LP-Proxy - Garantias de Privacidade em Serviços Baseados em Localização

Filipe Nunes Ribeiro e Sergio Donizetti Zorzo

Universidade Federal de São Carlos – UFSCar, São Carlos – SP, Brasil
GSDR – Grupo de Sistemas Distribuídos e Redes
filipe_ribeiro@dc.ufscar.br, zorzo@dc.ufscar.br

Resumo. A utilização dos Serviços Baseados em Localização (*LBS*) se tornou uma realidade para uma grande quantidade de usuários de dispositivos móveis, especialmente de celulares. Serviços como localização de restaurantes ou hotéis, previsão do tempo ou verificação das condições de tráfego nas regiões próximas se tornaram uma realidade. Para o oferecimento destes serviços é necessário a manipulação de informações pessoais e de localização, que se utilizadas de maneira incorreta podem ameaçar a privacidade dos usuários. A arquitetura mais comum de execução dos *LBS* é baseada em um modelo cliente-servidor, e apresenta carências de métodos que ofereçam garantias de privacidade. Visando suprir essas necessidades, este trabalho apresenta o *LP-Proxy* – um *proxy* desenvolvido com o intuito de atuar como um intermediário entre os dispositivos móveis e os servidores – buscando permitir a execução dos Serviços Baseados em Localização com garantias de privacidade para os usuários.

Palavras-chave: Serviços Baseados em Localização, Privacidade, *Proxy*, Aplicações *LBS*.

1 Introdução

Os Serviços Baseados em Localização ou *LBS* (*Location Based Services*) são aqueles que utilizam o posicionamento geográfico dos usuários para algum propósito específico [1]. 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 (hotéis, restaurantes, etc); verificação das condições de tráfego ou previsão do tempo nas regiões próximas e determinação da posição geográfica de outros usuários.

Se por um lado a utilização de informações de localização permite o oferecimento de uma nova qualidade de serviços, por outro, pode representar riscos no que diz respeito à privacidade e até mesmo à segurança dos usuários [2]. Ameaças como identificação não autorizada de perfil e revelação de informações sobre contatos sociais [3] ou informações de suporte em procedimentos de divórcio [4] representam

apenas alguns dos riscos que o usuário corre se suas informações forem utilizadas de maneira inadequada.

Um dos grandes mercados para os Serviços Baseados em Localização é o grupo de usuários de telefonia móvel, sendo que até o momento já existem diversos *LBS* específicos para esse grupo de usuários. No entanto, a arquitetura de execução de tais serviços se apresenta vulnerável a diversas ameaças de privacidade.

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 no ambiente de telefonia móvel.

Para isso é apresentado o *LP-Proxy*, que foi embutido na arquitetura de execução dos *LBS* com o intuito de oferecer maiores garantias de privacidade. Dentre as funcionalidades oferecidas pelo *LP-Proxy* destacam-se o canal seguro de comunicação e o ajuste dos dados de localização.

O trabalho aqui apresentado está organizado da seguinte maneira: na seção 2 são discutidos os trabalhos relacionados; a seção 3 apresenta as principais características dos Serviços Baseados em Localização e sua utilização na telefonia móvel; a seção 4 aborda os aspectos de privacidade envolvidos na execução de LBS; em seguida, na seção 5 são detalhados os aspectos do trabalho apresentado; finalmente a seção 6 apresenta os resultados obtidos e algumas conclusões acerca deste trabalho, bem como aponta trabalhos futuros.

2 Trabalhos Correlatos

O *LocServ* [20] é um middleware que se encontra entre as aplicações dos Serviços Baseados em Localização e os provedores de serviço. Ele tem como principal objetivo atuar no momento da liberação das informações de localização, impedindo que os dados sejam transferidos para terceiros sem autorização do usuário.

