.; ROMERO, J.; MELERO, J. **GSM, GPRS and EDGE performance - Evolution Towards 3G/UMTS.** 2. Edition, England: Wiley, 2003

HARLE, R. K.; HOPPER, A. **Deploying and evaluating a location- aware system**. In: THE 3RD INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS (MobiSys), 2005, Nova Yokr, EUA. **Proceedings…** pp. 219-232.

HONG, J. I.; LANDAY, J. A. **An architecture for privacy-sensitive ubiquitous computing**. In: 2ND INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS,

APPLICATIONS, AND SERVICES (MobiSys). 2004, Boston, EUA. **Proceedings** pp. 177-189.

JSSE. **Java Secure Socket Extension (JSSE) Reference Guide for Java Platform Standard Edition 6.** Disponível em: <http://java.sun.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html>. Acesso em: 29/04/09

JUELS, A.; RIVEST, R. L., SZYDLO, M. **The blocker tag: selective blocking of RFID tags for consumer privacy**. In: 10TH ACM CONFERENCE ON COMPUTER AND COMMUNICATION SECURITY, 2003, Washington, EUA. **Proceedings…** pp 103–111.

KALNIS, P.; GHINITA, G.; MOURATIDIS, K.; PAPADIAS, D. **Preventing Location-Based Identity Inference in Anonymous Spatial Queries**, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING (TKDE).Vol. 19, No 12, pp. 1719-1733, 2007.

KIDO, H.; YANAGISAWA Y.; SATOH, T. **An Anonymous Communication Technique using Dummies for Location-based Services.** In: IEEE INTERNATIONAL CONFERENCE ON PERVASIVE SERVICES (ICPS). 2005, Santorini, Greece. **Proceedings…** pp 88-97.

KÜPPER A. **Location Based Services – Fundamentals and Operation.** 1. ed., England: Willey, 2005. 386 p.

LANGHEINRICH, M. **A Privacy Awareness System for Ubiquitous Computing Environments**, In: 4th INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING (UbiComp), 2002, Göteborg, Sweden. **Proceedings…** Lecture Notes in Computer Science, Springer-Verlag. Vol. 2498, pp. 237–245.

LOC – **OMA Location Working Group**. Disponível em: <http://cms.openmobilealliance.org/Technical/LOC.aspx>. Acesso em : 05/02/2009.

LOYTANA, K. **JSR 179, Java Specification Request 179 - API Java Location Final Release 2**. 2006. Disponível em: http://jcp.org/en/jsr/detail?id=179 Acesso em: 29/04/2009.

MARTUCCI, L. A.; ANDERSSON, C.; SCHREURS, W.; FISCHER-HÜBNER, S. **Trusted Server Model for Privacy-Enhanced Location Based Service.** In: 11TH NORDIC WORKSHOP ON SECURE IT-SYSTEMS, 2006, Linköping, Sweden.

MENEZES, A. J.; OORSCHOT, P. V.; VANSTONE, S. A. **Handbook of Applied Cryptography**. USA: CRC Press, 1996. 816 p.

MLP – **Mobile Location Protocol** (*OMA - Open Mobile Alliance*). 2002. <http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/lif/LIF-TS-101-v3.0.0.zip> acesso em: 20/04/2009.

MOBIEXPLORE. MobiEXPLORE Travel Guide. 2009. Disponível em: http://www.mobiexplore.com/ Acesso em: 29/04/2009.

MOBILOCO. **Location Based Services for Mobile Communities**. Disponível em: <http://www.mobiloco.de> Acessado em: 20/04/2009.

MOKBEL, M. F.; CHOW, C. Y.; AREF, W. G. **The New Casper: Query Processing for Location Services without Compromising Privacy**. In: 32TH INTERNATIONAL CONFERENCE ON VERY LARGE DATA BASE (VLDB), 2006, Seoul, Korea. **Proceedings…** pp. 763–774.

MYLES, G.; FRIDAY, A.; DAVIES, N. **Preserving privacy in environments with location-based applications.** IEEE PERVASIVE COMPUTING, Vol.2, No.1, pp.56–64, 2003.

