UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MODELO DE COMPARTILHAMENTO DE LOCALIZAÇÃO EM REDES SOCIAIS MÓVEIS COM GARANTIAS DE PRIVACIDADE

TIAGO ANTÔNIO ROSA

ORIENTADOR: PROF. DR. SERGIO DONIZETTI ZORZO

São Carlos - SP
Janeiro/2015

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MODELO DE COMPARTILHAMENTO DE LOCALIZAÇÃO EM REDES SOCIAIS MÓVEIS COM GARANTIAS DE PRIVACIDADE

TIAGO ANTÔNIO ROSA

Dissertação 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, área de concentração: Sistemas Distribuídos e Redes.
Orientador: Dr. Sergio Donizetti Zorzo

São Carlos - SP
Janeiro/2015

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária UFSCar
Processamento Técnico
com os dados fornecidos pelo(a) autor(a)

Rosa, Tiago Antônio
R788m Modelo de compartilhamento de localização em redes sociais móveis com garantias de privacidade / Tiago Antônio Rosa. -- São Carlos : UFSCar, 2015.
102 p.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2015.

1. Redes Sociais Móveis. 2. Privacidade. 3. Compartilhamento de localização. I. Título.

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ciência da Computação

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Tiago Antonio Rosa, realizada em 23/03/2015:

Prof. Dr. Sergio Donizetti Zorzo
UFSCar

Prof. Dr. Helio Crestana Guardia
UFSCar

Profa. Dra. Luanna Lopes Lobato
UFG-Catalão

Prof. Dr. Robson Eduardo de Grande
uOttawa

Dedico este trabalho à minha família e à minha esposa, minhas maiores inspirações e motivação, meu alicerce e porto seguro durante todos os momentos, onde sempre pude buscar conforto e força nos momentos de fraqueza e desânimo.

AGRADECIMENTOS

Primeiramente, agradeço a Deus pela força, paciência, por estar sempre comigo nas viagens e guiar os meus passos. Enfim, agradeço-Lhe por tudo, pois, sem Ele eu não teria conseguido chegar até aqui. Aos meus pais, pelo apoio recebido e também aos familiares. À minha esposa, que esteve sempre presente na minha luta. Agradeço ao professor Zorzo pela orientação, amizade e, principalmente, pela confiança. Aos professores da PUC Minas – Poços de Caldas, pelo apoio e incentivo. Enfim, agradeço a todos que participaram e contribuíram para esta minha conquista.

Os grandes feitos são conseguidos não pela força, mas pela perseverança.

Samuel Johnson

RESUMO

Redes sociais móveis caracterizam-se pelo compartilhamento das informações de contexto dos usuários, como a localização de seus dispositivos móveis, aos demais usuários. A informação da localização em uma rede social possibilita que os provedores ofereçam produtos e serviços baseados na área geográfica. Alguns usuários, contudo, consideram essas informações como ganho pessoal, outros como invasão de privacidade. Por outro lado, o compartilhamento da localização de um usuário a um amigo particular ou a um grupo particular de amigos, sem que os provedores de redes sociais tenham acesso a essa informação com precisão, poderia garantir a segurança e a privacidade da informação. Neste trabalho é apresentado um modelo de rede social móvel com garantias de privacidade da localização de seus usuários a um grupo de amigos. Para tanto, permite configurar regras que determinam com quem, quando e onde a informação da localização pode ser disponibilizada. O modelo fornece três níveis de privacidade, escolhida pelo usuário, com o emprego de técnicas de anonimato e difusão/ajuste da localização que garantem a ocultação da informação antes desta ser disponibilizada na rede social. Uma prova de conceito do modelo proposto, denominada RSM Privacy, foi desenvolvida para a plataforma Android. Testes de desempenho evidenciaram que os atrasos gerados pelo uso do RSM Privacy são proporcionais e justificáveis aos níveis de privacidade desejáveis e escolhidos pelos usuários. A prova de conceito do modelo – RSM Privacy – foi avaliada por um grupo de 50 usuários quanto aos aspectos de usabilidade e foi evidenciada a eficiência das técnicas presentes no modelo proposto.

Palavras-chave: Redes Sociais Móveis, Privacidade, Compartilhamento de Localização.

ABSTRACT

Mobile social networks are characterized by the sharing of user context information, such as the location of one's mobile device, with one's friends and groups of friends. The location information in a social network enables providers to offer products and services based on geographical area, which is considered either a personal gain or an invasion of privacy by the users who receive these offers. A user sharing location information with a particular friend or group of friends, without social network providers having access to this information, ensures the safety and privacy of the information. This paper presents a model of mobile social networking with privacy guarantees regarding sharing the location of members with groups of friends; it allows users to configure rules that determine to whom, when and where location information can be made available. The model provides three levels of privacy, chosen by the user, using techniques of anonymity and diffusion, which adjust the location to ensure the concealment of the information before it is made available on the social network. The proof of concept of the proposed model, called RSM Privacy, was developed for the Android platform. Performance tests showed that delays generated by the use of RSM Privacy are proportional to and justifiable for the privacy levels desired and chosen by users. A group of 50 users evaluated the model proof of concept, RSMPrivacy, with respect to usability and verified the efficiency of the techniques included in the proposed model.

Keywords: Mobile Social Network, Privacy, Location-sharing.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

RSM - Redes Sociais Móveis

GPS - *Global Positioning Services*

API - *Application Programming Interface*

LPBS - *Location Privacy Based Services*

ISD - *Information Sharing Directory*

LBS - *Location-Based Services*

SBPL - Sistema Baseado em Privacidade de Localização

OECD - *Organization for Economic Co-Operationand Development*

SRS - Servidor de Rede Social

AC - Autoridade Certificadora

RSM Privacy - Rede Social Móvel com Privacidade

DAO - *Data Access Objetcs*

DFS - *Depth First Search*

SSL - *Secure Sockets Layer*

SOAP - *Simple Object Access Protocol*

TMR - Tempos Médios de Resposta

DP - Desvio Padrão

SUMÁRIO

Capítulo 1

CAPÍTULO 1 - INTRODUÇÃO

1.1 Contexto

Os provedores de mídias sociais fornecem meios de comunicação que são usados entre seus usuários para realizar interações sociais. As Redes Sociais são um tipo de mídia social com maior popularidade entre os usuários. Conceitualmente, uma Rede Social é uma estrutura de entidades conectadas umas com as outras através de um ou mais tipos específicos de interdependências, tais como amizade, parentesco, interesse em comum, troca financeira, empatia ou relações de crenças, conhecimento ou prestígio (Wassermane F 1994). Indivíduos, organizações ou grupos são exemplos de entidades. A interação entre essas entidades acontece e torna-se possível através das tecnologias existentes e meios de comunicação como, por exemplo, a Internet.

As Redes Sociais despertaram e despertam um grande interesse tanto na área acadêmica como no mundo empresarial e comercial. Diversos grupos de pesquisas têm focado seus esforços e trabalhos na tentativa de resolver problemas diversos em Redes Sociais ou criar novos recursos, como serviços para socialização e mecanismo de privacidade para os usuários. Além disso, esses grupos extraem conhecimentos que são utilizados em outras áreas, tais como comercial, psicologia, comunicação, econômica, ciências sociais, dentre outros (Teles et al. 2013).

Muitas organizações e empresas utilizam os conhecimentos adquiridos das redes sociais para promover seus produtos e serviços. Além disso, essas

organizações ainda utilizam as redes sociais para estabelecer comunicação direta com seus clientes e para realizar atendimentos e suporte.

As Redes Sociais Móveis (RSM) são uma subclasse das Redes Sociais, na qual os usuários interagem acessando as Redes Sociais através de seus dispositivos móveis com comunicação sem fio. RSM surgiram como consequência da popularidade de Redes Sociais e com a popularização de dispositivos móveis que, além de se tornarem cada vez mais baratos, permitem acesso, processamento e compartilhamento de informações a qualquer tempo e em qualquer lugar, fornecendo ubiquidade de acesso. Além disso, os dispositivos móveis atuais possuem um maior poder de processamento, múltiplas interfaces de redes, sistema global de localização (GPS) e uma variedade de sensores, como magnetômetro e acelerômetro.

Dessa forma, dispositivos móveis vêm permitindo a execução de aplicações cada vez mais sofisticadas e com capacidade de identificar alguns aspectos do contexto do usuário ou até sua atividade corrente. Utilizando RSM em seus dispositivos, os usuários podem acessar (ler), publicar (escrever ou inserir) e compartilhar (retransmitir ou divulgar) conteúdos criados ou obtidos através de sensores no dispositivo. O Facebook[1] é um exemplo de RSM que possuía mais de 680 milhões de usuários móveis em 2014 (Facebook 2014). Outras RSM populares são Twitter[2], Instagram[3], Foursquare[4] e WhatsApp[5].

Aplicações de RSM, também chamadas apenas de aplicações sociais móveis, podem auxiliar pessoas a manterem contato entre si em qualquer lugar, a qualquer momento. Além disso, os usuários podem compartilhar em uma RSM uma série de informações de contexto. Entre estas informações está a localização atual do usuário. Ao compartilhar a sua localização em RSM, os usuários possibilitam prover recomendações em tempo real e conteúdo personalizado, que pode ser, por exemplo, uma propaganda de uma loja próxima ao local em que o usuário se encontra.

Nesse cenário, RSM são caracterizadas por adicionar informações de contexto em Redes Sociais, uma vez que dispositivos móveis obtêm dados físicos

[1] https://www.facebook.com/
[2]https://twitter.com/
[3]https://instagram.com/
[4]https://foursquare.com/
[5] https://www.whatsapp.com

do ambiente através dos sensores e, assim, aplicações podem combinar dados de contexto e inferir a situação dos usuários. Isso possibilita melhorar as relações existentes entre os usuários ou criar novas a partir de interesses comuns, tais como esportes praticados, lugares frequentados, gostos musicais, mensagens publicadas, dentre outros.

O compartilhamento de localização em RSM possibilita a oferta de recomendações pela rede social, que para muitos usuários são ganhos pessoais, mas para outros geram preocupações com os aspectos de privacidade. Tosh (Tosh et al. 2010) e Benisch (Benisch et al. 2011) evidenciaram tais preocupações com a disponibilização da localização em aplicações de redes sociais, podendo afetar a iniciativa dos usuários na utilização dessas aplicações. A informação de localização compartilhada é utilizada pelo provedor de rede social para oferecer recomendações de novos amigos, lugares, produtos, entre outros. Porém, esses provedores podem fazer mau uso das informações de localização compartilhada, acarretando riscos à privacidade de seus usuários. Além disso, usuários mal-intencionados, pertencentes à rede social, também têm acesso às localizações compartilhadas pelos outros usuários e, dessa forma, esses também são uma ameaça à privacidade.

De posse de informações de localização compartilhada na rede social, os atacantes (provedor ou usuários mal intencionados) podem levar riscos à privacidade de usuários de RSM no que diz respeito a Privacidade da identidade, Privacidade da posição e Privacidade do caminho.

Privacidade da Identidade é quando um atacante pode adquirir a identificação do usuário associada ou inferida a partir das informações de localização. Informações de localização podem ser fornecidas a alguma entidade, mas a identidade do usuário deve ser preservada.

Privacidade de posição é quando o atacante ameaça a privacidade do usuário através da obtenção de sua real localização.

Privacidade de caminho é quando o atacante obtém localizações anteriores pelas quais o usuário passou, ou seja, o caminho atravessado pelo usuário.

Algumas redes sociais móveis, como o Facebook, já oferecem controle de privacidade aos seus usuários quando forem utilizar uma dada aplicação. Esse controle é realizado respeitando as políticas de privacidade estabelecidas, que determinam quem são os usuários da rede social que podem conhecer a sua localização e em quais locais, datas e horários essas informações podem ser

disponibilizadas. Tais políticas estabelecidas pelas redes sociais, quando existem, são implementadas com limitações nos aspectos de oferta ou não da localização real do usuário e quanto ao grupo de usuários que se aplicam. Em geral, as politicas se limitam no controle de coleta de informações, controle de acesso a dados pessoais dos usuários, segurança dos dados transmitidos e responsabilidade dos usuários.

1.2 Motivação e Objetivos

Em RSM existem conflitos entre o oferecimento de recursos aos usuários para socialização (como sugestão de novos amigos, produtos e serviços) e mecanismos de privacidade (privacidade da localização, permissão de acesso a informações, visualização de informações) para conter vazamento de dados pessoais dos usuários (Zhang et al. 2010). Assim, quanto maior a oferta de sociabilidade realizada pela RSM, maiores são as chances de ocorrerem problemas com a privacidade de seus usuários. Isso ocorre devido à existência de uma demanda em fornecer recursos para sociabilidade, tais como acesso a lista de contatos, acesso a conteúdo público, recomendação de amigos, recomendação de lugares que viola a privacidade de seus usuários. Muitos desses recursos só podem ser oferecidos com a utilização de informações de contexto (Zhang et al. 2010).

Informações de contexto fornecem recursos e a possibilidade de construir muitos tipos de serviços para RSM. Entretanto, elas também criam novos problemas referentes à violação de privacidade. Informações de contexto publicadas em Redes Sociais podem comprometer a privacidade do usuário por conterem, ou a partir delas poder-se inferir, muitas informações pessoais sensíveis que um usuário não quer deixar disponíveis para o provedor e para outros usuários da Rede Social. Uma prática comum realizada pelos usuários e que pode agravar ainda mais a violação de privacidade é a agregação de contexto a conteúdo sem o conhecimento do mesmo. Por exemplo, publicar uma foto adicionando a ela a localização, data e horário em que ela foi tirada. Em muitas aplicações sociais móveis essa agregação é feita sem o consentimento explícito do usuário.

A proteção de informações de contexto de localização é particularmente importante em RSM, devido à grande quantidade de aplicações que fornecem recursos baseados na localização do dispositivo móvel. Privacidade de localização pode ser definida como o direito do usuário de decidir como, quando e para qual propósito suas informações de localização podem ser reveladas a outros (Ardagna et al. 2007). Além disso, os usuários também têm o direito de decidir se o provedor da rede social pode ter acesso às suas informações de localização e como elas são manipuladas. O compartilhamento de localização em RSM pode revelar a identidade do usuário, sua posição atual e o seu caminho rotineiro ao provedor e aos usuários mal-intencionados. Essas informações podem comprometer a privacidade e a segurança dos usuários de RSM. Os problemas ocasionados pelo compartilhamento de localização em Redes Sociais Móveis motivaram a pesquisa e o desenvolvimento deste trabalho.

O objetivo deste trabalho é apresentar um modelo de compartilhamento de localização em Redes Sociais Móveis com garantias de privacidade. O modelo fornece mecanismos que buscam garantir a privacidade da localização individual do usuário e a localização de um grupo de usuários formado dentro da rede social. No modelo, a privacidade é personalizada pelo usuário e pode ser configurada utilizando níveis e políticas. Os níveis definem a precisão da localização que será compartilhada e as políticas possibilitam aos usuários definirem com quem, onde e quando compartilhar a localização. Todos os mecanismos de privacidade oferecidos pelo modelo são executados no dispositivo do usuário. Dessa forma, o modelo não permite que a localização real do usuário com alta precisão seja obtida pelo provedor da rede social e por usuários maliciosos.

De um modo geral, os objetivos do trabalho são:

- A proposta de um modelo de compartilhamento de localização em redes sociais móveis com garantias de privacidade;
- Ocultar do servidor e demais usuários a localização real e com alta precisão do usuário para evitar que, através desta informação, sua identidade seja inferida;
- Propor regras que permitam ao usuário configurar a sua privacidade e desta forma oferecer privacidade e possibilitar a ele usufruir dos benefícios oferecidos pela rede social;

- Implementar as técnicas e regras de privacidade de uma maneira que não prejudique o funcionamento da rede social ou cause atrasos excessivos.

1.3 Metodologia de Desenvolvimento do Trabalho

Ao compartilhar sua localização em uma RSM, os usuários possibilitam que esta informação seja obtida pelo provedor de rede social e, eventualmente, por usuários mal-intencionados. Não existem garantias de como essas informações são manipuladas pelo provedor, que pode apenas utilizá-las para recomendações de serviços, ou pode violar a segurança e a privacidade de seus usuários. Usuários maliciosos pertencentes à RSM podem fazer mau uso das informações de localização compartilhadas para obter o caminho realizado pelos usuários, uma posição real e outras informações que violam a privacidade e oferecem riscos à sua segurança.

Após detectar o problema do compartilhamento de localização em RSM citado anteriormente, pesquisas foram realizadas com o objetivo de encontrar técnicas e soluções que provessem privacidade aos usuários. Essas pesquisas foram realizadas em máquinas de indexação como IEEE, Springer, ACM. Os seguintes critérios foram utilizados para filtrar os resultados apresentados: *Privacy*, *Mobile*, *Location-sharing*, *Mobile Social Network*. Vários trabalhos foram encontrados, porém apenas alguns foram selecionados, sendo que alguns contribuíram diretamente com o problema. Além de buscas utilizando máquinas de indexação, pesquisas foram realizadas em artigos publicados em conferências internacionais na intensão de encontrar soluções para o problema da privacidade em RSM. Os trabalhos selecionados estão descritos no Capítulo 3 - Trabalhos Relacionados.

Com base nas técnicas e soluções encontradas nos trabalhos selecionados foi proposto um modelo de compartilhamento de localização em Redes Sociais Móveis com garantias de privacidade. No modelo, as técnicas e soluções aplicadas nos trabalhos relacionados foram combinadas em níveis e políticas de privacidade que podem ser configurados de acordo com a necessidade do usuário.

Com o intuito de validar o modelo proposto e suas técnicas de privacidade oferecidas, foi desenvolvido um protótipo de RSM denominado RSM Privacy. Para o desenvolvimento do protótipo foi necessária a utilização de algumas tecnologias como a plataforma Android (Android 2014) e linguagem de programação Java. A escolha da plataforma Android se deu pelo fato de ser livre e de código aberto (*Opensource).* Outras plataformas poderiam ser utilizadas, como o iOS e Windows Phone. Porém, essas plataformas são proprietárias e a sua utilização adicionaria custos ao projeto, devido ao uso de licença.

Com o objetivo de avaliar o protótipo – RSM Privacy – testes de desempenho e usabilidade foram realizados. Para a realização dos testes de desempenho foi utilizada a seguinte metodologia:

- Utilização de dois dispositivos *Smartphone* com a plataforma Android. Foi necessária a utilização de dois dispositivos, pois para os testes são necessárias duas localizações diferentes e dois usuários distintos utilizando a RSM;
- O protótipo foi executado automaticamente, sem a intervenção do usuário, através de um processo (serviço) que disparou varias requisições de localização;
- Para a análise de desempenho foram realizadas medições com o tempo de execução. Os resultados das medições foram utilizados para calcular o tempo médio de execução.

Com o intuito de validar as técnicas de privacidade e regras oferecidas pelo modelo foi utilizada a seguinte metodologia:

- Realização de um estudo de campo para medir o comportamento do usuário ao utilizar o protótipo RSM Privacy e qual o impacto das técnicas de privacidade oferecidas. Neste estudo foram utilizados questionários e gravações de vídeo;
- Os questionários foram aplicados através de um site. Desta forma, a avaliação das respostas foi simplificada. Para medir a satisfação do usuário, foi utilizada nos questionários a escala de *Likert* de cinco pontos;
- Os testes foram realizados em dois laboratórios localizados em locais distintos dentro do campus de uma universidade. A realização do

estudo em dois locais distintos se deveu à necessidade de duas localizações diferentes;

- Para a realização do estudo foram utilizados computadores com emulação da plataforma Android.

Os testes de desemprenho visaram a verificar o impacto causado pelas técnicas de privacidade na performance da aplicação. Os testes de usabilidade visaram a medir, além da usabilidade da aplicação, a aceitação e a eficiência dos mecanismos oferecidos. Para obter os resultados foi realizado um estudo de campo e foram aplicados questionários a potenciais usuários.

1.4 Organização do Trabalho

O trabalho está organizado da seguinte forma: no Capítulo 2 são apresentados os conceitos de Redes Sociais Móveis, suas características e questões de privacidade. No Capítulo 3 são apresentados os trabalhos relacionados, suas características e contribuições. No Capítulo 4 é apresentado o Modelo de Compartilhamento de Localização em Redes Sociais Móveis com Garantias de Privacidade, sua arquitetura, técnicas e regras de privacidade. No Capítulo 5 são apresentados os detalhes do desenvolvimento do protótipo de RSM com base no modelo proposto e os testes de desempenho. No Capítulo 6 são apresentados o estudo de usabilidade realizado e os resultados obtidos. No Capítulo 7 são apresentadas as conclusões e, por fim, as referências bibliográficas utilizadas.

Capítulo 2

CAPÍTULO 2 - REDES SOCIAIS MÓVEIS

2.1 Considerações iniciais

As Redes Sociais Móveis surgiram com a popularidade de Redes Sociais e no uso de dispositivos móveis. Esses dispositivos sofreram melhorias de hardware e o seu baixo custo possibilitou a popularização entre os usuários (Teles et al. 2013). Os usuários utilizam seus dispositivos móveis para acessar a rede social e assim compartilham, publicam ou apenas acessam conteúdos criados por si ou obtidos através de sensores presentes nos dispositivos. Dentre os conteúdos compartilhados está a informação da localização que pode ser compartilhada com um único usuário individualmente, ou com um grupo de usuários que podem ser formados por grau de parentesco, por afinidades ou de acordo com critérios definidos pelo próprio usuário. Além disso, entidades pertencentes à rede social (que podem ser serviços ou aplicações de terceiros) podem ter acesso a localização compartilhada.

Neste capítulo é apresentada, primeiramente, uma visão geral sobre as Redes Sociais Móveis, na seção 2.2. Na seção 2.3 é apresentada a arquitetura de Redes Sociais Móveis. Na seção 2.4 são apresentadas as questões referentes à privacidade em Redes Sociais Móveis e suas possíveis ameaças e, por fim, na seção 2.5, são apresentadas considerações finais sobre o tema.

2.2 Redes Sociais Móveis – Visão Geral

Redes Sociais Móveis (RSM) são caracterizadas por adicionar informações de contexto às redes sociais, uma vez que dispositivos móveis monitoram dados

físicos e, a partir disso, aplicações podem combinar e inferir o contexto dos usuários. Além disso, as RSM possibilitam ao usuário acessar, publicar ou compartilhar conteúdo gerado ou obtido através de sensores no dispositivo móvel para interação com os seus contatos na rede social.

Segundo Boyd e Ellison (Boyd e Ellison 2007), Redes Sociais Online podem ser definidas como um conjunto de serviços baseados na web que permitem ao indivíduo: (1) construir um perfil público ou semi-público dentro do sistema; (2) manter uma lista de contatos e se comunicar com os membros dessa lista e estabelecer elos para futuras interações; (3) consultar sua lista de contatos e de outros amigos e conhecidos dentro do sistema.

Nas Redes Sociais, a exibição pública dos contatos é um componente essencial. As listas de contatos são links para o perfil de cada usuário. Dessa forma, a Rede Social possibilita a navegação por essas listas de contatos. Na maioria das Redes Sociais, a lista de contatos permanece visível para quem está autorizado a visualizar o perfil do usuário.

A maioria das Redes Sociais também inclui o mecanismo de “comentários”, que são formas de deixar recados nos perfis dos contatos. Além disso, as Redes Sociais muitas vezes possuem o recurso de mensagens privadas, que são trocadas apenas com um contato ou com um grupo específico de contatos. Essas formas de comunicação (pública e privada) são comuns na maioria das Redes Sociais, embora existam algumas nas quais elas não estejam presentes.

Tipicamente, os usuários de Redes Sociais geram uma grande quantidade de conteúdos, tais como texto, fotos, áudio e vídeo. O conteúdo gerado pode ser acessado por contatos que pertencem à lista do usuário e, no caso do perfil ser público, pelos contatos dos contatos.

Segundo Kayastha (Kayastha et al. 2011), RSM compreendem um subconjunto das Redes Sociais Online. RSM podem ser vistas como uma combinação de três áreas do conhecimento: Redes Sociais, Computação Móvel e Ciência de Contexto. Na Figura 2.1 é apresentada a visão de RSM.

Figura 2.1. Definição de Redes Sociais Móveis.

FONTE: Kayastha *et al*., 2011

Esses usuários podem ser indivíduos, organizações ou sistemas. A Computação Móvel possibilita que os usuários fiquem sempre conectados, devido ao suporte à mobilidade fornecida pelos dispositivos e à ubiquidade da conectividade sem fio.

Os dispositivos móveis atuais possuem novos recursos que fornecem conectividade sem fio e podem permitir acesso, processamento e compartilhamento de informações a qualquer hora e em qualquer lugar. Além disso, os dispositivos possuem cada vez mais sensores e capacidade de processamento de informação que pode ser enviada diretamente para as RSM.

