Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Coordenação de Pós-Graduação em Ciência da Computação

Dissertação de Mestrado

Infraestrutura para o Desenvolvimento de Aplicações com Suporte a Comercialização de Serviços entre pares em Ambientes Pervasivos

Lucas Vieira de Souza

Campina Grande, Paraíba, Brasil
Fevereiro – 2012

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Coordenação de Pós-Graduação em Ciência da Computação

Infraestrutura para o Desenvolvimento de Aplicações com Suporte a Comercialização de Serviços entre pares em Ambientes Pervasivos

Lucas Vieira de Souza

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Campina Grande - Campus I como parte dos requisitos necessários para obtenção do grau de Mestre em Ciência da Computação.

Área de Concentração: Ciência da Computação
Linha de Pesquisa: Engenharia de Software

Orientadores:
Hyggo Oliveira de Almeida
Leandro Dias da Silva

Campina Grande, Paraíba, Brasil

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

S729i Souza, Lucas Vieira de.

Infraestrutura para o desenvolvimento de aplicações com suporte a comercialização de serviços entre pares em Ambientes Pervasivos / Lucas Vieira de Souza. - Campina Grande, 2012.

80 f.: il. color.

Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.

Orientadores: Prof. Dr. Hyggo Oliveira de Almeida e Prof. Dr. Leandro Dias da Silva

Referências.

1. Computação Pervasiva. 2. Comercialização. 3. Serviços Móveis. 4. Bilhetagem. I. Título.

CDU 004.4'2(043)

IFRAESTRUTURA PARA O DESENVOLVIMENTO DE APLICAÇÕES COM SUPORTE :OMERCIALIZAÇÃO DE SERVIÇOS ENTRE PARES EM AMBIENTES PERVASIVOS"

LUCAS VIEIRA DE SOUZA

DISSERTAÇÃO APROVADA EM 29/02/2012

HYGGO OLIVEIRA DE ALMEIDA, D.Sc
Orientador(a)

LEANDRO DIAS DA SILVA, D.Sc
Orientador(a)

ANGELO PERKUSICH, D.Sc
Examinador(a)

KYLLER COSTA GORGÔNIO, Dr.
Examinador(a)

CAMPINA GRANDE - PB

Resumo

O avanço dos recursos computacionais dos aparelhos portáteis e a convergência de novas funcionalidades nestes dispositivos, tem criado novas oportunidades para o universo da computação pervasiva. Esses novos atributos, aliados a facilidade de conectividade entre eles e a disponibilização de serviços móveis, tem motivado o compartilhamento e a bilhetagem de recursos entre os usuários desses dispositivos. São exemplos de serviços: o compartilhamento de conteúdo multimídia, o controle de equipamentos eletrônicos e eletrodomésticos, o acesso à Internet, entre outros.

Os aplicativos móveis que oferecem a bilhetagem de recursos, em sua maioria, apresentam apenas formas de cobrança online, com a necessidade de uma conexão com a Internet para a validação das transações. Outras aplicações apresentam uma forma de cobrança offline, porém são soluções que necessitam de um hardware específico para o seu funcionamento, o que inviabiliza a adoção de diversos dispositivos já presentes no mercado.

Tendo em vista esses aspectos, neste trabalho é apresentada uma infraestrutura para o desenvolvimento de aplicações com suporte a bilhetagem de serviços, que oferece uma nova forma de cobrança. A infraestrutura permite a bilhetagem em modo offline e sem a necessidade de um hardware específico para seu funcionamento. A validação do trabalho foi realizada partir da implementação de um estudo de caso de um serviço de envio de mensagens SMS, que encaminha mensagens texto para dispositivos celulares a partir da transferência de arquivos, demonstrando o suporte oferecido pela infraestrutura para o desenvolvimento de aplicações móveis que oferecem a bilhetagem de recursos.

Abstract

The improvement of computational resources of mobile devices and the convergence of new features in these devices has created new opportunities for the world of pervasive computing. These new attributes, combined with ease of connectivity between them and the provision of mobile services has motivated the sharing of resources and billing between the users of these devices. Examples of services: the sharing of multimedia content, the electronics control and appliances, Internet access, others.

Mobile applications that offer resource billing, most of them, have only online charging, with the need of an Internet connection to validate transactions. Other applications presents offline charging, but they are solutions that require specific hardware for its operation, which prevents the adoption of devices already on the market.

Considering these aspects, this work presents an infrastructure for developing applications that supports service billing, which offers a new way of charging. The infrastructure allows billing in offline mode without the need for specific hardware to function. The work validation was performed by implementing a case study of a service for sending SMS messages, which sends text messages to mobile phones through file transfer, showing the support offered by the infrastructure for the development of mobile applications that provide the service billing.

Agradecimentos

Agradeço a Deus, por sempre ter me dado força, saúde e vontade para vencer os obstáculos e atingir meus objetivos. Sem a permissão e bênção do nosso Criador, nada neste mundo seria possível. Obrigado meu bom Deus, pois tudo posso Naquele que me fortalece (Filipenses 4:13) e só Nele.

Agradeço aos meus pais Giselane Souza e Valder Filho, por terem me ensinado o valor da educação na formação do caráter das pessoas.

Agradeço especialmente à minha noiva Elaine Araújo, por sempre me apoiar e dar força em todos os momentos, bons ou ruins e por nunca ter me deixado desistir, pelo contrário sempre me incentivou.

Agradeço a todas os colegas de curso e as amizades conquistadas em Campina Grande que de alguma forma estiveram presentes na concretização de mais este objetivo. Em especial aos companheiros de todas as horas, mais do que amigos nos tornamos parte de uma família: José Athayde Neto, Leonardo Sampaio, Sebastião Rabelo, Daniel Alves, Lorena Maia e Marco Rosner.

Agradeço aos amigos da boa cidade de João Pessoa que também me apoiaram e me incentivaram a conquistar mais esse título em minha vida pessoal e profissional. Em especial ao amigo Gustavo Cavalcanti (in memoriam), exemplo de vida, de luta, perseverança, amizade e honestidade

Agradeço também aos demais colegas de laboratório que sempre estavam prontos a ajudar com suas opiniões e experiência.

Aos meus orientadores do programa de pós-graduação, pela credibilidade, pelas oportunidades oferecidas, pela paciência, ensinamentos e cobranças.

Aos professores que tive ao longo de todo o meu percurso acadêmico, todos de certa forma contribuíram com minha formação, em especial aos mais próximos como os professores Frederico Pereira, Lafayette Melo, Liliane Machado, Ronei Moraes e Hamilton Silva

Às secretárias da COPIN, Rebeka Lemos, e, especialmente, Aninha Sauvé e Vera Oliveira, por toda cooperação oferecida e pelos valiosos conselhos.

À UFCG e à CAPES pelo apoio financeiro durante o período da pesquisa.

Enfim, a todos que direta ou indiretamente participaram da realização deste trabalho.

Conteúdo

Lista de Símbolos

3G - *3rd Generation Mobile Telecommunications*

AES - *Advanced Encryption Standard*

API - *Application Programming Interface*

ATM - *Automated Teller Machine*

B2C - *Bussines-to-Commerce*

C2C - *Commerce-to-Commerce*

CA - *Certificate Authority*

GPRS - *General Packet Radio Service*

GPS - *Global Positioning System*

GUI - *Graphical User Interface*

NFC - *Near Field Communication*

P2P - *Peer-to-Peer*

PCI - *Payment Card Industry Data Security Standard*

PDAs - *Personal Digital Assistants*

PKI - *Public Key Infrastructure*

POS - *Point of Sale*

RFID - *Radio-frequency Identification*

SGBD - Sistema Gerenciador de Banco de Dados

SMS - *Short Message Service*

TI - *Tecnologia da Informação*

UPnP - *Universal Plug and Play*

W3C - *World Wide Web Consortium*

Lista de Figuras

Capítulo 1

Introdução

A partir do século XXI, com os avanços tecnológicos na área da comunicação sem fio (Wi-Fi, Wi-Max, 3G e Bluetooth), surgiu um novo nicho de mercado direcionado para os dispositivos portáteis, como *Smart Phones* e *Internet Tablets*. A pesquisa de Hui-Yi e Ling-Yin em [17] mostra que a oferta de diferentes tipos de aplicações e serviços móveis cresceu com o avanço desses dispositivos. Esta variedade de aplicações e serviços também se deve ao aumento das funcionalidades agregadas destes dispositivos. Percebe-se ainda uma evolução no grau de complexidade das aplicações móveis proporcionalmente à capacidade de armazenamento, à capacidade de processamento e ao aumento de memória desses dispositivos. Exemplos da evolução desses aplicativos são percebidos em jogos *multiplayer* para dispositivos portáteis, como os jogos desenvolvidos a partir do *framework* FMMG - Framework Mobile Multiplayer Games [23] e em sistemas de navegação como apresentado por Park *et al.* em [29]. A tendência da ampliação da computação móvel oferece novos desafios científicos a serem solucionados.