Para isso, o *LocServ* conta com os *validators*, componentes responsáveis por comparar as preferências dos usuários e as políticas de privacidade apresentadas pelos provedores, e permitir ou não a liberação das informações de localização, de forma análoga à Plataforma *P3P* (*Platform for Privacy Preferences Project*) para a Internet. *LocServ* não deixa claro o caso de execução de *Pull LBS.*

Algumas propostas na literatura visam garantir um conjunto de anonimato, ou seja, sempre que uma requisição for feita por um usuário em uma determinada área, certamente existirão outras requisições procedentes da mesma área, o que impediria a identificação dos usuários.

Para obter sempre um conjunto de anonimato, alguns modelos propõem a ocultação da precisão espacial e temporal [21, 22]. Esta abordagem funciona da seguinte maneira: se o usuário fizer uma requisição de um local no qual não existe nenhuma outra requisição, então a precisão da localização é diminuída. Se ainda assim não houver requisições na mesma área, a precisão temporal também pode ser reduzida, ou seja, pode-se esperar um tempo até que outra requisição seja feita.

Esse tipo de técnica para a proteção de privacidade pode gerar um atraso excessivo no tempo de resposta, caso existam dificuldades em compor o conjunto de anonimato,

comprometendo o desempenho de algumas aplicações, especialmente aplicações *Pull LBS*.

Outra técnica para obter o conjunto de anonimato, é a realização de requisições falsas [23, 24]. Tais propostas sugerem que a requisição contenha a localização exata do usuário, bem como localizações com falsas informações sobre a posição. Dessa forma, o provedor *LBS* não seria capaz de identificar a localização exata. Estas soluções, apesar de sempre oferecerem um conjunto de anonimato, ocasionam aumento nos custos de implementação, já que o servidor deverá processar um resultado para cada localização, o que aumentará o volume da transferência de dados.

Existe ainda o *Mix-Zone* [8], que propõe a criação de regiões especiais de tamanho definido, nas quais existem usuários que não estão registrados em nenhum dos serviços de localização. No entanto farão parte da composição do conjunto de anonimato. Essa técnica concentra a classe de aplicações cientes de localização que aceitam pseudônimos. Apesar de ser eficiente no combate à identificação do usuário, a implementação dessa proposta em ambientes reais é bastante complexa.

O *Trust Server Model* ou Modelo de Servidor Confiável[3] apresenta protocolos para a comunicação entre as entidades envolvidas durante a prestação do serviço e um protocolo de subscrição ao *Push* e *Peer-to-Peer LBS*. Este modelo propõe também a utilização de um canal de comunicação criptografado para evitar ataques através da espionagem dos dados trafegados.

Os trabalhos relacionados apresentam diversas soluções distintas para tratar o problema da privacidade em *LBS*. Alguns deles, *LocServ* e *Mix Zones* apresentam casos específicos para a utilização em celulares, no entanto, nenhum apresenta resultados concretos, na forma de um possível sistema que permita a utilização em ambientes práticos. O *LP-Proxy*, descrito neste artigo, apresenta a implementação de um *Proxy* que oferece técnicas para melhorias de privacidade na execução de *LBS*.

3 Serviços Baseados em Localização

A computação ubíqua é definida como a presença de dispositivos computacionais nos mais diversos objetos, de tal forma que sua utilização seja feita de forma imperceptível [5]. Essa variedade de dispositivos, que pelas suas características são capazes de atuar no ambiente de diversas maneiras, ocasionou mudanças na forma de obtenção de dados dos usuários. Houve um aumento expressivo na quantidade, qualidade e precisão dos dados gerados e coletados [6].

Dentre os novos dados passíveis de coleta com o advento da computação ubíqua estão as informações de posicionamento geográfico. Tais informações podem ser obtidas utilizando-se diversas tecnologias, que vão desde a utilização de satélites do Sistema de Posicionamento Global (*GPS – Global Positioning System*), até as infra-estruturas de redes sem fio existentes [7].

A utilização do posicionamento geográfico de usuários possibilitou o aparecimento de serviços que oferecem informações específicas para um local ou que permitam a interação entre pessoas próximas, bem como facilidades de orientação de direção. Todos estes serviços têm em comum o fato de tirarem proveito das informações de localização, sendo por isso, denominados Serviços Baseados em Localização.