Contexto é definido por Dey [2001] como sendo qualquer informação que pode ser usada para caracterizar a situação de uma entidade. Sistemas Sensíveis ao Contexto são capazes de adaptar suas funcionalidades de acordo com o contexto atual do usuário sem sua explícita intervenção. As RSM, por exemplo, adaptam as informações disponibilizadas e a lista de potenciais contatos para interação, bem como informações de presença, além de fornecerem serviços de acordo com as informações de contexto adquiridas (Day et al. 2000). As informações de contexto podem ser adquiridas a partir de sensores embarcados no dispositivo como o GPS,

que permite capturar a localização atual do usuário. A junção de informações de contexto com informações do usuário como dados do perfil, relacionamentos, são chamados de contexto pervasivo e contexto social.

O contexto pervasivo é aquele obtido a partir de sensores de hardware nos dispositivos móveis, que podem ser de vários tipos, por exemplo: de luz, visual (câmera), de áudio, de movimento (ou acelerômetro), de toque, de temperatura, físicos (bio-sensores) (Baldauf et al. 2007]. As informações de contexto pervasivo são extremamente úteis para RSM, pois a partir dos dados gerados pelos sensores, é possível inferir a situação do usuário, como por exemplo, o lugar em que se encontra (trabalho, residência, restaurante).

A inferência da situação do usuário fornece informações que são utilizadas por RSM para aumentar o nível de colaboração entre seus usuários. Por exemplo, obtendo informações do GPS, a RSM pode fornecer serviços ou propagandas de estabelecimentos próximos, ou informações de amigos que se encontram na região. Além disso, as informações podem revelar se o usuário entra em movimento e, a partir disso, notificar amigos do usuário de que está ocupado e não pode atender as chamadas.

Sistemas de Compartilhamento de Localização são focados em explorar a localização como informação de contexto (Schiller e Voisard 2004). A evolução dos sistemas de posicionamento, em destaque o GPS e as abordagens de redes sem fio, facilitaram o desenvolvimento de sistemas que exploram a localização.

O Contexto Social pode ter várias definições, mas a maior parte delas foca nas possíveis formas de relacionamento e interações entre pessoas, intermediadas ou não por alguma tecnologia de comunicação (Ling, 2008]. O contexto social está relacionado ao ambiente social do usuário, como por exemplo, uma festa ou uma reunião, e a relação que pode ser estabelecida com outros usuários. O conjunto de pessoas que um usuário conhece, o grau de confiança, as formas e intensidade das interações, a regularidade dessas interações e o assunto ou conteúdo das interações, são elementos centrais nos quais se baseia o contexto social.

As Redes Sociais estão sendo cada vez mais utilizadas através de dispositivos móveis. A associação de dados de contexto, como a localização, e as informações geradas a partir do dispositivo, revelam muito sobre o comportamento dos usuários, interesses, atividades, hobbies, expectativas, etc. A união da

Computação Móvel e informações de contexto possibilitou que Schuster et al. [Schuster et al. 2012] desenvolvessem o conceito de Contexto Social Pervasivo.

Contexto Social Pervasivo de um indivíduo é o conjunto de informações que surgem a partir de interações diretas entre pessoas que carregam dispositivos móveis equipados com sensores e que estejam conectadas através de uma mesma Rede Social. Schuster et al. (Schuster et al. 2012) classificaram as formas com que o Contexto Social Pervasivo pode ser utilizado baseados nas W5H questions, como visto abaixo:

- Quem - *Who*: expressa quem são os participantes envolvidos no consumo e produção das informações de contexto;
- O que - *What*: diz respeito a qual tipo de contexto é utilizado ou se é importante para a aplicação;
- Onde - *Where*: relacionado a onde (localização física) os laços ou interações sociais são estabelecidos;
- Quando - *When*: caracterização das interações entre usuários e as informações de contexto que eles produziram em uma perspectiva temporal;
- Porquê - *Why*: expressa o porquê de uma informação de contexto ser usada, determinando a causa ou razão dela estar sendo usada pela aplicação. Neste caso, isso é bem relacionado ao objetivo da aplicação;
- Como - *How*: expressa como a informação de contexto (originada a partir do mundo real, mundo virtual ou de ambos) pode influenciar ou comprometer aplicações.

No geral, o que caracteriza uma Rede Social Móvel é a obtenção de conteúdo através de recursos presentes no dispositivo, como, por exemplo, sensores de acelerômetro, temperatura, câmera e obtenção da localização por meio de GPS. Essas informações obtidas produzem conteúdos diversificados que são compartilhados em uma RSM. Esse compartilhamento pode ser realizado com ou sem o consentimento do usuário.

Em projetos de Redes Sociais há conflitos entre o oferecimento de recursos aos usuários para socialização (tais como recomendação de amigos, lugares e páginas, acesso à lista de contatos de outros usuários, acesso a conteúdos públicos, entre outros.) e mecanismos de privacidade para conter vazamento de dados

pessoais dos usuários (acesso não autorizado a dados, conteúdos e localização) [Zhang *et al*., 2010]. Recursos oferecidos em Redes Sociais para fornecer sociabilidade (recomendação de amigos, lugares, acesso a conteúdo publicado) contribuem para o surgimento de brechas de privacidade, que são usadas por usuários mal-intencionados para obter acesso indevido a informações. A seguir, serão discutidas questões de privacidade em Redes Sociais Móveis.

2.3 Arquitetura de Redes Sociais Móveis

No desenvolvimento de aplicações de RSM se destacam três principais arquiteturas: arquitetura centralizada, arquitetura distribuída e uma arquitetura híbrida [Teles *et al.*, 2013]. As arquiteturas centralizadas e distribuídas são ilustradas na Figura 2.2.

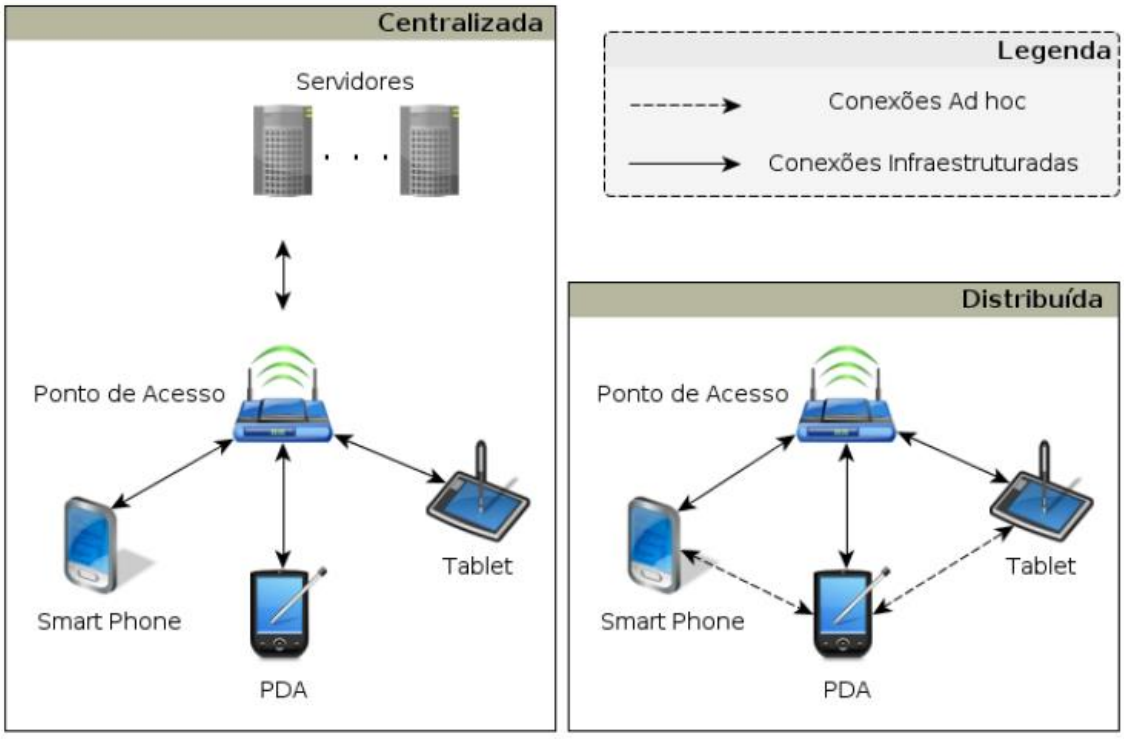

Figura 2.2. Arquiteturas de Redes Sociais Móveis.

FONTE: Teles et al. 2013

Na arquitetura centralizada, os dados estão centralizados em um ou mais servidores, que são responsáveis pelo gerenciamento e pela entrega dos dados aos usuários de RSM. Os dados podem ser informações de perfis, informações de

contexto, como por exemplo, a localização. Os usuários móveis são representados por aplicações de RSM instaladas em seus dispositivos. Os dispositivos podem ser *tablets*, *smartphones*, PDAs.

Na arquitetura distribuída, os usuários de dispositivos móveis se comunicam diretamente sem a necessidade de acessarem um servidor. As conexões entre os dispositivos móveis podem ser realizadas através de uma infraestrutura de rede ou por meio de conexões *ad-hoc*, como ilustrado na Figura 2.1. Essa arquitetura possibilita que os usuários compartilhem informações sem utilizar acesso à Internet, com um mínimo de infraestrutura de rede.

Uma terceira arquitetura para RSM é a arquitetura híbrida. É uma combinação da arquitetura centralizada com a arquitetura distribuída. A arquitetura híbrida permite que os usuários móveis acessem e compartilhem informações através de servidores (arquitetura centralizada) e com outros usuários próximos (co-localizados ou próximos uns dos outros), estabelecendo conexões diretas (arquitetura distribuída). Assim, a arquitetura híbrida pode usufruir das vantagens das duas arquiteturas.

A escolha da arquitetura para o desenvolvimento de uma RSM impacta diretamente nos serviços que serão disponíveis e, consequentemente, nos modelos de privacidade, pois a arquitetura escolhida pode não ser adequada para os requisitos de determinadas aplicações. Além disso, influencia na escolha de algoritmos que serão utilizados no desenvolvimento da RSM.

Para tanto, neste trabalho foi utilizada a arquitetura centralizada, visto que apresenta as características de funcionamento da maioria das aplicações de RSM e se encaixa nos requisitos do modelo proposto neste trabalho.

2.4 Privacidade em Redes Sociais Móveis

Em RSM, a proteção de informações de contexto de localização é essencialmente importante, devido ao grande número de aplicações que exploram esse tipo de informação para fornecer recursos baseados na localização dos dispositivos móveis. Dessa forma, essas aplicações podem fazer mal uso das informações adquiridas e exploradas. Privacidade de localização pode ser definida

como o direito do usuário de decidir como, quando, com quem e para qual finalidade suas informações de localização podem ser reveladas a outros (Ardagna et al. 2007). Anthony et al. (2007) identificaram as seguintes categorias de privacidade de localização:

- Privacidade da Identidade: na qual o objetivo é proteger a identificação do usuário, associada ou inferida a partir das informações de localização. Informações de localização podem ser fornecidas a alguma entidade, mas a identidade do usuário deve ser preservada;
- Privacidade de Posição: na qual o objetivo é ocultar a localização exata do usuário a fim de proteger sua real localização;
- Privacidade de Caminho: na qual o objetivo é não revelar localizações anteriores nas quais o usuário passou, ou seja, o caminho atravessado pelo usuário.

Todo o conteúdo publicado, em especial a localização, pode ser acessado ou compartilhado com outras entidades, que representam possíveis origens de ataques de privacidade. Gao et al. (2011) consideraram estas origens como brechas de segurança que podem ser classificadas em função do acesso por: (i) outros usuários da Rede Social, (ii) aplicações de terceiros e (iii) o próprio provedor de serviços.

Outros usuários da Rede Social representam uma ameaça devido à facilidade que atacantes têm para ingressarem na Rede Social, criando uma conta no provedor de serviços e se tornando um usuário autêntico. Esses usuários maliciosos também podem produzir informações de contexto falsas para a RSM que serão usadas pelo usuário mal-intencionado para ganhar acesso a recursos, ganhar uma identidade temporária e integrar grupos de usuários formados automaticamente pela RSM. Ao compartilhar sua localização com um grupo, formado automaticamente pela RSM, o usuário permite que estes usuários maliciosos também obtenham esta informação. Estes, por sua vez, podem fazer mal uso da localização, trazendo riscos à privacidade do usuário. O mau uso das informações é caracterizado pelo monitoramento do deslocamento do usuário sem o seu consentimento ou conhecimento, posicionamento atual do usuário, descoberta de lugares frequentados, rotina inferida através do histórico de localizações, entre outros. Essas informações podem não só violar a privacidade dos usuários como causar danos à sua segurança.

Aplicações de terceiros são desenvolvidas utilizando a API (*Application Programming Interface*) disponibilizada pela RSM. Essa API fornece a possibilidade da criação de novos recursos para a RSM. Essas aplicações são desenvolvidas por terceiros e, portanto, não são sempre confiáveis. Aplicações de terceiros podem ser jogos, aplicativos de músicas, fotos e vídeos, e até aplicativos de agências de publicidade que realizam campanhas promovendo produtos e serviços. Essas aplicações requerem ao usuário a permissão de acesso livre às suas informações pessoais, dentre elas, sua localização compartilhada, histórico de movimentação.

O provedor de serviços da rede social é responsável por fornecer os recursos necessários aos usuários de RSM. Ele tem acesso a todas as informações pessoais, relacionadas aos usuários, que foram inseridas ou publicadas. O provedor é responsável pela gerência e pela entrega da localização compartilhada por um usuário com um amigo ou grupo de amigos. Dessa forma, o provedor também tem acesso à localização compartilhada. Por este motivo, os usuários vêm deixando de confiar no provedor de serviços e se preocupando cada vez com o fato de não saberem realmente por quem suas localizações compartilhadas estão sendo manipuladas.

2.5 Considerações finais

Para o modelo proposto neste trabalho, a arquitetura selecionada foi a arquitetura centralizada. É a mais adequada para os requisitos do modelo, pois, na maioria das vezes, os usuários estão distantes uns dos outros e por isso requisitam a localização.

A utilização de RSM permite que os usuários fiquem sempre conectados. Eles acessam o conteúdo publicado na rede social, visualizam a sua lista de contatos e compartilham informações geradas por si ou obtidas através de sensores presentes nos dispositivos dos usuários. Um exemplo de informação compartilhada é a localização que é obtida através do uso do GPS. Ao compartilhar sua localização com um amigo ou um grupo de amigos, os usuários abrem possibilidades de que usuários maliciosos e mesmo o provedor também tenham acesso a esta informação, comprometendo, assim, sua segurança e privacidade. O objetivo principal do modelo

proposto neste trabalho é garantir a privacidade dos usuários no compartilhamento de localização. Essa garantia é realizada através do oferecimento de técnicas que ocultam a localização real do usuário e de políticas que asseguram a permissão de acesso. Na literatura, alguns trabalhos contribuíram diretamente para a concepção das garantias de privacidade oferecidas pelo modelo. Esses trabalhos são apresentados na seção seguinte.

Capítulo 3

TRABALHOS RELACIONADOS

3.1 Considerações iniciais

A questão da privacidade em RSM é um problema relevante e que tem despertado interesse em pesquisadores. Na literatura são encontrados vários trabalhos que propõem formas de fornecer privacidade a usuários em RSM. Os trabalhos apresentados neste capítulo propuseram técnicas que fornecem privacidade aos usuários no compartilhamento de localização em RSM e em LBS (*Location-Based Services*). Esses trabalhos contribuíram diretamente para o desenvolvimento do modelo aqui proposto.

Este capítulo está organizado da seguinte forma: na seção 3.2 são apresentados os trabalhos relacionados ao compartilhamento de localização em redes sociais móveis e suas contribuições. Na seção 3.3 são apresentados os trabalhos relacionados à privacidade em LBS e suas contribuições. Por fim, na seção 3.4 são apresentadas as considerações finais.

3.2 Compartilhamento de Localização em Redes Sociais Móveis

Smith et al. (2005) realizaram uma investigação inicial sobre tecnologias que permitiam às pessoas compartilharem sua localização em redes sociais móveis. O resultado deste trabalho foi o desenvolvimento de um sistema denominado Reno.

Reno é um sistema que permite a seus usuários compartilhar suas localizações com outras pessoas. Além disso, esse sistema permite que seus usuários decidam, de forma manual, quando compartilhar a sua localização e predefinir os locais ou regiões onde esta informação será compartilhada. Reno utiliza SMS para notificar a localização dentro da rede social, e as coordenadas são adquiridas mediante triangulação de torres de celular. A escolha da utilização dessas tecnologias se deu devido ao alto custo na época para a aquisição dos dispositivos mais modernos, com GPS embutido.

A privacidade no sistema Reno é realizada apenas através da decisão de quando e onde o usuário deseja compartilhar a sua localização. Quando ele receber uma requisição de sua localização enviada por outro usuário, por exemplo, um amigo, o usuário requisitado decide quando responder a requisição com sua localização. O usuário pode definir no sistema alguns locais fixos, formando uma lista de locais predefinidos. Quando ele recebe uma, o sistema verifica a localização atual do usuário e se esta localização está registrada na lista de locais. Se estiver, a localização é automaticamente enviada sem a necessidade de intervenção do usuário. Por utilizar triangulação de torres de celular, a localização compartilhada é de baixa precisão.

O trabalho de Smith et al. contribuiu para a definição inicial dos parâmetros disponibilizados pelo modelo na criação de politicas de compartilhamento de localização.

Toch et al. (Toch et al. 2010) apresentaram um sistema de Rede Social Móvel, o Locaccino, que permite a seus usuários compartilharem sua localização com membros da sua RSM. Locaccino aproveita dados de redes sociais existentes, como o Facebook. Para se registrar no sistema, o usuário informa sua conta no Facebook e, dessa forma, a lista de contatos no Locaccino é gerada a partir dos contatos existentes no Facebook. A localização é obtida usando uma combinação de métodos: GPS, triangulação de torres de celulares e posicionamento Wi-Fi.

Locaccino possui uma arquitetura centralizada. O sistema é composto por um servidor de Rede Social, uma aplicação cliente para dispositivos móveis e uma pagina web. O servidor é responsável por armazenar as informações da rede social, realizar a conexão com os clientes móveis e disponibilizar uma interface onde os usuários podem acessar sua lista de contatos, realizar configurações de privacidade e ter acesso à auditoria, que apresenta todo o histórico de requisições de

compartilhamento de localização recebidas e realizadas. A aplicação cliente permite que os usuários acessem sua lista de contatos, requisitem a localização de seus amigos, e também permite acessar a auditoria. Essa aplicação foi desenvolvida para funcionar em dispositivos móveis (Android, Symbian e iPhone) e em dispositivos portáteis, como notebooks (Windows e Mac).

No Locaccino, a privacidade é tratada a partir de criações de políticas de privacidade. As políticas podem ser definidas utilizando as seguintes restrições:

- Amigos (Quem): Especifica com qual contato (amigo) ou grupo de contatos o usuário está disposto a compartilhar a sua localização;
- Tempo (Quando): Permite que os usuários definam intervalos de tempos (por exemplo, das 09:00 as 12:00) e dias da semana em que estão dispostos a compartilhar suas localizações;
- Localização (Onde): Permite que os usuários definam a área geográfica ou um local específico em que pretendem compartilhar suas localizações.

Locaccino também permite que o usuário combine as restrições acima, de forma a criar políticas de privacidade mais robustas. No primeiro acesso, a política padrão definida para todos os contatos do usuário é a lista negra. Dessa forma, todas as requisições de compartilhamento de localização recebidas serão negadas. Quando uma requisição é negada, Locaccino envia uma mensagem que não permite que quem as requisitou perceba que sua requisição foi negada. Na Figura 3.1 são apresentadas as interfaces das aplicações cliente de Locaccino.

Figura 3.1. Interface do Sistema Locaccino.

FONTE: Toch et al. 2010

Os autores realizaram testes de usabilidade com 2000 usuários, que comprovaram a eficiência da técnica. Porém, a localização que é compartilhada na Rede Social é uma localização com alta precisão. Usuários podem adquirir esta informação e inferir a identidade do usuário com base em sua rotina.

As contribuições do trabalho realizado por Toch et al. para o desenvolvimento do modelo proposto foram: a visão geral de funcionamento de uma RSM, a arquitetura centralizada utilizada para o desenvolvimento, novos parâmetros para restrições de compartilhamento, como o amigo, o período de tempo, o local e a possibilidade de combinar essas restrições em uma mesma política, a integração com o Facebook para formar a rede social, a lista negra e os resultados obtidos com a avaliação com usuários.

Bilogrevic et al. (Bilogrevic et al. 2013) desenvolveram o SPISM, um sistema de compartilhamento de informações de contexto em Redes Sociais Móveis. Estas informações de contexto são a localização, co-presença e as atividades do usuário. SPISM utiliza políticas semelhantes às desenvolvidas no Locaccino para fornecer privacidade aos seus usuários. Os autores realizaram um teste de campo com o intuito de medir o comportamento dos usuários quanto a definir políticas de compartilhamento de localização. Dos resultados obtidos, duas conclusões foram encontradas. Primeiro, que os usuários particularmente não são bons em definir políticas de privacidade e, segundo, que as mesmas evoluem com o tempo. O diferencial do SPISM é a aplicação de aprendizagem de máquina para definir, de uma forma semi-automática, a melhor política de privacidade aos seus usuários.

A arquitetura selecionada para o desenvolvimento do sistema SPISM foi a centralizada. O SPISM é composto por uma aplicação cliente (desenvolvida em Android) e um servidor denominado de *Information Sharing Directory* (ISD).

O principal objetivo do ISD é permitir que os usuários descubram o endereço IP atual dos seus contatos e, podendo, assim, enviar-lhes requisições de compartilhamento de informações. Além disso, o ISD armazena a lista de usuários do sistema, a lista de contatos de cada usuário, suas credenciais, e os endereços MAC das interfaces Bluetooth dos dispositivos móveis. Os usuários interagem com o ISD na fase de registro (apenas uma vez), durante a fase de login (se necessário), ao baixar as listas de contatos, ao relatar periodicamente o endereço IP e status atual e quando enviam pedidos de compartilhamento de informações aos seus contatos.

O aplicativo cliente presente no dispositivo do usuário permite-lhe enviar pedidos de compartilhamento de informações aos seus contatos e visualizar, a qualquer momento, a lista de contatos online. Além disso, a aplicação envia o endereço IP e status atual ao ISD, coleta informações de contexto através de sensores e GPS e executa as políticas de privacidade do usuário e os algoritmos de tomada de decisão. Para a tomada de decisão, os autores utilizaram a biblioteca WEKA3 para Android. Na Figura 3.2 são ilustradas as principais telas do aplicativo cliente.

Para aumentar a segurança das comunicações entre os dispositivos móveis e o ISD, todas as mensagens trocadas são criptografadas com uma chave pública obtida a partir de uma Autoridade Certificadora (AC) confiável.

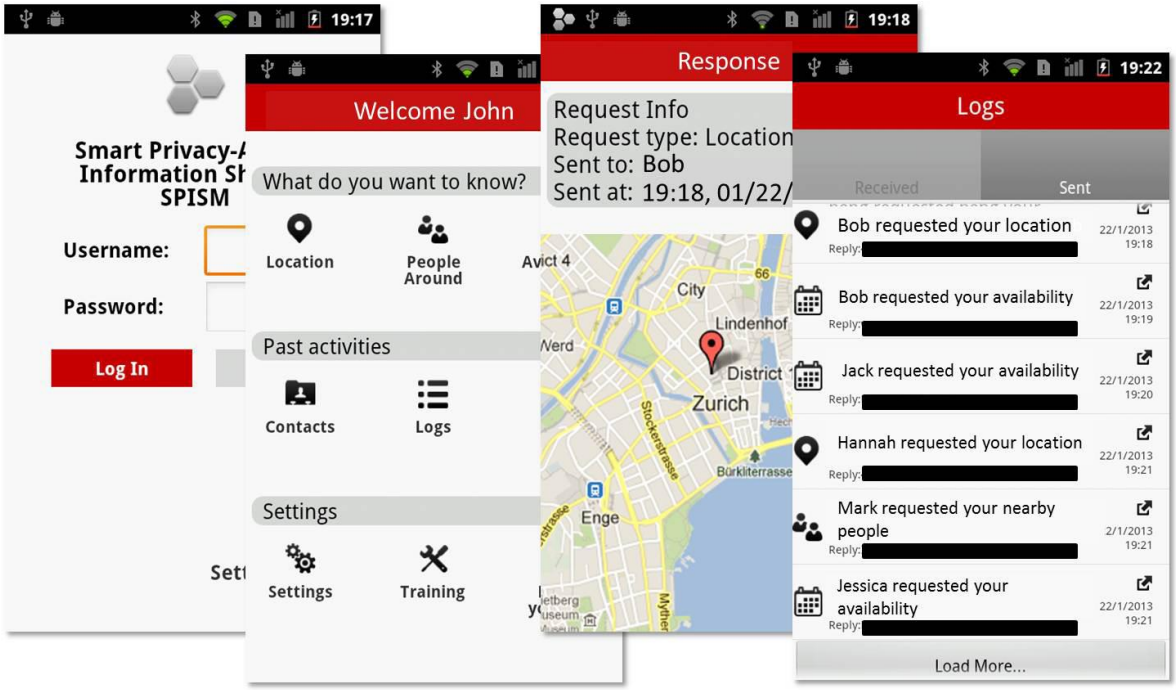

Figura 3.2. Interface do Sistema SPISM.