Com o crescente uso da computação móvel e o avanço das tecnologias portáteis, surgiu a computação pervasiva [34], que busca a redução da intrusão do usuário tornando os sistemas cada vez mais transparentes às pessoas, a partir de sistemas inteligentes e cientes de contexto [26]. Como consequência, a computação pervasiva permite a disponibilização de serviços de um modo personalizado aos seus usuários, o que demanda mecanismos para sistematizar a resolução dos problemas de disponibilização de serviços em redes pervasivas. Estes mecanismos operam em um ambiente dinâmico, onde a entrada e a saída de dispositivos da rede (conexão e desconexão) são frequentes e, portanto, devem suportar este dinamismo

oferecendo meios de comunicação acessíveis a todo instante e da forma mais simples possível. Uma alternativa é a utilização de mecanismos para descoberta e requisição de serviços.

O crescimento e a consolidação da computação pervasiva permite uma mudança de paradigma quanto ao projeto de sistemas, provocando a migração do modelo computacional voltado a processos para modelos centrados nas atividades dos usuários e ambiente. Essa nova visão necessita de alguns pré-requisitos como uma infraestrutura de conectividade sem fio entre os dispositivos da rede, equipamentos portáteis com o menor nível de consumo de energia possível e aplicações pervasivas inteligentes. Além disso, soluções baseadas nessa abordagem devem dar suporte à customização de serviços, sensibilidade de contexto e adaptação ao alto grau de heterogeneidade do ambiente, existente devido à diversidade de recursos envolvidos.

Devido ao avanço dos recursos computacionais desses dispositivos e sua facilidade de conectividade, eles passaram a disponibilizar serviços de rede e não somente consumi-los. Em seguida, o surgimento de padrões de conectividade e acesso a serviços de rede P2P impulsionou a adoção dos aparelhos portáteis, permitindo o controle de outros equipamentos e compartilhamento de serviços de rede. Exemplos desses serviços são: acessar conteúdo multimídia localmente ou remotamente, controlar equipamentos como condicionadores de ar, controlar a iluminação e pontos de acesso a rede sem fio.

O avanço tecnológico e a agregação de novas funcionalidades aos aparelhos portáteis juntamente aos padrões de conectividade e disponibilização de serviços oferecem novas oportunidades para o universo dos dispositivos pervasivos. Desta forma, um usuário pode optar por vender recursos de seus dispositivos pervasivos (serviços ou conteúdos) diretamente a outro usuário, surgindo, assim, a oportunidade de comercializar tais recursos entre eles em um ambiente *ad-hoc*. Neste contexto, torna-se possível considerar uma abordagem de compra e venda de recursos ou conteúdo através de um modelo consumidor-consumidor a qualquer hora e em qualquer lugar.

1.1 Problemática

De acordo com o que foi apresentado anteriormente é possível identificar diversos tipos de serviços disponibilizados nas diferentes redes de computadores. Nas redes pervasivas, por exemplo, identifica-se a oferta de serviços que controlam aparelhos residenciais [7] [36], equipamentos de rede [20], serviços de localização, entre outros. Ainda, é possível destacar a bilhetagem de serviços em um ambiente pervasivo. Uma aplicação que exemplifica a bilhetagem de serviços em ambientes pervasivos é o Ubipay [25], que apresenta um sistema de pagamentos cujo autorizador das transações é uma aplicação instalada em um dispositivo móvel. Ele proporciona o pagamento de serviços como passagem de metrô e ingresso de shows, através da checagem de preferências do usuário e informações de contexto da forma menos intrusiva possível para o portador do aparelho móvel. Seu escopo soluciona apenas a autorização do pagamento, que seria a efetivação desse pagamento através de uma rede móvel que utiliza um dispositivo celular como ponto de controle e acesso a ação de transferência do dinheiro. O Ubipay necessita de comunicação contínua com uma terceira entidade confiável, responsável pela transferência do dinheiro entre as partes envolvidas na transação. Essa necessidade apresenta um ponto central de risco, já que uma possível falha de comunicação com qualquer um dos atores envolvidos neste cenário pode resultar no cancelamento ou até mesmo na impossibilidade de realização da transação.

Outras abordagens neste mesmo contexto de bilhetagem de recursos, também utilizam um terceiro ator durante a transação. Esse terceiro ator deve ser considerado confiável e seguro pelos usuários participantes da transação. Soluções como esta, estão presentes no modelo de negócio do Paypal [1] e do Mercado Pago [2]. Essa terceira entidade tem o papel de mediação da transação, pois somente através dela, transferências entre contas são realizadas. Essas contas são virtuais e devem possuir saldo financeiro positivo, provenientes da compra de dinheiro virtual com dinheiro real - exemplos: depósitos eletrônicos e transferência de crédito utilizando um cartão de crédito. Cada usuário deve possuir uma conta virtual na infraestrutura oferecida pela solução para que o cenário descrito seja concretizado. Esse modelo é bastante utilizado na Internet e também já está acessível a celulares, como é o próprio PayPal. Embora essa solução seja bastante difundida na Internet e disponível para

[1] https://www.paypal.com/

[2] http://www.mercadolivre.com.br/jm/mercadopago

aparelhos móveis com acesso a Internet, a necessidade de comunicação ininterrupta durante a transação com uma terceira entidade confiável, impossibilita o processo de bilhetagem de bens e serviços em uma rede móvel ponto a ponto sem acesso a Internet.

Portanto, mesmo que alguns modelos de bilhetagem utilizados na Internet tenham sido adaptados para ambientes pervasivos, como apresentado por Lehdonvirta *et al.* em [25] e também por Pillai *et al.* em [30], o problema em aberto identificado nestas abordagens é que elas não funcionam sem uma conexão com a Internet durante todo o processo de bilhetagem dos recursos comercializados, o que inviabilizaria a bilhetagem de serviços móveis entre pares em redes pervasivas.

1.2 Cenário e Discussões

Para entender melhor o problema considere o cenário ilustrado na Figura 1.1, nela é apresentado o exemplo de duas pessoas proprietárias de um *smart phone* cada uma. Estes dispositivos detêm diversas funcionalidades em comum, como *Bluetooth*, infravermelho e Wi-Fi, contudo um deles possui conexão com a Internet e o outro não. O proprietário do *smart phone* B é provedor de um serviço de conexão com a Internet sob demanda. Já o *smart phone* A não possui conexão com a Internet, mas precisa acessá-la para executar uma determinada ação, como por exemplo, o envio de um e-mail. Assim, A é um consumidor em potencial de um serviço de conexão com a Internet, disponibilizado por B. Este é um caso típico de um modelo provedor/consumidor de serviços.

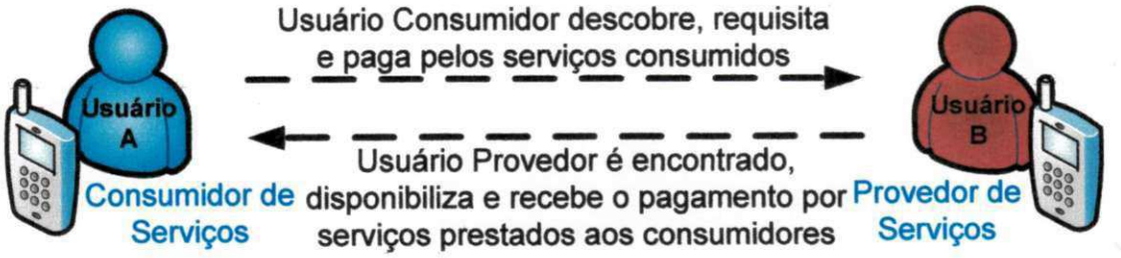


Figura 1.1: Relação entre os usuários consumidor de serviços e provedor de serviços.

Através de um mecanismo de descoberta de dispositivos e serviços, como disponibilizado

pelo UPnP [3], o usuário consumidor encontra o usuário provedor e carrega todas as informações dos serviços oferecidos pelo provedor. Com estas informações sobre o provedor, o consumidor pode solicitar um determinado serviço, como por exemplo, o acesso à Internet, consultar o valor cobrado e as formas de bilhetagem disponíveis (por minuto ou por Kbyte). Acertados os parâmetros de compra do serviço, o consumidor efetua o pagamento.

A forma de pagamento adotada pode variar. Dinheiro, cartão de crédito e cheque são algumas possíveis formas de pagamento. Entretanto, como o cenário ilustrado mostra um ambiente que não possui conexão com a Internet, a opção por utilizar o cartão de crédito ou outra forma que necessite de acesso à Internet para autorização da transferência de fundos, torna-se impraticável. Já a opção por meios de pagamento como dinheiro ou cheque, obrigaria as partes a estabelecerem um contato para a troca de dinheiro, o que pode não ser o desejo de algum usuário mais tímido e comedido. Além disso, o valor cobrado pela utilização de um serviço móvel pode ser tão baixo que não valha a pena a emissão de cheques ou até mesmo não seja interessante para algum dos usuários envolvidos usar dinheiro, já que para valores baixos certamente moedas estariam envolvidas na forma de pagamento pelo serviço, acarretando em transtornos com troco e transporte de moedas. Por outro lado, por tratar-se da disponibilização de um serviço de *software*, cobrado por demanda e em um momento oportuno, onde as partes envolvidas podem não se encontrar outra vez, a opção pelo uso de um modo eletrônico de pagamento, onde é possível efetuar um pagamento anonimamente, sem a necessidade de preocupação com o valor, nem com o troco, de forma segura e confiável, pode ser uma opção viável para as partes. Para isso, propõe-se a criação e a utilização de um dinheiro virtual como discutido por Guo e Chow em [12].