OECD. Organization for Economic Co-Operation and Development. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Setembro, 1980. Disponível em: <http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html>. Acesso em 29/04/2009.

OMA – **OMA Privacy Guidelines**. 2002. Disponível em: < http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/lif/lif-tr-101-v2.0.0.zip> Acesso em: 21/02/2009.

OMA - **Open Mobile Alliance Web Site**. Disponível em: <http://www.openmobilealliance.org/> acesso em: 05/02/2009.

OPENLS - **Open Location Services Interface Standard version 1.2**, OGC Standard, 2008. Disponível em: <http://portal.opengeospatial.org/files/?artifact_id=22122>. Acesso em: 30/04/2009

PARESCHI, L.; RIBONI, D.; BETTINI C. **Protecting User`s Anonymity in Pervasive Computing Environments**, In: SIXTH ANNUAL IEEE INTERNATIONAL CONFERENCE PERVASIVE COMPUTING AND COMMUNICATIONS (PerCom), 2008, Hong Kong, China. **Procedings…** pp 11-19.

PFITZMANN, A.; KOHNTOPP, M. **Anonymity, unobservability, and pseudonymity: a proposal for terminology**. DESIGNING PRIVACY ENHANCING TECHNOLOGIES. Springer-Verlag, New York, pp. 1-9, 2001.

PRIYANTHA, N. B., CHAKRABORTY, A., BALAKRISHNAN, H. **The Cricket Location-Support System**. In: MOBILE COMPUTING AND NETWORKING (MobiCOM), 2000, Boston, USA. **Proceedings...** pp. 32–43.

RIBEIRO, F. N.; ZORZO, S. D. **LP-Proxy – Garantias de Privacidade em Serviços Baseados em Localização**. In: XXXIV CONFERENCIA LATINOAMERICANA DE INFORMÁTICA, 2008, Santa Fe, Argentina.

RIBEIRO, F. N.; ZORZO, S. D. LPBS – **Location Privacy Based System**. In: XIV IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, 2009, Sousse, Tunísia. A ser apresentado.

RIBEIRO, F. N.; ZORZO, S. D. **A Quantitative Evaluation of Privacy in Location Based Services**. In: XVI INTERNATIONAL WORKSHOP ON SYSTEMS, SIGNALS AND IMAGE PROCESSING, 2009, Chalkida, Grécia. A ser apresentado.

SACRAMENTO, V. **Gerência de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis.** 2006. 136 p. Tese de Doutorado (Doutorado em Informática) – Departamento de Informática, PUC-RIO, Rio de Janeiro, 2006.

SACRAMENTO, V.; ENDLER, M.; NASCIMENTO, F.N do**. Design of a Context Privacy Service for Mobile Collaboration.** In: XXIII SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES (SBRC*)*, 2005, Fortaleza, Brasil. **Proceedings…** pp 323-336.

SMAILAGIC, A.; SIEWIOREK, D. P.; ANHALT, J.; KOGAN, D.; WANG, Y. **Location Sensing and Privacy in a Context Aware Computing Environment**. IEEE WIRELESS COMMUNICATIONS. Vol. 9, No 5, pp. 10-17, 2002.

SMART, S. W. **TextBook on Spherical Astronomy.** 6. ed., England: Cambridge University Press, 1977. 415 p.

SINNOTT, R. W. **Virtues of the Haversine**. SKY AND TELESCOPE. Vol.68, No.2, p. 158, 1984.

TENTORI, M.; FAVELA, J.; RODRIGUEZ, M. D.; GONZALEZ V. M. **Supporting Quality of Privacy (QoP) in Pervasive Computing**. In: SIXTH MEXICAN INTERNATIONAL CONFERENCE ON COMPUTER SCIENCE, 2005, Puebla, Mexico. **Proceedings…** pp. 58-67.

TOGuide. **Interactive Turin Guide**. Disponível em: <http://www.lobase.it/en/?TOguide> Acesso em: 21/04/2009.

