Uma Estratégia para Gerenciar o Compartilhamento de Recursos entre Dispositivos Moveis

A Strategy for Managing Resource Sharing Between Mobile Devices

DOI: 10.46814/lajdv3n2-024

Recebimento dos originais: 23/12/2020
Aceitação para publicação: 31/02/2021

Tiago H. Bono
Departamento de Informática - Universidade Estadual de Maringá (UEM)
Avenida Colombo, 5790 – 87020-900 – Maringá – PR – Brazil
E-mail: thbono@gmail.com

Luciana A. F. Martimiano
Departamento de Informática - Universidade Estadual de Maringá (UEM)
Avenida Colombo, 5790 – 87020-900 – Maringá – PR – Brazil
E-mail: luciana@din.uem.br

RESUMO
A intensificação do uso das redes sem fio tem elevado a quantidade de recursos que podem ser compartilhados entre os dispositivos móveis e, consequentemente, provocado um aumento do consumo dos recursos desses dispositivos. Assim, torna-se importante desenvolver uma estratégia que defina quais recursos devem ser compartilhados entre os usuários, considerando restrições de acesso às informações confidenciais e à capacidade do dispositivo, mantendo-o disponível para o usuário. Uma solução proposta para este cenário é a ontologia denominada PrOHand (Privacy Ontology for Handovers). Este artigo descreve a PrOHand, seu sistema de reputação e a aplicação desenvolvida para validar suas regras.

ABSTRACT
The use of wireless networks has increased the amount of resources that can be shared amongst mobile devices and consequently caused an incre- ase in consumption of these devices. Thus, it becomes important to develop a strategy that defines which resources can be shared among users (devices), considering restrictions on access to confidential information and on devices capacities, keeping it available to the user. One proposed solution for this sce- nario is the ontology named PrOHand (Privacy Ontology for Handovers). This paper describes PrOHand, its reputation system and the application developed to validate its rules.

1 INTRODUÇÃO

Diversos fatores têm influenciado na intensificação do uso das redes sem fio. Dentre esses fatores podemos citar o aumento da área de abrangência e da velocidade de transmissão dessas redes. Adendo ao crescimento do número de usuários, esta á expansão dos tipos de mídias transmitidas entre os dispositivos móveis diretamente.

Torna-se então interessante desenvolver uma estratégia que possibilite a esses dispositivos selecionar os recursos e serviços (como cache de Web, sinal WiFi, lista de contatos, entre outros) que

podem ser compartilhados entre seus usuários. Com tal estratégia, seria possível filtrar as informações trocadas, e estabelecer padrões de segurança com o intuito de bloquear o acesso e a manipulação de informações confidenciais por meio de ataques de intrusos na rede.

Uma proposta de estratégia foi desenvolvida por [Gonçalves 2008] e é denominada PrOHand (Privacy Ontology for Handovers). A PrOHand é uma ontologia de privacidade que propõe o estabelecimento de níveis de confiança entre os dispositivos móveis por meio do armazenamento e compartilhamento de informações de privacidade entre os usuários. A ontologia foi criada para gerenciar o compartilhamento de recursos que são disponibilizados de acordo com o n´nível de confiança que um usuário tem com relação a outro em uma rede ad-hoç na qual a comunicação entre os dispositivos é efetuada de maneira direta, ou seja, sem a necessidade de uma estação base (rede infraestruturada).

Para validar as regras da PrOHand, uma aplicação foi desenvolvida e testada.

Nessa aplicação é possível simular o compartilhamento de recursos e serviços entre usuários de dispositivos móveis a partir dos n´níveis de confiança previamente definidos pelo usuário para o acesso ou uso do recurso.

Este artigo está organizado da seguinte forma: a Seção II descreve a ontologia PrOHand; a Seção III descreve a aplicação desenvolvida; a Seção IV apresenta os resultados alcançados; e a Seção V apresenta as considerações finais e os trabalhos futuros.