O dinheiro virtual é uma moeda como o Real (R$), porém disponibilizado sob a forma de créditos eletrônicos, ou cédulas eletrônicas. A cédula eletrônica pode ser um número gerado por alguma entidade emissora como um banco. Portanto, diante do exposto, a utilização de uma moeda eletrônica é a alternativa encontrada como forma de pagamento para o cenário apresentado anteriormente na Figura 1.1.

A sugestão dessa nova forma de pagamento não necessita de uma entidade para fazer a conferência deste dinheiro virtual em tempo real. Esse dinheiro deve ser previamente emitido por um órgão seguro e certificado analogamente ao modelo monetário utilizado por diversos

[3]http://www.upnp.org/

países em seus bancos centrais, como é o caso do Brasil. Por esse motivo, a conferência desta moeda eletrônica cabe ao provedor do serviço, que deve portar em seu dispositivo eletrônico, um *software* capaz de reconhecer se o dinheiro virtual é válido ou não. Esta moeda eletrônica recebida como pagamento, também pode ser utilizada pelo provedor de outras formas, e a troca desse dinheiro virtual pela moeda real deve ser realizada junto a um órgão credenciado e certificado para efetuar este tipo de resgate.

É possível, ainda, ocorrer a disponibilidade de dois ou mais serviços semelhantes ou iguais no ambiente que o consumidor se encontra. O consumidor pode optar pelo serviço que cobra mais barato ou pelo serviço de melhor qualidade definido pelo usuário consumidor, mesmo que seja com um custo mais elevado. Um mecanismo de negociação pode ser disponibilizado por uma infraestrutura que permita a negociação entre os consumidores e provedores de serviços.

Além disto, faz-se necessário um modelo financeiro virtual que permita que usuários consumidores e provedores paguem e recebam dinheiro, respectivamente. Consequentemente, para que um usuário saque dinheiro virtual ou converta esse dinheiro virtual em real (similar a um depósito) é necessária uma infraestrutura bancária disponível eletronicamente, permitindo a compra e venda de serviços entre eles.

Para contemplar um cenário completo, seria necessário determinar um conjunto de atividades para o tratamento adequado de cada parte do cenário de aplicação descrito nessa seção. Algumas dessas atividades seriam:

- Prover segurança na identificação de usuário e reputação;
- Prover segurança em transferências financeiras entre dois usuários, inclusive considerando a possibilidade disto ocorrer sem conexão com a Internet;
- Prover verificação de qualidade de serviço de um usuário provedor;
- Prover mecanismo para bilhetagem de serviços no modelo C2C, o qual permitirá, por exemplo, que um provedor verifique se um consumidor possui fundos suficientes para pagar por um determinado serviço;
- Representar, garantir legitimidade e emitir dinheiro virtual;

- Sincronizar os sistemas dos usuários caso ocorra alguma desconexão entre eles e retornar ao estado de execução no momento da desconexão;

1.3 Objetivo

Neste trabalho tem-se como objetivo desenvolver uma infraestrutura para a construção de aplicações baseadas na comercialização de recursos que disponibilizem a bilhetagem de serviços P2P em ambientes pervasivos, permitindo novas formas de cobrança por estes serviços sem a constante necessidade de conexão com a Internet durante a execução e bilhetagem da transação P2P. A infraestrutura proposta deve: fornecer a segurança da informação durante a transação, para impedir que os dados trocados sejam alterados indevidamente e permitir que o dinheiro virtual seja armazenado de tal forma que o valor para quebrar a segurança utilizada, ultrapasse o valor da informação; garantir a integridade dos dados, para não permitir a geração indevida de créditos eletrônicos nem a manipulação desse dinheiro que não seja através de uma biblioteca de desenvolvimento específica de bilhetagem; e adaptável, facilitando o desenvolvimento de novas aplicações e serviços.

Para alcançar o objetivo principal, os seguintes objetivos específicos são considerados:

1. Definição de uma arquitetura para aplicações com suporte a bilhetagem de serviços enter pares;

2. Definição de um protocolo de comunicação para permitir o controle e o repasse dos créditos eletrônicos entre os usuários;

3. Definição uma API (*Application Programming Interface*) para o desenvolvimento de novas aplicações utilizando a infraestrutura de bilhetagem;

4. Desenvolvimento de uma aplicação como estudo de caso utilizando a infraestrutura proposta a fim de validá-la.

A segurança dos dados contra alterações indevidas durante a transação foi alcançada utilizando a assinatura de todas as mensagens trocadas. Além disso, todos os dados são armazenados em um sistema de arquivos criptografados com uma chave conhecida apenas pela infraestrutura e todas as ações das transações são rastreadas e marcadas para que não seja

possível reproduzir as funções do sistema fora dele. Dessa forma, é garantida a integridade dos dados utilizados na infraestrutura protegendo o sistema contra a geração indevida de dinheiro eletrônico. Ainda, para garantir a adaptação da infraestrutura, utiliza-se uma biblioteca de desenvolvimento que pode ser utilizada por outros aplicativos que ofereçam o suporte a bilhetagem.

Por fim, utilizando a infraestrutura, uma aplicação com suporte a bilhetagem de serviços entre pares foi desenvolvida para um dispositivo compatível com a plataforma Android que realiza a cobrança de um serviço de envio de mensagens SMS.

1.4 Relevância

Atualmente, as formas de bilhetagem encontradas para sistemas P2P dividem-se em: modelos que necessitam de conexão com a Internet durante todo o processo da transação - disponibilização, consumo e pagamento do serviço - e modelos que não precisam de conexão com a Internet durante todo o processo da transação. Os sistemas que se encaixam no primeiro caso são baseados no modelo de negócio onde há explicitamente a presença da terceira entidade, mediadora, confiável aos usuários envolvidos na comercialização do recurso, que é responsável pela certificação e validação das transações entre as partes. Este modelo é análogo ao modelo C2C do comércio eletrônico presente na Internet. O valor do recurso é negociado entre os usuários, o consumidor autoriza a liberação do dinheiro, a entidade mediadora valida à operação e certifica-se de que o consumidor está apto a proceder com a transação e, caso autorizado, a transferência é efetuada para o provedor do recurso. Portanto, aplicações deste modelo não funcionam sem a conexão com a Internet. Já os sistemas que se encaixam no segundo caso apresentam soluções que dependem de um *hardware* específico, como por exemplo, sistemas dependentes de um circuito integrado embarcado aos dispositivos, ou dependentes de uma tecnologia específica, como NFC - Near Field Communication. Portanto as aplicações deste modelo não funcionam em dispositivos que não possuem o *hardware* específico exigido pelos sistemas classificados nesse segundo modelo.

A proposta de uma infraestrutura de bilhetagem de serviços móveis para redes pervasivas P2P independentes de um *hardware* específico, permitiria que os próprios usuários do

sistema verificassem e avaliassem as suas operações financeiras em tempo real. Além disso, a solução poderia ser adotada por usuários com dispositivos presentes no mercado atual, já que a solução não exigiria um aparelho com uma tecnologia de *hardware* específica. Dessa forma, seria retirada do sistema a necessidade de uma terceira entidade para efetuar a validação da transação, descartando, também, a necessidade de conexão com a Internet durante a operação. Assim, com a eliminação desse pré-requisito de conexão com a Internet, os usuários realizariam suas transações em qualquer lugar e a qualquer momento. Portanto, esta solução apresenta um novo meio de suporte a pagamentos de bens e serviços, oferecendo uma nova forma de bilhetagem entre usuários P2P.

Por fim, o trabalho está inserido no contexto do projeto PerComp, do Laboratório de sistemas Embarcados e Computação Pervasiva[4] da UFCG, servindo como base para a proposição de novas abordagens de sistemas com suporte a bilhetagem e contribuindo com o grupo de pesquisa da instituição.

1.5 Organização

Essa dissertação segue estruturada da seguinte forma:

- O segundo capítulo apresenta os fundamentos teóricos para a compreensão do assunto abordado neste trabalho.
- O terceiro capítulo apresenta os trabalhos relacionados e estado da arte do contexto de bilhetagem de serviços móveis em ambientes pervasivos, alvo deste trabalho, que procura analisar a viabilidade deste tipo de sistema em redes P2P.
- O quarto capítulo apresenta o projeto da infraestrutura proposta que oferece o suporte a bilhetagem de serviços móveis entre pares em ambientes pervasivos.
- O quinto capítulo traz a prova de conceito e um estudo de caso do projeto apresentado no quarto capítulo, além de algumas discussões sobre a viabilidade da aplicação.
- O sexto capítulo expõe a conclusão do trabalho com as considerações finais do autor e as propostas de trabalhos futuros.

[4] http://www.embeddedlab.org/

- Por fim é relacionada as referências utilizadas no trabalho.

Capítulo 2

Fundamentação teórica

Neste capítulo serão descritos os principais conceitos pertinentes à elaboração deste trabalho. Inicialmente é apresentada uma descrição do paradigma de computação pervasiva e suas características. Em seguida são detalhados alguns conceitos de redes P2P e serviços entre pares. Por último, são apresentadas algumas definições sobre a comercialização de serviços móveis e bilhetagem.