Os Serviços Baseados em Localização podem ser agrupados em três categorias com base na participação do usuário na requisição do serviço: *pull LBS, push LBS* e *peer-to-peer LBS* [3].

Na categoria *pull LBS* o usuário explicitamente realiza a requisição do serviço e envia sua informação de localização. Exemplos típicos de serviços deste tipo incluem a localização de serviços como farmácia ou restaurante mais próximo.

Nos serviços baseados em localização denominados *push LBS,* o usuário não envia uma requisição diretamente ao servidor *LBS* para que o serviço seja oferecido, contudo, a presença do usuário é detectada e o servidor pode oferecer algum serviço. Um exemplo possível seria o recebimento de informações acerca das ofertas de um supermercado, ao se passar nas proximidades do estabelecimento.

A última categoria, *peer-to-peer LBS*, engloba os serviços nos quais as requisições envolvem outros usuários, ou seja, é necessária a localização de outros além daquele que realiza a requisição. Caracterizam-se por este tipo de serviço, por exemplo, encontrar amigos que estão próximos, ou determinar a localização dos empregados de uma empresa.

Outra classificação para os *LBS* é quanto ao anonimato do usuário [8]. Anonimato pode ser definido como a capacidade de não ser identificado dentro de um conjunto de indivíduos o conjunto de anonimato [9].

Algumas aplicações requerem a revelação da identidade do usuário, como por exemplo, localização de colegas de trabalho durante o seu período de trabalho. Outras podem ser completamente anônimas como, por exemplo, ao passar próximo a uma cafeteria, ser alertado com relação ao preço do café. Por fim, existem as aplicações intermediárias, nas quais não é possível a prestação do serviço anonimamente, mas não é necessária a real identidade real do usuário. Nesses casos pode ser utilizado um pseudônimo, como se fosse um apelido para identificá-lo.

Um dos mercados mais promissores para a utilização de *LBS* é o da telefonia celular, que vem apresentando considerável crescimento. Além do aumento do número de aparelhos, observa-se também maior poder de processamento e comunicação com a Internet [10].

O impulso inicial dos serviços baseados em localização para celulares nos EUA se deu em 1996, com a determinação do governo de que as empresas de telefonia celular deveriam ser capazes de identificar a localização dos celulares em chamadas de emergência, *Enhanced 911* [2]. Tal fato ocasionou o desenvolvimento de técnicas de localização que obtivessem maior precisão e que pudessem ser integradas às redes de telefonia celular [11].

A arquitetura de execução mais comum de *LBS* para celulares é apresentada na figura 1 e funciona da seguinte maneira. O dispositivo acessa o servidor que oferece o *LBS*, denominado provedor *LBS*, através do acesso à Internet oferecido pela operadora, representado pela antena. Diversas tecnologias, tais como *GPRS (General Packet Radio Service)* possibilitam acesso à Internet via aparelho de celular.

Nessa arquitetura, o dispositivo móvel, freqüentemente, executa uma aplicação oferecida pelo próprio provedor *LBS*, que é responsável por gerenciar a conexão do dispositivo com o provedor, enviar os dados necessários para a prestação do serviço e processar os dados recebidos.

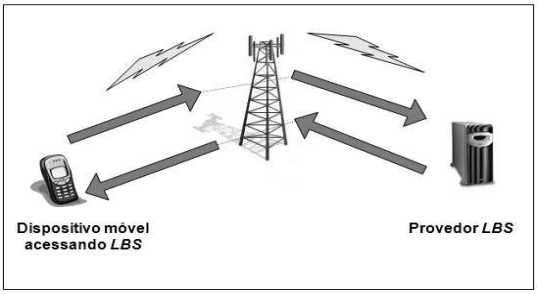

Fig. 1. Atual arquitetura de *LBS* para celulares.