2 A ONTOLOGIA PROHAND

Segundo [Misztal 1996], confiança é um grau subjetivo de crença sobre determinados agentes. O nível de confiança que se tem sobre uma pessoa reflete o quão bem- intencionada esta pessoa é julgada. Segundo [Gambetta 2000], quando confia-se em uma pessoa, pressupõe-se muito provavelmente que ela efetuará ações benéficas, ou pelo menos não prejudiciais, de forma que uma cooperação seja possível. Para o meio virtual, as definições de confiança tradicionais podem ser traduzidas por meio do desenvolvimento de um modelo de confiança que regulamente as relações de confiabilidade neste meio.

De acordo com [Westin 1967], privacidade é “a necessidade que indivíduos, grupos ou instituições possuem em determinar por si próprios, com quem, quando, e como compartilhar informações no sistema nos quais atuam”.

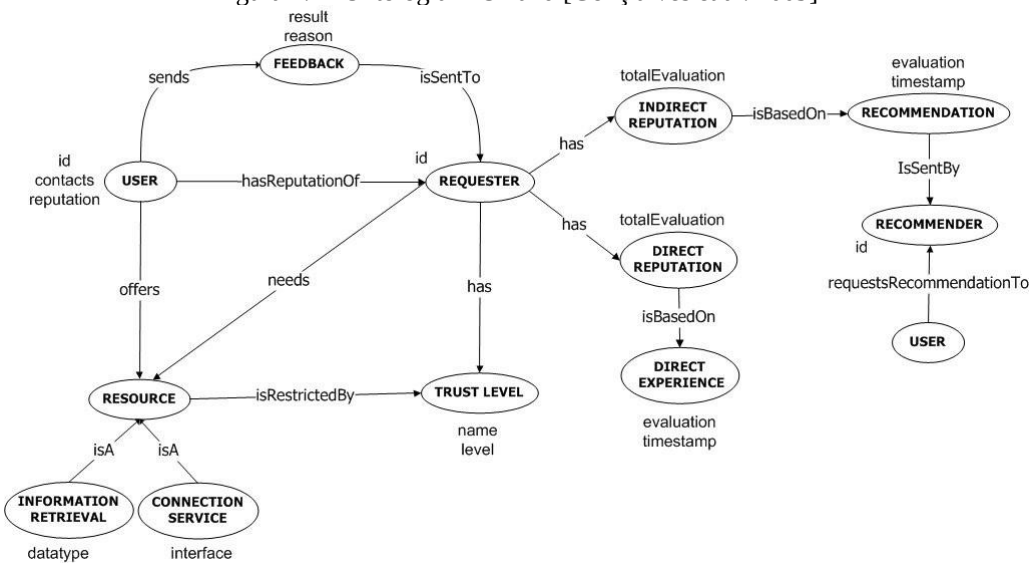
A PrOHand, ilustrada na Figura 1, fornece um mecanismo para controlar o compartilhamento de recursos e serviços entre dispositivos móveis em redes ad-hoc. O acesso a algum destes recursos e/ou serviços de um dispositivo é permitido somente mediante certo nível de confiança.

O nível de confiança entre os dispositivos (ou usuários) é calculado segundo um sistema de reputação, e pode variar de pouco confiável a muito confiável. As reputações utilizadas para o cálculo são a direta (direct reputation) e a indireta (indirect reputation). A reputação direta é baseada no histórico de conexões diretas com o dispositivo solicitante, ou seja, de experiências passadas. A reputação indireta é obtida a partir de terceiros que já tiveram experiências diretas com o solicitante, e atuam como recomendantes sobre o mesmo.

Na PrOHand são definidos três atores: user, requester e recommender. O reques- ter tem intenção de solicitar acesso a algum recurso disponibilizado pelo user. Para isso, o user deve verificar o nível de confiança, ou trust level, do requester. Caso este nível es- teja de acordo com o valor pré-estabelecido pelo user, o requester terá acesso ao recurso. Caso haja um recommender, as suas recomendações também são utilizadas para definir o nível de confiança do requester [Gonçalves et al. 2009].