FONTE: Bilogrevic et al. 2013

Uma grande desvantagem do sistema SPISM é que o usuário solicitante conhece o endereço IP atual do seu contato solicitado. Portanto, ele pode ser capaz de inferir a localização com alta precisão desse contato (com base no IP-geolocalização). Este também pode inferir a co-presença de outros contatos se eles compartilham o mesmo endereço IP (quando utilizadas redes Wi-Fi). Os autores sugerem que este problema pode ser facilmente resolvido inserindo um *proxy* confiável ou redes anônimas como TOR.

O SPISM possui um núcleo de tomada de decisão de compartilhamento de localização. Esse núcleo processa cada pedido de compartilhamento de informações recebido no nível de sistema operacional. Para tomar a decisão, várias características são levadas em consideração: a identidade do solicitante e os laços sociais, a localização atual, sua atividade e a hora do dia. Além disso, também é levado em consideração o histórico das requisições e decisões tomadas anteriormente.

Os resultados obtidos nos testes apontam que a proposta do SPISM foi alcançada. Entretanto, problemas como o do compartilhamento do endereço IP não foram resolvidos. Além disso, a localização atual do usuário e a co-presença dos demais são informações com alta precisão. Dessa forma, quando essa informação for compartilhada com usuários maliciosos, eles saberão exatamente a posição atual de seus contatos e podem ocorrer problemas com a violação de privacidade.

As contribuições do trabalho de Bilogrevic et al. para o desenvolvimento do modelo aqui apresentado foram: a sequência de interação realizada entre a aplicação cliente e o servidor no compartilhamento de localização, a rotina de atualização de IP periodicamente, a utilização de AC para certificação da conexão, a utilização de *proxy* para ocultar o endereço IP do usuários, o algorítmo de cálculo do anonimato em um grupo de usuários formado na RSM e a utilização de auditoria.

3.3 Privacidade em Sistema Baseado em Localização

Ribeiro e Zorzo (Ribeiro e Zorzo 2009) propuseram um Sistema Baseado em Privacidade de Localização (SBPL) que é capaz de oferecer controle na liberação das informações de localização e permite a execução de LBS (*Location-Based Services*) com garantias de privacidade para usuários de dispositivos móveis.

Com uma arquitetura centralizada, o sistema é composto por uma aplicação cliente, executada no dispositivo móvel do usuário, e um servidor confiável, que atua entre o dispositivo móvel e o provedor de serviço LBS. O servidor confiável funciona como um *proxy* que executa as técnicas de privacidade propostas pelo sistema sobre a requisição antes de enviá-las ao provedor de serviços. Na Figura 3.3 é ilustrada a arquitetura do SBPL.

No SBPL foram definidos cinco níveis de privacidade baseados no controle da coleta e do armazenamento de dados, bem como na utilização das seguintes técnicas de privacidade: canal seguro de comunicação, ajuste de precisão e técnicas de obtenção de conjunto de anonimato. Esses níveis foram denominados nível mínimo, nível baixo, nível médio e nível alto, e são detalhados a seguir.

O nível mínimo possui essa denominação porque apenas garante o controle da coleta e armazenamento de dados. Está diretamente ligado aos princípios da limitação da coleta e da limitação de uso, propostos no guia de privacidade OECD (*Organization for Economic Co-Operation and Development*). Esse controle impede que informações subsequentes possam ser analisadas, uma vez que não serão armazenadas após a execução do serviço.

Figura 3.3. Arquitetura do SPBL.

FONTE: Ribeiro e Zorzo 2009.

O nível baixo possui essa denominação porque garante o canal seguro de comunicação entre o dispositivo móvel e o servidor confiável, de forma a dificultar o roubo de informações pessoais através da observação do tráfego na rede.

O nível médio possui essa denominação porque oferece o ajuste de precisão sobre as informações de localização do usuário, o que é muito importante na utilização LBS com privacidade. A utilização deste nível impede que o usuário seja identificado, devido à alta precisão de suas informações de localização.

O nível alto possui essa denominação porque garante a privacidade do usuário através do conjunto de anonimato. O conjunto é obtido através do envio de requisições LSB do mesmo tipo, provenientes de usuários diferentes, para um fornecedor de serviços. 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 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.

O nível garantido utiliza a técnica de envio de requisições falsas para a 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 gera 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.

Apesar do trabalho de Ribeiro e Zorzo ser voltado para privacidade em LBS, importantes contribuições foram encontradas para o desenvolvimento do modelo aqui proposto. Essas contribuições foram: a definição dos níveis de privacidade, o algoritmo de ajuste de precisão e a técnica de anonimato utilizando a geração de falsas localizações.

3.4 Considerações finais

Os trabalhos relacionados apresentam algumas soluções que visam tratar o problema da privacidade em RSM e a privacidade em LBS.

Os trabalhos desenvolvidos por Smith et. al., Toch et. al. e Bologrevic et. al. oferecem técnicas capazes de minimizar as ameaças à privacidade dos usuários no compartilhamento de localização em RSM. As técnicas são baseadas na definição de politicas de privacidade que permitem aos usuários definir parâmetros para a permissão de liberação da localização. Entretanto, quando o compartilhamento de localização é permitido, além do usuário requisitante, o servidor também obtém acesso a essa informação com alta precisão. Além disso, a facilidade encontrada pelos usuários maliciosos em ingressarem na RSM aumenta os riscos de perda de

privacidade, uma vez que a localização pode ser compartilhada com esses usuários.

O trabalho desenvolvido por Ribeiro e Zorzo apresenta técnicas que ocultam a localização real do usuário que utiliza LBS. Essas técnicas minimizam as ameaças à privacidade através do ajuste de precisão da localização, o cálculo do anonimato em grupo utilizando outras requisições e a técnica de anonimato utilizando a geração de falsas requisições. Essas técnicas são oferecidas aos usuários através de níveis de privacidade que são executadas por um intermediário confiável, ou seja, um *proxy*. Entretanto, este trabalho não é aplicado em RSM. Outro pronto importante é a utilização do *proxy* para a execução das técnicas de privacidade, que apenas transfere o problema caso não existam garantias de confiabilidade.

O modelo proposto neste trabalho realiza a junção das técnicas propostas nos trabalhos relacionados. O modelo oferece a possibilidade de personalização de politicas de privacidade que permitem o compartilhamento da localização e níveis de privacidade que ocultam do provedor e usuários maliciosos a localização com alta precisão. Além disso, todas as técnicas de privacidade presentes nos níveis e as políticas configuradas são executadas no próprio dispositivo do usuário. O uso de um servidor *proxy* é opcional, sendo utilizado apenas para ocultar o endereço IP do dispositivo. A tabela 3.1 apresenta um resumo das contribuições dos trabalhos relacionados ao desenvolvimento deste trabalho.

Tabela 3.1. Contribuições dos trabalhos relacionados

Trabalho	Aplicação	Contribuições
Smith *et. al.* (Smith *et. al*., 2005)	RSM	Definição de parâmetros para a personalização da privacidade, como: Local e momento (horário)
Toch *et. al.* (Toch *et. al.,* 2010)	RSM	- A visão geral de funcionamento de uma RSM - Arquitetura centralizada - Novos parâmetros para restrições de compartilhamento, como o amigo, o período de tempo, o local e a possibilidade de combinar essas restrições em uma mesma política

		- Integração com o Facebook - Lista negra
Bilogrevic *et al.* (Bilogrevic *et al.,* 2013)	RSM	- A sequência de interação realizada entre a aplicação cliente e o servidor no compartilhamento de localização -Rotina de atualização de IP periodicamente - Utilização de AC para certificação da conexão - Utilização de *proxy* para ocultar o endereço IP - Algoritmo de cálculo do anonimato em um grupo
Ribeiro e Zorzo (Ribeiro e Zorzo, 2009)	LBS	- A definição dos níveis de privacidade - Técnica e algoritmo de ajuste de precisão -Técnica de anonimato utilizando a geração de falsas localizações

Capítulo 4

MODELO DE COMPARTILHAMENTO DE LOCALIZAÇÃO EM REDES SOCIAIS MÓVEIS COM GARANTIAS DE PRIVACIDADE

4.1 Considerações iniciais

O modelo aqui apresentado foi projetado para permitir que os usuários de Redes Sociais Móveis possam ter maneiras de controlar como suas informações de localização serão compartilhadas durante a utilização de Redes Sociais. O modelo foi projetado para contar com os seguintes requisitos:

- Personalização: é oferecida aos usuários a personalização das politicas de privacidade, possibilitando a eles especificar com quem, onde e quando suas informações de localização serão compartilhadas. Dessa forma, o modelo permite que ocorra a sociabilidade;
- Controle de precisão: é permitido aos usuários determinarem as situações em que suas informações de localização deverão sofrer o ajuste de precisão;
- Anonimato: os usuários podem utilizar mecanismos de anonimato para que sua localização seja compartilhada com segurança com seus contatos, grupos e com o provedor de Rede Social;

- Simplicidade: apesar de oferecer suporte à utilização de técnicas e politicas de privacidade, o modelo conta com uma forma simples de configuração de privacidade;
- Eficiência: apesar da inserção de mecanismos de privacidade, a utilização de Redes Sociais Móveis não deve sofrer atrasos excessivos. Estes atrasos não deverão exceder o tempo médio de acesso ao GPS, que é de 30 segundos.

O objetivo básico do modelo é permitir que o usuário tenha controle sobre como as suas informações de localização serão compartilhadas na Rede Social. Dessa maneira, usuários maliciosos e o provedor de Rede Social não terão acesso a tais informações e não poderão inferir a identidade do usuário (em determinadas redes sociais ou em grupos formados dentro da própria rede social), a posição atual ou armazenar um histórico que possibilite determinar o caminho realizado pelo usuário. Em outras palavras, o modelo permite que o usuário personalize a sua privacidade dependendo do fator, momento, pessoas ou circunstâncias. Permitindo a personalização da privacidade, o modelo possibilita ao usuário usufruir dos recursos oferecidos pela rede social, ao mesmo tempo em que fornece mecanismos para a proteção da privacidade.

Este capítulo esta organizado da seguinte forma: na Seção 4.2 são apresentados a arquitetura do modelo e seus elementos. Na seção 4.3 apresentam-se as políticas de privacidade disponíveis para o usuário e na seção 4.4 são apresentados os níveis de privacidade oferecidos aos usuários e suas características.

4.2 Arquitetura do Modelo

A arquitetura do modelo proposto para o compartilhamento de localização em Redes Sociais Móveis com garantias de privacidade, ilustrada pela Figura 4.1, caracteriza-se pela presença de usuários e máquinas conectados.

A arquitetura base escolhida para o modelo proposto foi a arquitetura centralizada. Conforme visto na figura 4.1, a arquitetura é composta por uma aplicação cliente, representada pelos usuários usuário 1 e usuário 2, um *proxy*

confiável, representado pela Maq A e um Servidor de Rede Social (SRS), representado pela Maq B.

O SRS é responsável por armazenar a lista de usuários, a lista de contatos de cada usuário, por manter o endereço IP atualizado e o status dos usuários e processar as requisições de compartilhamento de localização entre os usuários.

A aplicação cliente executada no dispositivo móvel é responsável por permitir ao usuário acessar a sua lista de contatos, verificar quais contatos estão online, configurar as políticas e os níveis de privacidade para cada usuário individualmente ou para um grupo destes, requisitar a localização de um membro de sua lista de contatos e receber a requisição de compartilhamento de localização. Além disso, a aplicação manipula as requisições de compartilhamento de localização recebidas e executa as técnicas de anonimato e as políticas adequadas à requisição, armazena as informações das requisições recebidas e realizadas e permite que o usuários realizem auditorias sobre essas informações.

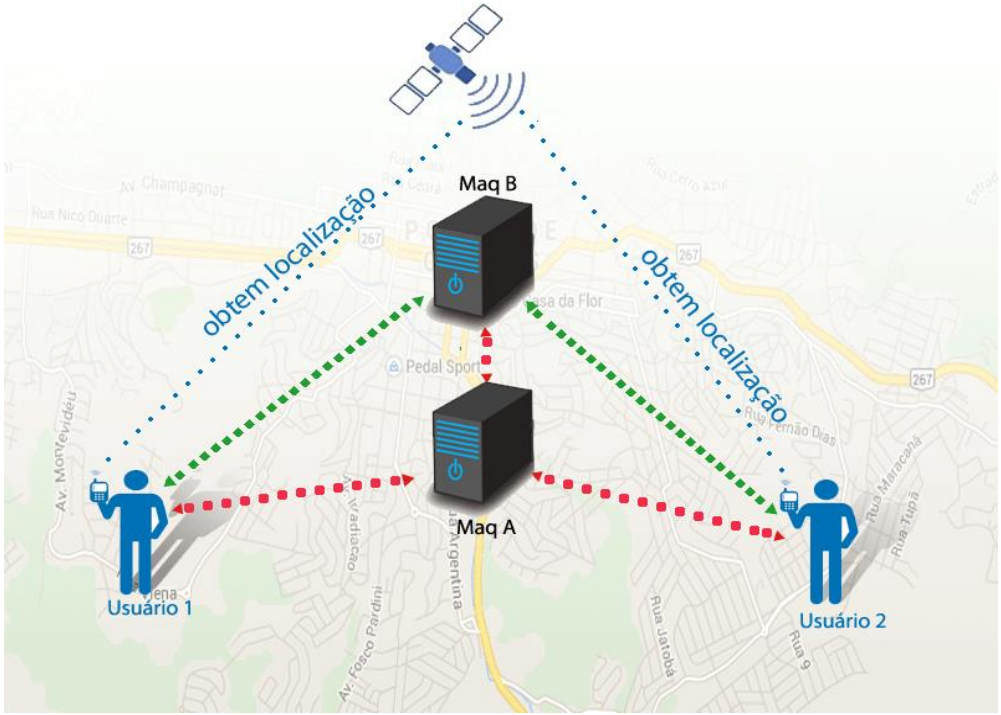

Figura 4.4. Arquitetura do Modelo.

O *proxy* confiável é responsável por intermediar as requisições de compartilhamento enviadas ou/e recebidas dos usuários e por manter o anonimato de endereço IP dos dispositivos. O *proxy* armazena temporariamente o endereço IP

dos usuários para retornar os resultados das requisições. A existência do *proxy* confiável não é sempre possível, pois, para ser confiável, deve existir um órgão ou entidade que administre o *proxy*, como por exemplo, uma universidade que disponibiliza um *proxy* aos seus alunos ou uma empresa que disponibiliza um *proxy* aos seus funcionários.

Para aumentar a segurança e garantir autenticação nas comunicações entre os usuários, o *proxy* e o SRS, todas as requisições trocadas são criptografadas usando um certificado de chave pública do usuário destino, obtida a partir de uma Autoridade Certificadora (AC) confiável.

O modelo garante a privacidade de seus usuários no compartilhamento de localização em RSM, através da definição de políticas e níveis de privacidade. Através da configuração de politicas, os usuários definem restrições para a liberação das suas localizações e, através dos níveis, os usuários definem o nível de anonimato que será aplicado sobre sua localização antes que ela seja compartilhada. O modelo ainda possibilita a combinação de políticas e níveis, oferecendo garantias de privacidade mais robustas. Os detalhes desses mecanismos são apresentados a seguir.

4.3 Políticas de Privacidade

De modo a obter um melhor esclarecimento do uso das políticas oferecidas pelo modelo, o seguinte cenário é apresentado: um determinado usuário de Redes Sociais Móveis só está disposto a compartilhar a sua localização com seus colegas de trabalho durante a semana, no período das nove da manhã às cinco da tarde e quando está nas instalações da empresa onde trabalha. O modelo permite aos seus usuários definir políticas de privacidade com um usuário individualmente ou um grupo. Um grupo pode ser formado de duas formas: automaticamente, através de interesses comuns, ou pelo próprio usuário, que inclui manualmente os contatos que participaram do grupo.

Para a definição das regras de privacidade, o modelo disponibiliza os seguintes parâmetros:

- Quem (Amigo): o usuário determina com quais membros da sua lista de contato ele está disposto a compartilhar a sua localização. A Política pode ser para um contato individual ou para um grupo de usuários;
- Quando (Dias da Semana): o usuário determina os dias da semana em que está disposto a compartilhar sua localização com seus contatos da Rede Social;
- Período (Horário): o usuário determina o período do dia em que sua localização será compartilhada com o membro da sua lista de contatos;
- Onde (Local): o usuário determina o local especifico ou região geográfica na qual ele esta disposto a compartilhar a sua localização.

O usuário tem liberdade para definir políticas com apenas um dos parâmetros citados acima, ou por combinação dos parâmetros. Além disso, o modelo permite que se crie políticas preestabelecidas e as associe quando for necessário, sem a necessidade de repetir os mesmos parâmetros a contatos diferentes.

As políticas garantem a privacidade dos usuários e ainda permitem que as questões de sociabilidade sejam executadas pela Rede Social, pois o modelo permite o compartilhamento da localização de acordo com os parâmetros especificados. Dessa forma, será possível a recomendação de serviços a amigos próximos. Porém, um ponto importante que deve ser ressaltado é que as políticas não garantem o anonimato da localização, elas apenas especificam condições para divulgação da localização. Quando o compartilhamento for permitido, o usuário requisitante e o provedor terão acesso à localização real do usuário com alta precisão. Neste contexto, o modelo garante o anonimato e a precisão das informações de localização compartilhadas através dos níveis de privacidade.

O modelo trata o conflito de políticas de duas formas: primeiramente, o usuário pode apenas criar regras que permitem o compartilhamento de sua localização e não é possivel a criação de regras que negam o compartilhamento. Por exemplo, "Maria pode ver minha localização no período entre nove horas a cinco horas", mas não é possível especificar, por exemplo, "Meus amigos não podem ver a minha localização nos fins de semana". Em segundo lugar, a regra criada é verificada antes de ser confirmada. Essa verificação é realizada para impedir a existência de regras com parâmetros conflitantes. Por exemplo, Maria cria uma regra que permite a seus amigos verem sua localização no fim de semana, então ela não

conseguirá criar uma nova regra que especifique que seus amigos podem ver sua localização nos finais de semana, no período de nove horas a cinco horas.

4.4 Níveis de Privacidade

Visando oferecer diferentes garantias de privacidade no compartilhamento de localização em redes sociais móveis, o modelo disponibiliza aos seus usuários quatro níveis que oferecem 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 oferecidos pela Rede Social, que possui diferentes restrições de precisão de dados. A seguir são detalhadas as características de cada nível.

4.4.1 Nível 0 – Ajuste de Precisão

A questão da precisão ou, mais especificamente, do ajuste de precisão, é muito importante no oferecimento de garantias de privacidade aos seus usuários quando estes compartilham suas localizações em Redes Sociais utilizando seus dispositivos móveis. A capacidade de fazer com que informações de localização com alta precisão representem áreas diferentes ou maiores do que a área inicial é fundamental para evitar a identificação dos usuários.

O modelo no nível 0 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, ou seja, um raio. Dessa forma, ao compartilhar sua localização na Rede Social com esse nível de privacidade, os membros da lista de contato do usuário e o provedor de Rede Social não terão acesso à sua localização exata. A Figura 4.2 ilustra o ajuste de precisão.

Na Figura 4.2, a localização real do usuário é ilustrada pelo círculo central A, o coeficiente de ajuste de precisão é ilustrado pela letra “r”. Ao sofrer o ajuste de precisão, a localização do usuário recebe um deslocamento aleatório para qualquer

direção dentro da área ilustrada pelo circulo maior. A localização calculada é representada pelo círculo B.

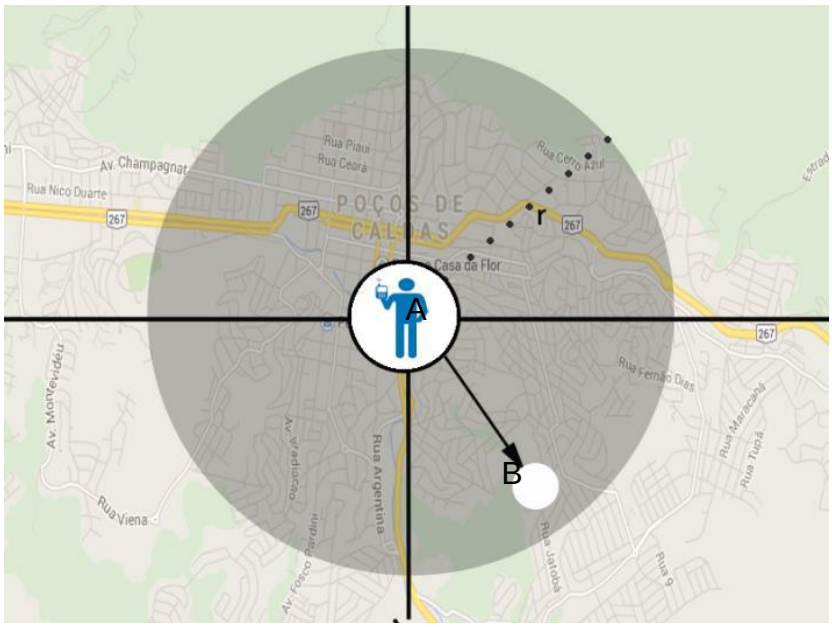

Figura 4.5. Ajuste de Precisão.

A técnica funciona da seguinte forma: dada uma localização inicial e um raio de deslocamento, denominado de coeficiente de ajuste de precisão, ocorrerá um deslocamento aleatório para qualquer parte da área calculada pelo coeficiente de ajuste de precisão. Por exemplo, supondo que o coeficiente seja definido com o valor de 500 metros, a nova localização calculada poderá estar em qualquer um dos pontos internos em 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.

Para o cálculo do ajuste de precisão foi utilizada a fórmula abaixo, que é baseada no triângulo esférico formado pelo ponto inicial, ponto final e o polo norte (SMART, 1977). Na fórmula, o lado entre o ponto inicial e o polo norte, e o lado referente à distância de deslocamento, são conhecidos. Além disso, também é conhecido o ângulo formado por estes dois lados, caracterizado pela direção de movimento fornecida. Estando de posse dessas informações e utilizando a relação entre os ângulos e lados específicos da trigonometria esférica, são obtidos os outros dados e o ponto final, que será utilizado no ajuste de precisão (WILLIAMS, 2014).

$$lat2 = \arcsin\left(\sin(lat1) * \cos\left(\frac{d}{R}\right) + \cos(lat_1)\right) \quad * c$$

$$dlon = arctan2\left(\sin(\theta) * \sin\left(\frac{d}{R}\right) * \cos(lat1), \cos\left(\frac{d}{R}\right) - \sin(lat1) * \sin(lat2)\right)$$

$$lon2 = mod(lon1 - dlon + pi, 2 * pi) - pi$$

Na fórmula acima, θ representa a direção do deslocamento, lat1 e lat2 são coordenadas do ponto inicial, e d/R a distância angular, onde “d” é a distância desejada do ajuste e “R” o raio da terra. O objetivo da função do módulo é tratar os casos em que os pontos estão em meridianos opostos. As coordenadas da localização final calculada são dadas por lat2 e lon2, respectivamente.

O modelo ainda possibilita que os usuários combinem o ajuste de precisão presente no nível 0 com as políticas de privacidade apresentadas na seção anterior.

4.4.2 Nível 1 – Anonimato

O Módulo de Privacidade no nível 1 garante a privacidade no compartilhamento da localização do usuário dentro de um grupo formado na RSM. Este grupo pode ser formado pelo usuário, que seleciona e inclui os amigos que irão pertencer ao grupo, ou formado por interesses comuns e outras características, como grau de parentesco ou posição geográfica. A privacidade da localização é ajustada através da ocultação da localização real do usuário. Esta ocultação é feita através da seleção de uma das localizações dos membros pertencentes ao grupo. Uma vez selecionada representará a localização de todos os membros do grupo. Esta seleção é feita através do algoritmo que resolve o problema do k-*center*. No problema do k-*center*, o objetivo é encontrar o local K entre todas as localizações compartilhadas, tal que a máxima distância de qualquer usuário para os demais é minimizada. A Figura 4.3 ilustra um exemplo de um cenário modelado com o problema do k-*center*, no qual o cálculo do ponto justo é realizado com a localização de quatro usuários.

Na Figura 4.3, as linhas tracejadas representam as máximas distâncias, enquanto a linha sólida representa a mínima distância dentre todas as máximas. Portando, neste cenário, o ponto justo é User2(x2, y2).