2.1 Computação Pervasiva

O aumento da oferta de dispositivos portáteis que reúnem cada vez mais funcionalidades, oferece aos seus usuários a oportunidade de se manterem cada vez mais conectados à Internet, mesmo que estejam em constante movimento. Com o barateamento desses dispositivos e com a disseminação de redes de dados móveis, como a rede 3G, a tendência do mercado é a difusão desses dispositivos e o crescimento da quantidade de pessoas conectadas à Internet. Dessa forma, os usuários podem interagir entre si, como por exemplo, a partir das redes sociais, em qualquer lugar e a qualquer momento desde que estejam conectados a uma rede móvel com acesso a Internet. Isso se torna possível, pois os atuais dispositivos como os *smartphones*, ao longo de sua evolução, adquiriram recursos que proporcionam essa rápida interação, como é o caso do GPS, onde o usuário pode compartilhar sua localização de forma rápida e transparente. Essa tecnologia de localização não é a única inovação dos *smartphones*, que também passaram a contar com cada vez mais tecnologias de comunicação, por exemplo o Bluetooth e Wi-fi, possibilitando a descoberta de serviços

disponíveis e outros usuários aos quais estes possam interagir de modo a transferir dados multimídia, sejam eles textos, vídeo ou áudio, em qualquer lugar com rede disponível e a qualquer hora.

O avanço da tecnologia vem mostrando que cada vez mais dispositivos que antes funcionavam de forma isolada, como uma geladeira ou micro-ondas, podem chegar a estar interligados através de chips em uma rede. Além disso, os dispositivos passaram a interagir com os humanos de forma transparente. Essa ideia está ligada ao conceito de computação pervasiva, que procura mostrar que o computador pode estar presente em qualquer lugar sem que o usuário tenha a percepção de sua presença. Mark Weiser [34], ex-cientista chefe da Xerox PARC[1] trata a computação pervasiva como uma tecnologia que permite construir aplicações onde a interação homem-máquina se torna imperceptível e natural para os usuários. Ele apresentou um conceito onde o computador faz parte do ambiente de maneira invisível para o usuário. Atrelado a esse conceito, também está a capacidade do computador estar associado à aplicações cientes de contexto, se adaptando ao ambiente ao qual está imerso e atualizando-se de forma automática e imperceptível ao usuário, de forma a melhor atender as suas necessidades, demonstrando o caráter evolutivo da tecnologia.

Um sistema de computação pervasiva pode ser definido como um sistema que intercala informações entre os mundos físico e digital com o objetivo de fornecer assistência, ou a informação de que o usuário precisa na realização de suas atividades, de forma proativa e conveniente [5]. A proatividade só é efetivamente concretizada quando o sistema em questão consegue perceber a intenção do usuário [31]. Isso é possível através da ciência de contexto, de forma a traçar e a adequar o sistema a um perfil específico para aquela ação em questão.

Essa tecnologia tem se tornado promissora devido à popularização dos dispositivos portáteis como *smartphones*, *netbooks* e *tablets*, bem como, a ascensão e avanços das tecnologias em redes de telecomunicações e tecnologia da informação. O fato tem se mostrado fator determinante para o desenvolvimento de cada vez mais aplicações pervasivas. O que antes era um desenvolvimento para um tipo de usuário, em um determinado contexto, agora deve levar em consideração um ambiente extremamente heterogêneo onde diversos dispositivos com propósitos diferentes e seus sistemas, devem se comunicar através de um protocolo comum. Essa nova realidade representa um novo paradigma em computação, onde

[1] http://www.parc.com/

a interação deixa de ser centrada na máquina e agora é centrada no ser humano.

Um exemplo clássico de um sistema pervasivo é aquele que faz uso de etiquetas RFID [24]. Etiquetas de identificação por rádio (*RFID-Radio Frequency Identification*) são chips de silício sem fio, associados a uma pequena antena embutida em um invólucro, capazes de transmitir dados para um receptor a uma certa distância. As aplicações são inúmeras e podem ser usadas para rastrear qualquer objeto ou pessoa. A Computação Pervasiva faz uso dessa tecnologia para rastrear e monitorar pessoas e objetos em um ambiente inteligente. Inúmeras aplicações podem ser criadas no sentido de enriquecer a interação entre o usuário e todo o sistema computacional que o cerca. Com o uso da tecnologia RFID, todo o ambiente pervasivo fica ciente da localização do usuário, podendo até prever suas ações através da análise do seu histórico de movimentações.

Um dos problemas enfrentados no desenvolvimento desses sistemas está em manter essas aplicações sempre adaptadas ao meio. Outro desafio é não deixar que seu funcionamento seja interrompido nesse processo, levando-se em consideração que os usuários estão em constante deslocamento [11]. Vários requisitos são necessários para o desenvolvimento de aplicações pervasivas, como por exemplo, o suporte à ciência de contexto e interoperabilidade. Esses conceitos são tratados nas subseções seguintes.

2.1.1 Interoperabilidade

O mundo está rodeado de diversos dispositivos tecnológicos e sistemas computacionais funcionando integrados de forma a facilitar a vida das pessoas. Ao comprar um produto em um *site* de comércio eletrônico com o cartão de crédito, por exemplo, o sistema de informação do comércio eletrônico não tem como validar os dados do cartão de crédito do cliente. Por questões de confiabilidade e segurança, quem tem autorização para isso é o sistema da operadora de cartão de crédito, que de forma interligada ao sistema de comércio eletrônico, valida os dados do cartão e devolve ao sistema de comércio eletrônico uma mensagem que define se a compra pode ser efetivada. Todo esse processo é feito de forma transparente para o usuário, que acredita estar utilizando apenas um sistema, esse é um exemplo do que é a interoperabilidade.

O uso constante da Internet vem contribuindo para criar essa realidade onde os sistemas devem trabalhar em conjunto, aumentando o alcance da disseminação da informação. Para

desenvolver aplicações, os desenvolvedores possuem uma extensa variedade de linguagens de programação e ambientes de desenvolvimento, utilizando-se da tecnologia que melhor se adaptar à sua necessidade. Isso faz com que existam diversos sistemas feitos de forma diferente, utilizando tecnologias diferentes, porém é necessário que eles consigam interagir. Essa heterogeneidade não irá acabar com o tempo, pois todos os dias surgem novas tecnologias. Então, no contexto da computação pervasiva, os sistemas devem suportar os diversos dispositivos e sistemas de natureza diferente, efetuando o que seu próprio conceito delimita, que é o fato de vários sistemas e dispositivos convergirem de forma invisível ao utilizador [15].

Além de interoperar, os sistemas de computação pervasiva, devem ser escaláveis, ou seja, devem estar preparados para crescer caso seja necessário e, adaptar-se de forma transparente para o usuário às novas demandas e contextos que forem surgindo com o passar do tempo. Uma alternativa para atender à essa exigência é que os desenvolvedores usem o desenvolvimento orientado à componentes, criando suas aplicações a partir de componentes de *software* disponíveis de forma dinâmica. Diante disso, a infraestrutura de computação pervasiva terá que ser interoperável também à nível de componentes. Esses componentes são responsáveis por conhecer a interface uns dos outros de forma dinâmica, de forma a interagir com os outros componentes que forem surgindo [15].

2.1.2 Ciência de Contexto

É fato que as pessoas se deslocam constantemente, seja para o trabalho, escola, lazer, entre outros. O que é uma necessidade para aquele usuário em um determinado ambiente, pode não ser mais no outro ambiente, é a essa variável que damos o nome de contexto. Uma aplicação ciente de contexto é capaz de se adaptar às preferências do usuário em determinadas situações ou ambientes. Esse conceito é muito relevante para a computação pervasiva, pois quanto maior a adaptabilidade da aplicação ao contexto, menor será a quantidade de entradas efetuadas pelo usuário, o que torna a aplicação ainda mais transparente como é citado por Weizer em [34]. Outra questão também importante é o fato de que a ciência do contexto pode permitir a adaptação às mudanças que puderem ocorrer no ambiente, como por exemplo a entrada ou saída de um dispositivo.

As informações pertinentes a sistemas cientes de contexto podem ser derivadas de

diversas fontes, sendo estas de qualidade ou não. Perceber o contexto é algo extremamente dinâmico e suscetível a ruídos e erros de detecção. Caso o usuário atualize constantemente suas informações, como perfil ou histórico de interações com a aplicação, essas informações são consideradas bastante confiáveis, caso contrário elas passam a perder a importância [14].

Uma definição bastante difundida é a de que contexto pode ser considerado qualquer informação que pode ser utilizado para caracterizar a situação de uma entidade. Uma entidade é um pessoa, lugar ou objeto que é considerado relevante para a interação entre um usuário e uma aplicação, incluindo o usuário e a aplicação em si [10]. As aplicações cientes de contexto podem explorar várias informações dependendo do seu foco, por exemplo a localização dos postos de gasolina que estão mais próximos da localização do usuário naquele momento. Outras informações que podem ser exploradas pelos componentes cientes de contexto são, por exemplo: outros usuários geograficamente próximos, atividades aos quais os usuários estão envolvidos, condições meteorológicas, entre outras [2].