Os usuários são capazes de se comunicar sem uma infraestrutura de rede tradicional. Esta comunicação é possível devido aos encontros oportunísticos (ou haggle [Su et al. 2007]), típicos de redes móveis. Nesses encontros os usuários podem com- partilhar informações e serviços, justificando o caráter colaborativo em acordos usuário para acessar o recurso. Esse nível, definido pelo usuário. Esse compartilhamento se dá por meio do tráfego de dados entre dispositivos vi- zinhos. Se tal compartilhamento for ilimitado, há um espaço de atuação para dispositivos causadores de incidentes maliciosos. Há também a possiblidade de inundar o dispositivo, incapacitando-o de efetuar tarefas essenciais do usuário.

Figura 1. A Ontologia PrOHand [Gonç alves et al. 2009]



A PrOHand, considerando este cenário, permite ao usuário manter níveis de controle sobre seus recursos. Esse controle é gerenciado com base no modo como ele e seus contatos confiam no requisitante do recurso. Para tal, é utilizado um sistema de reputação entre usuários baseado no sistema proposto por [Abdul-Rahman and Hailes 2000].

Em um cenário de sistema colaborativo, um usuário pode efetuar requisições por recursos a outro usuário. O usuário que recebeu a requisição pode optar por aceitá-la ou rejeitá-la, de acordo com o nível de confiança necessário detentor do recurso, é confrontado com nível de confiança que o requisitante possui. Se tal nível for suficiente, a requisição é atendida, caso contrário, um feedback negativo é enviado ao requisitante.

Esse nível de confiança sobre um dispositivo, ao contrário do nível de confiança necessário para acessar determinado recurso que é definido previamente, é calculado dinamicamente. Tendo como exemplo os usuários A (user) e B (requester), o nível de confiança que A mantém sobre B é baseado na reputação de B no sistema. A reputação de B é formada por sua reputação direta e também por sua reputação indireta. A reputação direta é definida pelo histórico de experiências diretas, chamadas de comunicações, que A já teve com B. A reputação indireta é definida por opiniões, chamadas de recomendações, de outros usuários sobre B. As informações necessárias para o cálculo da reputação e da reputação em si são armazenadas pelo user.

Os recursos do usuário A podem ser associados a um determinado nível de confiança (Trust Level), com base na importância que cada recurso representa para ele. Aspectos como confidencialidade e disponibilidade são considerados para determinar o nível de confiança de cada recurso. A confidencialidade se refere à proteção de informações confidenciais (como dados pessoais) e a disponibilidade se refere à manutenção da operabilidade do dispositivo (como banda de conexão).

A PrOHand prevê cinco níveis de confiança: Very Untrustworthy, Untrustworthy, No Opinion, Trustworthy, Very Trustworthy (definidas de acordo com o trabalho de [Abdul-Rahman and Hailes 2000]). Cada recurso disponibilizado pelo dispositivo pode ter seu nível configurado pelo usuário, ficando disponível somente para requisitantes de nível de confiança compatível. Por exemplo, o usuário pode configurar sua lista de contatos como um recurso de categoria Very Trustworthy, seu cache de navegação Web como Trustworthy, e assim por diante. Assim, somente usuários classificados com no mínimo estes níveis poderão acessar o recurso.

Com os valores das reputações direta e indireta, é possível calcular o valor final da reputação. Esse valor determinará o nível de confiança que, por sua vez, determinará se o recurso poderá ser acessado pelo requisitante. Seguindo a ordem semântica das categorias de confiança, se a confiança calculada for maior ou igual à definida pelo detentor do recurso solicitado, o acesso será permitido.

Ao final da comunicação, ambos os usuários adicionam uma nova entrada no histórico de interações, de modo que possam calcular a reputação direta e enviar recomendações sobre o outro. Este processo ocorre mesmo que o acesso não seja permitido, pois um feedback é enviado.