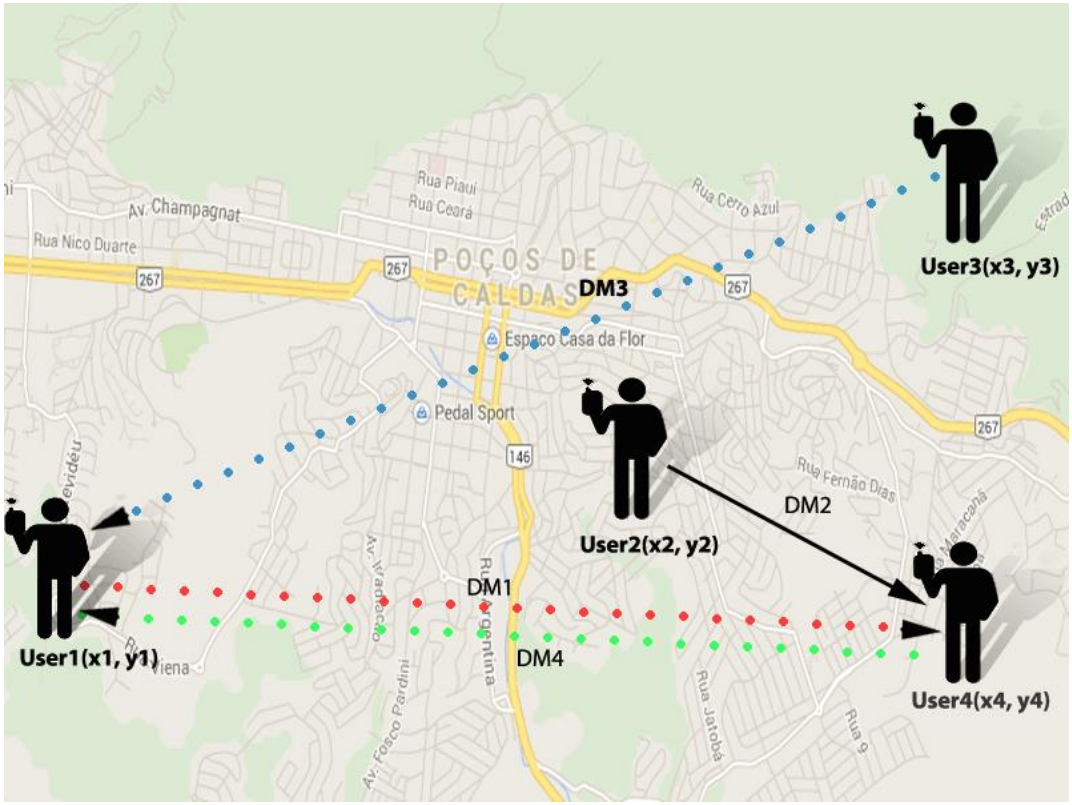

Figura 4.6. Cenário Modelado do problema k-*center*.

Na criação de um grupo dentro de uma RSM, todos os integrantes deste grupo são organizados internamente no sistema em uma estrutura de dados grafo, conforme ilustrado na Figura 4.4.

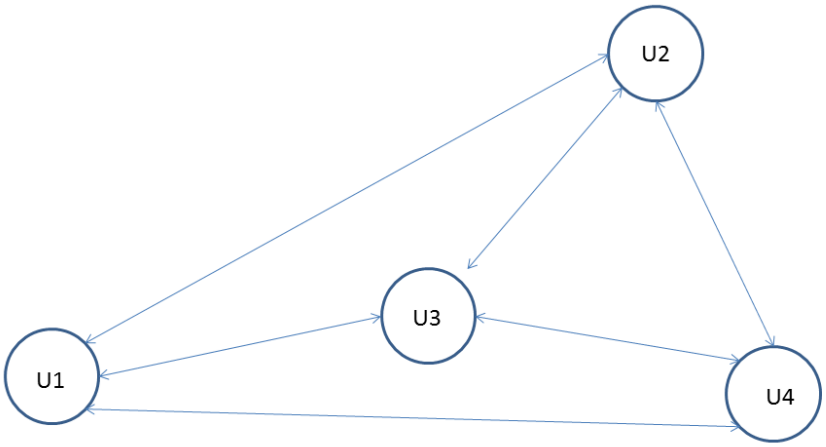

Figura 4.7 - Grafo da organização interna do Grupo.

Na Figura 4.4, os vértices representam cada usuário da RSM adicionado a um grupo e as arestas são a distância calculada entre os membros. No cenário exemplificado pela Figura 4.4, a localização selecionada seria a do usuário representado por “U3”, uma vez que ele é o usuário que possui a mínima distância para os demais usuários.

O algoritmo que define a localização a ser compartilhada dentro do grupo de usuários funciona da seguinte forma: primeiramente, é calculada a distância entre todos os membros para os demais. Para realizar este cálculo foi utilizada a fórmula da Distância Euclidiana que calcula a distância entre dois pontos. Após o cálculo das distâncias entre os usuários, o algoritmo seleciona as mínimas distâncias de cada usuário. Após obter estas distâncias, o algoritmo seleciona a menor distância entre as mínimas distâncias selecionadas. A localização do usuário que possui a distância selecionada será a localização que representará o grupo. Além disso, antes de compartilhar esta localização, será aplicado sobre ela o ajuste de precisão.

A técnica de anonimato característico deste nível nem sempre poderá ser aplicada, pois ela depende de localizações de outros usuários pertencentes ao grupo. Caso estas localizações não sejam obtidas dentro de 10 segundos, a aplicação faz incidir o ajuste de precisão sobre a posição atual do usuário, com a ocultação da sua localização real. Esses 10 segundos foram utilizados no SPIMS e justificados por Bilogrevic (2013).

4.4.3 Nível 2 – Anonimato Garantido

O modelo no nível 2 utiliza a técnica de geração de localizações falsas para a obtenção do conjunto de anonimato. Essa técnica funciona da seguinte maneira: ao receber uma requisição de compartilhamento de localização, a aplicação presente no dispositivo móvel ajusta a localização real do usuário utilizando a técnica de ajuste de precisão. Além disso, a aplicação calcula outras quatro localizações a partir da posição real do usuário. Por fim, a técnica do cálculo do ponto justo característico do nível 1 é realizada e a localização resultante é compartilhada. Com relação ao número de localizações falsas geradas, chegou-se à conclusão de que a quantidade ideal seria quatro, uma vez que com duas o número de localizações não foi expressiva e com seis aumentou a complexidade no cálculo do anonimato. A Figura 4.5 ilustra a técnica característica deste nível.

Na Figura 4.5, a posição real é ilustrada pelo circulo central A. Esta coordenada é adquirida através do uso de GPS. As demais localizações falsas geradas são representadas pelos círculos escuros e a localização resultante é representa pelo círculo menor B.

Figura 4.8. Geração de Localizações Falsas.

A utilização dos níveis 0, 1 e 2 ainda permite que haja sociabilidade e recomendações realizadas pela Rede Social, uma vez que a localização resultante das técnicas de privacidade ainda se encontra dentro de uma área geográfica aceitável, dependendo do valor do coeficiente de ajuste de precisão configurado pelo usuário. Usuários e serviços próximos ainda podem ser oferecidos com base na região em que o usuário se encontra.

As técnicas de privacidade características dos níveis 1 e 2 ainda garantem a privacidade da localização dos usuários dentro de um grupo. Essa garantia é necessária, pois, como o usuário pode pertencer a grupos com finalidades diferentes (profissional, familiar, amigos), pode querer que sua localização seja divulgada em determinados momentos ou situações.

4.4.4 Nível 3 – Lista Negra

A lista negra é o último nível oferecido pelo modelo. Consiste em uma lista onde o usuário relaciona membros da sua lista de contatos ou grupos com quem sua localização nunca será compartilhada. Ao utilizar este nível ao receber uma requisição de compartilhamento de localização, o aplicativo automaticamente irá negar o pedido. Este nível deve ser utilizado em último caso, pois prejudicará a existência da sociabilidade e recomendações realizadas pela Rede Social com base na localização do usuário. Porém, assim como os demais níveis, este nível pode ser

combinado com as políticas de privacidade apresentadas na seção 4.3. Dessa forma, o usuário pode especificar quem, o período e a localização onde pretende que este nível seja aplicado.

4.4.5 Considerações finais

O modelo desenvolvido oferece garantias de privacidade aos seus usuários no compartilhamento de localização em Redes Sociais Móveis através da configuração de políticas e níveis de privacidade. As políticas de privacidade possibilitam que os usuários determinem com quem, quanto ou um grupo, um período de tempo, o dia e o local onde eles estão dispostos a compartilhar sua localização. Os níveis garantem o anonimato e a precisão da localização que será compartilhada. Realizando a combinação de políticas e níveis de privacidade, o usuário conseguirá obter um nível alto de privacidade. Todas as técnicas oferecidas pelo modelo são processadas no próprio dispositivo móvel do usuário. Dessa forma, o modelo garante que o Provedor de Rede Social não terá acesso à localização do usuário dentro dos parâmetros especificados nas políticas, ou não terá acesso à sua localização com alta precisão quando utilizados os níveis. Porém, membros da lista de contatos e provedor ainda possuem acesso ao endereço IP do usuário. Para resolver este problema, o modelo disponibiliza a utilização de um *proxy* confiável que intermediará as comunicações realizadas, aumentando ainda mais a segurança e a privacidade dos usuários.

No intuito de validar o modelo, foi realizada a implementação de uma Rede Social Móvel com as garantias de privacidade citadas neste capitulo, o RSM Privacy- Rede Social Móvel com Privacidade. Os detalhes desta implementação são apresentados no capítulo seguinte.

Capítulo 5

CAPÍTULO 5 - RSMPRIVACY – REDE SOCIAL MÓVEL COM PRIVACIDADE

5.1 Considerações iniciais

Ao compartilhar sua localização em sua rede social, o usuário possibilita a outros usuários, a aplicações de terceiros e ao próprio provedor de serviços inferirem sua localização, permitindo a obtenção exata do local e caminho realizado por ele através do armazenamento do histórico de localizações. O modelo descrito no capítulo 4 propõe uma Rede Social que permite aos usuários compartilharem informações de localização com garantias de privacidade. Essas garantias são baseadas em políticas e níveis de privacidade que dificultam inferir a identidade do usuário através da localização (em algumas redes sociais móveis ou em grupos formados), obter a localização com alta precisão e obter o caminho realizado pelo usuário.

Para validar o modelo proposto no capítulo 4, foi implementado um protótipo de Rede Social Móvel, denominado RSM Privacy (Rede Social Móvel com Privacidade). A implementação deste protótipo foi baseada em uma RSM popularmente conhecida, porém com funcionalidades bem resumidas, pois o principal objetivo é medir a eficiência das técnicas e políticas de privacidade oferecidas no compartilhamento de localização. Dessa forma, também foi descartada a utilização de um *Framework* de RSM existente, pois esses Frameworks

oferecem todas as funcionalidades existentes em uma RSM, o que aumenta a complexidade do desenvolvimento.

Este capítulo está organizado da seguinte forma: na Seção 5.2 apresenta-se a arquitetura do protótipo; na seção 5.3 são apresentados os detalhes da implementação da aplicação cliente; na seção 5.4 são apresentados os detalhes da implementação da aplicação do servidor de Rede Social; na seção 5.5 são apresentados os detalhes da aplicação do *proxy* confiável e, para finalizar, na seção 5.6 são apresentadas as considerações finais.

5.2 Arquitetura Geral do RSM Privacy

O protótipo de Rede Social Móvel é composto por um aplicativo cliente para dispositivos móveis, um Servidor de Rede Social (SRS) e um intermediário confiável.

O aplicativo cliente permite aos usuários a utilização das funcionalidades disponíveis, tais como configuração de políticas e níveis de privacidade, requisitar o compartilhamento de localização de um de seus membros pertencentes à sua lista de contatos e visualizar a auditoria com o histórico de todas as requisições de compartilhamento de localização solicitadas e recebidas. Além disso, o aplicativo é responsável por executar as técnicas de privacidade presentes em cada nível, aplicar as políticas de privacidade sobre as requisições recebidas e realizar comunicação com SRS e com o *proxy* confiável.

O Servidor de Rede Social (SRS) é responsável por manter uma lista com os IPs atualizados de seus usuários, intermediar as requisições de compartilhamento de localização realizadas e manter um status atualizado de todos os usuários pertencentes à Rede Social. A lista de IPs é necessária, pois o SRS, quando recebe uma requisição, necessita estabelecer uma conexão com a aplicação do cliente para envio da requisição e recepção da resposta.

O *proxy* confiável é responsável por intermediar a comunicação entre o aplicativo presente nos dispositivos móveis dos usuários e o SRS. O único objetivo do *proxy* confiável é ocultar o endereço IP real dos usuários da RSM.

A implementação do protótipo foi organizada em módulos, como ilustrado na Figura 5.1. A escolha da implementação em módulos foi devida à facilidade de manutenção e evolução do protótipo.

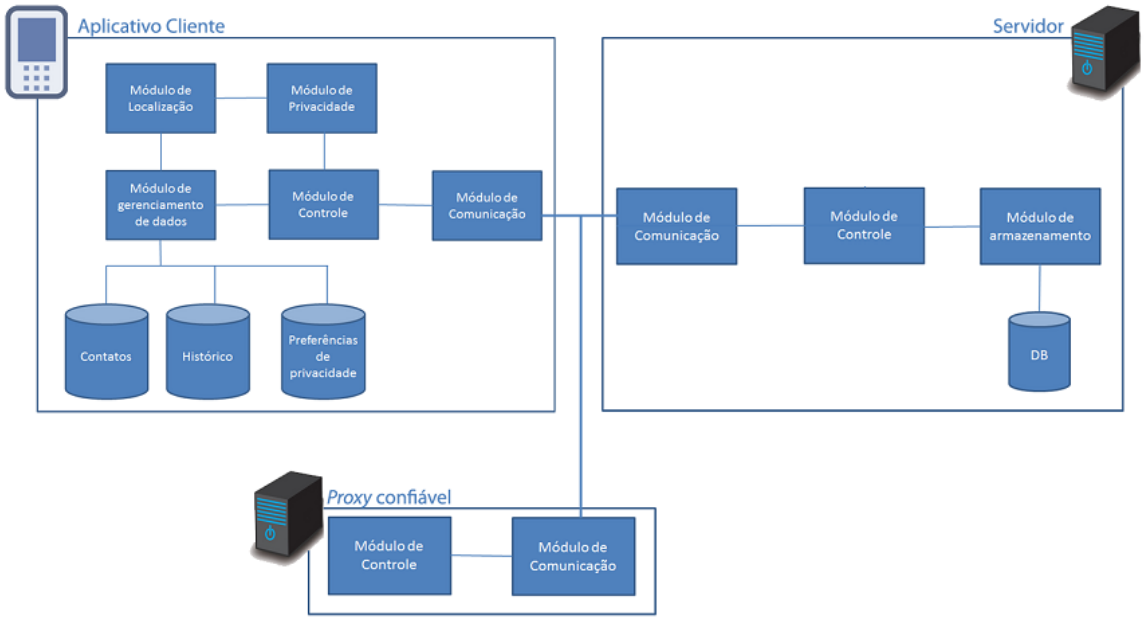

Figura 5.9. Módulos do protótipo RSM Privacy.

5.3 Aplicação Cliente

O aplicativo cliente foi desenvolvido para a plataforma Android. A escolha do Android se deu devido à plataforma ser de código aberto e estar presente na maioria dos dispositivos móveis. Como Java é a linguagem oficial da plataforma Android, Java foi a linguagem utilizada no desenvolvimento do aplicativo. Além disso, Java é uma linguagem robusta.

Conforme ilustrado na Figura 5.1, o aplicativo cliente é composto por cinco módulos e um banco de dados com três tabelas.

O Módulo de Localização é responsável por obter a localização atual do usuário. O Módulo de Privacidade é responsável por aplicar as políticas e níveis de privacidade sobre as requisições de compartilhamento de localização recebidas. O Módulo de gerenciamento de dados é responsável por manipular os dados utilizados pelo aplicativo que são armazenados nas tabelas de contatos, histórico e preferências de privacidade. O Módulo de Comunicação é responsável por conectar

e manter esta conexão com o servidor e o *proxy* confiável. O Módulo de Controle possui duas funcionalidades principais: gerenciar a execução dos demais módulos e oferecer aos usuários acesso às opções oferecidas pelo aplicativo por meio de uma interface gráfica. Os detalhes de cada módulo são apresentados a seguir.

5.3.1 Módulo de Localização

O Módulo de Localização é responsável por obter a localização atual do usuário que será compartilhada na Rede Social. Para obter esta informação é utilizado o GPS do dispositivo e triangulação de antena. O Android oferece uma API (*Application Programming Interface*) que fornece métodos para obter e manipular dados de localização. Esses métodos estão encapsulados em classes e interfaces que estão presentes no pacote android.location. Dentre essas classes, a principal é a Location Manager, que permite o acesso a serviços de localização do dispositivo. Esses serviços dependem do hardware e podem ser utilizados para se obter periodicamente atualizações sobre a localização do usuário.

O Módulo de Localização adquire a localização atual do usuário. Mas para isso é necessário que o usuário permita. Nenhum aplicativo pode utilizar recursos do dispositivo sem a autorização explícita do usuário.

A localização atual do usuário é obtida no momento em que ele efetua o *login* no aplicativo ou o inicia. Além disso, a localização é atualizada periodicamente. Esta atualização ocorre em períodos de cinco minutos, podendo variar de acordo com o deslocamento do usuário. Esse deslocamento é obtido através dos sensores de acelerômetro. Dessa forma, sempre que solicitado o compartilhamento de localização, o aplicativo já possui a informação atualizada e o tempo de execução não é comprometido. A utilização do GPS permite obter a localização com alta precisão, porém pode ocorrer um atraso no retorno do primeiro resultado, que pode variar de 30 segundos a alguns minutos. Além disso, um ponto negativo a ser considerado é que o GPS é um dos grandes vilões de consumo de energia. O consumo de energia é reduzido quando for utilizada a triangulação de antenas de celulares para obtenção da localização. O tempo de retorno do primeiro resultado é muito menor. Porém a localização adquirida não possui alta precisão e as coordenadas retornadas podem possuir vários metros de diferença, pois esta informação foi adquirida por meio de triangulação de antenas.

Para resolver os problemas apresentados, as abordagens de projeto utilizadas foram: (i) o aplicativo utiliza a triangulação de antenas de celulares para obter a primeira localização, evitando atrasos no primeiro acesso ao aplicativo. As demais atualizações de localização são obtidas utilizando GPS; (ii) para evitar o consumo excessivo de bateria, a atualização da localização é realizada inicialmente a cada 30 segundos. Esse tempo é atualizado através do cálculo que considera a média de tempo de requisições de compartilhamento de localização recebidas. Além disso, toda vez que o aplicativo é parado ou pausado (o aplicativo sofre uma pausa toda vez que recebe uma ligação, por exemplo), o GPS é desativado.

A localização obtida é armazenada temporariamente e passada para o modulo de controle.

5.3.2 Módulo de Gerenciamento de Dados

O Módulo de Gerenciamento de Dados tem o objetivo de manipular o banco de dados e manter os registros com as informações que são utilizadas pelo aplicativo cliente. Conforme ilustrado na Figura 5.2, o módulo de gerenciamento de dados manipula seis tabelas, cada uma armazenando informações utilizadas para o aplicativo.

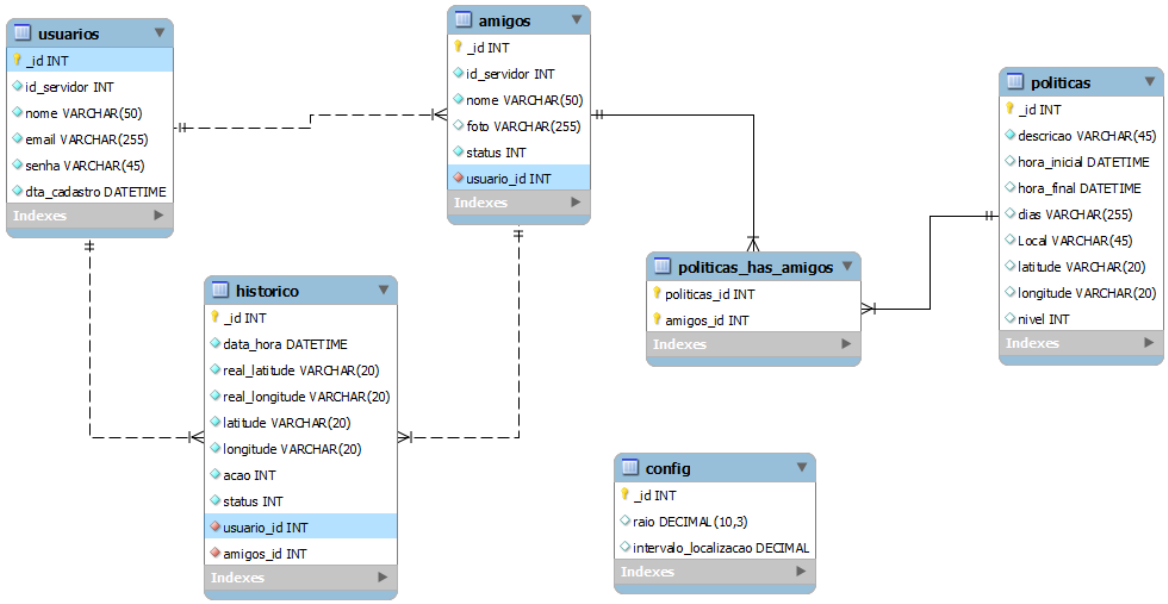

Figura 5.10. Diagrama de Entidade e Relacionamento do aplicativo.

A tabela usuários armazena os dados do usuário ativo no aplicativo. A tabela amigos armazena a lista de contatos do usuário na RSM. A tabela políticas

armazena a privacidade criada pelo usuário. Como possibilita ser observada, uma política de privacidade pode ser reaproveitada para mais de um contato. Os campos hora_inicial e hora_final armazenam o período de tempo em que usuário está disposto a compartilhar a sua localização. O campo dias armazena os dias da semana em que poderá ocorrer o compartilhamento de localização. O campo nível armazena o nível de privacidade que será aplicado sobre a localização antes de ser compartilhada. A tabela histórico armazena todas as requisições de compartilhamento enviadas e recebidas. Através do acesso aos registros da tabela histórico, o aplicativo possibilita ao usuário realizar auditoria sobre a utilização do aplicativo e a eficácia das políticas e níveis de privacidade. Para os níveis, a eficácia é percebida comparando a localização real (campos real_latitude e real_longitude) com a localização compartilhada (campos latitude e longitude). Quanto à eficácia das regras, o campo acao indica se a requisição de compartilhamento de localização foi atendida ou não.

Para acesso e manutenção do banco de dados, o Android disponibiliza uma API que realiza a integração com o SQLite. O SQLite (SQLite.org) é uma biblioteca escrita em linguagem C com recursos de um banco de dados relacional. Esta biblioteca permite trabalhar com bancos de dados leves e robustos. O sistema Android, através de sua API, permite aos aplicativos ter acesso a um banco de dados relacional sem o uso de um SGBD (Sistema de Gerenciamento de Banco de Dados).

O padrão DAO (*Data Access Objects*) foi utilizado no desenvolvimento do aplicativo na camada de acesso aos dados. Foi desenvolvida uma classe que manipula cada tabela especificamente. A utilização do padrão DAO possibilita desenvolver um aplicativo escalável e de fácil manutenção.

As classes desenvolvidas para manipular o banco de dados são usadas no módulo de controle.

5.3.3 Módulo de Privacidade

O Módulo de Privacidade é responsável por executar as políticas (amigo, o dia da semana, o período do dia - horário - e o local) e técnicas de privacidade presentes em cada nível (ajuste de precisão, anonimato, anonimato garantido e lista

negra) de acordo com as configurações definidas pelo usuário e as características da requisição recebida.

Ao receber uma requisição de compartilhamento de localização, o Módulo de Controle a encaminha ao Módulo de Privacidade. O Módulo de Privacidade, por sua vez, analisa os detalhes da requisição recebida e seleciona a política mais adequada e, caso exista algum nível de privacidade definido, a técnica presente neste nível é aplicada. Os detalhes analisados da requisição são o horário em que ela foi recebida, o local onde se encontra o usuário requisitado, o dia da semana e quem enviou a requisição. Se existir alguma política que satisfaça alguns desses parâmetros (ou todos), esta é selecionada e aplicada. A política é selecionada executando uma instrução SQL com os parâmetros analisados. Essa seleção poderia ser realizada de outra maneira, carregando e organizando todas as políticas existentes, de acordo com seus parâmetros, em uma árvore de decisão. Porém, esse método consome recursos de memória do celular e causa perda de performance.

O módulo consiste de duas classes principais: uma classe que encapsula os métodos que selecionam a política de privacidade apropriada e os métodos que executam as técnicas de privacidade características de cada nível, denominadas *Privacy*, e uma classe que aguarda as requisições enviadas, denominada Request Listener.