VIVO. **Vivo Encontra**. Disponível em: <http://www.vivo.com.br/vivodownloads/aplicativos.php?cat=12>. Acesso em: 20/04/2009.

WANT, R.; HOPPER, A.; FALCÃO, V.; GIBBONS, J. **The Active Badge Location System**. ACM TRANSACTIONS ON INFORMATION SYSTEMS, Vol.10, No 1, pp. 91–102, 1992.

WARD, A.; JONES, A.; HOPPER, A. **A New Location Technique for the Active Office**. IEEE PERSONAL COMMUNICATION, Vol. 4, No 5, pp. 42–47, 1997.

WARREN, S. D., Brandeis, L. D. **The Right to Privacy**. HARVARD LAW REVIEW vol. 04, p. 193, 1890.

WARRIOR, J.; MCHENRY, E.; MCGEE, K. **They Know Where You Are**. IEEE SPECTRUM, Volume 40, No. 7, pp 20-25, 2003.

WEISER, Mark. **Some Computer Science Problems in Ubiquitous Computing**. COMMUNICATIONS OF THE ACM, 1993. Vol. 36, No. 7, pp 74-83

WILLIAMS, Ed. **Aviation Formulary 1.44**. Disponível em: http://williams.best.vwh.net/avform.htm#LL. Acesso em: 29/04/2009.

Apêndice I - *OpenLS* e *MLP*

Acompanhando a expansão na utilização de serviços baseados em localização, a necessidade de critérios para a troca de informações durante a comunicação entre as entidades envolvidas tornou-se evidente. Diversos provedores lançaram mão de protocolos próprios para representar tipos de requisição *LBS*, dados de localização de usuários e pontos de interesse, além de mapas e notificações ao usuário. A falta de interesse, por boa parte dos envolvidos, no oferecimento de *LBS* em criar um protocolo comum de comunicação, acabou por incentivar a criação de protocolos proprietários e, em geral, não-disponíveis.

Seguindo uma direção contrária à tendência observada, alguns grupos se mobilizaram no intuito de criar padrões que pudessem ser abertos e disponíveis para a comunicação e interoperabilidade entre diversos serviços e provedores.

Um dos grupos interessados no oferecimento de padrões para o ambiente móvel é a *OMA – Open Mobile Alliance* (OMA, 2009), ou Aliança Móvel Aberta, que tem como um dos principais objetivos zelar pela interoperabilidade dos serviços para a comunicação voltados à comunicação móvel e possui para isso vários grupos de trabalho, dentre eles o grupo de trabalho sobre localização, *LOC (Location Work Group)*. Este grupo foi criado com o intuito de desenvolver especificações que assegurem a interoperabilidade de serviços baseados em localização para dispositivos móveis.

Um dos resultados desse grupo de trabalho foi a proposição do Protocolo para Localização Móvel ou *Mobile Location Protocol* (*MLP*) (MLP, 2002), cujo principal objetivo é oferecer um meio pelo qual seja possível a obtenção de informações de localização de estações móveis, independente da tecnologia de rede utilizada. Ele é geralmente utilizado como interface entre a aplicação *LBS* cliente e o servidor de localização.

A troca de conteúdos proposta pelo *MLP* é baseada em *XML*, o que permite a fácil adaptação e comunicação, uma vez que, sendo disponibilizado o formato dos documentos *XML*, as partes interessadas na comunicação necessitam apenas seguir o padrão proposto para a realização da troca de informações.

Além disso, o protocolo *MLP* visa obter a interoperabilidade entre diferentes plataformas e diferentes protocolos de comunicação e, para isso, ele é dividido em três camadas: camada de serviço, camada de elemento e camada de transporte.

As duas primeiras são as camadas superiores e tratam dos aspectos de localização, como relatórios de localização, identificação de usuário, qualidade da localização que envolve questões de precisão, dentre outros. Já a camada inferior, ou camada de transporte, permite a utilização de vários protocolos para o transporte das informações, dentre eles o *HTTP*, protocolo bastante difundido com a utilização da Internet. A Figura 27 representa, de forma sucinta, a organização em camadas do *MLP*.