2.2 Redes P2P

Redes P2P são redes cuja arquitetura é distribuída entre os nós envolvidos na rede, onde cada um dos nós possui um papel equivalente aos demais. Redes P2P [3] são sistemas distribuídos capazes de se organizar em topologias que permitem o compartilhamento de recursos, como conteúdos diversos, espaço em disco, processamento, etc. São classificadas em descentralizadas - todos os nós tem a mesma função, centralizadas - alguns nós assumem funções específicas e híbridas - existem nós específicos, porém a interação entre os nós é direta entre eles. Ainda, segundo Taenenbaum em [33] , as redes ponto a ponto consistem em muitas conexões entre pares de máquinas individuais. Para ir da origem ao destino, um pacote nesse tipo de rede não é encaminhado para um concentrador central de requisições e talvez ele trafegue primeiro por uma ou mais máquinas intermediárias até seu destino. A comunicação entre essas máquinas intermediárias também é P2P. Como normalmente é possível haver várias rotas com diferentes tamanhos, encontrar "boas" rotas é algo importante em redes ponto a ponto.

2.2.1 Redes Móveis

A tecnologia de redes sem fio permitiu a interconexão de dispositivos em uma rede cujos nós não precisam estar necessariamente fixos em um determinado local para o funcionamento da rede. Este tipo de rede é chamada de rede móvel. A característica fundamental dos nós dessa rede é que eles podem estar em movimento sem perder a conexão com a rede. Além disso, a rede não sofre interrupções ou quebras devido a saída ou entrada de nós.

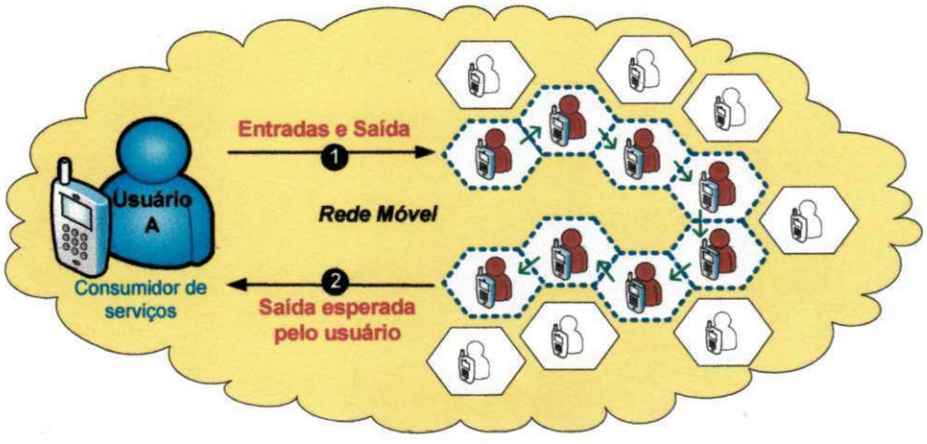


Figura 2.1: Comunicação em uma rede móvel

Um exemplo conhecido e presente no cotidiano de diversas pessoas são as redes estabelecidas pela tecnologia de redes Bluetooth [16] que determinam uma rede entre dois dispositivos celulares, por exemplo, para troca de conteúdos, como imagens, músicas, vídeos e outros formatos suportados por esses aparelhos. A Figura 2.1 representa a característica de resiliência de uma rede móvel, que suporta a entrada e saída de nós da rede sem alterar o estado da rede, além de demonstrar a comunicação entre os nós de uma rede móvel mostrando bem que não é necessário a presença de uma base fixa na rede.

Wi-Fi

O nome Wi-Fi (*Wireless Fidelity*) é um termo que identifica redes sem fio [1] e os dispositivos que implementam a especificação IEEE 802.11. Maia escreveu em [27] que "uma rede Wi-Fi estruturada é composta por dispositivos que se comunicam por sinais de rádio-frequência dentre os quais um ou mais são pontos de acesso (PA). Pontos de acesso são dispositivos que, por um lado, conectam-se à rede cabeada e, por outro, comunicam-se com os outros

dispositivos Wi-Fi, servindo como ponte para que tais dispositivos acessem a rede".

2.3 Bilhetagem

O termo bilhetagem deriva-se do verbo bilhetar e dentro do contexto do trabalho está relacionado ao conceito de cobrança. Esta cobrança é proveniente da comercialização de um bem concreto ou abstrato ou até mesmo de um serviço, nesse caso um serviço móvel. A bilhetagem em redes P2P habilita o comércio de serviços disponibilizados pelos usuários, permitindo a transferência de valores monetários em troca de serviços ofertados entre eles, definindo um modelo de comércio eletrônico de micro-pagamentos móveis.

O modelo de comércio eletrônico o qual a bilhetagem de serviços móveis entre pares se enquadra é o modelo entre consumidores. Este modelo é detalhado a seguir.

2.3.1 Modelo C2C

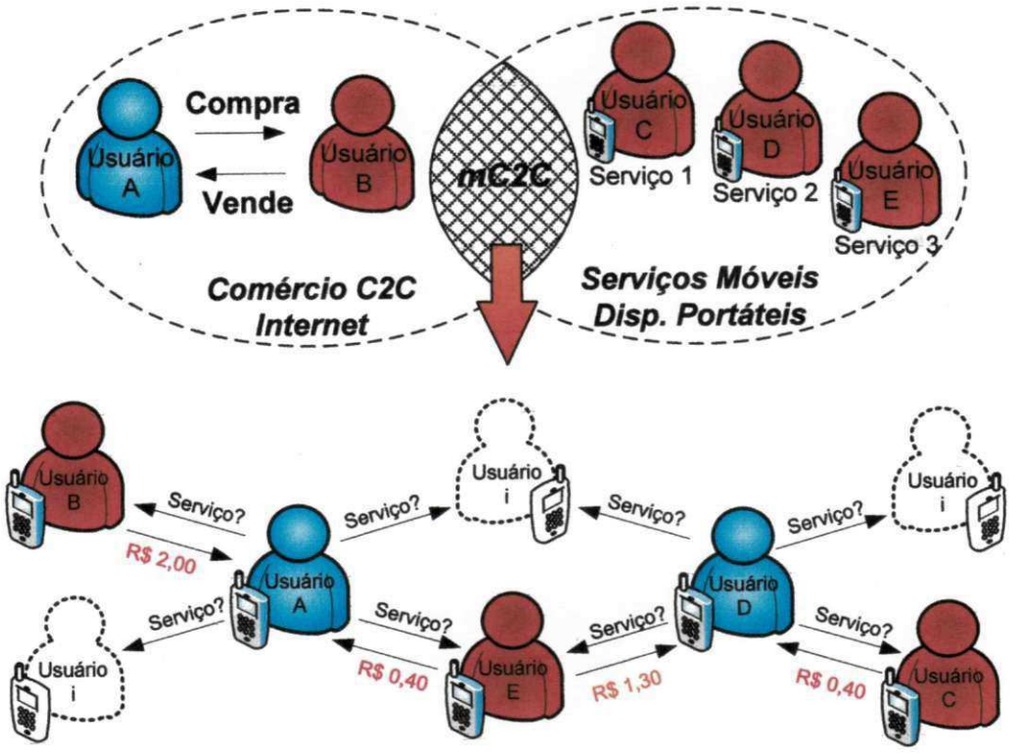


Figura 2.2: Comércio Eletrônico de Serviços Móveis entre Consumidores

É o comércio eletrônico efetuado entre consumidores. Geralmente há a presença de uma terceira pessoa envolvida no modelo de comércio, o intermediador ou entidade confiável. Por exemplo, um negócio onde pessoas oferecem seus produtos a outras pessoas, como o Mercado Livre[2] disponível na WEB. A figura 2.2 apresenta outro exemplo do modelo de comércio C2C, praticado diretamente entre duas pessoas sem a presença de uma terceira entidade.

A Figura 2.2 ilustra um modelo de comércio eletrônico de serviços móveis entre consumidores. Na Figura 2.2 é possível identificar que usuários estão a procura de serviços em uma rede móvel e que está sendo realizado a bilhetagem pela prestação de serviços móveis. Do cenário resultante da interseção do fornecimento de serviços móveis em dispositivos portáteis com o comércio eletrônico, surge o conceito de *Mobile Commerce*, que é o comércio eletrônico de recursos praticados por usuários em redes móveis.

[2]http://www.mercadolivre.com.br/

Capítulo 3

Trabalhos relacionados

A literatura apresenta diversos trabalhos relacionados à bilhetagem em ambientes móveis. Contudo, poucos exploram um cenário de comercialização de serviços entre pares. Grandes partes dos trabalhos recentes exploram o modelo de bilhetagem difundido pela Internet entre consumidores e empresas, que utiliza uma terceira entidade para verificar e validar as transações, exercendo um papel de mediação. Não há hoje um grupo ou consórcio internacional como o W3C[1] , que desenvolve padrões para a WEB, que defina um padrão de comunicação para o comércio eletrônico móvel. Essa falta de padronização levou a indústria de *software* em geral a pesquisar mais sobre o assunto. Karnouskos [21] em seu trabalho apresenta uma visão geral dos esforços e iniciativas de padronização do comércio eletrônico móvel. O autor apresenta uma classificação para sistemas de pagamento móveis baseado nos atributos desse tipo de sistema. As seções abordadas neste capítulo apresentam o estado da arte de acordo com a classificação sugerida por Karnouskos e os atributos utilizados como critérios de agrupamento presentes neste trabalho são baseados na localização geográfica, na forma de pagamento e na validação dos créditos eletrônicos trocados.