Existem diversos *LBS* para celulares. Alguns deles são pagos e oferecidos pela própria operadora [12]. Outros serviços também pagos, mas oferecidos por empresas que possuem parcerias com as operadoras para o fornecimento da localização dos dispositivos, como a empresa alemã MOBILOCO [13]. Existem ainda, os serviços gratuitos, como o TOguide [14], um guia interativo do centro da cidade de Turin e o *Google Maps Mobile* [15], que é um serviço capaz de fornecer várias funcionalidades, como a determinação da posição de um usuário e sua respectiva localização em um mapa, localização de serviços mais próximos como pizzarias e bares dentre outros.

A tendência é que os Serviços Baseados em Localização se tornem cada vez mais comuns e disponíveis para um número ainda maior de usuários. No entanto, *LBS* podem oferecer sérios riscos com relação à privacidade, que serão discutidos a seguir.

4 Privacidade

A obtenção de informações de localização isoladamente não representa risco direto à privacidade, mas a partir do momento em que um usuário pode ser relacionado à sua respectiva localização, podem ser ocasionadas diversas situações de quebra de privacidade ou até mesmo situações que afetem a segurança. A atual arquitetura de execução dos Serviços Baseados em Localização, ilustrado pela figura 1, é susceptível a algumas formas de ataque que podem levar a identificação dos usuários:

Observação do tráfego na rede [16]. É possível capturar as informações transferidas no canal de comunicação entre o dispositivo móvel e o provedor *LBS*, e dessa forma obter informações que levariam à identificação do usuário.

Precisão dos dados. Informações com precisão elevada tornam-se um quase-identificador [17], que são informações que podem levar à identificação de um único usuário apesar de não ser sua identidade especificamente.

Requisições solitárias [4]. Requisições que são realizadas a um provedor isoladamente, sem um conjunto de anonimato e podem levar a um único usuário. Este caso é mais grave quando a precisão dos dados é alta. Nos casos em que as requisições possuem informações com baixa precisão de localização a identificação é dificultada, especialmente em áreas mais povoadas.

Aplicativos de terceiros. Podem ser inseridos trechos de código maliciosos que captem informações capazes de levar a 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.

Histórico de movimentação. A partir de uma análise minuciosa das localizações subseqüentes e dos padrões de movimentos realizados é possível inferir a identidade do usuário [17].

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.

Com posse das informações de localização de um usuário, é possível identificar locais freqüentados, como grupo de auto- ajuda, ou até mesmo grupo de apoio a soro-positivo. Tais informações podem ser utilizadas para extorsão de usuários ou exposição pública.

É possível ainda em alguns casos identificar todos os passos de um usuário durante o dia no decorrer de várias semanas e determinar sua rota diária e os principais pontos visitados, como por exemplo, a escola na qual os filhos estudam. Estes dados poderiam ser utilizadas até mesmo no planejamento de um seqüestro.

Além destas questões mais graves, o usuário pode ter sua privacidade invadida pelo simples fato de receber mensagens com propagandas indesejadas que foram enviadas com base em sua atual localização.

5 *LP-Proxy*

O *LP-Proxy* (*Location Privacy Proxy*) objetiva oferecer privacidade de localização, ou seja, ser capaz de prevenir que terceiros obtenham conhecimento sobre a atual localização do usuário ou localizações passadas desnecessariamente.

O *LP-Proxy* foi projetado para atuar nos *LBS* destinados à telefonia móvel, domínio específico da computação ubíqua, e oferece suporte às aplicações *Pull LBS.* A segurança e privacidade dos usuários é tratada em trabalhos relacionados para as outras classes de serviços e, dessa forma, *LP-Proxy* se apresenta como uma proposta que considera a localização como um dos requisitos de segurança e privacidade nas aplicações *Pull LBS* na telefonia movel.

A figura 2 descreve a organização dos Serviços Baseados em Localização com a inserção do *LP-Proxy.* Ele está localizado entre o dispositivo móvel e o provedor *LBS,* e todas as requisições provenientes do dispositivo móvel deverão sem exceção passar pelo *proxy*.