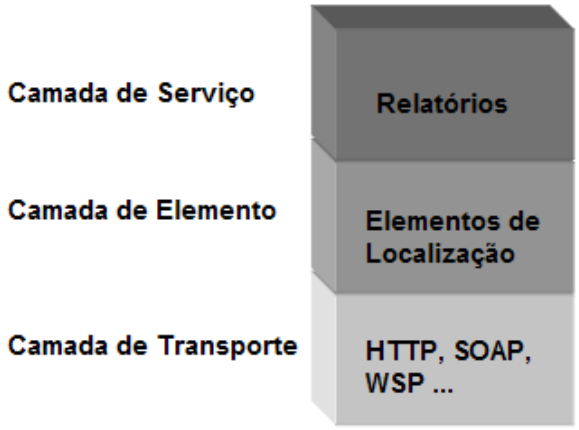


Figura 27 – Divisão em camadas do *MLP*

O *MLP* permite a representação de vários elementos necessários na comunicação em *LBS's*, como, por exemplo, a localização de usuário, elementos de rede envolvidos na localização (identificador da célula utilizada pelo celular – *cellid* etc.), ou a representação da solicitação de localização, além de diversos relatórios, como o relatório imediato de localização padrão, *SLIREP* (*Standard Location Immediate Report*), que é apresentado na Figura 28.

Figura 28 – Exemplo de um relatório imediato de localização padrão do *MLP*

Como pode ainda ser observado na Figura 28, esse relatório permite a representação das informações de localização em resposta a uma requisição. Dentre os campos presentes neste documento *XML*, estão: o identificador da requisição, *req_id*; o identificador do usuário que fez a requisição, *msid type*; e a representação da posição do usuário, *shape*.

O *MLP* permite também a representação das informações de localização, seguindo diversas padronizações diferentes. No exemplo apresentado, as coordenadas foram representadas pela latitude e longitude no formato de graus, minutos e segundos, como pode ser observado no campo *X*, que indica a latitude 35º 03’ 28.244’’ Norte. O atributo *srsName* indica justamente a forma de representação adotada.O campo *radius* indica o raio de possível localização do usuário a partir das coordenadas dos campos *X* e *Y*.

Outro padrão desenvolvido é chamado de *OpenLS* (*Open Location Services Interface Standard*), ou padrão aberto para interfaces de serviços de localização, que também oferece uma interface para a utilização de diversos *LBS*. O *OpenLS,* desenvolvido pelo Consórcio Geoespacial Aberto (*Open Geospatial Consortium - OGC*), apresenta a definição de documentos *XML* projetados para a representação dos dados necessários nas transações com provedores *LBS*.

Diversas aplicações são suportadas pelo *OpenLS,* tais como: navegação pessoal, serviço de informações de tráfego, serviços de proximidade, direções de viagem, busca por pontos de interesse próximo, solicitação de mapas, dentre outros. Essas aplicações são suportadas através de diferentes interfaces que implementam serviços *OpenLS*, sendo alguns deles: Serviço de Diretório, Serviço de Apresentação e Serviços de *Geocoding* e *Geocoding* Reverso.

O Serviço de Diretório oferece aos usuários acesso a um diretório *online* para a busca de lugares, produtos ou serviços. Existe a opção de busca por critérios de proximidade ou busca de elementos específicos como, por exemplo, lanchonetes de uma determinada rede de *fast-food*.

Um caso de uso desse tipo de serviço é a solicitação dos restaurantes mais próximos a uma determinada posição geográfica. A Figura 29 apresenta parte de um documento XML desse tipo de requisição, segundo o padrão *OpenLS* . No elemento '*<gml:pos>*' do documento XML é representada a posição geográfica do usuário que realiza a requisição em latitude e longitude. Já no campo '*<xls:POIProperty name =“keyword” value =“restaurant”>*', destaca-se que a busca será feita pela palavra-chave 'restaurante'. Outros campos importantes a serem destacados são o *methodName=DirectoryRequest”'*, que indica o serviço de diretório e o '*maximumResponses*=“5”', que determina o número máximo de restaurantes que deve compor a resposta retornada pelo provedor *LBS*.

```
- <xls:Request version="1.0" maximumResponses="5" methodName="DirectoryRequest">
  - <xls:DirectoryRequest freeformAddrLang="EN">
    - <xls:POILocation>
      - <xls:Nearest>
        - <xls:POI ID="1">
          - <gml:Point>
              <gml:pos>41.003 -72.002896</gml:pos>
            </gml:Point>
          </xls:POI>
        </xls:Nearest>
      </xls:POILocation>
    - <xls:POIProperties>
        <xls:POIProperty name="Keyword" value="restaurant" />
      </xls:POIProperties>
    </xls:DirectoryRequest>
  </xls:Request>
</xls:XLS>
```