3 O SISTEMA DE REPUTAÇÃO

De acordo com [Yu et al. 2004], sistemas de reputação são mecanismos que permitem a usuários (peers) avaliar comportamentos alheios sem a necessidade de acesso a uma entidade terceira centralizada. Cada integrante do sistema incorpora conhecimentos de outras pessoas que, juntos, produzem um novo conhecimento.

O acesso às entidades terceiras é de fato muito mais simples do que a abordagem de se calcular periodicamente reputações. Porém, com as informações sobre o comporta- mento dos usuários armazenadas de forma distribuída, a disponibilidade de um conteúdo altamente dinâmico é garantida. O dinamismo do conhecimento do sistema reflete a atualização do mesmo a cada interação entre os integrantes.

A reputação direta de um peer Pj do ponto de vista do peer Pi é calculada utili- zando a Equação 1.

$$RP(Pi, Pj) = \begin{cases} \dfrac{\sum_{k=1}^{h} e_{ij}^{k}}{h} & h \neq 0 \\ 0 & h = 0 \end{cases} \qquad (1)$$

Nesta equação, $e_{ij}^{k} \in [0, 2]$ representa o valor da k-ésima experiência direta mais recente de Pi com Pj e h é o nu´mero de entradas consideradas. A equação corresponde a uma média simples que, apesar de pouco robusta, não apresenta complexidade elevada. Esse é um fator importante considerando o uso da mesma em operações frequentes e em dispositivos móveis de processamento limitado.

A reputação indireta de um peer **P*j*** do ponto de vista do peer **P*i*** é calculada utilizando a Equação 2.

$$RI(Pi, Pj) = \begin{cases} \dfrac{\sum_{k=1}^{L} Rep(Pi,Pk) \cdot Rep(Pk,Pj) \cdot \alpha(Ti,Tk)}{L} & L \neq 0 \\ 0 & L = 0 \end{cases} \qquad (2)$$

Nesta equação, L é o nu´mero de recomendações, Rep(Pi, Pk) a reputação, do ponto de vista de Pi, do usuário Pk que enviou a recomendação e Rep(Pk, Pj) a recomendação em si, ou seja, a reputação de Pk sobre Pj. Observando a equação, percebe-se que as recomendações sobre o requisitante são ponderadas de acordo com o nível de confiança do usuário sobre quem as envia.

O tempo em que cada recomendação foi atualizada pela última vez é ponderado pelo termo α(Ti, Tk). A adição desse fator permite obter resultados mais próximos à realidade do sistema em questão. O termo é descrito na Equação 3.

$$\alpha(Ta, Tb) = \frac{1}{\frac{(Ta-Tb)}{\mu} + 1} \qquad (3)$$

Nesta equação, Ta é o tempo atual no dispositivo do requisitado, Tb o tempo no qual a recomendação foi atualizada pela última vez, e μ uma constante que representa o fator de decaimento para as recomendações.

Com os valores das reputações parciais, é possível calcular o valor de reputação de Pj do ponto de vista de Pi, pela Equação 4.

$$\text{Rep}(Pi, Pj) = \theta \cdot \text{RD}(Pi, Pj) + (1 - \theta) \cdot \text{RI}(Pi, Pj) \qquad (4)$$

Nesta equação, $\theta \in [0, 1]$ é uma constante que indica a importância da reputação direta sobre a indireta.

Mapeando os intervalos de confiança, têm-se que:

Pj será mapeado para Very Untrustworthy ↔ Rep(Pi, Pj) ∈ [0.0, 0.4)

Pj será mapeado para Untrustworthy ↔ Rep(Pi, Pj) ∈ [0.4, 0.8)

Pj será mapeado para No Opinion ↔ Rep(Pi, Pj) ∈ [0.8, 1.2)

Pj será mapeado para Trustworthy ↔ Rep(Pi, Pj) ∈ [1.2, 1.6)

Pj será mapeado para Very Trustworthy ↔ Rep(Pi, Pj) ∈ [1.6, 2.0]