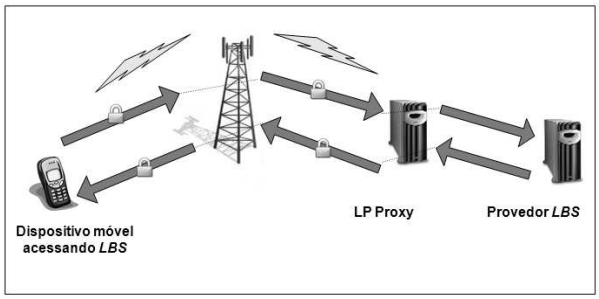

Fig. 2. Arquitetura de execução dos *LBS* com o LP-Proxy

O modelo proposto apresenta técnicas para manter a privacidade do usuário, eliminando as vulnerabilidades existentes na atual arquitetura. Primeiramente, é apresentada a transferência segura entre o dispositivo móvel e o *LP-Proxy*. Dessa forma, espiões que analisam o tráfego da rede terão muito mais trabalho em descobrir as informações pessoais transferidas.

Para tratar das questões de precisão dos dados e requisições solitárias, é apresentado um mecanismo de ajuste de precisão dos dados, que leva em consideração o tipo de solicitação. Requisições de pontos de interesse mais próximos, por exemplo, podem ter resolução de 500 metros dependendo da necessidade do usuário. Já requisições de previsão do tempo podem ter uma precisão mais baixa, enquanto requisições de condições de tráfego deverão ter maior precisão.

A figura 3 demonstra como funciona o ajuste da precisão das informações no *LP-Proxy*. A figura 3(a) representa a precisão alta, na qual o ponto central é a localização exata do usuário. As figuras seguintes 3(b) e 3(c), são informações que quando obtidas já possuem precisão média e baixa respectivamente, sendo que a circunferência maior representa uma área dentro da qual o usuário está presente.

Já a figura 3(d) representa o ajuste de uma informação com precisão alta para uma informação de baixa precisão. A circunferência menor central representa a informação original de localização e o raio da circunferência maior representa a precisão desejada, ou seja, se a precisão desejada é de 500 metros então o raio terá esse valor. Para o cálculo da nova posição é realizado um deslocamento aleatório para algum dos lados do plano de forma que a posição resultante ainda esteja no interior da circunferência. Dessa forma é obtida uma nova posição que não representa a posição exata do usuário, mas que se encontra a uma distância máxima da posição original.

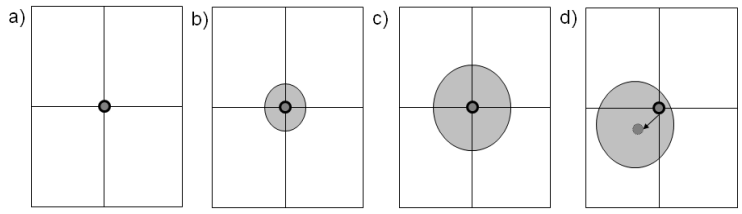

Fig. 3. Ajuste de precisão.

O ajuste de precisão possui valores padrões para os tipos de aplicações oferecidos, contudo, o usuário pode a qualquer momento alterar suas preferências de privacidade e diminuir ou aumentar os valores com que os dados serão ajustados.

Com o *LP-Proxy* todas as informações referentes à identidade do usuário ou ao dispositivo portado por ele são omitidas. Dessa forma, para o provedor *LBS* cada requisição recebida pertencerá a uma fonte diferente e não será possível a relação entre as movimentações nem a criação de um histórico para cada dispositivo.

Além disso, o *LP-Proxy* está em conformidade com os princípios de privacidade para a manipulação de informações de localização [19], baseados nos guias de proteção de privacidade para a manipulação de dados pessoais da Organização para Cooperação Econômica e Desenvolvimento (*OECD*) [18].

Dentre os princípios seguidos destacam-se o princípio do limite da coleta, segundo o qual os dados devem apenas ser coletados quando a localização é necessária para oferecer algum serviço. O princípio da qualidade dos dados, que determina que os dados devem ser coerentes com o propósito para o qual foram coletados, ou seja, não devem conter mais informações do que aquelas necessárias para a finalidade especificada. Já o princípio da limitação do uso estabelece que os dados pessoais só devem ser utilizados para os propósitos especificados.