3.1 Localização

Este critério é baseado na localização geográfica do usuário iniciador da ação, que determina a necessidade de meios de pagamentos de acordo com a distância dos atores envolvidos, como mecanismos que envolvem tecnologias de rede de curtas distâncias e tecnologias de

[1] http://www.w3c.org/

rede de longas distâncias. De acordo com a localização, o tipo de pagamento é classificado em duas formas: transações remotas e transações locais ou próximas.

3.1.1 Transações remotas

São as transações independentes da localização do usuário. Essa característica deve-se em parte às tecnologias de redes móveis (como Wi-Fi e GPS) que oferecem comunicação em qualquer lugar. Dessa forma os usuários de sistemas de comércio eletrônico móveis realizam suas negociações sem a necessidade de um POS/ATM e sem a necessidade de proximidade entre eles. As pessoas inseridas neste grupo não precisam estar próximas para realizar suas transações, o que mantém o anonimato dos usuários.

- Green e Maknavicius [8] apresentam em seu trabalho um *framework* de bilhetagem direcionado à ambientes pervasivos que prestam serviços móveis. Os autores apresentam uma solução para a questão da segurança em sistemas de bilhetagem para redes móveis. Green e Maknavicius adotam uma forma de cobrança baseada no modelo de mediação da transação, onde há a presença de uma entidade confiável mediadora da negociação entre o consumidor e o provedor do serviço, como encontrado também no sistema do Paypal. Os autores baseiam sua solução no cenário de que pessoas podem utilizar serviços e efetuar o pagamento desses serviços de forma confiável através de um sistema de bilhetagem seguro.

  A Figura 3.1 mostra o esquema de autenticação e comunicação da solução de Green e Maknavicius. Eles propõem que os usuários desse *framework* se cadastrem previamente (1° passo) em um servidor seguro de bilhetagem, o Provedor de Bilhetagem, que oferece um serviço de negociação e agenciamento de todas as transações. Esse serviço funciona como um agente representante das ações financeiras do usuário. Feito esse cadastro, o usuário consumidor, troca informações com o Provedor de serviços desejado (2° passo). O Provedor de serviços interage com o Provedor de Bilhetagem para saber a reputação do usuário e efetuar a mediação da transação, prosseguindo com a autenticação desse usuário (3° e 4° passos). O Provedor de Bilhetagem é uma entidade segura e certificada por uma Autoridade Certificadora

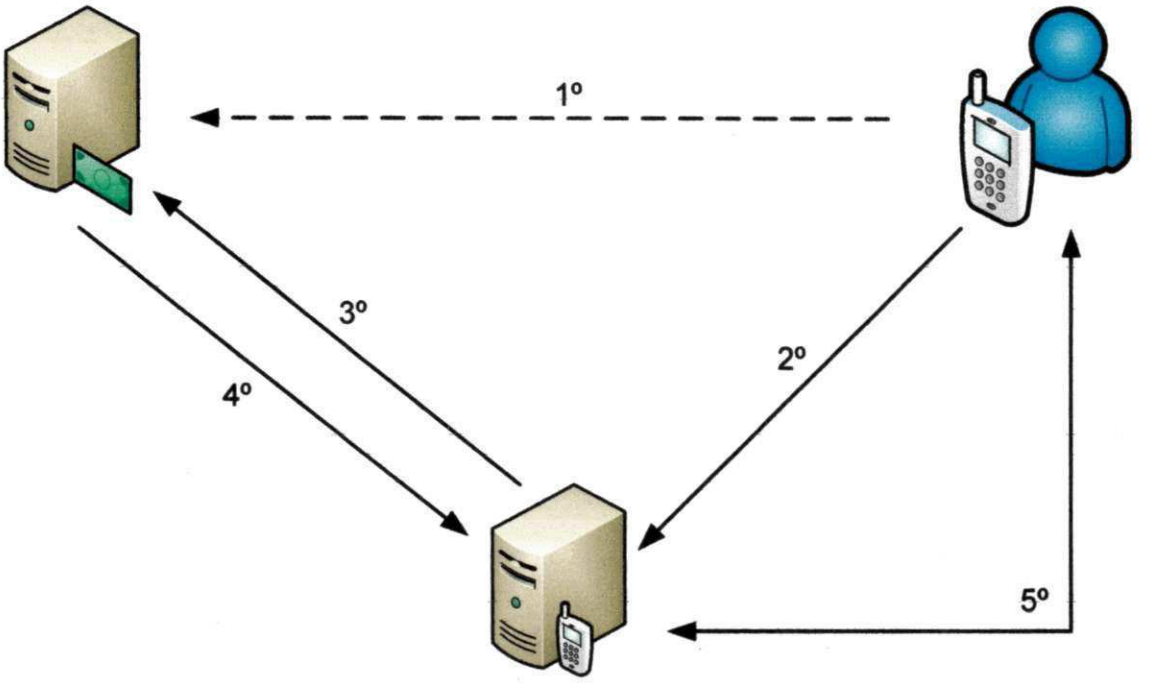


Figura 3.1: Arquitetura Green e Maknavicius

(como a VeriSign[2], por exemplo) que certifica os provedores de serviços de que os consumidores são quem eles realmente dizem ser, assinando toda as suas transações, exercendo também o papel de agenciador financeiro desses consumidores (3º e 4º passos). Por fim, em caso de autenticação confirmada, o serviço é consumido pelo usuário iniciador da transação (5º passo).

Embora Green e Maknavicius abordem a questão de segurança sugerindo meios confiáveis para efetuar transações entre usuários P2P, utilizando infraestrutura de chave pública e privada, autoridades certificadoras e outras formas de representação de conhecimento, a solução torna-se impraticável em ambientes pervasivos com ausência de acesso à Internet, meio de conexão utilizado para o estabelecimento da comunicação entre o Provedor de serviços e o Provedor de Bilhetagem. Por isso, essa necessidade de acesso à Internet juntamente à figura mediadora da transação é apontada como um problema em aberto a ser resolvido pelo cenário geral proposto neste trabalho de pesquisa.

[2]http://www.verisign.com.br/

- Pillai *et al.* [30] apresenta um sistema de bilhetagem para redes móveis baseado no conjunto de protocolos UPnP. Eles ampliaram a ideia do *framework* do UPnP para ambientes móveis, permitindo que pessoas em movimento, como a bordo de um veículo em trânsito, obtenham acesso à Internet e a outros serviços, como os de telefonia móvel. Eles fazem uso do ideal do *zero-configuration* do UPnP, que sugere a utilização de serviços sem a necessidade de configuração, para inserção dinâmica das redes móveis à outras redes, como as de telefonia. Esta solução assemelha-se a de Green e Maknavicius apenas no critério necessidade de acesso a Internet e entidade mediadora das transações. Os dois sistemas diferem no fato de que Pillai et al. baseou sua solução na arquitetura e protocolos do UPnP, apresentando uma estrutura diferente.

  A solução proposta por Pillai *et al.* faz uso dos benefícios do *Plug na Play*, permitindo o desenvolvimento de mecanismos de descoberta e consumo de serviços sem nenhuma configuração. Apesar disso, a infraestrutura apresentada é baseada e, portanto, amarrada a outras redes de comunicação. Os usuários que desejam comercializar serviços entre si devem também seguir o padrão da solução, contratando outras redes a fim de servir de canal para efetuar suas transações financeiras. Diante disso o usuário com impossibilidade de conexão com essas redes, como por exemplo, perda de sinal temporário da rede telefônica não estaria apto nem a vender nem a consumir serviços, o que não contempla o que está sendo proposto neste trabalho de pesquisa.

Transações que independem da localização do usuário é um pré-requisito para a comercialização entre pares acontecer em qualquer lugar. O objetivo dos trabalhos relacionados deste subgrupo é oferecer a comercialização de bens e serviços independente da localização do usuário.

3.1.2 Transações locais ou próximas

O critério de classificação dos trabalhos relacionados neste subgrupo é de que as partes envolvidas, para efetuar transações, devem estar próximas. O grau de proximidade neste caso depende da tecnologia de rede utilizada. No caso dos trabalhos que sugerem o uso da tecnologia de NFC, os dispositivos dos usuários devem estar a poucos centímetros de distância, o mesmo ocorre para os que sugerem o uso de Infravermelho. Outro exemplo

inserido nesta classificação são os modelos que possuem um POS (*Point of sale*)/ATM (*Automated Teller Machine*), como os sistemas de cartão de crédito. Nesse último, o usuário deve portar um cartão ou qualquer outro mecanismo de identificação, utilizado para autenticação e liberação de fundos.