A classe Request Listener foi implementada como um serviço que herda a classe android.app.Service. A classe android.app.Service é utilizada no Android para executar um processamento assíncrono em background por tempo indeterminado. Para a implementação desta classe, existem dois recursos: Implementar android.app.Service ou implementar uma Thread simples. A escolha pela implementação utilizando android.app.Service se deveu ao fato de que o sistema Android conhece a classe Service e pode gerenciar o seu ciclo de vida juntamente com outros processos do sistema operacional. Em outras palavras, se optar pelo desenvolvimento utilizando Threads, o Android poderia eliminar a execução a qualquer momento porque as Threads não fazem parte do ciclo de vida que ele conhece. Essa eliminação poderia ocorrer, por exemplo, quando o dispositivo recebesse uma chamada telefônica. Como o Módulo de Privacidade tem a necessidade de monitorar constantemente o recebimento de novas requisições, a implementação utilizando a classe andoid.app.Service é mais recomendada. O

Módulo de Privacidade só é finalizado com uma ação explícita do usuário, ou seja, quando ele finaliza a RSM acessando a opção “sair”. A Figura 5.3 ilustra o diagrama de sequência da execução do Módulo de Privacidade.

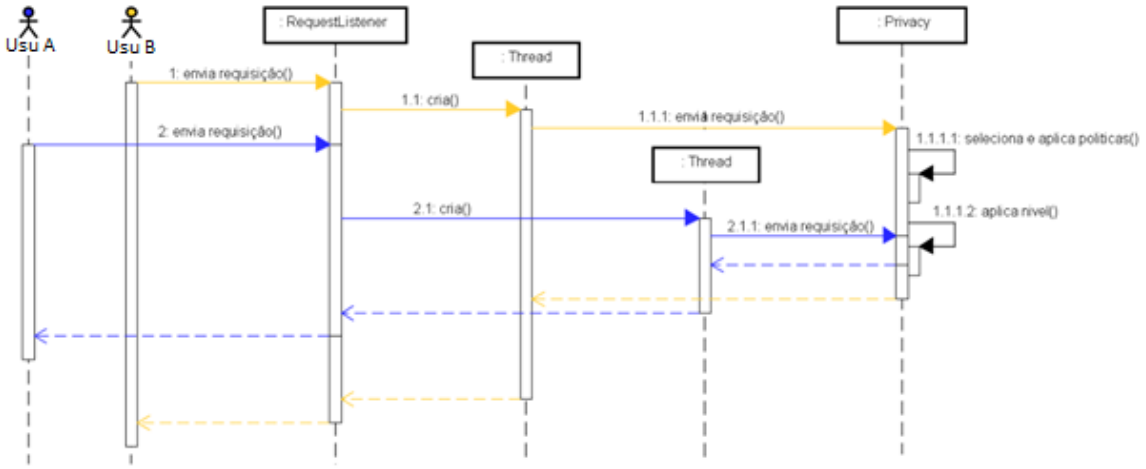

Figura 5.11. Diagrama de Sequência do Módulo de Privacidade.

No diagrama da Figura 5.3, o usuário A, representado pelo diagrama “Usu A”, requisita o compartilhamento de localização de um de seus contatos enviando-lhe uma requisição. O Módulo de Privacidade executado em segundo plano, representado no diagrama por Request Listener, intercepta a requisição enviada. Em seguida, o Request Listener inicia uma Thread que irá tratar a requisição recebida. A Thread instancia um objeto da classe Privacy e encaminha a requisição recebida. O objeto da classe Privacy, por sua vez, analisa a requisição recebida e seleciona a política de privacidade apropriada. Caso exista um nível de privacidade associada a essa regra, o objeto executa a técnica associada a ele. Ao final do processo, o resultado será a localização alterada ou o compartilhamento negado. Paralelamente, outro usuário requisita o compartilhamento da localização do mesmo contato. O processo executado sobre a requisição recebida será o mesmo executado sobre a requisição recebida do “Usu A”.

O usuário tem a possibilidade de associar um nível de privacidade à política de privacidade. O Módulo de Privacidade possui quatro níveis de privacidade: nível 0 (ajuste de precisão), nível 1 (anonimato), nível 2 (anonimato garantido) e nível 3 (lista negra).

5.3.3.1 Nível 0 – Ajuste de Precisão

Na Figura 5.4 é ilustrado o código implementado que realiza o ajuste de precisão. No código, no trecho entre as linhas 11 e 22, é realizado o cálculo do deslocamento que deverá ser utilizado no ajuste de precisão. A direção em graus, minutos e segundos é calculada aleatoriamente no trecho entre as linhas 11 e 13. Por fim, no trecho entre as linhas 19 a 22, é definido aleatoriamente se a posição será positiva ou negativa. Na linha 24 é calculado o valor do deslocamento aleatório, que será entre 0 e o valor máximo que foi definido pelo usuário no coeficiente de ajuste de precisão. No trecho entre as linhas 28 a 35, é calculada uma nova localização com o ajuste de precisão. Esta localização resultante será compartilhada com o usuário que a requisitou ou com um grupo de usuários.

```
 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 5.12. Código que Calcula o Ajuste de Precisão.

Com a implementação do ajuste de precisão apresentada no código da Figura 5.4, é possível manipular e ocultar com eficiência a localização atual do usuário. Dessa forma, o protótipo no nível 0 atende às categorias de privacidade identificadas por Anthony *et al*. [Anthony *et al*., 2007], apresentadas na seção 2.4, que são: a privacidade da posição, pois com o ajuste de precisão a localização exata do usuário

é adulterada a fim de proteger a sua localização real; a privacidade da identidade, pois, com a divulgação da localização ajustada se torna mais difícil inferir a identidade do usuário a partir da localização e a privacidade do caminho, uma vez que a localização alterada pelo ajuste de precisão pode representar qualquer ponto aleatório dentro de um raio, é impossível traçar um caminho realizado pelo usuário.

É importante ressaltar, ainda, que o tempo de execução do código apresentado na Figura 5.4 não acrescentou atraso excessivo, como pode ser constatado nos resultados de desempenho aferidos e descritos no próximo capítulo.

5.3.3.2 Nível 1 – Anonimato

O Módulo de Privacidade no nível 1 garante a privacidade no compartilhamento da localização do usuário dentro de um grupo formado na RSM.

O algoritmo que define a localização a ser compartilhada dentro do grupo de usuários funciona da seguinte forma: primeiramente é calculada a distância entre todos os membros para os demais. Para realizar este cálculo foi utilizada a fórmula da Distância Euclidiana que calcula a distância entre dois pontos. A Figura 5.5 ilustra o trecho de código que calcula a distância entre dois pontos.

```
31      public static double geoDistanceInKm(double firstLatitude,
32              double firstLongitude, double secondLatitude, double secondLongitude) {
33
34          // Conversão de graus pra radianos das latitudes
35          double firstLatToRad = Math.toRadians(firstLatitude);
36          double secondLatToRad = Math.toRadians(secondLatitude);
37
38          // Diferença das longitudes
39          double deltaLongitudeInRad = Math.toRadians(secondLongitude
40                  - firstLongitude);
41
42          // Cálcula da distância entre os pontos
43          return Math.acos(Math.cos(firstLatToRad) * Math.cos(secondLatToRad)
44                  * Math.cos(deltaLongitudeInRad) + Math.sin(firstLatToRad)
45                  * Math.sin(secondLatToRad))
46                  * EARTH_RADIUS_KM;
47      }
```

Figura 5.13. Código do Cálculo da Distância entre Dois Pontos.

No código acima, as coordenadas do primeiro ponto são armazenadas na variável firstLatitude e firstLongitude, assim como as coordenadas do segundo ponto são armazenadas nas variáveis secondLatitude e secondLongitude, respectivamente. Nas linhas 35 e 36 as coordenadas das latitudes são convertidas de graus para radianos. Na linha 39 é calculado o valor delta das latitudes em radianos que será utilizado no cálculo da distância. Por fim, na linha 43 é calculada a

distância entre os dois pontos utilizando as coordenadas de latitude convertidas em radianos, o delta e o raio médio da terra em KM representado pela constante EARTH_RADIUS_KM. Outra opção para o cálculo da distância é a utilização da API da matriz de distâncias do Google. Esta API é um serviço que fornece a distância e o tempo de deslocamento para uma matriz de origem e destino. Porém, para obter o resultado seria necessário realizar um acesso ao serviço, o que acarretaria um atraso significativo.

Para percorrer o grafo e calcular as distâncias de todos os usuários para os demais foi adaptado o algoritmo DFS (*Depth First Search*). O tempo de execução deste algoritmo depende da quantidade de membros do grupo. Assim, quanto maior o número de usuários pertencentes ao grupo, maior será o tempo de execução. Porém, como em média o número de usuários pertencentes aos grupos não é grande, o atraso inserido no tempo de execução é aceitável.

Após o cálculo das distâncias entre os usuários, o algoritmo seleciona a mínima distância de cada usuário. De posse desta informação, é selecionada a menor distância entre todas as mínimas distâncias selecionadas.

O nível 1 garante o anonimato da localização do usuário dentro de um grupo, insere um atraso que não é significativo e não compromete a execução da aplicação. O nível também garante que os membros pertencentes ao grupo não terão acesso à localização real do usuário, porque não poderão obter o caminho feito por ele e sua identidade é preservada.

Porém, para ser preciso, o grupo necessita ser formado por mais de quatro usuários, pois um número menor facilita a descoberta da localização real do usuário que foi compartilhada entre todos os membros. Nem sempre é garantido que o grupo possua acima de quatro usuários. Para amenizar esse problema, antes de compartilhar a localização selecionada é aplicada a técnica do ajuste de precisão presente no nível 0, garantindo, assim, que a localização compartilhada não possua alta precisão.

5.3.3.3 Nível 2 – Anonimato Garantido

Como mencionado no tópico anterior, não é garantinda a existência de mais de quatro usuários em um grupo na RSM. O nível 2 utiliza a técnica de geração de localizações falsas para formar um conjunto de anonimato acima de quatro usuários. Além disso, o nível 2 pode ser utilizado para ocultar a localização do usuário dentro

de um grupo ou em um compartilhamento de localização realizado individualmente com outro usuário. A Figura 5.6 ilustra a técnica de geração de localizações falsas utilizada neste nível.

A técnica funciona da seguinte forma: inicialmente é aplicado o ajuste de precisão sobre a localização do usuário e esta é resultante e representada na Figura 5.6 pelo círculo maior central. A partir da localização calculada, outras quatro localizações falsas são geradas. Para a geração delas, também é utilizado o ajuste de precisão. A localização é ajustada a partir da localização real do usuário e as demais localizações falsas geradas são adicionadas a um grafo. A partir da formação do grafo, a técnica utilizada no nível 1 é aplicada para encontrar a localização que será compartilhada. As quatro localizações falsas servem para dificultar a possibilidade de uma engenharia reversa, ou seja, de encontrando o raio aplicado no ajuste de precisão, usuários mal-intencionados conseguirem calcular a localização exata do usuário. Quanto maior o número de localizações falsas geradas maior a complexidade da execução de uma engenharia reversa.

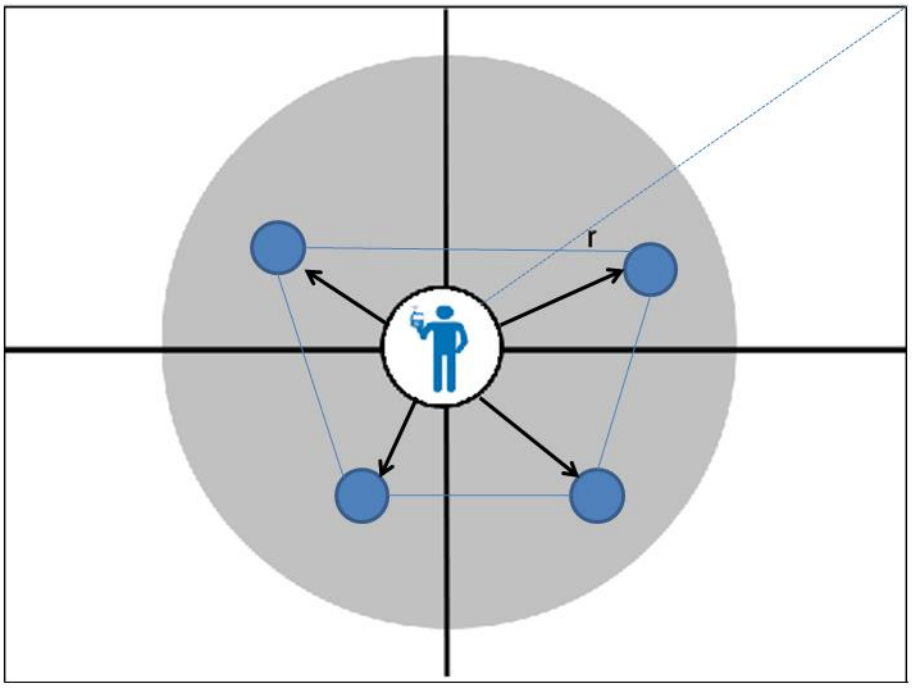

Figura 5.14. Técnica de Geração de Localizações Falsas.

O Módulo de privacidade no nível 2 garante a privacidade no compartilhamento da localização real do usuário, não insere atraso significativo e não compromete o uso da aplicação. Além disso, este nível também atende às categorias identificadas por Anthony et al. (Anthony et al. 2007) que foram apresentadas na seção 2.4, garantindo que a localização real e com alta precisão do

usuário seja compartilhada, impedindo que sua identidade seja inferida a partir de sua localização e impossibilitando que o caminho realizado pelo usuário seja obtido. As localizações calculadas não possuem uma direção lógica.

5.3.3.4 Nível 3 – Lista Negra

O nível 3 garante que a localização do usuário nunca seja compartilhada com nenhum de seus usuários de sua RSM que foram relacionados a esta lista. A lista negra nada mais é que uma marcação que o usuário realiza sobre um usuário ou um grupo de usuários com os quais não pretende compartilhar sua localização. Ao realizar a marcação, o aplicativo define o valor "*TRUE*" em um campo da tabela de contatos denominado "boqueado". Dessa forma, ao receber requisições de compartilhamento de localização de algum membro de sua RSM, o módulo de privacidade verifica se o campo "bloqueado" está definido com o valor "*TRUE*" e, caso positivo, a requisição é negada.

Este nível não adiciona atrasos na execução do aplicativo, uma vez que a verificação do valor de tal campo é simples e não possui complexidade. Porém, em uma aplicação real de RSM, este nível compromete a sua utilização, uma vez que a RSM utiliza a informação de localização do usuário para oferecer recursos como oferecimento de serviços próximos, sugestão de novos amigos localizados na região, entre outros.

5.3.4 Módulo de Comunicação

O Módulo de Comunicação tem a função de gerenciar as conexões entre o servidor de rede social e o intermediário confiável.

A conexão com o servidor de rede social é realizada de duas formas diferentes: no primeiro acesso, quando a conexão com o servidor é realizada utilizando um *webservice* e ao receber e enviar uma requisição de compartilhamento de localização que utiliza conexão via *socket*.

No primeiro acesso, o usuário informa seu *login* e senha para acesso à RSM ou se conecta utilizando sua conta no Facebook. Caso o usuário escolha se registrar utilizando sua conta no Facebook, o aplicativo estabelece uma conexão com o servidor de Rede Social utilizando um *Webservice*. O servidor irá acessar a base de dados do Facebook, copiar os contatos e gravar essas informações no banco de

dados (popular) da RSM. Dessa forma, o usuário não necessita iniciar uma nova RSM do zero. A conexão entre aplicativo e servidor através de um *webservice* é necessária, pois a API do Facebook utiliza conexão através de *webservices*. O resultado da requisição é retornado no formato XML que, depois de recebido pelo servidor, é transmitido para o aplicativo do usuário também no formato XML.

O Android não possui uma API nativa para acessar um *webservice.* Então, para a implementação do protótipo foi utilizado o *framework* ksoap2. O *framework* ksoap2 é uma biblioteca de conexão com *webservices* bem leve, desenvolvida especialmente para dispositivos móveis com menos capacidade de processamento. A Figura 5.7 ilustra o código da classe que realiza a conexão com o *webservice* do servidor de Rede Social utilizando a biblioteca ksoap2.

```
8  public class WebService {
9
10     private static final String NAMESPACE = "projetorsti.com.br";
11     private static final String URL = "http://192.168.1.2:8080/axis/serverrsm.jws?wsdl";
12     private static final String SOAP_ACTION = "getFriends";
13
14     public void webServiceBanco( Context context, String login, String senha) {
15
16         SoapObject request = new SoapObject(NAMESPACE, "getFriends");
17         SoapSerializationEnvelope envelope = new SoapSerializationEnvelope(SoapEnvelope.VER11);
18         String retorno = null;
19
20         // Adiciona parâmetros
21         request.addProperty("login", login);
22         request.addProperty("numB", senha);
23
24         envelope.setOutputSoapObject(request);
25         HttpTransportSE androidHttpTransport = new HttpTransportSE(URL);
26
27         try {
28             androidHttpTransport.call(SOAP_ACTION, envelope);
29             SoapObject resultsRequestSOAP = (SoapObject) envelope.bodyIn;
30             retorno = resultsRequestSOAP.toString();
31
32             ManagerFacebook mf = ManagerFacebook.processResult( retorno );
33
34         } catch (Exception e) {
35             Uteis.exibeAlerta(e.getMessage(), context);
36             e.printStackTrace();
37         }
38     }
39 }
```

Figura 5.15. Conexão com o Servidor Através de Webservice Utilizando KSOAP2.

No código acima, nas linhas 16 e 17 é preparada a requisição que será enviada ao servidor. Nas linhas 21 e 22 são definidos os parâmetros com o *login* e senha do Facebook informados pelo usuário. No trecho de código entre as linhas 24 a 30 é realizada a comunicação com o *webservice* e o recebimento do resultado. O resultado recebido é passado para o método estático denominado processResult, que irá tratar o resultado obtido do *webservice*. O resultado consiste na lista de contados do usuário no Facebook que está no formato XML. O método processResult repassa o MXL para o Módulo de Gerenciamento de Dados que, por

sua vez, processa o XML e armazena a lista de contato no banco de dados utilizando SQLite.

Nas requisições de compartilhamento de localização solicitadas pelo usuário, o Módulo de Comunicação realiza e gerencia as conexões com o servidor de Rede Social utilizando socket. Para a escolha da utilização de sockets foram consideradas as questões de segurança, desempenho e gerenciamento de conexões por parte do servidor. Para que haja segurança e privacidade nas conexões entre o aplicativo cliente e o servidor foi utilizado o protocolo SSL (*Secure Sockets Layer*). O SSL é utilizado para comunicações criptografadas entre clientes e servidores e garantem que o conteúdo não é diretamente identificado. As conexões entre o aplicativo cliente e o servidor são autenticadas utilizando um certificado de chave pública e privada assinado por um AC (Autoridade Certificadora) confiável. O diagrama de sequência da Figura 5.8 ilustra a sequência de conexão e autenticação entre o aplicativo cliente e o servidor. Neste diagrama não está abordada a sequência de recepção da requisição e execução da privacidade por parte do usuário alvo, pois esta sequência foi exemplificada na Figura 5.3.

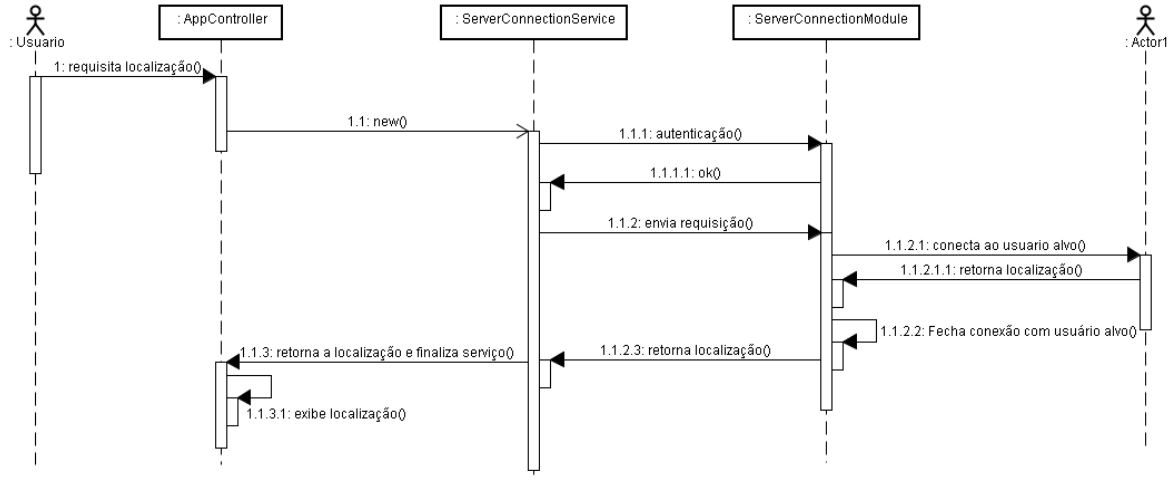

Figura 5.16. Diagrama de sequência da conexão entre aplicativo cliente e servidor.

Na sequência acima, o usuário seleciona um de seus contatos e requisita o compartilhamento de sua localização. O Módulo de Controle solicita ao Módulo de Comunicação que inicie uma nova conexão com o servidor de Rede Social. O Módulo de Comunicação inicia um novo serviço que irá gerenciar a conexão instanciando um objeto da classe *Server Connection Service*. A classe *Server Connection Service* implementa android.app.Service, que executa a tarefa em *background* e só é finalizada com um comando da aplicação. Dessa forma, mesmo

que o Android interrompa o aplicativo com a recepção de uma chamada telefônica, ou o aplicativo seja interrompido pelo usuário, o serviço iniciado continuará sua execução e será finalizado apenas após a recepção da localização. A Figura 5.9 ilustra o trecho de código onde é realizada a conexão utilizando *socket* SSL.

No trecho de código entre as linhas 41 a 44 é iniciada uma conexão com o servidor de Rede Social utilizando *socket* SSL. Após a conexão estabelecida e a certificação realizada, os canais de comunicação que irão enviar e receber as informações são estabelecidos nas linhas 55 e 56 e, então, os canais de comunicação e a conexão estabelecida são passadas como parâmetro para uma nova instância do serviço iniciado na linha 58.