4 DESENVOLVIMENTO DA APLICAÇÃO

A implementação das regras da PrOHand em um aplicativo para dispositivos móveis, denominado PrOHand Manager, foi realizada utilizando a tecnologia J2ME, com o desenvolvimento de uma MIDLet gráfica. Essa tecnologia provê uma portabilidade entre diversos dispositivos, através do conceito de máquina virtual. Disponibiliza também uma API (Application Programming Interfaces)

de comunicação que provê o estabelecimento de comunicação em rede de forma independentemente do protocolo. O kit de desenvolvi- mento utilizado foi o Java Wireless Toolkit 2.5.2, da Sun Microsystems [Muchow 2006]. Este software disponibiliza a API J2ME, o compilador, a KVM, e outras ferramentas como emuladores de execução em dispositivos de recursos limitados. As versões da API utilizadas foram CLDC 1.1 e MIDP 1.0.

4.1 O MODELO DE CONEXÃO

A conexão entre os dispositivos ocorre por meio do tráfego de dados em uma rede sem fio, através do uso de sockets. É utilizado um protocolo próprio de envio e recebimento de informações de sequências de caracteres. Caracteres especiais são utilizados como forma de separação semântica dos dados.

Cada dispositivo é identificado na rede por meio de seu hostname, necessário para estar presente na rede. O ideal é utilizar uma identificação única, o número IMEI dos dis- positivos móveis. O número IMEI é fornecido pelo fabricante do hardware do aparelho, sendo u´nico pois é dividido em faixas entre fabricantes distintos. Porém, por questões de segurança, a plataforma J2ME não provê acesso à essa identificação do aparelho.

A tecnologia J2ME, na versão 1.0 da API MIDP, impõe outra restrição para a implementação do aplicativo de acordo com o planejado, não permitindo que os dispositivos atuem como servidores de socket, mas somente como clientes. Essa limitação impede a utilização do modelo de conexão ad-hoç pois um dispositivo não é capaz de fazer requisições diretamente para outro. Para contornar esse problema, foi criado um aplicativo que intermedia as conexões entre os dispositivos. Cada dispositivo realiza requisições para esse aplicativo, chamado de PrOHand Access Point, e também consulta as requisições pendentes para ele.

Como ao final deste trabalho de graduação em 2011 não foi possível superar essa limitação por falta de tempo, o aluno que está continuando o trabalho em 2012 já está trabalhando na solução.

4.2 O MODELO DE EXECUÇÃO

Todos as requisições que o dispositivo envia, e também o tratamento e resposta para as requisições que recebe, via consulta ao PrOHand Access Point, são executadas em threads separadas. Esse modelo foi adotado visando a permitir que o usuário manipule a interface gráfica do aplicativo enquanto este efetua as operações referentes à regras da PrOHand.comunicação e às Outra razão para o uso desse modelo é a separação da interface gráfica destas operações essenciais, permitindo evoluir o aplicativo para um software do tipo daemon. Atualmente o usuário necessita cadastrar os recursos, cujo conteúdo deve ser em formato texto, e também efetuar as requisições por recursos de

outros dispositivos. Um aplicativo daemon poderia receber comandos de outros aplicativos solicitando os recursos, e o conteúdo dos mesmos poderia estar em formato binário, por exemplo, arquivos. Outra vantagem seria permitir que o usuário utilize outros aplicativos no dispositivo enquanto o gerenciador de recursos permanece em execução.

4.3 A IMPLEMENTAÇÃO

A ontologia PrOHand não foi implementada em sua totalidade. As requisições por recursos e por recomendações foram implementadas, bem como seus respectivos cálculos e respostas ao dispositivo solicitante. Além disso, a estrutura de dados criada contém todas as informações necessárias para o cálculo do nível de confiança, e o modelo de conexões contempla as operações de comunicação. Porém, durante o cálculo da reputação do dispositivo que solicita um recurso, as recomendações não estão sendo solicitadas, assim, o cálculo do nível de confiança considera apenas a reputação direta. O mecanismo que solicita as recomendações e aguarda pelas respostas para então calcular a reputação de modo completo já está em fase de implementação.