Figura 29 – Requisição dos restaurantes mais próximos segundo o OpenLS.

Um segundo caso de uso seria a busca por restaurantes em raio de quinhentos metros de proximidade da atual localização do usuário. A Figura 30 apresenta um exemplo de documento *XML* responsável por tal solicitação. Na requisição apresentada anteriormente, o campo '*<gml:pos>*' está circundando pelo campo '*<xls:Nearest>*'. Já nesta, o campo de determinação da localização está circundado pelo campo '*<xls:WithinDistance>*' que possui ainda, em seu interior, o campo '*<xls:MaximumDistance value*=“500”>', indicando que os restaurantes retornados devem estar dentro de um raio de quinhentos metros.

```
- <xls:Request version="1.0" maximumResponses="10" requestID="10" methodName="DirectoryRequest">
  - <xls:DirectoryRequest>
    - <xls:POILocation>
      - <xls:WithinDistance>
        - <xls:POI ID="1">
          - <gml:Point>
              <gml:pos>41.003 -72.002896</gml:pos>
            </gml:Point>
          </xls:POI>
          <xls:MaximumDistance value="500" />
        </xls:WithinDistance>
      </xls:POILocation>
    - <xls:POIProperties>
        <xls:POIProperty name="Keyword" value="restaurant" />
      </xls:POIProperties>
    </xls:DirectoryRequest>
  </xls:Request>
</xls:XLS>
```

Figura 30 – Requisição dos restaurantes dentro de um raio de quinhentos metros.

A seguir, na Figura 31, é apresentado um documento *XML* de resposta ao serviço de diretório.

```
- <xls:DirectoryResponse>
  - <xls:POIContext>
    - <xls:POI phoneNumber="+(55)-(21)-32525182" ID="0" POIName="Restaurante A">
      - <xls:POIAttributeList>
        - <xls:POIInfoList>
            <xls:POIInfo name="ID" value="936008125" />
          </xls:POIInfoList>
        </xls:POIAttributeList>
      - <gml:Point>
          <gml:pos>-22.91944 -43.177996</gml:pos>
        </gml:Point>
      - <xls:Address countryCode="BR">
        - <xls:StreetAddress>
            <xls:Building number="181" />
            <xls:Street>RUA PEDRO ALVARES CABRAL</xls:Street>
          </xls:StreetAddress>
          <xls:Place type="CountrySubdivision">SUDESTE</xls:Place>
          <xls:Place type="CountrySecondarySubdivision">RIO DE JANEIRO</xls:Place>
          <xls:Place type="Municipality">RIO DE JANEIRO</xls:Place>
          <xls:Place type="MunicipalitySubdivision">CENTRO</xls:Place>
          <xls:PostalCode>20241</xls:PostalCode>
        </xls:Address>
      </xls:POI>
      <xls:Distance uom="M" value="4966.71" />
    </xls:POIContext>
  </xls:DirectoryResponse>
```

Figura 31 – Resposta de serviço do tipo diretório.

Por essa figura, que apresenta o resultado da busca por restaurantes mais próximos, é possível verificar que cada elemento retornado é encapsulado dentro de um campo '*<xls:POIContext>*', possuindo uma série de outros campos internos que permitem a representação de informações, como nome do ponto de interesse, endereço, distância entre

o ponto de interesse e a atual localização do usuário, dentre outros. O campo '*<xls:Distance uom="M" value="4966.71" />*' indica que a distância em que o ponto de interesse se encontra é de 1966,71 metros ('*uom = "M"*').