```
38      private void Connect(){
39
40          // abrindo SSLSocket com o servidor de rede social
41          SocketFactory sf = SSLSocketFactory.getDefault();
42          SSLSocket socket = (SSLSocket) sf.createSocket("192.168.0.1", 443);
43          HostnameVerifier hv = HttpsURLConnection.getDefaultHostnameVerifier();
44          SSLSession s = socket.getSession();
45
46          // Verifica se o hostname certificado é para o servidor de rede social
47          if (!hv.verify("localhost", s)) {
48              throw new SSLHandshakeException( s.getPeerPrincipal() );
49          }
50
51          // At this point SSLSocket performed certificate verificaiton and
52          // we have performed hostname verification, so it is safe to proceed.
53
54          if ( ConnetionModulo.validaCertificado ( socket ) ) {
55              ObjectOutputStream out = new ObjectOutputStream(socket.getOutputStream());
56              ObjectInputStream input = new ObjectInputStream(socket.getInputStream());
57
58              new ServerConnectionSerivce( socket, out, input );
59      }
```

Figura 5.17. Conexão com o servidor utilizando *socket* SSL.

Para gerenciar as requisições de compartilhamento de localização recebidas de outros usuários, o Módulo de Comunicação inicia um serviço que monitora a recepção de conexões. Esse serviço se comporta de forma semelhante a um servidor e todas as requisições recebidas que são processadas paralelamente em *backgroud* por uma Thread. Dessa forma, o Módulo de Comunicação garante sempre a disponibilidade do serviço. A execução deste serviço pode consumir o recurso de bateria do dispositivo se executado constantemente. Para resolver este problema, o serviço é finalizado sempre que o usuário realiza o *logaut* na aplicação.

Além de gerenciar a comunicação com o *webservice* e o servidor *socket* disponibilizados pelo servidor de Rede Social, o Módulo de Comunicação também

gerencia a comunicação com o *proxy* confiável. A forma de conexão e o processo de execução das requisições são semelhantes aos do servidor.

5.3.5 Módulo de Controle

O Módulo de Controle possui três funcionalidades principais, que são: oferecimento do acesso às opções da RSM e configuração de políticas e níveis de privacidade através de uma interface gráfica; gerência da execução dos demais módulos.

A gerência da execução consiste em iniciar os serviços oferecidos pelos demais módulos e coordenar o relacionamento entre eles. Por exemplo, o módulo de controle inicia um servidor que monitora as requisições recebidas de outros usuários que são gerenciadas pelo Módulo de Comunicação. As requisições recebidas pelo Módulo de Comunicação são encaminhadas ao Módulo de Controle que, por sua vez, inicia um serviço do Módulo de Privacidade que irá validar a requisição com as preferências de privacidade definidas pelo usuário. Além disso, é iniciado também um serviço do módulo de gerenciamento de dados que irá armazenar as dados da requisição recebida de modo a oferecer auditoria futura.

Uma funcionalidade do Módulo de Controle é o oferecimento de uma interface gráfica que possibilita ao usuário o acesso às opções do aplicativo e configuração das políticas e níveis de privacidade. A Figura 5.10 ilustra as principais interfaces do aplicativo disponíveis ao usuário.

Primeiramente, a interface de *login* ilustrada na Figura 5.10 pela interface de letra “a” que é apresentada ao usuário no primeiro acesso ou em todos os acessos realizados quando não estiver *logado*. No primeiro acesso, o usuário tem a opção de se registrar informando um novo usuário e senha ou utilizar sua conta no Facebook. Para a utilização da conta do Facebook, o usuário deverá estar logado no Facebook para que o aplicativo possa recuperar as informações de acesso. Após informar a conta para registro, o aplicativo, através do Módulo de Controle, inicia um serviço que irá se conectar ao *webservice* do servidor e recuperar a lista de contatos que o usuário possui no Facebook.

Após recuperar e armazenar a lista de contato, esta é apresentada para o usuário na interface principal do aplicativo, que é representada na Figura 5.11 pela interface de letra “b”.

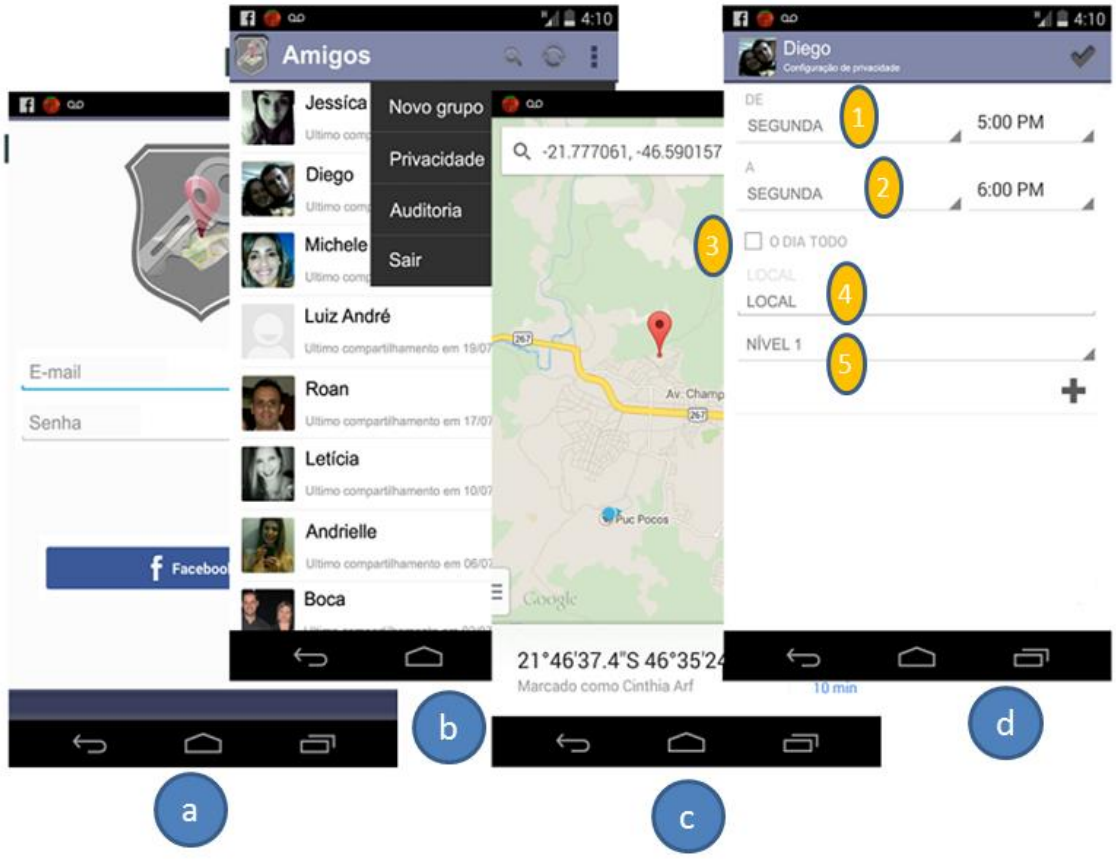

Figura 5.18. Principais interfaces do aplicativo de RSM cliente.

A interface principal oferece acesso a todas as funcionalidades do aplicativo, tais como a criação de grupos, visualização da auditoria e as principais, que são a requisição de compartilhamento de localização e a configuração das políticas e níveis de privacidade. A requisição de compartilhamento de localização é realizada pressionando o contato na lista. O aplicativo inicia o processo de requisição em *background* e, quando o resultado é retornado, é apresentado no mapa ilustrado pela interface “c”. A interface que oferece ao usuário a configuração das políticas e níveis de privacidade é representada pela interface de letra “d”. Esta interface possui cinco campos: os campos 1 e 2 permitem que o usuário configure o período e os dias da semana em que ele se sente confortável em compartilhar a sua localização; o campo 3 permite que o usuário especifique que sua localização poderá ser compartilhada o dia todo; o campo 4 permite configurar o local em que é permitido o compartilhamento e o campo 5 permite especificar o nível de privacidade que será executado sobre as requisições recebidas. Todos os campos são opcionais, porém o usuário deverá especificar no mínimo um deles para que o sistema crie a política.

Quando criada toda ela poderá ser reutilizada com outros membros da RSM ou com um grupo.

5.4 Aplicação Servidor

A aplicação do servidor de Rede Social foi implementada com base nos quatro módulos apresentados na Figura 5.1. A seguir, os detalhes de cada módulo são apresentados separadamente.

5.4.1 Módulo de Comunicação

O Módulo de Comunicação do servidor possui três funcionalidades principais: disponibilizar um webservice para o primeiro acesso na RSM, realizar a comunicação com o webservice do Facebook e intermediar as conexões entre os usuários nas requisições de compartilhamento de localização.

Para a implementação do servidor de Rede Social foi utilizado o servidor Apache (Apache 2014). O motivo da escolha do Apache foi devido ao servidor ser configurável, de alto desempenho, de fácil instalação e seu código fonte ser distribuído gratuitamente pela equipe de desenvolvedores do *Apache software Foundation*.

O webservice disponibilizado para o primeiro acesso foi desenvolvido utilizando o *Framework* Zend PHP (Zend 2014). O Zend *Framework* é um dos principais *frameworks* PHP disponíveis no momento que possibilita o desenvolvimento de aplicações limpas e organizadas por ser orientado a objetos e permitir desenvolvimento utilizando MVC. Além disso, Zend disponibiliza diversas APIs de consumo de webservices para Google, Amazon, Twitter e, principalmente, Facebook. Para a implementação do webservice optou-se pela utilização do protocolo SOAP (*Simple Object Access Protocol*). SOAP é um protocolo de comunicação baseado em XML que permite que aplicações troquem informações utilizando o protocolo http, que é o protocolo mais comum da internet e facilita a comunicação evitando que a transmissão seja bloqueada por um *firewall* ou *proxy*. A

Figura 5.12 ilustra o diagrama de sequência de execução do webservice no primeiro acesso do usuário.

Conforme sequência apresentada na Figura 5.12, o usuário informa os dados de conexão com o Facebook. O Módulo de Controle presente no aplicativo cliente inicializa um serviço de conexão com o webservice através do módulo de comunicação. A comunicação com o webservice da RSM é estabelecida e os dados são enviados. Do outro lado, o webservice da RSM inicia uma conexão com o webservice do Facebook utilizando a API disponibilizada pelo próprio Facebook e, em seguida, envia uma requisição solicitando a lista de contatos pertencentes ao usuário. O webservice do Facebook, por sua vez, solicita a permissão explícita do usuário para enviar tais informações. Esta solicitação de permissão é enviada ao aplicativo do cliente que apresenta a solicitação ao usuário. Após a permissão concedida do usuário, o Facebook encaminha a lista de contatos pertencentes a ele. Ao receber o retorno, o aplicativo servidor armazena a lista de contatos e, logo após, encaminha o XML retornado pelo Facebook ao aplicativo do usuário para que possa ser armazenado. Depois de armazenado, o aplicativo apresenta a lista atualizada ao usuário.

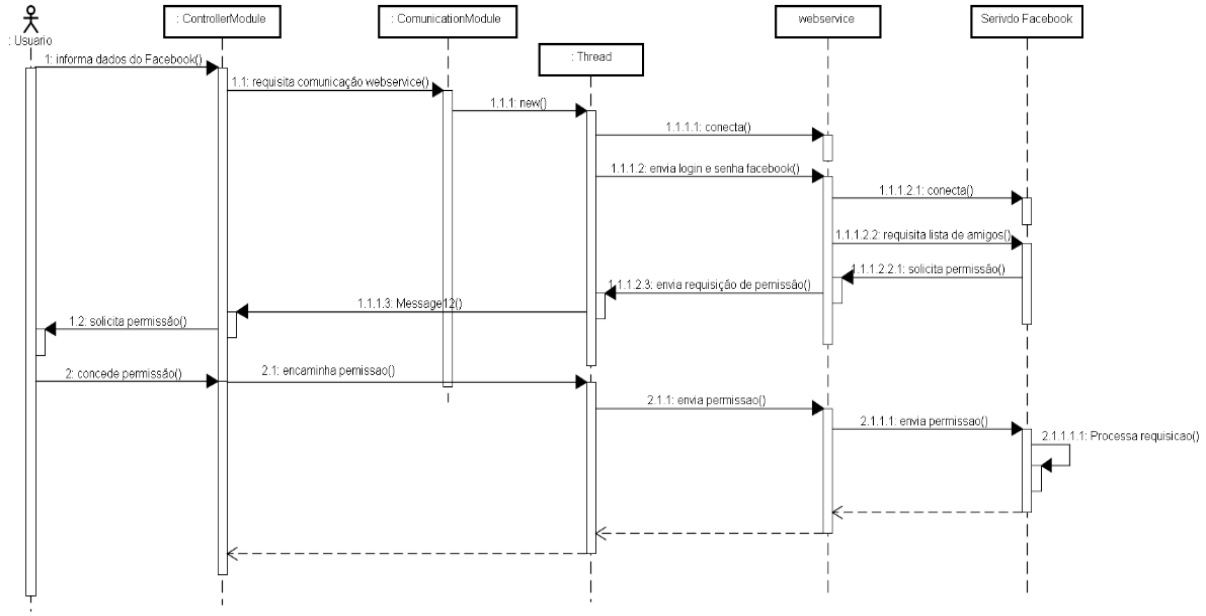

Figura 5.19. Sequência de execução no primeiro acesso.

Após a RSM do usuário estar preenchida com os mesmos contatos existentes no Facebook, o aplicativo usuário se comunica com o servidor em dois momentos: quando atualiza o endereço IP do aplicativo e o *status* atual e quando o usuário

requisita o compartilhamento de localização de algum dos seus contatos. Para intermediar as conexões entre os usuários e atualizar seu IP e *status*, o Módulo de Comunicação possui uma segunda aplicação desenvolvida em Java. Esta aplicação utiliza *sockets* para a conexão com o aplicativo do cliente. A Figura 5.12 ilustra o trecho de código implementado para o servidor.

No trecho de código ilustrado pela figura 5.12, na linha 32 é configurada a certificação através da utilização do método estático da classe Server Validate Certification.get SSLServer. Este método configura os parâmetros para certificação da conexão e retorno um objeto do tipo SSL Server que irá aguardar conexões. No trecho de código entre as linhas 37 e 48 é executado um while infinito e, dentro deste while são aguardadas novas conexões. A linha 40 aguarda novas conexões SSL e, quando recebe uma nova conexão, é passada para uma Thread que irá gerenciar as conexões em paralelo, conforme ilustrado na linha 43. A execução do servidor continua normalmente e novas conexões são aguardadas. A classe Manager Connection é quem realiza o tratamento da conexão. Esta classe que implementa Runnable identifica a ação (atualização de IP e status ou requisição de compartilhamento de localização) e executa a rotina correspondente. A Figura 5.13 ilustra o diagrama de atividades executadas em uma requisição entre o aplicativo cliente, o servidor e o usuário requisitado.