A PrOHand provê as equações para o cálculo do nível de confiança com base no histórico de interações entre os mesmos. Porém, a ontologia não contempla uma política que defina a forma como a confiança aumenta e/ou diminui ao longo do tempo. Na aplicação, quando uma requisição é bem sucedida, ou seja, a reputação do dispositivo solicitante é maior ou igual ao nível de confiança necessário para acessar o recurso soli- citado, o nível de confiança no dispositivo solicitante aumenta em 0.2 para o dispositivo detentor do recurso. Foi adotado um modelo no qual em nenhum momento o nível de confiança em um dispositivo é reduzido, pois em requisições não atentidas, por exemplo, quando o nível de confiança não é suficiente e/ou o recurso não existe, a reputação permanece inalterada. Esse foi modelo foi adotado com o propósito de simplificar os testes da aplicação, não se caracterizando como uma limitação da ontologia ou da aplicação, mas sim uma decisão de projeto.

4.4 A APLICAÇÃO EXEMPLO

A aplicação exemplo desenvolvida tem os seguintes objetivos: 1) demonstrar o uso do aplicativo móvel; e 2) validar as regras da PrOHand, por exemplo, se o aplicativo somente libera o recurso solicitado para o dispositivo solicitante se o nível de confiança calculado do mesmo for igual ou superior ao nível de confiança requerido pelo recurso.

Para a execução do teste, foi utilizado um dos emuladores disponibilizados pelo kit de desenvolvimento, que emula um telefone celular sem o recurso de toque na tela. Para utilizar o PrOHand Manager, é necessário instalar o software em um dispositivo compatível com as versões

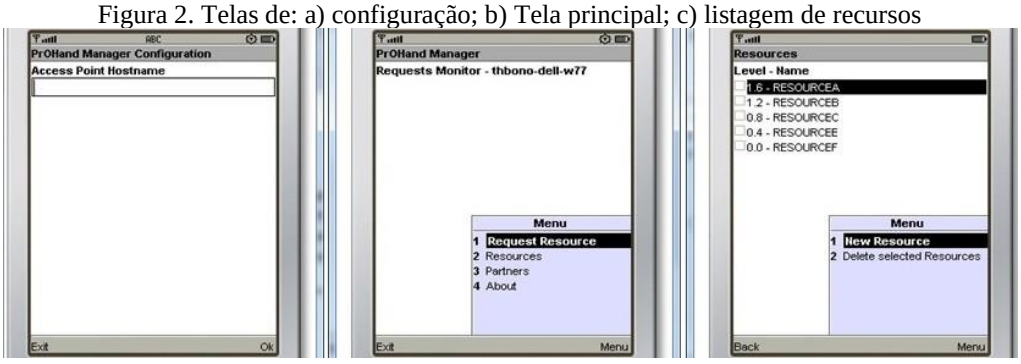
da API J2ME utilizadas no desenvolvimento (CLDC 1.1 e MIDP 1.0), através dos arquivos PrOHandJ2ME.jad (Java Application Descriptor) e PrOHandJ2ME.jar (Java Archive).

A execução do aplicativo se inicia com o carregamento dos dados necessários, seguido da exibição da tela de configuração, conforme a Figura 2a. Nesta tela é necessário informar o endereço (hostname ou IP) da máquina na qual o PrOHand Access Point está sendo executado. Para que o aplicativo funcione, o dispositivo móvel deve possuir uma conexão de rede local e/ou Internet passível de acessar esta máquina. A seguir, o aplica- tivo exibe a tela principal (Figura 2b), de monitoramento das requisições realizadas e/ou solicitadas. Nesta tela é exibida a opção para encerrar o aplicativo, e também o menu principal. No topo da tela, abaixo do título do aplicativo, é exibida a identificação do dispositivo, logo após a frase Requests Monitor.