O serviço de *Geocoding* é a determinação de uma posição geográfica com base em um lugar, endereço ou código postal e *Geocoding* Reverso é exatamente o contrário, ou seja, a partir de uma coordenada geográfica, determinar um endereço, lugar ou endereço de maneira completa e em conformidade com os padrões de endereçamento.

A Figura 32 apresenta um exemplo de requisição de *Geocoding* Reverso com o envio apenas da coordenada geográfica da qual se deseja o endereçamento completo, e a Figura 33 exibe o documento retornado em resposta à requisição feita. É válido observar que é retornado o endereçamento completo composto pelo código do país (BR), rua, cidade, estado, faixa de números das construções e código postal.

```
- <xls:Request maximumResponses="25" requestID="10" methodName="ReverseGeocodeRequest">
  - <xls:ReverseGeocodeRequest>
    - <xls:Position>
      - <gml:Point>
          <gml:pos>-23.53457 -46.640053</gml:pos>
        </gml:Point>
      </xls:Position>
    </xls:ReverseGeocodeRequest>
  </xls:Request>
</xls:XLS>
```

Figura 32 – Requisição de *Geocoding* Reverso

```
  - <xls:Response numberOfResponses="1" version="1.0" requestID="10">
    - <xls:ReverseGeocodeResponse>
      - <xls:ReverseGeocodedLocation>
        - <gml:Point>
            <gml:pos>-23.534621 -46.640153</gml:pos>
          </gml:Point>
        - <xls:Address countryCode="BR">
          - <xls:StreetAddress>
              <xls:Building number="(378 - 384)" />
              <xls:Street>ALAMEDA CLEVELAND</xls:Street>
            </xls:StreetAddress>
            <xls:Place type="CountrySubdivision">SUDESTE</xls:Place>
            <xls:Place type="CountrySecondarySubdivision">SAO PAULO</xls:Place>
            <xls:Place type="Municipality">SAO PAULO</xls:Place>
            <xls:PostalCode>01218</xls:PostalCode>
          </xls:Address>
        </xls:ReverseGeocodedLocation>
      </xls:ReverseGeocodeResponse>
    </xls:Response>
  </xls:XLS>
```

Figura 33 – Resposta à requisição de *Geocoding* Reverso

O serviço de apresentação é indicado para os casos em que é necessária a exibição de informações geográficas em mapas, na tela do dispositivo móvel. Quaisquer um dos outros serviços podem utilizar-se desse para a incorporação de mapas. Por exemplo, a exibição dos pontos de interesse mais próximos da posição usuário em um mapa deve utilizar o serviço de apresentação.

Esse serviço permite a edição de diversas configurações presentes nos mapas, como tamanho e largura em pixels (*height*, *width*), cor de fundo (*background color*), ponto central do mapa (*Center Point*), escala de exibição (*Display Scale*), dentre outros.

A Figura 34 destaca a requisição de um mapa cujo centro está na posição '**-23.53457**' de latitude e '**-46.640053**' de longitude. Além disso, o mapa retornado deverá ter '**220'** pixels de altura por '**200'** pixels de largura e deverá apresentar, na imagem, o equivalente a '**300**' metros de raio ('*<xls:Radius unit="KM">0.3</xls:Radius>*'). O mapa solicitado ainda deverá conter uma camada superior ao mapa ('*<xls:Overlay>*') que, no caso, é um ponto verde ('*<xls:Style><xls:Name>green-dot.gif</xls:Name></xls:Style>*') localizado também na posição central do mapa ('*<gml:pos>-23.53457 -46.640053</gml:pos>*').

```
- <xls:Request methodName="PortrayMapRequest" requestID="10" version="1.0">
  - <xls:PortrayMapRequest>
    - <xls:Output height="220" width="200">
      - <xls:CenterContext SRS="WGS-84">
        - <xls:CenterPoint>
            <gml:pos>-23.53457 -46.640053</gml:pos>
          </xls:CenterPoint>
          <xls:Radius unit="KM">0.3</xls:Radius>
        </xls:CenterContext>
      </xls:Output>
    - <xls:Overlay>
      - <xls:Position>
        - <gml:Point xmlns:gml="http://www.opengis.net/gml">
            <gml:pos>-23.53457 -46.640053</gml:pos>
          </gml:Point>
        </xls:Position>
      - <xls:Style>
          <xls:Name>green-dot.gif</xls:Name>
        </xls:Style>
      </xls:Overlay>
    </xls:PortrayMapRequest>
  </xls:Request>
</xls:XLS>
```