```
26      // inicia o servidor
27      public void startServer() {
28          // cria o executor para as Runnables que serão responsaveis pela execução da conexão com os clientes
29          serverExecutor = Executors.newCachedThreadPool();
30          // cria o servidor e gerencia novas conexões
31          try {
32              SSLServer server = new ServerValidateCetification.getSSLServer();
33              // cria ServerSocket para conexões com os clients
34              SSLServerSocket ss = (SSLServerSocket) server.createServerSocket( SERVER_PORT );
35              System.out.printf( "%s%d%s", "MSNServer: Servidor escutando conexões na porta ", SERVER_PORT, " ..." );
36              // ouve conexões de clientes constantemente
37              while ( true ) {
38
39                  // Aguarda e aceita novas conexões de clientes
40                  SSLSocket clientSocket = (SSLSocket) ss.accept();
41
42                  // cria MessageReceiver para receber gerenciar a conexão com o cliente
43                  serverExecutor.execute( new ManagerConnection( this, clientSocket ) );
44
45                  // imprime informações sobre a conexão
46                  System.out.println( "\nMSNServer: Conexão recebida de: " + clientSocket.getInetAddress() );
47
48              }
49          } catch ( IOException ioException ) {
50              ServerRSM.retornaErro(ioException.printStackTrace());
51          }
52
53      }
```

Figura 5.20. Código implementado para o servidor.

5.4.2 Módulo de Armazenamento

O Módulo de Armazenamento tem a finalidade de inserir e atualizar a lista de contatos de cada usuário pertencente à Rede Social, atualizar seu status e o endereço IP.

O Módulo de Comunicação, após realizar a comunicação com o Facebook, processa o XML com a lista de contatos de usuário retornada e armazena temporariamente em uma lista. Esta lista é enviada ao Módulo de Armazenamento juntamente com os dados iniciais do usuário, como nome, login e senha. De posse de tais informações, o Módulo de Armazenamento insere o nome do usuário e seus contatos.

Para a implementação do Módulo de Armazenamento foi utilizado o banco de dados MySQL (MYSQL 2014). O Módulo foi implementado utilizando o padrão de projetos DAO (*Data Access Object*), pois, dessa forma, o Módulo de Armazenamento se torna escalável e de fácil manutenção. Conforme aumenta a demanda e o volume de dados, caso seja necessário, o banco de dados pode ser trocado sem causar impacto nos demais módulos da aplicação. O esquema do banco de dados na aplicação servidor é o mesmo esquema da aplicação cliente ilustrado na Figura 5.2.

O Módulo de Informações armazena apenas as informações do usuário como nome, endereço IP atualizado, login e senha, bem como a sua lista de contatos. Dados como a localização do usuário ou histórico de movimentação não são armazenados pelo servidor.

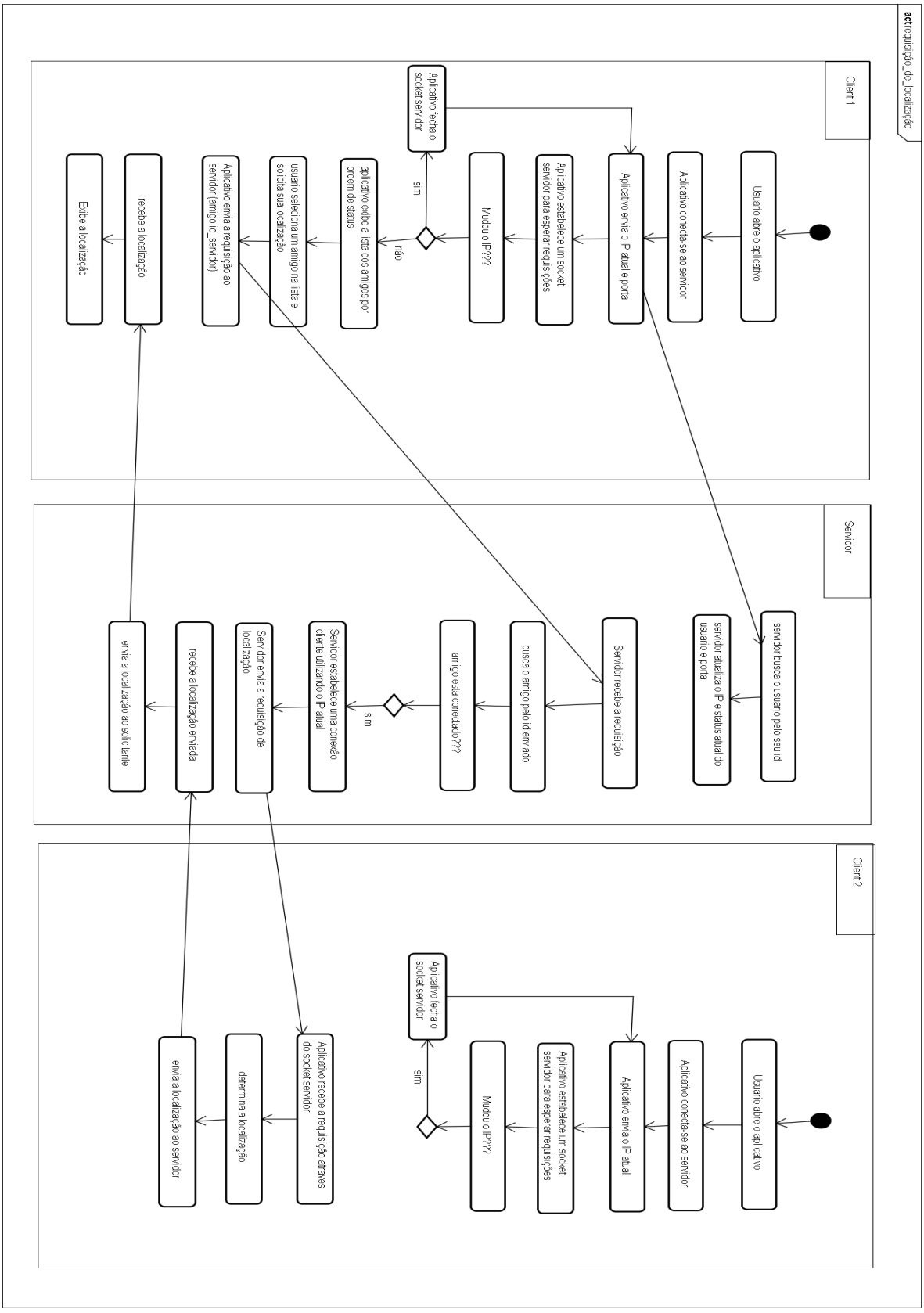

Figura 5.21. Diagrama de atividades usuário requisitante x servidor x usuário requisitado.

5.4.3 Módulo de Controle

O Módulo de Controle possui função semelhante ao Módulo de Controle da aplicação cliente no que se refere ao gerenciamento do relacionamento entre os demais módulos. Para que ocorra a execução da aplicação de maneira eficiente, é necessário que as tarefas realizadas por cada módulo sejam coordenadas, especialmente em casos em que um módulo depende da execução e retorno de outros módulos. O Módulo de Controle do servidor é responsável por comandar a execução da aplicação de maneira geral.

5.5 Aplicação do *Proxy* Confiável

As políticas e níveis de privacidade oferecidas pelo protótipo RSM Privacy garantem a privacidade da localização do usuário quando compartilhada na RSM, evitando assim que sua identidade seja inferida através da localização. Porém, o endereço IP real e atualizado do usuário é divulgado ao servidor de Rede Social, possibilitando que ele descubra a localização do usuário, possibilitando-lhe também inferir a identidade deste usuário. Uma alternativa para resolver tal problema é a utilização de um *proxy* confiável. O protótipo RSM Privacy oferece a possibilidade da utilização de uma aplicação para um *proxy* confiável.

A principal função da aplicação do *proxy* confiável é ocultar o endereço IP real do usuário quando ele interage com a RSM. O diagrama de sequência da Figura 5.14 ilustra a visão geral do funcionamento da aplicação do *proxy* confiável.

Conforme diagrama de sequência acima, um usuário, ao interagir com a RSM enviando uma requisição de compartilhamento de localização a outro usuário ou atualizando informações, se conecta com o *proxy* confiável ao invés de ser conectar diretamente com o servidor. A aplicação presente no *proxy* confiável inicia uma Thread que irá intermediar a conexão entre o usuário e o servidor. O servidor recebe a requisição enviada pelo usuário e intermediada pelo *proxy*. Neste momento, o endereço IP que o servidor possui é o endereço IP do *proxy* e não do usuário. O servidor envia a requisição ao usuário alvo, que por sua vez a processa aplicando a política e nível apropriado. Em seguida, o resultado é retornado ao servidor. O

servidor retorna o resultado ao *proxy* e finaliza a conexão. O *proxy*, por sua vez, retorna o resultado ao usuário e encerra a conexão e a Thread. A aplicação do usuário recebe e exibe o resultado retornado. Neste processo, o *proxy* obtém os dados de acesso dos usuários. Por este motivo, um *proxy* confiável deve ser mantido por uma instituição que garante a segurança das informações.

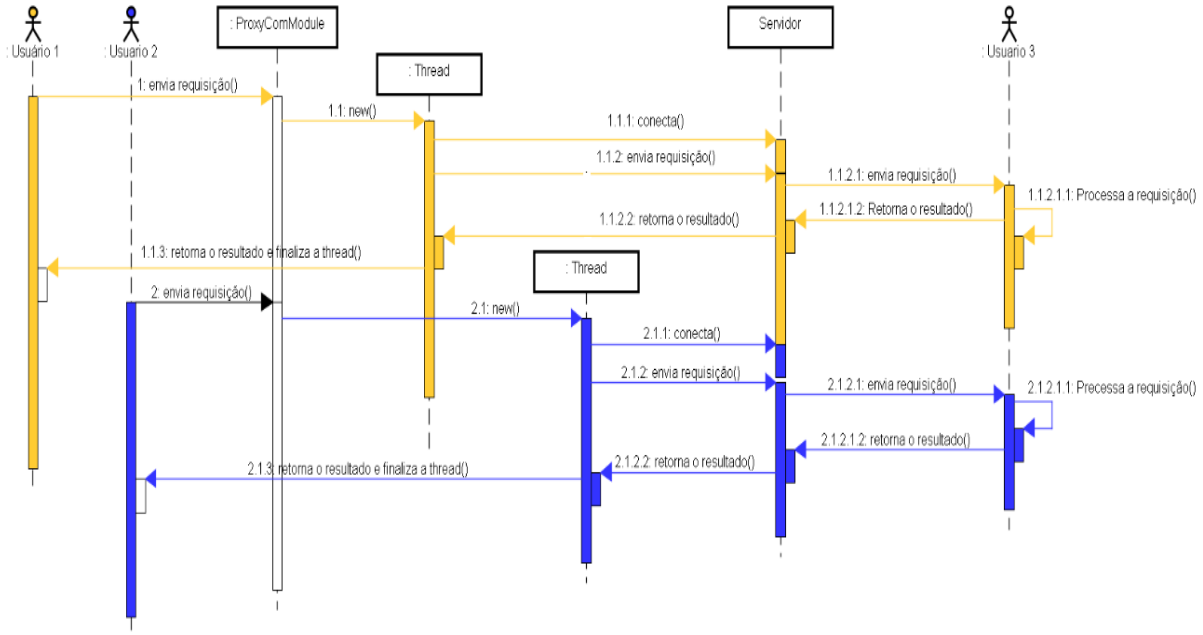

Figura 5.22. Diagrama de sequência de execução do *proxy* – visão geral.

A aplicação do *proxy* foi desenvolvida utilizando a linguagem de programação Java e o servidor utilizado foi o Apache. A implementação foi realizada com base nos dois módulos ilustrados na Figura 5.1. A seguir são apresentados os detalhes de cada módulo.

5.5.1 Módulo de Comunicação

A função principal do Módulo de Comunicação da aplicação do *proxy* é intermediar a comunicação entre a aplicação cliente e a aplicação servidora. O módulo recebe as conexões dos clientes e estabelece a conexão com o servidor. O Módulo de Comunicação utiliza *socket* SSL para realizar as conexões. A implementação do código é semelhante ao código implementado no servidor de Rede Social. A diferença está no tratamento de cada conexão realizada pelas Thread que são gerenciadas pelo Módulo de Controle.

5.5.2 Módulo de Controle

Como mencionado no tópico anterior, o Módulo de Controle da aplicação do *proxy* tem a função de gerenciar as conexões estabelecidas entre cliente e servidor. Quando o Módulo de Comunicação recebe uma conexão do cliente, ele inicia uma Thread que irá tratar da conexão estabelecida. Além disso, será estabelecida a conexão com o servidor e uma nova Thread é iniciada para tratar esta conexão. O Módulo de Controle, por sua vez, cuidará do sincronismo entre essas duas Threads.

5.6 Considerações finais

A prova de conceito do modelo, o RSM Privacy, oferece garantias de privacidade aos seus usuários no compartilhamento de localização em RSM. Essas garantias são realizadas através da configuração de politicas e níveis de privacidade.

As políticas de privacidade permitem que os usuários configurem restrições para o compartilhamento de sua localização. Nas políticas, o usuário pode determinar qual amigo poderá ter acesso à sua localização, um período de horário, dias da semana e um local especifico que sua posição atual será compartilhada. Além disso, o RSM Privacy permite que os usuários combinem essas restrições gerando políticas de privacidade mais robustas. A utilização destas visa obter garantias de privacidade e não compromete o oferecimento de recomendações oferecidas pela rede social, pois as politicas determinam critérios para divulgação da localização e não para negar esta divulgação. Dessa forma, o provedor ainda obtém a informação de localização precisa do usuário, possibilitando a oferta de recomendações de serviços e novos amigos com base na região geográfica. Porém, o acesso à localização do usuário pelo provedor gera outros riscos à privacidade. Além disso, o uso de políticas também permite que usuários maliciosos pertencentes à lista de contatos dos usuários também obtenham sua localização. O usuário nem sempre reconhece que determinado usuário é malicioso, pois este consegue facilmente entrar nas listas de contatos devido a algum fator como, por exemplo, interesses em comum ou relacionamento com outros usuários pertencentes à lista

de contato. O uso de politicas de privacidade apenas garante que a localização seja compartilhada em determinadas condições. Para suprir esse problema, o modelo oferece níveis de privacidade que ocultam a localização real do usuário.

O RSM Privacy disponibiliza quatro níveis com características distintas de privacidade. O modelo de execução baseado em níveis possibilita a configuração das preferências de privacidade, 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. A utilização das técnicas de privacidade dificulta consideravelmente a possibilidade de identificação da localização exata de um usuário, uma vez que suas informações de localização não serão repassadas ao provedor ou a usuários maliciosos com precisão elevada. Além disso, não será possível descobrir o caminho realizado pelos usuários e os lugares exatos frequentados por eles.

A combinação de politicas e níveis oferecidos pelo modelo fornece garantias robustas de privacidade. Porém, se o usuário não for capaz de definir politicas eficientes, o funcionamento do modelo será comprometido consideravelmente. Quanto maior o número de regras definidas pelo usuário pior será o desempenho da aplicação. Para que haja garantias de privacidade eficientes sem comprometer o funcionamento do modelo, os usuários devem ser capazes de definir regras que atendam sua necessidade. Porém, é difícil medir a quantidade ideal de regras que o usuário deve configurar, uma vez que ele tem dificuldade em configurar tais regras, o que é mostrado no capitulo 6, no teste de usabilidade.

A utilização do *proxy* confiável é mais uma garantia de privacidade para os usuários, pois oculta o endereço IP real do dispositivo. Dessa forma, é evitada a identificação do usuário com base no endereço IP. Porém, a existência do *proxy* confiável nem sempre será possível, uma vez que, para ser confiável, é necessário que exista uma organização responsável que mantenha a confiabilidade do *proxy*.

Capítulo 6

AVALIAÇÃO DO MODELO

6.1 Avaliação de Desempenho do Protótipo

Nesta seção serão descritos os testes práticos realizados no protótipo que permitiram a sua avaliação de desempenho em sua principal função, que é a garantia de privacidade através da configuração das políticas e dos níveis.

Para os testes com o aplicativo cliente foi utilizado o dispositivo móvel Nexus 4 da LG, com o sistema operacional Android versão 4.4.1, acesso à localização via GPS e acesso à Internet via Wi-Fi ou 3G, e um celular *Samsung Galaxy* 5, com Android 2.2 , acesso à localização via GPS e acesso à Internet via Wi-Fi ou 3G. Para o servidor foi utilizado um *notebook* com as seguintes configurações: processador *Intel Core* i3, 4 GB de memória RAM, sistema operacional Windows 7 e plataforma Java JDK 1.7.0_25-b17. Para o *proxy* confiável, a máquina utilizada possuía a seguinte configuração: processador *Intel Pentium* (2.1 GHz), 3 GB de memória RAM, sistema operacional Windows 7 e plataforma Java JDK 1.7.0_25-b17. A Figura 6.1 ilustra a arquitetura geral da execução dos testes.

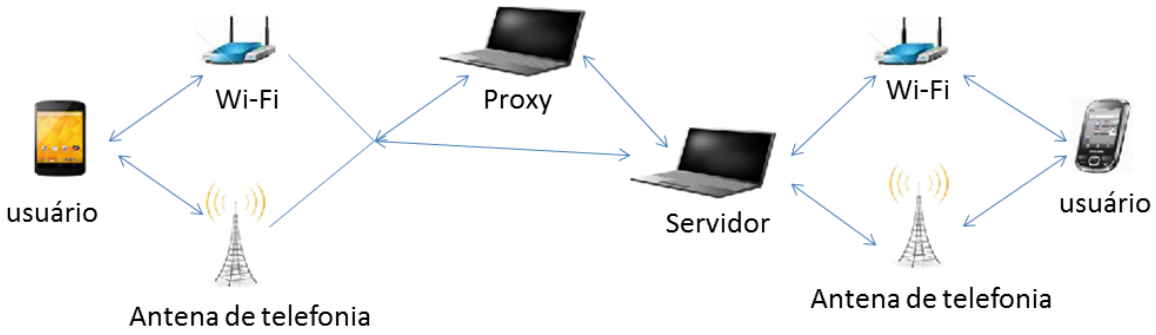

Figura 6.23. Arquitetura geral utilizada nos testes.

Os primeiros testes objetivam avaliar o tempo de resposta observado durante as requisições de compartilhamento de localização de um dispositivo móvel para o outro. Para um primeiro momento foram realizadas requisições com dez localidades predefinidas, isto porque os testes seriam dificultados se fossem realizados em locais diferentes devido a problemas que ocorreriam, como a disponibilidade de outros locais com conexão Wi-Fi aberta. Além disso, a não utilização do GPS para obter a localização se deveu à variação de tempo muito grande que o GPS apresenta durante a execução. Essa variação poderia comprometer o tempo médio de execução. Questões como condições climáticas e baixas condições de visibilidade do receptor podem atrasar ou até mesmo impossibilitar a determinação da localização.

Para os testes foram realizadas requisições para todos os níveis disponíveis e para todas as configurações de políticas possíveis. Além disso, cada requisição foi realizada dez vezes para evitar que os resultados fossem influenciados por interferências na comunicação.

A Tabela 6.1 e a Tabela 6.2 apresentam os resultados dos tempos médios de resposta (TMR) e do desvio padrão (DP) obtidos durante a execução das requisições de compartilhamento de localização para cada nível. O intervalo de confiança utilizado foi de 95%. Os resultados referentes do tempo médio e desvio padrão são apresentados em segundos. As linhas das tabelas especificam o nível de privacidade aplicado. O alto valor de tempo apresentado nos testes com o nível 1 se deve ao fato de que, para adquirir um grupo com quatro usuários, foi necessária a utilização do emulador do Android. É um atraso que não deve ocorrer caso exista um

grupo de usuários utilizando dispositivos reais. A Tabela 6.1 destaca os resultados obtidos através das comunicações utilizando redes *Wi-Fi* e na Tabela 6.2 são apresentados os resultados obtidos com a utilização de redes 3G para a comunicação.

Tabela 6.1. Tempo Médio de Execução (em segundos) com Wi-Fi.

Nível	TMR	DP
0	1,17	0,33
1	2,20	0,21
2	7,23	0,36
3	1,91	0,40

Tabela 6.2. Tempo Médio de Execução (em segundos) com 3G.

Nível	TMR	DP
0	1,26	0,21
1	2,93	0,41
2	8,45	0,89
3	3,33	0,28

Os tempos de execução podem ser considerados aceitáveis se os compararmos ao tempo gasto com a obtenção da localização através do uso de GPS ou se os compararmos ao tempo de execução do aplicativo móvel do Facebook que é em média seis minutos (Facebook, 2014) .

A Figura 6.2 ilustra o tempo de execução do modelo considerando o número e o tipo de regras configuradas. Para medir o desempenho foram realizados três testes: o primeiro foi realizado com dez regras inseridas, o segundo com 100 regras e o terceiro com 1000 regras. Ou seja, a cada teste, os números de regras foram calculados de uma forma logarítmica (dobrando-se o valor da entrada adiciona-se uma constante ao valor do sinal de saída). Cada regra foi configurada com todos os parâmetros possíveis, considerando-se o pior caso.

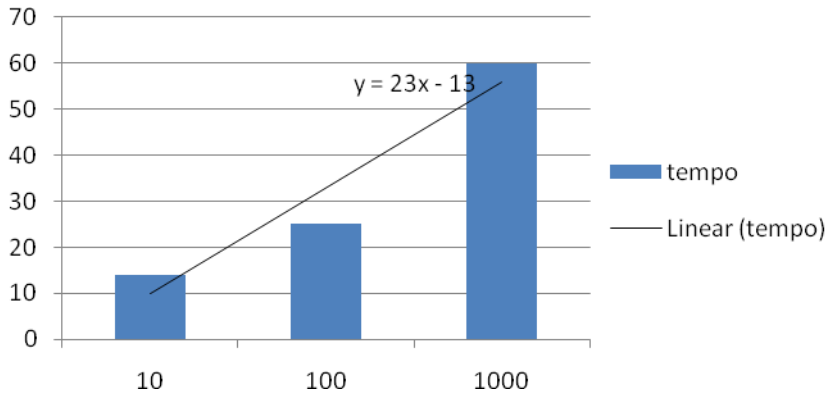

Figura 6.24. Tempo de execução x número de regras.

Analisando-se os resultados exibidos no gráfico da figura 6.2, para um conjunto de regras (n) tendendo ao infinito o comportamento do tempo tende a crescer linearmente, ou seja, o tempo de execução do modelo configurado com n regras é O(n).

Com base nos resultados obtidos com os testes realizados nos níveis de privacidade e os testes realizados com as regras, a média de atraso adicionada é 35 segundos. Porém, esse tempo é proporcional à execução dos níveis 2 e 3 com dez usuários. O atraso inserido pode variar de acordo com o número de usuários em um grupo. Em um grupo formado com mais de 100 usuários, a execução do nível 2 pode se tornar inviável. A solução para esse problema é ajustar a quantidade de localizações utilizadas no cálculo do anonimato. O nível 3 não é comprometido neste caso, pois as localizações utilizadas são geradas pela aplicação e o número inicial de pontos gerados é quatro.

6.2 Avaliação da Usabilidade

Na seção anterior foram apresentados resultados dos testes para avaliar o desempenho do aplicativo com a inserção das técnicas de privacidade oferecidas. Os resultados dos testes mostraram que o atraso inserido é aceitável comparando o tempo de execução de RSM existente com o modelo. Esta seção apresenta a avaliação da usabilidade realizada no protótipo de RSM desenvolvido e seus resultados obtidos.

De acordo com Holzinger (Holzinger 2005), uma observação de campo deve ser conduzida quando se pretende medir a usabilidade de um software. Esta observação de campo tem o objetivo de identificar problemas óbvios que podem impactar o produto final. O estudo de campo consiste na observação da utilização de um software que é realizada por um ou mais participantes, registrando em notas e vídeos os fatos observados. Além disso, métodos auxiliares, como a aplicação de questionários, também podem ser utilizados para auxiliar na análise e obtenção dos resultados.

Com o intuito de mensurar a eficácia das políticas e níveis de privacidade oferecidos, a usabilidade e a aceitação do protótipo de RSM desenvolvido, foi realizado o estudo de campo.

6.2.1 Método

O estudo foi realizado nos laboratórios da Pontifícia Universidade Católica de Minas Gerais (PUC Minas), no campus de Poços de Caldas – MG, e contou com a participação de 50 estudantes. Estudos anteriores demostraram que muitos problemas que são prováveis de ocorrer em uma dada população podem ser identificados com apenas cinco participantes (Leon 2012). Os participantes pertencem a uma faixa de idade entre 19 e 30 anos e têm formação em áreas de conhecimento de exatas, humanas e saúde. O objetivo de selecionar participantes de áreas e idades diferentes foi obter vários pontos de vista e um resultado não tendencioso. O recrutamento foi realizado através do envio de e-mails a todos os alunos do campus e da publicação de comunicados em todos os murais da universidade. Além disso, houve uma grande colaboração dos coordenadores de cada curso, que se prontificaram a comunicar seus alunos sobre o software a ser avaliado. Os participantes não receberam nenhum tipo de recompensa para participar do estudo, sendo que a motivação da participação foi colaborar com a pesquisa, pois o tema é de grande interesse de todos, especialmente estudantes.

Para a realização do estudo, foram elaborados e aplicados dois testes. O primeiro teste teve o objetivo de medir a usabilidade do protótipo de RSM. O objetivo do segundo teste foi medir a eficácia das políticas e dos níveis de privacidade oferecidos pelo protótipo.

Com o intuito de obter a opinião dos participantes e informações complementares, foram elaborados dois questionários com itens para medir o grau de segurança dos participantes ao utilizarem RSM e a sua satisfação com o protótipo. Para auxiliar na análise das respostas obtidas nos questionários, eles foram colocados em um site e todas as respostas foram armazenadas em um banco de dados.

Para a realização dos testes foi utilizado um emulador do sistema operacional Android executado em um computador com 8 GB de memória RAM, processador *Intel* i7, com o sistema operacional Windows 7. Para o servidor e o *proxy* confiável foram utilizados computadores com as mesmas configurações.

6.2.2 Protocolo de Teste

Os testes foram realizados em sessões de 40 minutos. Cada sessão foi realizada com dois participantes, sendo que ambos deveriam pertencer à Rede Social do outro. Esse relacionamento foi necessário, pois nos testes os participantes deveriam requisitar a localização do outro. Para registro e documentação dos testes, em casa sessão foi realizada a gravação de áudio e a captura das telas. As sessões foram realizadas em dois laboratórios localizados em pontos distintos da universidade e cada participante foi alocado em um laboratório diferente. O motivo da separação foi à necessidade de obter duas coordenadas diferentes.

As sessões foram iniciadas solicitando aos participantes que respondessem a um primeiro questionário composto de nove afirmativas. O objetivo deste primeiro questionário foi medir o nível de conhecimento dos participantes sobre o sistema operacional Android e medir o grau de segurança que os participantes acreditavam ter sobre o uso de dispositivos móveis. As afirmativas presentes no primeiro questionário são apresentadas na Tabela 6.3. Após o questionário, os participantes tiveram o primeiro contato com o aplicativo. Depois testaram algumas funcionalidades, como o registro na RSM utilizando a conta do Facebook, visualização dos membros da sua Rede Social e requisição de localização do colega de teste.

Tabela 6.3. Afirmativas presentes no primeiro questionário.

Afirmativas
1 - Entendo como minhas permissões são utilizadas pelos aplicativos instalados em meu dispositivo
2 - Considero importante poder configurar as permissões dos aplicativos instalados em meu dispositivo
3 - Considero importante conhecer como os meus dados são utilizados
4 - Confio na forma como os aplicativos utilizam os recursos do dispositivo
5 - Sinto-me seguro quando utilizo meu dispositivo
6 - Considero que meus dados armazenados em meu dispositivo estão seguros
7 - Considero seguro o uso de GPS
8 - Entendo como funcionam os mecanismos de segurança e privacidade presentes em meu dispositivo
9 - Sinto-me seguro em compartilhar minha localização utilizando o meu dispositivo

Fonte: Elaborado pelo autor.

As respostas obtidas neste primeiro questionário aplicado antes da utilização do protótipo de RSM são importantes para a realização de uma comparação com as respostas que serão obtidas após a apresentação e a utilização do aplicativo.

Com o objetivo de medir a eficácia dos mecanismos de privacidade oferecidos pelo protótipo de RSM e o grau de satisfação dos participantes, foi solicitado a eles que respondessem a um segundo questionário. Porém, antes que o questionário fosse apresentado, os participantes leram um pequeno texto sobre privacidade em Redes Sociais Móveis. Após a leitura apresentada, cada participante realizou a configuração de políticas e níveis de privacidade e definiu uma dessas politicas configuradas ao seu parceiro de teste. Em seguida, cada participante requisitou o compartilhamento de localização ao seu parceiro de teste e foi requisitado por ele. Para visualizar o resultado obtido através da configuração das políticas e níveis definidos, os participantes acessaram a opção de auditoria. Após a realização desse teste, os participantes responderam ao último questionário. As afirmativas presentes no segundo questionário são apresentadas na Tabela 6.4.

Tabela 6.4. Afirmativas presentes no segundo questionário.

Afirmativas
1 - Considero importante poder configurar as permissões dos aplicativos instalados em meu dispositivo
2 - Considero importante conhecer como os meus dados são utilizados
3 - Confio na forma com que as aplicações utilizam os recursos do dispositivo
4 - Considero que os dados em meu dispositivo estão seguros
5 - Considero seguro o uso de GPS
6 - Sinto-me seguro quando utilizo meu dispositivo móvel
7 - Sinto-me seguro em compartilhar minha localização utilizando o meu dispositivo

8 - Pude facilmente utilizar as opções existentes no aplicativo
9 - Fui capaz de definir as regras de privacidade corretas para os meus contatos
10 - Pude facilmente configurar minhas regras de privacidade
11 - Eu utilizaria esta rede social em meus dispositivos
12 - Eu considero válida a proteção oferecida à minha privacidade pelo aplicativo
13 - O aplicativo me permite alterar facilmente as regras de privacidade aplicada
14 - Quando uma requisição de localização de um contato é negada, a mensagem apresentada pelo aplicativo me ajuda a entender perfeitamente que a minha requisição foi negada.
15 - A forma com que a privacidade é configurada é clara.
16 - No geral, estou satisfeito com o aplicativo
17 - Sinto-me confortável em permitir o acesso à minha conta no Facebook
18 - Sinto-me seguro em utilizar redes sociais móveis em meu dispositivo
19 - Sinto-me seguro em compartilhar minha localização com os membros de minha rede social móvel
20 - O aplicativo possibilitou que, a partir de agora, prestarei mais atenção na segurança de meus dispositivos móveis, tomando mais cuidado ao instalar aplicações.
21 - O aplicativo possibilitou que, a partir de agora, prestarei mais atenção antes de compartilhar minha localização nas redes sociais e demais aplicativos.

Fonte: Elaborado pelo autor.

Os dois questionários possuíam algumas afirmativas em comum. O objetivo dessas afirmativas foi a realização da comparação das respostas obtidas antes, durante e depois do uso do protótipo e suas características de privacidade. As respostas obtidas dos participantes para cada afirmativa possuíam um valor da Escala de *Likert*, com possibilidade da realização de comentário.

A Escala de *Likert* é um tipo de escala psicométrica que é geralmente aplicada quando se tem o intuito de medir atitudes ou comportamentos dos indivíduos. Esse tipo de escala é especialmente útil quando o objetivo é coletar informações sobre assuntos sensíveis ou desafiadores.

Ao fornecerem respostas aos questionários com base na Escala de *Likert*, os participantes informam sua concordância com uma afirmação. Ao contrário de questionários com respostas simples, como por exemplo, “sim” e “não”, as respostas obtidas através dessa escala permitem avaliar o nível de opinião dos participantes.

Os dados obtidos através da utilização da Escala de *Likert* possibilitam a realização de dois tipos de análise, ordinal ou por intervalo, dependendo da forma como a escala é considerada. Essa definição é essencial, pois valores ordinais não podem ser analisados por métodos estatísticos como média ou desvio. O método de análise selecionado para este estudo foi o método por intervalo. Os intervalos de valores utilizados na Escala de *Likert* neste estudo e seus significados são apresentados na Tabela 6.5.

Tabela 6.5. Valores e significados dos intervalos utilizados na Escala de Likert.

Valores	Significado
1	Concordo
2	Concordo Parcialmente
3	Indiferente
4	Discordo Parcialmente
5	Discordo

6.2.3 Limitações