- Lehdonvirta et al. [25] apresenta o Ubipay , um sistema que minimiza os custos da transação para o usuário na comercialização de bens e serviços. O Ubipay é um sistema embarcado para dispositivos móveis, que possui informações financeiras do usuário, como escala de valores e o registro de entidades confiáveis. O Ubipay tem como principais características a coleta de informações de contexto em tempo real, a análise de informações expressas pelo usuário armazenadas no dispositivo, a oferta de três diferentes métodos de interação e o registro de todas as transações efetuadas. O pagamento de bens e serviços é realizado através da checagem das preferências do usuário e informação de contexto da forma menos intrusiva possível para o portador do dispositivo móvel. A forma usada, bem como o nível de intrusão, é selecionada a partir do valor do bem a ser consumido. É de acordo com as faixas de valor expressas nas configurações do dispositivo em que se enquadra o bem, que a forma de liberação e pagamento do produto é estabelecida. A solução proposta por Lehdonvirta *et al.* visa o pagamento de bens e serviços através de uma rede local utilizando um dispositivo móvel como mecanismo de autorização do repasse monetário. Além disso, ele propõe a utilização de uma entidade confiável que efetua a transferência de fundos do consumidor para o comerciante do produto. Essa terceira parte envolvida pode ser um banco ou um agente financeiro mediador da transação. Essa entidade mediadora deve estar em constante comunicação com o dispositivo portado pelo usuário para o estabelecimento da comunicação e consequente autorização da transferência eletrônica. Diante disso, Lehdonvirta sugere com sua solução, a oferta de novas aplicações, com modelos de negócio diferentes, como a cobrança diferenciada de serviços (como assentos diferenciados em transportes e restaurantes), a utilização de heurísticas sobre os dados do histórico do usuário e a abertura do mercado para ambientes pervasivos.

  Da mesma forma que a solução proposta por Green e Maknavicius, o Ubipay necessita de conexão com a Internet, fato já esclarecido anteriormente. O Ubipay é

uma solução que não foi idealizada especificamente para usuários P2P, tratando-se de um modelo de negócio entre empresa e consumidor, o que não se assemelha aos cenários de comercialização propostos por este trabalho. Porém ele apresenta aspectos diferenciados em relação aos demais trabalhos relacionados citados, como a possibilidade de disponibilizar bilhetagem automática, dependendo do valor do serviço ou bem e o rastreamento das transações realizadas pelo usuário, que são características relevantes para o escopo desse trabalho.

- Balan et al. [4] apresenta em seu trabalho uma aplicação para pagamentos móveis P2P baseado na tecnologia *Near Field Communication* (NFC), o mFerio. O mFerio é uma aplicação móvel destinada a celulares com suporte a NFC, que oferece transferência de valores eletrônicos entre dispositivos. A motivação para o desenvolvimento dessa aplicação surgiu devido à falta de um sistema capaz de efetuar pagamentos móveis sem a necessidade de conexão com uma infraestrutura de servidores *back-end*por pelo uma das partes envolvidas no pagamento. Balan aponta essa necessidade de conexão das soluções atuais como um problema. As tecnologias de conectividade utilizadas nessas soluções são baseadas em mensagens de texto (SMS), redes de telefonia (GPRS, 3G) e Wi-Fi. As limitações dessas tecnologias são relacionadas como os problemas desses sistemas, como as soluções apresentadas por Green [8] e Pillai [30].

  O mFerio [4] é uma aplicação que foi desenvolvida para realizar pagamentos apenas através do contato entre celulares. Os autores da solução se preocuparam em satisfazer dois critérios de segurança, a segurança física, evitando o ataque pelo meio físico utilizado, uma das justificativas da adoção de NFC, e a segurança no processo de pagamento, evitando o ataque por alguma falha de sistema, explicando o desenvolvimento de um protocolo fechado à solução. Para Balan a preocupação com fraudes encontra-se em dois pontos, na criação e validação dos créditos eletrônicos e no protocolo de comunicação utilizado. A escolha pela tecnologia de NFC é justificada pela restrição de comunicação imposta pela própria tecnologia. Apesar de ser uma tecnologia sem fio, a comunicação entre os dispositivos só é estabelecida a poucos centímetros de distância, o que reduz a quantidade de ataques à rede estabelecida, como ataques de *man-in-the-middle* [28], por exemplo.

Uma das vantagens citada por Balan é a opção que o usuário tem de realizar suas transferências apenas para pessoas que ele pode manter um contato próximo, isto é, o usuário vê quem está participando da troca de créditos. Isto, porém, elimina o anonimato entre os usuários. Por outro lado, os autores oferecem a oportunidade de auditoria de sua aplicação. Essa auditoria é possível devido ao registro das transações, que é efetuada todas as vezes que há a troca dos créditos eletrônicos entre os usuários.

O mFerio apresenta como diferencial em relação as outras soluções discutidas anteriormente, a oportunidade de efetuar transferência de créditos eletrônicos entre usuários P2P sem a necessidade de conexão com a Internet durante a transação. Este é um dos objetivos deste trabalho de pesquisa, porém, para atender esse requisito, o mFerio exige a utilização exclusiva de celulares com suporte a NFC. Entretanto, exclusividade de tecnologia pode ser apontada como um risco para o projeto inteiro, o ideal seria uma infraestrutura de comercialização com serviços de pagamento P2P, independente da tecnologia de comunicação utilizada. Imaginando um cenário onde pessoas estão em um espetáculo de teatro, umas sentadas mais próximas do palco que outras, seria bem difícil a adoção do mFerio como solução de gravação do espetáculo por alguém que não esteja a alguns centímetros do provedor do serviço (por exemplo, alguém sentado na primeira fileira disponibilizando o serviço de gravação e outra pessoa sentada na fileira mais distante do palco querendo consumir um serviço de gravação da peça). No contexto do trabalho e desse exemplo, uma rede Wi-Fi resolveria esse problema de distância.

Os trabalhos citados neste grupo oferecem mecanismos de bilhetagem entre consumidores e empresas e entre pessoas. Esses trabalhos não contemplam uma infraestrutura de comercialização de serviços P2P independente da tecnologia de rede utilizada. Enquanto a primeira aplicação citada aplica-se apenas a cenários de comercialização B2C, inviabilizando casos de comercialização P2P, a segunda aplicação citada, o mFerio, necessita que os dispositivos utilizados pelas partes envolvidas no modelo proposto estejam à poucos centímetros de distância. Esta última característica identificada não permitiria o consumo de serviços que são disponibilizados a maiores distâncias entre os dispositivos.

3.2 Forma de cobrança

Este critério é determinado pelo método de cobrança, o momento de aquisição e repasse dos créditos eletrônicos. A forma de cobrança de sistemas de comércio eletrônico móveis pode ser efetuada antes do consumo de bens e serviços, após o consumo ou em tempo de execução.

3.2.1 Prépago

- O sistema de e-Cash pré-pago proposto por Kreft e Adi em [22] apresenta uma carteira eletrônica baseada em uma tecnologia de *hardware*, protegida contra violações, que armazena dinheiro eletrônico. A proposta de Kreft e Adi foi criar um sistema capaz de trocar valores eletrônicos entre dispositivos de forma segura, *off-line* [3] e que os *tokens* trocados pudessem ser repassados ou reutilizados com outras pessoas que também possuíssem dispositivos com a mesma tecnologia de *hardware* proposta. O cenário geral descrito em [22] apresenta três entidades diferentes, cada uma delas também representa uma operação diferente da solução. A primeira entidade seria a e-Wallet (carteira eletrônica), que é um dispositivo móvel que contém um chip que guarda os créditos eletrônicos e a chave para a assinatura digital do dono do dispositivo. A produção desse dispositivo depende de uma Autoridade Certificadora que proverá a solução de autenticação do sistema durante o período de troca dos *tokens* eletrônicos.

O sistema e-Cash funciona similar a um cartão de vale-transporte. É preciso carregar o cartão para poder utilizá-lo no transporte público. A carga desse cartão é realizada antes do usuário utilizá-lo como forma de pagamento. Essa característica de carregar créditos em um dispositivo antes da ação da bilhetagem apresentada pelo sistema e-Cash é um dos aspectos observados no estado da arte que viabilizaria a bilhetagem de serviços móveis entre pares. A troca de créditos eletrônicos se torna possível já que um dos usuários está apto à transferência pelo fato de portar créditos eletrônicos em seu dispositivo.

[3] A definição da forma de validação *off-line* de créditos eletrônicos será discutida na seção 3.3 de validação dos créditos eletrônicos trocados, deste capítulo.

3.2.2 Póspago

- "A Cielo inovou lançando o primeiro aplicativo que transforma o iPhone®, iPad®, iPod touch® ou smartphone e tablet com Android® em uma máquina da Cielo®. Com este aplicativo os profissionais liberais podem aceitar os principais cartões de crédito: Visa®, MasterCard®, American Express®, Elo® e, em breve Paggo® de forma rápida e simples. Para garantir a integridade dessas transações, esta solução assegura que os dados são criptografados e que nenhuma informação permanece armazenada no aparelho. Indicado para médicos, dentistas, advogados, outros profissionais liberais e estabelecimentos que necessitam de praticidade e mobilidade no seu dia a dia." (Cielo[4], 2011).