Figura 34 – Requisição de mapa segundo o *OpenLS*

A Figura 35 apresenta o *XML* retornado como resposta à requisição presente na Figura 34. A imagem retornada para essa requisição e apresentada na Figura 36 pode ser obtida

através de um *link* contendo o destino da figura (‘*<xls:URL> </xls:URL>*’). Existe também a possibilidade de a imagem ser enviada no documento *XML* de resposta, bastando para isso ser inserido na requisição o atributo ‘*content=“Data”*’, no interior do campo *Output* . O campo ‘*<xls:BBoxContext>*’ indica as coordenadas da área retangular que é mostrada no mapa retornado.

```
- <xls:Response numberOfResponses="1" version="1.0" requestID="10">
  - <xls:PortrayMapResponse>
    - <xls:Map>
      - <xls:Content width="200" format="GIF" height="220">
          <xls:URL>http://wsdds1-new.dz.decarta.com:80/openls/image/-980170575.GIF</xls:URL>
        </xls:Content>
      - <xls:BBoxContext>
          <gml:pos>-23.537556792 -46.642997964</gml:pos>
          <gml:pos>-23.531583142 -46.637108036</gml:pos>
        </xls:BBoxContext>
      - <xls:CenterContext SRS="WGS-84">
        - <xls:CenterPoint>
            <gml:pos>-23.53457 -46.640053</gml:pos>
          </xls:CenterPoint>
          <xls:Radius unit="KM">0.3</xls:Radius>
        </xls:CenterContext>
      </xls:Map>
    </xls:PortrayMapResponse>
  </xls:Response>
```

Figura 35 – XML de resposta à requisição de um mapa

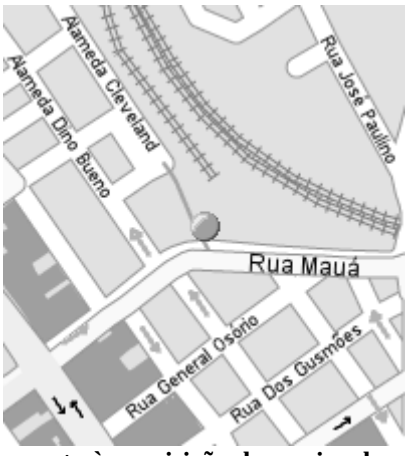


Figura 36 – Mapa retornado em resposta à requisição de serviço de apresentação

O *OpenLS* ainda permite a representação das informações de coordenadas geográficas de outras maneiras, além de simplesmente um único ponto, o que garante a aplicação do nível de privacidade 3, no qual devem ser enviadas informações de coordenadas geográficas que sejam compostas por uma área e não por um único ponto. Dentre as possibilidades de representação encontra-se a ‘*PolygonType*’, que permite a definição de polígonos e a ‘*CircleByCenterPointType*’, que permite a definição de um círculo com base em um ponto central. Este último foi utilizado no oferecimento do nível de privacidade 3.

Os protocolos apresentados foram definidos para atuarem em diferentes momentos da execução de *LBS*. O *MLP* foi projetado para solucionar principalmente a questão da determinação da localização dos dispositivos móveis, enquanto o *OpenLS* tem sua principal utilidade na interoperabilidade dos serviços baseados em localização através da disponibilização de uma interface comum para *Geocoding*, buscas por pontos de interesse, mapas etc. Pode-se dizer que tais protocolos são complementares, uma vez que é possível a utilização simultânea de ambos durante a execução de *LBS*.