Para que o dispositivo possa disponibilizar recursos, é necessário previamente cadastrá-los. A lista dos recursos cadastrados é acessada pela opção de menu Resources. Nesta tela (Figura 2c), são exibidos os recursos com seus respectivos níveis de confiança necessários para acesso, uma opção para voltar à tela principal, e um menu de operações.

Para inserir um novo recurso, existe a opção de menu New Resource, que abre a tela para preenchimento das informações do recurso (Figura 3a). O usuário deve indicar o nome do recurso, seu conteúdo, e o nível de confiança que o dispositivo deve ter no dispositivo solicitante para liberar seu acesso. Existem as opções para voltar para a tela anterior, e confirmar a inclusão do recurso. Ao confirmar, os dados são validados, e se houver algum valor inconsistente, uma mensagem de aviso é exibida. Se a inserção ocorrer de modo satisfatório, uma mensagem de informação precede o retorno para a tela anterior.

Figura 2. Telas de: a) configuração; b) Tela principal; c) listagem de recursos



A opção de menu Request Resource da tela principal abre a tela (Figura 3b) para que o usuário possa solicitar um recurso a outro dispositivo, indicando o nome do recurso e o nome do dispositivo detentor do mesmo. São disponibilizadas as opções de voltar para a tela anterior e confirmar a requisição.

Figura 3. Telas para: a) inclusão de recurso; b) requisição de recurso

Ao confirmar a requisição, os dados são validados, e se houver algum valor inconsistente, uma mensagem de aviso é exibida. Se a requisição for enviada, é exibida uma mensagem indicando ao usuário que acompanhe o andamento da requisição no monitor

na tela principal, tendo em vista que a requisição é requisição, e em outra conexão consulta sua resposta. Assíncrona. O dispositivo envia a Ao solicitar um novo recurso, a requisição é exibida no monitor do dispositivo, indicando seu ID (único na rede), o dispositivo solicitado e o nome do recurso solicitado.

No monitor do dispositivo solicitado, é exibida a requisição, composta por seu ID, o dispositivo solicitante e o nome do recurso solicitado. O dispositivo solicitado calcula a reputação do dispositivo solicitante de acordo com a PrOHand, e pode responder: i) recurso não foi encontrado; ii) recurso está indisponível, pois o dispositivo solicitante não possui nível de confiança necessário; e iii) conteúdo do recurso solicitado.

Quando a requisição é satisfatória, as informações do dispositivo solicitante são atualizadas no dispositivo solicitado. Se o mesmo não estiver na base de dados, é incluído, caso contrário, seu nível de confiança é incrementado.

5 RESULTADOS

Com este trabalho obteve-se o desenvolvimento de uma aplicação base para a construção de um software funcional com o objetivo de gerenciar o compartilhamento de recur- sos entre dispositivos móveis. O aplicativo implementado, em versão inicial, requer a manipulação do usuário para efetuar a troca de recursos cadastrados pelo próprio usuário, cujo conteu´do está em formato texto. Para que o usuário possa utilizar o dispositivo para outros fin enquanto a aplicação está em execução, esta deve

ser evoluído para um modelo de execução do tipo daemon. Não havendo a intervenção do usuário para manipular os re- cursos, é possível também que os mesmos possuam conteu´do em formato binário, prove- niente de outros aplicativos. Para facilitar essa evolução, a arquitetura da implementação criada provê uma separação entre a interface gráfica e os algoritmos essenciais, como o de comunicação, que implementa a PrOHand, e o do gerenciamento das threads.

A partir do aplicativo desenvolvido, foram efetuados testes visando a comprovar a eficácia da PrOHand quanto ao controle dos recursos. Foi elaborado um plano de testes, com a utilização de recursos de diferentes níveis de confiança exigidos. O aplicativo se comportou de maneira satisfatória segundo as regras da ontologia, de modo que os recursos tiveram seu repudio garantido até que o nível de confiança do requerente atingisse o valor necessário. A progressão da confiança ocorreu conforme o planejado, por meio das interações bem sucedidas. Por exemplo, para acessar um recurso cujo nível de confiança exigido era 0.4, um dispositivo não o pôde fazer sem antes interagir satisfatoriamente com o dispositivo detentor do recurso, aumentando assim sua reputação.