Devido à limitação da área de recrutamento, os participantes não representam a população geral de usuários de Redes Sociais Móveis. O intuito do experimento foi entender as questões referentes à privacidade dos participantes e as dificuldades enfrentadas por eles quanto à usabilidade do protótipo. Por isso, não foram realizados esforços para obter conclusões estatísticas significativas. Como em qualquer estudo em laboratório, os participantes não estavam em seu ambiente normal e, ainda utilizaram o emulador ao invés de um dispositivo real para realizar os testes. Os participantes utilizaram o protótipo por um curto período de tempo, em média 40 minutos. Um experimento em um período de tempo prolongado pode revelar novas perspectivas sobre como os usuários interagem com as Redes Sociais Móveis e pode revelar mudanças no comportamento desses usuários quando compartilham sua localização com os seus amigos. No entanto, é possível observar que um usuário que está insatisfeito com o uso de um aplicativo nos primeiros minutos pode optar por não continuar a utilizá-lo. Isso pode ser constatado através do estudo de campo.

6.2.4 Avaliação dos Resultados

Com o intuito de facilitar a análise das respostas obtidas pelos participantes, os questionários foram elaborados com três grupos de afirmativas: o primeiro grupo tem o objetivo de medir o nível de conhecimento dos participantes na plataforma Android; o segundo grupo tem o objetivo de medir a usabilidade do protótipo e o terceiro grupo tem o objetivo de medir o sentimento de segurança dos participantes na utilização de Redes Sociais Móveis, bem como a eficácia das técnicas de privacidade oferecidas pelo protótipo. Além disso, foram inseridas sete perguntas

repetidas em ambos os questionários a fim de mensurar a percepção de segurança dos participantes antes e depois de utilizarem o protótipo.

Para uma melhor análise dos resultados e para mensurar o grau de concordância dos participantes, foi realizada uma abordagem quantitativa para estabelecer a Média Ponderada (MP) de cada item contido nos questionários utilizando a Escala de *Likert*. A Média Ponderada atribuída às respostas obtidas possibilitou a verificação da concordância ou discordância das questões. Para o cálculo da Média Ponderada foi utilizada a equação descrita a seguir, onde Si representa a quantidade de vezes que o valor da Escala de Likert foi selecionada como resposta pelos participantes e os números ordinais representam o valor atribuído a cada resposta.

$$MP = \frac{(1xS1) + (2xS2) + (3xS3) + (4xS4) + (5xS5)}{S1 + S2 + S3 + S4 + S5}$$

A equação de MP calcula o valor de cada uma das respostas multiplicando o valor da resposta na Escala de Likert pela soma de vezes que a resposta foi escolhida, dividido pela soma das vezes que o valor foi selecionado.

Sobre os resultados obtidos da média ponderada, considerou-se que os valores maiores que três são discordantes. O valor de três exato foi considerado “indiferente”, “sem opinião” ou “neutro”.

Todas as afirmativas inseridas nos questionários têm o objetivo de observar três pontos importantes: Usabilidade, sentimento de segurança e aceitação das técnicas de privacidade oferecidas.

As questões presentes no questionário 1 estão relacionadas com a percepção de segurança dos participantes e com o conhecimento dos mesmos quanto ao uso da plataforma Android. A Tabela 6.6 apresenta os valores das frequências de cada resposta e a MP para cada questões contida no questionário 1.

Tabela 6.6. Dispersão das respostas e Média Ponderada para o Questionário 1.

Perguntas	Contagem de Respostas					MP
	1	2	3	4	5	
1 - Considero importante poder configurar as permissões dos aplicativos instalados em meu dispositivo	15	35	0	0	0	1,7
2 - Considero importante conhecer como os meus dados são utilizados	23	27	0	0	0	1,5
3 - Confio na forma como os aplicativos utilizam os recursos do dispositivo	0	31	0	8	11	2,9
4 - Considero que meus dados armazenados em meu dispositivo estão seguros	0	38	0	12	0	2,4
5 - Considero seguro o uso de GPS	1	46	0	3	0	2,1
6 - Sinto-me seguro quando utilizo meu dispositivo	0	41	0	9	0	2,8

7 - Sinto-me seguro em compartilhar minha localização utilizando o meu dispositivo	10	33	0	7	0	2,8
8 - Entendo como minhas permissões são utilizadas pelos aplicativos instalados em meu dispositivo	3	17	0	15	15	3,4
9 - Entendo como funcionam os mecanismos de segurança e privacidade presentes em meu dispositivo	0	4	0	36	10	4

Fonte: Elaborado pelo autor.

Como mencionado anteriormente, as afirmativas foram agrupadas por objetivo. As afirmativas de 1 a 7 estão relacionadas ao sentimento de segurança dos participantes. O acúmulo das respostas e as afirmativas estão principalmente no valor 2 e a MP está entre 1 e 3. Dado o fato de que nenhum participante possuía o conhecimento sobre a proposta do estudo ao responder o questionário, o resultado evidência o desejo dos mesmos em segurança e privacidade no uso de dispositivos móveis. As afirmativas 8 e 9 estão relacionadas ao nível de conhecimento sobre a plataforma Android. O acúmulo das respostas estão principalmente no valor 4 e a MP está entre 3 e 4. Esse resultado indica que o nível de conhecimento da plataforma Android por parte dos participantes é mínima.

A Tabela 6.7 apresenta as respostas obtidas no questionário 2 cujo objetivos são: medir a usabilidade do protótipo, a satisfação dos participantes com relação as garantias de privacidade oferecidas e o sentimento de segurança dos mesmos em relação ao uso de dispositivos móveis e RSM. Além disso, os resultados obtidos dessa avaliação irão proporcionar o desenvolvimento de melhorias no aplicativo.

Tabela 6.7. Dispersão das respostas e Média Ponderada para o Questionário 2.

Perguntas	Contagem de Respostas					MP
	1	2	3	4	5	
1 - Considero importante poder configurar as permissões dos aplicativos instalados em meu dispositivo	50	0	0	0	0	1
2 - Considero importante conhecer como os meus dados são utilizados	46	0	0	4	0	1,2
3 - Confio na forma com que as aplicações utilizam os recursos do dispositivo	0	5	0	20	25	4,3
4 - Considero que os dados em meu dispositivo estão seguros	0	0	0	37	13	4,2
5 - Considero seguro o uso de GPS	0	0	0	17	33	4,6
6 - Sinto-me seguro quando utilizo meu dispositivo móvel	0	0	0	37	13	4,2
7 - Sinto-me seguro em compartilhar minha localização utilizando o meu dispositivo	0	0	0	32	18	4,3
8 - Pude facilmente utilizar as opções existentes no aplicativo	0	12	0	35	3	3,5
9 - Fui capaz de definir as regras de privacidade correta para os meus contatos	0	11	0	36	3	3,6
10 - Pude facilmente configurar minhas regras de privacidade	0	1	0	48	1	3,9
11 - Eu utilizaria esta rede social em meus dispositivos	22	28	0	0	0	1,5
12 - Eu considero valida a proteção oferecida a minha privacidade pelo aplicativo	49	0	0	0	1	1
13 - O aplicativo me permite alterar facilmente as regras de privacidade aplicada	0	6	0	44	0	3,7
14 - Quando uma requisição de localização de um contato é negada, a mensagem apresentada pelo aplicativo me ajuda a	0	2	0	9	39	4,7

entender perfeitamente que a minha requisição foi negada.						
15 - A forma com que a privacidade é configurada é clara.	0	5	1	43	1	3,8
16 - No geral, estou satisfeito com o aplicativo	1	49	0	0	0	1
17 - Sinto-me confortável em permitir o acesso a minha conta no Facebook	0	0	0	36	14	4,2
18 - Sinto-me seguro em utilizar redes sociais móveis em meu dispositivo	0	0	0	30	20	4,4
19 - Sinto-me seguro em compartilhar minha localização com os membros de minha rede social móvel	0	0	0	35	15	4,3
20 - O aplicativo possibilitou que, a partir de agora, prestarei mais atenção na segurança de meus dispositivos móveis, tomando mais cuidado ao instalar aplicações.	50	0	0	0	0	1
21 - O aplicativo possibilitou que, a partir de agora, prestarei mais atenção antes de compartilhar minha localização nas redes sociais e demais aplicativos.	45	5	0	0	0	1,1

Fonte: Elaborado pelo autor.

No Questionário 2, as perguntas de 8 a 16 foram inseridas para medir a usabilidade do protótipo. As respostas da maioria das questões estão acumuladas no valor 4, e o valor da MP esta entre 3 e 4. Esses valores demostram que, apesar dos participantes afirmarem que, no geral, eles estão satisfeitos com o aplicativo, como demostrado pela questão 11 e 16, o protótipo necessita de modificações e melhorias no que diz respeito à usabilidade, em especial, na forma como a privacidade é configurada, como demostra as questões 9, 13 e 16.

Um ponto importante a ser observado neste grupo de questões é que a mensagem emitida do usuário requisitante (quando o usuário requisitado nega a requisição de compartilhamento de localização) não indica e nem revela explicitamente essa negação. Este fato é muito importante, pois, garante aos usuários a privacidade da escolha e não cria atrito entre eles. A questão 14 comprova este fato, pois a maioria das respostas obtidas está acumulada no valor 4, indicando que a maioria dos participantes discorda de que a mensagem de negação seja clara.

O grupo formado pelas questões 17 a 21 tem o objetivo de medir o sentimento de segurança dos participantes em relação ao uso de Redes Sociais Móveis e compartilhamento de localização. O acúmulo das respostas às questões 17, 18 e 19 entre os valores de negação 4 e 5 e a MP calculada está no intervalo de 4 a 5. Esses valores indicam que os participantes não se sentem seguros em utilizar Redes Sociais Móveis e compartilhar a sua localização utilizando seus dispositivos móveis. Este resultado justifica o desenvolvimento deste trabalho e conclui que, para o uso de Redes Sociais Móveis, é extremamente necessário que existam garantias de privacidade, em especial no compartilhamento de localização.

O objetivo das questões 20 e 21 foi medir o impacto causado pelo estudo nos usuários. O resultado obtido foi unânime: foram despertadas nos usuários as questões de segurança e privacidade.

Os gráficos apresentados nas Figuras 6.3 e 6.4 possibilitam a visualização e análise dos resultados da MP obtidos nos dois grupos de questões inseridas no Questionário 2.

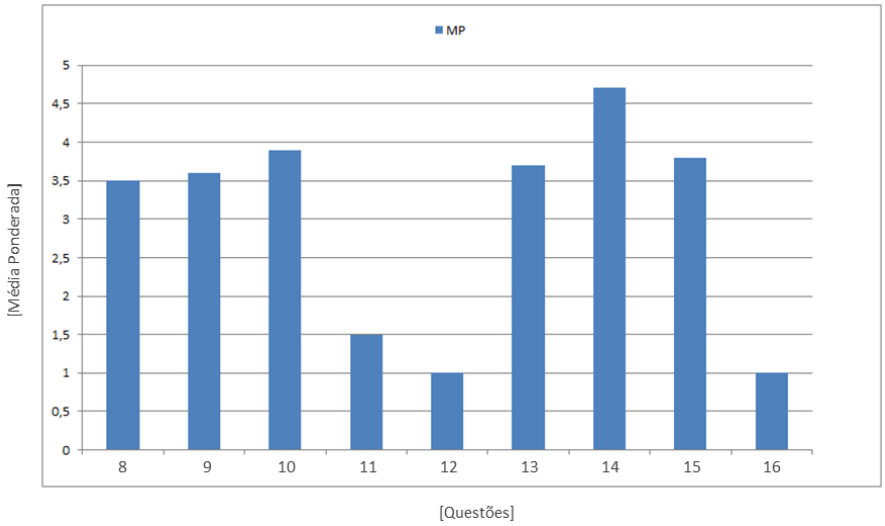

Figura 6.25. Gráfico com os valores da MP obtida para o primeiro grupo de questões do Questionário 2.

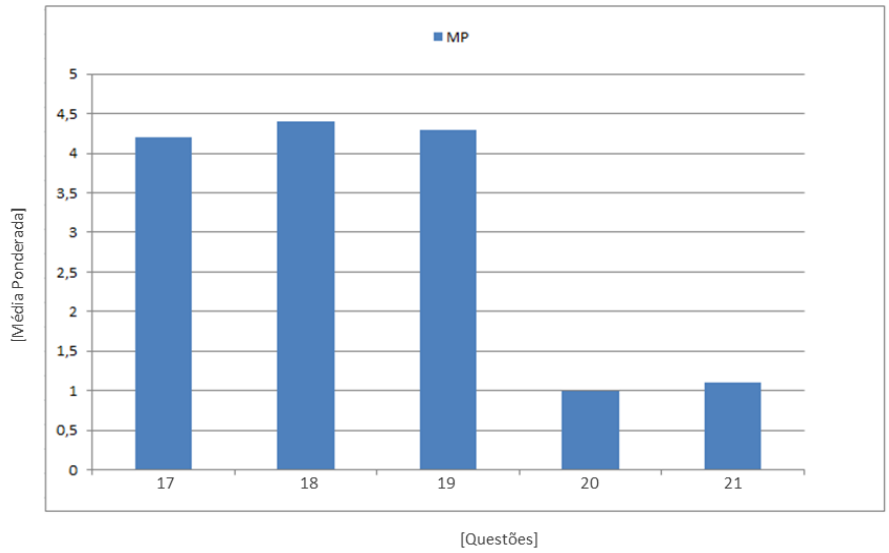

Figura 6.26. Gráfico com os valores da MP obtida para o segundo grupo de questões do Questionário 2.

Como mencionado no início desta seção, sete questões foram inseridas em ambos os questionários com o objetivo de medir a percepção de segurança dos participantes antes e depois da utilização do protótipo e da realização do

experimento. A Tabela 6.8 demonstra o acúmulo das respostas obtidas em cada questão presentes no Questionário 1 (Q1) e Questionário 2 (Q2).

Tabela 6.8. Respostas para as perguntas presentes nos dois questionários.

Pergunta		Valores				
		1	2	3	4	5
1	Q1	15	35	0	0	0
	Q2	50	0	0	0	0
2	Q1	23	27	0	0	0
	Q2	46	0	0	4	0
3	Q1	0	31	0	8	11
	Q2	0	5	0	20	25
4	Q1	0	38	0	12	0
	Q2	0	0	0	37	13
5	Q1	1	46	0	3	0
	Q2	0	0	0	17	33
6	Q1	0	41	0	9	0
	Q2	0	0	0	37	13
7	Q1	10	33	0	7	0
	Q2	0	0	0	32	18

Fonte: Elaborado pelo autor.

O gráfico ilustrado na Figura 6.5 demonstra os valores obtidos no cálculo da MP para cada questão. O objetivo é analisar o impacto causado na sensação de privacidade e de segurança após o uso do protótipo. No gráfico, a primeira barra representa a MP das questões no Questionário 1 e a segunda barra a MP das questões no Questionário 2.

O comparativo entre as MPs obtidas nas questões 1 e 2 demonstra que, antes da utilização do protótipo e da realização do teste, os participantes manifestaram a importância de configurar corretamente as permissões solicitadas pelos aplicativos e como estes manipulam seus dados.

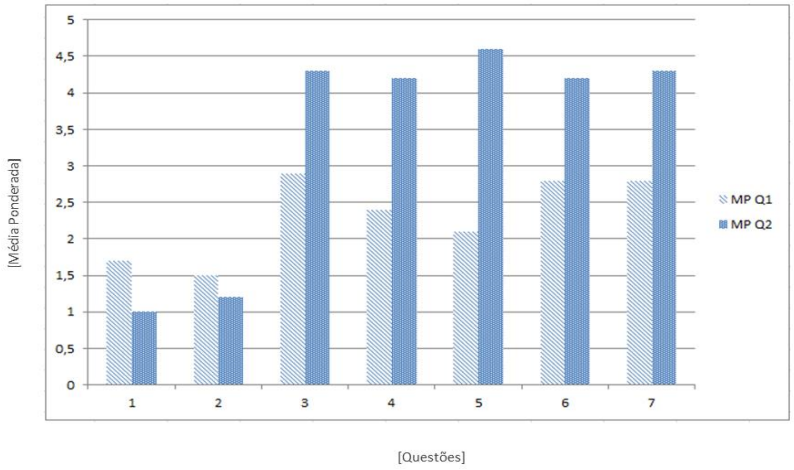

Figura 6.27. Gráfico com a MP obtida para as questões presentes em ambos os questionários.

Para as questões de 3 a 4, podemos observar que os usuários passaram a desconfiar ainda mais da forma como os aplicativos manipulam seus dados e utilizam os recursos do dispositivo, na utilização de GPS e compartilhamento de localização. O estudo despertou o interesse dos participantes em privacidade e segurança no uso de dispositivos móveis, em especial aplicativos como Redes Sociais Móveis e aplicativos que utilizam suas informações de localização para fornecer algum tipo de serviço.

6.3 Considerações finais

Os resultados obtidos nos testes de desempenho evidenciam que o modelo apresenta um bom tempo de execução, apesar da existência de atrasos. Analisando pelo pior caso, o tempo de execução do modelo para processar uma requisição recebida é, em média, de 28 segundos. Este atraso adicionado à execução da rede social é aceitável se o compararmos ao tempo médio gasto pelo GPS em obter a primeira localização, que é de 30 segundos. Os resultados dos testes também evidenciaram que os atrasos gerados pelo uso das técnicas de privacidade são proporcionais aos níveis da privacidade desejada pelo usuário.

O teste de usabilidade tem a finalidade de verificar se o software ou aplicação pode ser facilmente manipulado pelos usuários, sem dificuldades. Além disso, o

teste possibilita medir a eficácia de algoritmo e funcionalidades oferecidas. O teste de usabilidade apresentado neste capítulo tem a finalidade de avaliar as questões de uso, e, mais importante, a eficiência das técnicas de privacidade oferecidas. Como pode ser observado nos resultados obtidos, o protótipo alcançou o seu objetivo principal que é fornecer garantias de privacidade aos usuários de RSM. Porém, deverão ser realizadas melhorias na questão da usabilidade, principalmente nas opções que permitem a configuração das políticas e níveis de privacidade oferecidos. Um ponto importante a ser observado pelos resultados é que os usuários possuem uma falsa sensação de segurança e privacidade no uso de aplicativos móveis. No início das seções de testes, a maioria dos participantes possuía confiança excessiva nos aplicativos e na forma como estes manipulavam dados e recursos dos seus dispositivos. Outro ponto importante é a questão das permissões solicitadas pelos aplicativos. A maioria dos participantes não lia, ou não dava importância a tais solicitações. Os usuários concedem as permissões solicitadas, porém não conhecem a sua finalidade e nem mesmo os riscos envolvidos se a permissões forem concedidas a aplicativos maliciosos.

Capítulo 7

CAPÍTULO 7 - CONCLUSÕES E TRABALHOS FUTUROS

Atualmente, o uso constante de Redes Sociais é uma realidade que faz parte do cotidiano da sociedade. As pessoas utilizam a Rede Social como meio de manter contato e relacionamentos com seus amigos, familiares, colegas de trabalho, entre outros. Além disso, o uso de Redes Sociais permite às pessoas iniciar novos relacionamentos e formar novos círculos de amizade. Ao publicar conteúdos em uma Rede Social, tais como pensamentos, acontecimentos, fotos e vídeos, as pessoas permitem que seus contatos fiquem sempre atualizados com o que ocorre em seu cotidiano.

Por outro lado, também é possível constatar a evolução dos dispositivos móveis. Esses equipamentos que há pouco tempo possibilitavam apenas a realização de chamadas e envio de mensagens hoje estão dotados de uma série de novos recursos. Os recursos, como poder de processamento e armazenamento, múltiplas interfaces de rede, GPS e uma variedade de sensores físicos, como acelerômetro e magnetômetro, permitem a execução de aplicativos mais sofisticados. Além disso, esses dispositivos estão se tornando cada vez mais baratos. Como consequência dos novos recursos fornecidos, aliados ao preço acessível, cresce cada vez mais a popularidade dos dispositivos móveis.

As Redes Sociais Móveis surgiram devido à popularidade das Redes Sociais e dos dispositivos móveis. Os novos recursos presentes nos dispositivos permitem aos usuários acessar, publicar ou compartilhar recursos gerados ou obtidos através dos sensores, gerando informações de contexto. Dentre essas informações de contexto compartilhadas está a localização.

Ao compartilhar sua localização atual em uma Rede Social, os usuários mantêm seus amigos e familiares sempre informados de sua posição e sobre onde estiveram. Além disso, o compartilhamento desta informação possibilita o fornecimento de uma série de recursos e servidos oferecidos pela Rede Social, tais

como recomendação de novos amigos e lugares. Porém, essa informação de localização pode oferecer riscos se for obtida e utilizada por entidade e usuários maliciosos. Além de oferecer novos recursos e serviços, as RSM devem também oferecer mecanismos que ofereçam privacidade aos seus usuários.

O modelo proposto neste trabalho oferece garantias de privacidade aos usuários no compartilhamento de localização em RSM. A privacidade é oferecida através da personalização de políticas de compartilhamento e níveis com técnicas de ocultação da posição real e com alta precisão. As contribuições alcançadas neste trabalho são apresentadas a seguir.

7.1 Contribuições e Limitações

As principais contribuições deste trabalho são: a proposta e desenvolvimento de um modelo de compartilhamento de localização em RSM com garantias de privacidade e o resultado de um estudo de usabilidade realizado com 50 participantes que pode servir de referência para pesquisas futuras.

O protótipo de RSM desenvolvido com base no modelo proposto oferece garantias de privacidade sem comprometer a Rede Social e os serviços oferecidos. Os usuários personalizam suas políticas de privacidade de acordo com a necessidade. Estas permitem o compartilhamento de localização de acordo com as preferências do usuário, como horário, dias da semana, local específico e o contato. Essa permissão possibilita que a Rede Social utilize a informação de localização para oferta de produtos e serviços, bem como sugestão de novas amizades com base na área geográfica. Os níveis oferecem privacidade ocultando a localização exata e com alta precisão antes de ser compartilhada. Esta ocultação pode ou não comprometer os recursos oferecidos pela Rede Social, dependendo do coeficiente de ajuste de precisão configurado. A eficiência das técnicas de privacidade oferecidas pelo protótipo foi comprovada pelos testes de usabilidade realizados.

Os resultados obtidos nos testes de desempenho evidenciam que o modelo apresenta um bom desempenho, apesar da existência de atrasos. Analisando pelo pior caso, o tempo de execução do modelo para processar uma requisição recebida é, em media, 28 segundos. Este atraso adicionado à execução da rede social é

aceitável se compararmos ao tempo médio gasto pelo GPS em obter a primeira localização, que é 30 segundos. Os resultados dos testes também evidenciaram que os atrasos gerados pelo uso das técnicas de privacidade são proporcionais aos níveis da privacidade desejada pelo usuário.

Os resultados do estudo de usabilidade realizado com 50 participantes demonstraram, além da eficiência do protótipo, que usuários de Redes Sociais Móveis possuem sentimento equivocado ou ingênuo sobre privacidade. Eles compartilham sua localização e demais informações de contexto sem a preocupação com a segurança. Outro ponto importante é a má compreensão das finalidades das permissões solicitadas pelo sistema operacional do dispositivo. A maioria dos participantes acredita que as aplicações manipulam os dados e os recursos do dispositivo de modo seguro.

7.2 Trabalhos Futuros

O modelo garante a privacidade das informações de localização de seus usuários em uma rede social móvel através de técnicas que ocultam a posição real. Essa ocultação, na maioria das vezes, é realizada através do deslocamento da posição real para qualquer ponto dentro de uma área. Porém, o modelo não garante que a nova posição definida seja válida, por exemplo: que a nova localização não seja dentro do mar. Para que a nova posição gerada seja validada será necessária a realização de um *marshup* com algum aplicativo de mapas, o GoogleMaps, por exemplo (Google Maps 2015).

Outro ponto importante do modelo é a oferta de privacidade no caminho realizado pelo usuário. Este caminho é obtido através do histórico das localizações compartilhadas. Todos os níveis oferecidos pelo modelo garantem a privacidade do caminho realizado pelo usuário. Entretanto, será necessário um estudo para analisar se o caminho obtido através do histórico das localizações ocultadas possibilita chegar ao ponto final do usuário. Ou seja, se for feito o *marshup* dos pontos compartilhados, será que outro usuário mal-intencionado não conseguirá chegar ao ponto final onde o usuário se encontra, mesmo se o caminho real ocultado? Com

base no resultado deste estudo, será necessário ou não realizar uma otimização nos algoritmos de ofuscação de localização.

As regras possibilitam que os usuários configurem parâmetros que fornecem privacidade no compartilhamento de localização em determinadas situações. Isso permite que os usuários ainda aproveitem dos recursos de socializações. Porém, quanto maior o número de regras definidas pelo usuário pior será o desempenho da aplicação. Este problema terá que ser resolvido no futuro. Uma das possibilidades será criar um mecanismo mais eficiente de análise de regras. Uma alternativa de implementação deste mecanismo é utilizando uma estrutura de dados árvore.

Além dos trabalhos citados anteriormente, ainda destacam-se: o desenvolvimento de uma Rede Social Móvel com funcionalidade e opções semelhantes a uma Rede Social Móvel como, por exemplo, o Facebook, e analisar o impacto da privacidade; evoluir os algoritmos que realizam o anonimato a fim de otimizar o tempo de execução; a realização de estudos para detectar os conflitos e dificuldades dos usuários em definir políticas de privacidade; pesquisar e desenvolver técnicas de privacidade para outros tipos de informações de contexto compartilhadas na RSM e implementar novas técnicas que garantem a privacidade no compartilhamento de informações de localização.

REFERÊNCIAS

APACHE Software Foundation. Disponível em: http://www.apache.org. Data do ultimo acesso: 01/07/2014

Ardagna CA et al. Privacy-enhanced location services information. In: Digital privacy: theory, technologies and practices. Auerbach Publications (Taylor and Francis Group); 2007. p. 307-326.

Baldauf M. et al. A survey on context-aware systems. In: International journal of ad hoc and ubiquitous computing. 2007; 2(4):263-77.

Benisch M et al. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. In: Personal and ubiquitous computing. 2011; 15:679-94.

Bilogrevic I et al. Adaptive information-sharing for privacy-aware mobile social networks. In: ACM international joint conference on pervasive and ubiquitous computing; 2013. p. 657-66.

Day M et al. Instant messaging / presence protocol requirements. RFC 2779.

Dey AK. Understanding and using context. Personal and ubiquitous computing. 2001; 5(1):4-7.

Dong W et al. Secure friend discovery in mobile social networks. In Proceedings of 30th IEEE international conference on computer communications, Infocom'11; 2011. IEEE Computer Society; 2011. p. 1647-55.

Facebook analytics. [Citado 2014 dez 15]. Disponivel em: https://developers.facebook.com/docs/analytics

Gao H et al. Security issues in online social networks. In: IEEE internet computing. 2011; 15(4):56-63.

Holzinger A. Usability engineering methods for software developers. Communications of the ACM; 48(1):71-4; 2005. [Citado 2012 abr 22].

Hughes E. A cypherpunk's manifesto. 1993. [Citado 2014 nov 1]. Disponível em: http://www.activism.net/cypherpunk/manifesto.html

Kayastha N et al. Applications, architectures and protocol design issues for mobile social networks: a survey. Proceedings of the IEEE; 2011.

Leon P et al. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In: SIGCHI conference on human factors in computing systems; 2012; New York: p. 589-98. .

Lewis JR. Handbook of human factors and ergonomics. John Wiley & Sons, Inc., 2006, ch. 49: usability testing. p. 1275-1316.

Ling RS. New tech, new ties: how mobile communication is reshaping social cohesion. MIT Press; 2008.

Lubke R et al. Mobilis groups: location-based group formation in mobile social networks. In: Proceedings of the 9th annual IEEE international conference on pervasive computing and communications, workshop proceedings, PerCom'11; 2011. Seattle; IEEE; 2011. p. 502-7.

MYSQL. [Citado 2014 ago 10]. Disponível em: http://www.mysql.com

Ribeiro FN, Zorzo SD. LPBS - Location privacy based system. In: IEEE symposium on computers and communications; 2009. p. 374-9.

Schiller J, Voisard A. Location-based services. In: Elsevier Morgan Kaufann Publishers; 2004.

Schuster D et al. Pervasive social context - taxonomy and survey. In: ACM transactions on intelligent systems and technology. 2012; 9(4):1-22.

Smart SW. TextBook on spherical astronomy. 6th. ed. England: Cambridge University Press, 1977. 415 p.

Smith I et al. Social disclosure of place: from location technology to communication practices. In: Third international conference on pervasive computing; 2005. p. 134-51.

Teles AS. Redes sociais móveis: conceitos, aplicações e aspectos de segurança e privacidade. In: 31º Simpósio brasileiro de redes de computadores e sistemas distribuídos - SBRC, cap. 2; 2013. p. 52-100.

The statistics portal. [Citado 2014 jul 10]. Disponível em: http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Toch E et al. Empirical models of privacy in location sharing. In: 12th ACM international conference on ubiquitous computing; 2010. p. 129-38.

Toch E et al. Locaccino: a privacy-centric location sharing application. In: 12th ACM international conference adjunct papers on ubiquitous computing; 2010. p. 381-82.

Wasserman S, Faust K. Structural analysis in the social sciences. Cambridge University Press, 1994.

Weiser M.The computer for the 21st century. Scientific American. 1991; 265(3):66-75.

Williams, E. Aviation formulary 1.44. [Citado 2014 abr 4]. Disponível em: http://williams.best.vwh.net/avform.htm#LL

Zend Framework. [Citado 2014 jul 10]. Disponível em: http://framework.zend.com

Zhang C et al. Privacy and security for online social networks: challenges and opportunities. IEEE Network. 2010; 24(4):13-8.