Foi desenvolvida a aplicação para o dispositivo móvel e o *LP-Proxy*. A primeira é responsável pela gerência da comunicação com o *LP-Proxy*, armazenamento das preferências de privacidade dos usuários, e controle dos provedores *LBS* que serão utilizados.

O *LP-Proxy* possui um conjunto de módulos e funcionalidades, conforme apresentado na figura 4. Para esclarecer o funcionamento dos mecanismos do *LP-Proxy* será descrito um exemplo de execução.

Fig. 4. Módulos do *LP-Proxy.*

A execução é iniciada com a requisição realizada pelo dispositivo móvel (DM), contendo o tipo de solicitação (ex: localizar restaurante mais próximo), a localização atual do dispositivo e a precisão desejada (ex: 1000 metros). O módulo de comunicação com o DM recebe a requisição e a encaminha para o módulo de ajuste de precisão que realiza os ajustes necessários às informações geográficas. Em seguida uma nova requisição é construída em um documento *XML* e encaminhada ao provedor *LBS* que retorna a resposta da requisição também em formato *XML*. A resposta é interpretada, convertida em um formato legível pelo usuário e encaminhada ao DM finalizando a comunicação.

Para o suporte ao canal seguro de comunicação foi utilizada a transferência segura via *HTTP* (*HyperText Transfer Protocol*). A linguagem Java foi utilizada para o desenvolvimento do *LP-Proxy*, e para o dispositivo móvel utilizou-se a API *JavaME.*

6 Resultados

Foram realizados alguns testes de utilização de *LBS* no ambiente de telefonia móvel para avaliar a atuação do *LP-Proxy*. Para isso, foi desenvolvida e instalada em um

dispositivo móvel uma aplicação capaz de submeter requisições *LBS* ao *LP-Proxy* ou diretamente ao provedor *LBS,* dependendo do interesse por garantias de privacidade. Os fornecedores dos dados geográficos e de localização de pontos de interesse para os testes foram TeleAtlas[25] e deCarta[26].

O primeiro conjunto de testes foi realizado com o intuito de avaliar o ajuste da precisão da localização e foi dividido em duas etapas. A primeira consistiu de solicitações de pontos de interesse sem a utilização de técnicas ajuste de precisão. Em seguida, as mesmas requisições foram submetidas ao *LP-Proxy* com ajustes na precisão da ordem de 500 e 1000 metros. Pretendia-se verificar se os novos pontos de interesse mais próximos retornados eram similares aos encontrados na primeira etapa.

O segundo teste realizado tinha por objetivo verificar os tempos de resposta com a utilização do *LP-Proxy* em comparação com o mesmo parâmetro obtido sem nenhum intermediário, e avaliar a viabilidade de utilização do *proxy* apresentado no que diz respeito ao tempo de execução. Diferentemente do primeiro teste que foi executado em emuladores, este teste foi realizado a partir de um dispositivo móvel, para se obter resultado preciso de tempos de execução.

Com o primeiro teste concluiu-se que os pontos de interesse encontrados foram bastante semelhantes na grande maioria dos experimentos, o que leva a conclusão que é possível utilizar as técnicas de ajustes de precisão e ainda assim se obter serviços de boa qualidade.

O segundo teste também apresentou resultados satisfatórios. Enquanto o tempo de execução sem a utilização de um intermediário foi em média 2,536 segundos, o valor encontrado com a utilização do *LP-Proxy* foi de 3,231segundos, inserindo um atraso de apenas 695 milissegundos.

Com estes resultados conclui-se que o *LP-Proxy* permitiu a utilização dos Serviços Baseados em Localização para celulares com garantias de privacidade sem perdas expressivas no tempo de resposta. O *proxy* apresentado possui funcionalidades de ajuste de precisão, canal seguro de comunicação e bloqueio de transmissão informações que possam levar à identificação dos usuários. Essas características permitem oferecer garantia de privacidade ao usuário.