Durante o desenvolvimento do aplicativo, algumas limitações foram impostas pela tecnologia J2ME utilizada. Uma dessas limitações impede a obtenção do número IMEI dos dispositivos, inicialmente planejado para ser utilizado como forma de identicação, porém, foi utilizado o hostname para esse fim, tendo em vista que os dispositivos devem estar conectados a uma rede para a execução do aplicativo. Outra limitação, esta mais grave, impede que os dispositivos atuem como servidores de requisições, acarretando na necessidade da criação de um aplicativo que atue como intermediador das conexões. Sendo assim, a aplicação ainda não utiliza o modelo ad-hoc de fato. Para eliminar essa limitação, é necessário migrar a aplicação para a versão 2.0 da API MIDP, que possibilita a criação de servidores socket. A aplicação também precisa evoluir para utilizar as recomendações no cálculo da reputação

Com relação à PrOHand, ainda é preciso modificá-la para que ela possa representar regras de segurança, e uma política de aumento e redução do nível de confiança.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Em uma rede composta por dispositivos móveis, é interessante estabelecer uma estratégia que defina o nível de informações que podem ser trocadas entre os mesmos, visando a bloquear o acesso a informações confidenciais e manter a disponibilidade dos dispositivos. Este trabalho faz uso da PrOHand como modelo de privacidade, que propõe o estabelecimento de níveis de confiança entre os dispositivos através do armazenamento e compartilhamento de informações de privacidade entre os usuários.

Com o trabalho já realizado, parte da ontologia PrOHand foi implementada considerando as restrições do ambiente móvel, que são limitação de banda, memória e pro- cessamento. Atualmente, um outro aluno de graduação está desenvolvendo o trabalho e pretende sanar as limitações discutidas neste artigo, bem como evoluir a ontologia para que ela possa representar outros termos relacionados ao domínio em questão.

REFERÊNCIAS

Abdul-Rahman, A. and Hailes, S. (2000). Supporting trust in virtual communities. In Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS), pages 6007–, Washington, DÇ USA. IEEE Computer Society.

Gambetta, D. (2000). Can We Trust Trust. Trust: Making and Breaking Cooperative Relations, chapter 13, pages 213–237. University of Oxford Press, New York, NY.

Gonçalves, M. R. P. (2008). Uso de ontologias para apoiar o gerenciamento de privacidade e segurança durante handovers em ngn (next generation networks. Technical report, Instituto de Ciências Matemáticas e de Computação - Universidade de São Paulo, São Carlos, SP.

Gonçalves, M. R. P., Moreira, E. S., and Martimiano, L. A. F. (2009). Trust and privacy: informal ways to assess risk on opportunistic exchanges. International Journal of Computer Science and Applications, 6(2):66–85.

Misztal, B. A. (1996). Trust in Modern Societies: The Search for the Bases of Social Order. Polity Press, Cambridge MA, second edition.

Muchow, J. W. (2006). Core J2ME Tecnologia e MIDP. Sun Microsystems Press.

Su, J., Scott, J., Hui, P., Crowcroft, J., Lara, E. D., Diot, C., Goel, A., Lim, M. H., and Upton, E. (2007). Haggle: seamless networking for mobile applications. In Procee- dings of the 9th International Conference on Ubiquitous Computing, pages 391–408, Berlin, Heidelberg. Springer-Verlag.

Westin, A. (1967). Privacy and Freedom. Atheneum, New York.

Yu, B., Singh, M., and Sycara, K. (2004). Developing trust in large scale peer-to-peer systems. In Proceedings of 1st IEEE Symposium on Multi-Agent Security and Survi- vability, pages 1–10.