Com os resultados obtidos nos testes realizados neste trabalho, pode-se garantir a viabilidade de adaptação do *LP-Proxy* para a utilização de outros tipos de *LBS*, como o *pull* e *peer-to-peer*, preservando as garantias de privacidade. Ressalta-se também a viabilidade do desenvolvimento de um módulo para a adaptação da comunicação com os provedores *LBS*, uma vez que existem diferenças no formato das informações trocadas dependendo do provedor utilizado.

Referências

1. Perusco, L., Michael, K.: Control, trust, privacy, and security: evaluating location-based services. Technology and Society Magazine, IEEE, Volume 26, Issue 1, Spring, pp 4 – 16, (2007).
2. Warrior, J., Mchenry, E., Mcgee, K.: They Know Where You Are. IEEE Spectrum, Volume 40, No. 7, pp 20-25, (2003).

3. 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, Sweden, (2006).
4. 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, p 163c. IEEE Computer Society Press, Havaii (2007).
5. Weiser, M.: The Computer for the 21st Century, Scientific American, Volume 265, Issue 3, pp.94-104, (1991).
6. Cas, J.: Privacy in pervasive computing environments - a contradiction in terms?. Technology and Society Magazine, IEEE. Volume 24, Issue 1, Spring, pp 24 – 33, (2005).
7. 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), Austria, (2004).
8. Beresford, A. R., Stajano, F. J.: Location Privacy in Pervasive Computing. IEEE Pervasive Computing, Volume 2, Issue 1, pp 46-55, (2003).
9. Pfitzmann, A., Kohntopp, M.: Anonymity, unobservability, and pseudonymity: a proposal for terminology. In International Workshop on Designing privacy enhancing technologies, pp. 1-9, Springer-Verlag, New York (2001).
10. Etoh, M.: Next Generation Mobile Systems: 3G and Beyond. Wiley, San Francisco (2005).
11. Küpper A.: Location Based Services – Fundamentals and Operation. Willey, England (2005).
12. Vivo Encontra, http://www.vivo.com.br/vivodownloads/aplicativos.php?cat=12
13. Mobiloco, http://www.mobiloco.de/index.php
14. TOGuide - Interactive Turin Guide, http://www.lobase.it/en/?TOguide
15. GMM – Google Maps Mobile, http://www.google.com/gmm/index.html
16 Cheng, H. S., Zhang, D., Tan, J. G.: Protection of Privacy in Pervasive Computing Environments. In: International Conference on Information Technology: Coding and Computing, pp. 242-247, (2005).
17. Bettini, C., Wang, X. S., Jajodia, S.: Protecting Privacy Against Location-Based Personal Identification. In: The *Second VLDB Workshop Secure Data Management (SDM '05)*. LNCS 3674, Springer-Verlag Berlin Heidelberg, pp. 185-199, (2005).
18. OECD. Organization for Economic Co-Operation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. September, (1980).
19. OMA – (Open Mobile Alliance) - OMA Privacy Guidelines, (2002). http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/lif/lif-tr-101-v2.0.0.zip
20. 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).
21. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: The 1st International Conference on Mobile systems, applications and services, pp 31–42, ACM, New York (2003).
22 Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing Location-Based Identity Inference in Anonymous Spatial Queries. IEEE Transactions on Knowledge and Data Engineering (IEEE TKDE), Volume: 19, Issue: 12, pp. 1719-1733 (2007).
23 Cheng, H. S., Zhang, D., Tan, J. G.: Protection of Privacy in Pervasive Computing Environments. In: International Conference on Information Technology: Coding and Computing, pp. 242-247, IEEE Computer Society, Washington (2005).
24 Kido, H., Yanagisawa Y., Satoh, T.: An Anonymous Communication Technique using Dummies for Location-based Services. In: IEEE International Conference on Pervasive Services, pp 88-97, (2005).
25 Tele Atlas, http://www.teleatlas.com/index.htm.
26 deCarta, http://www.decarta.com/.