  Essa é a publicidade anunciada pela empresa Cielo®, uma empresa que oferece soluções em tecnologia de pagamentos para os diversos segmentos comerciais. A Cielo®, lançou no mercado um *software* para dispositivos móveis que funciona como um POS. Esta aplicação oferece ao lojista a capacidade de utilizar o cartão de crédito de um cliente como se o mesmo estivesse passando o cartão em um POS. A Cielo® afirma que, assim como um terminal POS, a nova solução segue as regras estabelecidas pelo padrão PCI (*Payment Card Industry*[5]), que prevê que os dados do pagamento sejam criptografados e que nenhuma informação do cartão fique armazenada nos aparelhos. Diante disso, a cobrança da operação realizada só será feita após o consumo do serviço ou compra do bem. Mais informações sobre o produto da Cielo® basta acessar o *site* que está disponível na WEB.

O modelo pós-pago é similar à forma de pagamento por cartão de crédito, onde o cliente e o provedor do serviço são faturados após a comercialização do serviço. É um modelo que não se adequaria a proposta de bilhetagem entre pares, já que os créditos eletrônicos não são transferidos em tempo de execução como no modelo pré-pago, porém demonstra a viabilidade de bilhetagem de serviços móveis em ambientes pervasivos com faturamento póstumo do serviço.

[4]http://www.cielo.com.br/portal/iphone_android/home.html

[5]https://www.pcisecuritystandards.org/

3.2.3 Pagamento em tempo de execução

- As aplicações que se encaixam dentro desta classificação poderiam também se enquadrar no modelo pré-pago. Tudo que foi discutido sobre o modelo pré-pago se aplica as aplicações que realizam o pagamento em tempo de execução. A diferença entre eles é que os casos classificados como em tempo de execução apresentam a característica de prover o pagamento ao mesmo tempo em que o serviço está sendo provido. Um exemplo disso é o SEMOPS [9] que oferece um meio de bilhetagem de um serviço durante o provimento do mesmo. Exemplo disso seria a transmissão de um fluxo de vídeo. Ao mesmo tempo em que os bytes do vídeo estão sendo decodificados e enviados para o consumidor, a bilhetagem está sendo realizada e os créditos estão sendo transferidos entre os dispositivos, como se a cada instante de tempo, esse modelo realizasse o mesmo que as aplicações do grupo pré-pago fazem.

Os trabalhos citados neste grupo apresentam formas de transferências de créditos entre os usuários de um sistema de bilhetagem. Os trabalhos citados nos grupos pré-pago e em tempo de execução oferecem mecanismos de transferência de créditos eletrônicos nas operações de bilhetagem entre consumidores em redes pervasivas, sugerindo que a hipótese levantada neste trabalho é possível no critério transferência de créditos entre pessoas, sem a necessidade de conexão com a Internet durante as transações entre os usuários.

3.3 Validação dos créditos eletrônicos trocados

A validação dos créditos eletrônicos trocados, é a classificação que vai analisar como a moeda que serve de pagamento para a bilhetagem de recursos é validada, se necessita de entidade mediadora confiável e se precisa de conexão com a Internet a todo tempo. A validação é o processo que determina se o dinheiro eletrônico que irá ser transferido é válido ou não. Essa classificação subdivide-se em *Online* e *Offline*.

3.3.1 *Online*

- A validação *Online* dos créditos eletrônicos é o tipo de validação que ocorre com o auxílio de uma terceira entidade confiável e mediadora da transação, isto é, precisa de

conexão com a Internet durante a transação. Todos os trabalhos apresentados até aqui se encaixam neste perfil. Portanto, exemplos e referências para esta classificação foram apresentados anteriormente neste mesmo capítulo. Qualquer solução que faça uso de entidades mediadoras ou necessite de conexão com a Internet, durante a transação, para validação dos créditos trocados pode ser classificada também como uma solução cuja validação dos créditos eletrônicos trocados é *Online*.

3.3.2 *Offline*

A validação *Offline* dos créditos eletrônicos é o ponto principal deste trabalho. Trata-se da capacidade que a solução tem de validar os créditos eletrônicos trocados, que servem como moeda de pagamento, sem a necessidade de uma terceira entidade confiável e mediadora da transação, isto é, também sem a necessidade de conexão com a Internet durante a transação. Todos os trabalhos apresentados até aqui não oferecem algo que se enquadre nesta definição exceto o trabalho descrito a seguir.

- Na economia de hoje em dia os aplicativos móveis podem ser facilmente aplicáveis para o pagamento de bens e serviços. A falta de tal capacidade no mundo da Internet é um obstáculo fundamental que deve ser superado, a fim de conectar todas as partes e os usuários. O fairCASH [6] é uma solução oferece um sistema de transação segura distribuído que protege a privacidade do cliente. fairCASH é o primeiro sistema mundial de Dinheiro Digital que tem todas as características do dinheiro tradicional, acrescentando características contemporâneas de comunicação: é utilizável como moeda dentro da Internet; transferências ilimitadas entre todos os usuários; incondicionalmente anônimo; não é necessário nenhum registro antes de usar o fairCASH nos estabelecimentos credenciados; funcional, mesmo que a infraestrutura da Internet não esteja disponível; segurança jurídica, devido à geração automática de recibos; capacidades de reembolso limitado; livre de taxas ou custos de transação para usuários privativos. O fairCASH não é considerado uma nova moeda, mas sim uma forma inovadora de incentivo e tentativa de complementar o sistema de dinheiro físico.

  A solução proposta pelo autor combina tecnologia de *hardware* e de *software* com o intuito de realizar transações pré-pagas e-Cash, imitando o comportamento do dinheiro

físico. Dessa maneira ele evolui a forma executar pagamentos. O sistema fairCASH propõe um protocolo de transferência baseada em técnicas criptográficas mais avançadas, as assinaturas digitais, e o uso de criptografia de chave pública e privada intimamente ligado ao e-Wallet. Essa e-Wallet é a carteira eletrônica que armazena o dinheiro digital. Ele também oferece um nível de anonimato bem abrangente para indivíduos, bem como transações seguras e robustas para bancos e comerciantes, respectivamente. O fairCASH oferece a capacidade de repasse do dinheiro digital entre seus usuários em combinação com o não-repúdio do que foi repassado. Estas duas características são importantes para a solução de pagamentos privados através da Internet ou conexões sem fio de curto alcance, que permite transferências diretas de dinheiro P2P sem a intermediação de uma entidade funcionando como um banco ou agente, uma vez que o não repúdio não permite que um usuário negue seus atos e o repasse de dinheiro digital funciona similar ao repasse de dinheiro real. Essa característica de não repúdio, associado a identificação por chaves, torna-se o principal método para uma troca segura de moedas eletrônicas (e-Coins) entre dois dispositivos protegidos (e-Wallets).

O fairCASH é uma solução que é baseada em *hardware*. O conceito de e-Wallet que ele apresenta é um chip que contém todas as funções propostas pelo autor. Portanto para que a solução do autor seja utilizada de forma abrangente, os dispositivos móveis devem possuir esse chip, como vários deles já possuem chips de *GPS*, por exemplo. O fairCASH foi a primeira solução que oferece a validação dos créditos sem a necessidade de conexão com a Internet durante a transação, que é o que se pretende verificar neste trabalho de pesquisa. Portanto o fairCASH é um exemplo de aplicação que já sugere que a hipótese levantada nos objetivos deste trabalho de pesquisa são possíveis. O problema deste trabalho é que a solução parece inviável a curto e médio prazo pelo fato de que nenhum dos aparelhos que móveis que existem hoje estariam aptos ao uso desta solução, já que nenhum deles possui o chip (chamado chip CASTOR) imprescindível para o funcionamento do sistema fairCASH.

Os trabalhos citados neste capítulo serviram de base teórica para o desenvolvimento da solução e como fonte de pesquisa para a elaboração do estudo de caso deste trabalho.

Capítulo 4

A Infraestrutura

4.1 Visão Geral

A infraestrutura desenvolvida neste trabalho disponibiliza uma forma de bilhetagem voltada a aplicações que realizem a comercialização de bens e serviços móveis. Entende-se por bens e serviços móveis os diversos recursos oferecidos pelos dispositivos móveis encontrados no mercado de aparelhos móveis.

O sistema tem uma arquitetura híbrida, a qual é possível distinguir um arquitetura P2P que envolve diretamente a interação entre dois usuários e um serviço de sincronização de usuários com a infraestrutura desenvolvida, que apresenta uma arquitetura cliente/servidor. A Figura 4.1 ilustra a disposição dessa estrutura híbrida onde é possível identificar a parte da arquitetura P2P e a parte cliente/servidor.

Para fazer parte de toda essa estrutura o desenvolvedor deve adicionar em sua aplicação a biblioteca de desenvolvimento que oferece o suporte a bilhetagem e o acesso a todo o sistema. Desta forma, os usuários que possuem em seus dispositivos aplicações com suporte a bilhetagem, iniciam a interação com a infraestrutura a partir da comunicação com uma agência virtual, ou *Internet banking* (agência virtual disponível na WEB) de sua própria residência. Nessa primeira etapa o usuário deve sincronizar sua aplicação e efetuar um saque de créditos eletrônicos em seu dispositivo. Este dispositivo funciona como uma e-Wallet, discutida no capítulo de trabalhos relacionados na subseção que apresenta o fairCash.

A infraestrutura apresenta três diferentes componentes em seu modelo de funcionamento: o componente que emite e assina o dinheiro eletrônico é o Banco Central Virtual, que

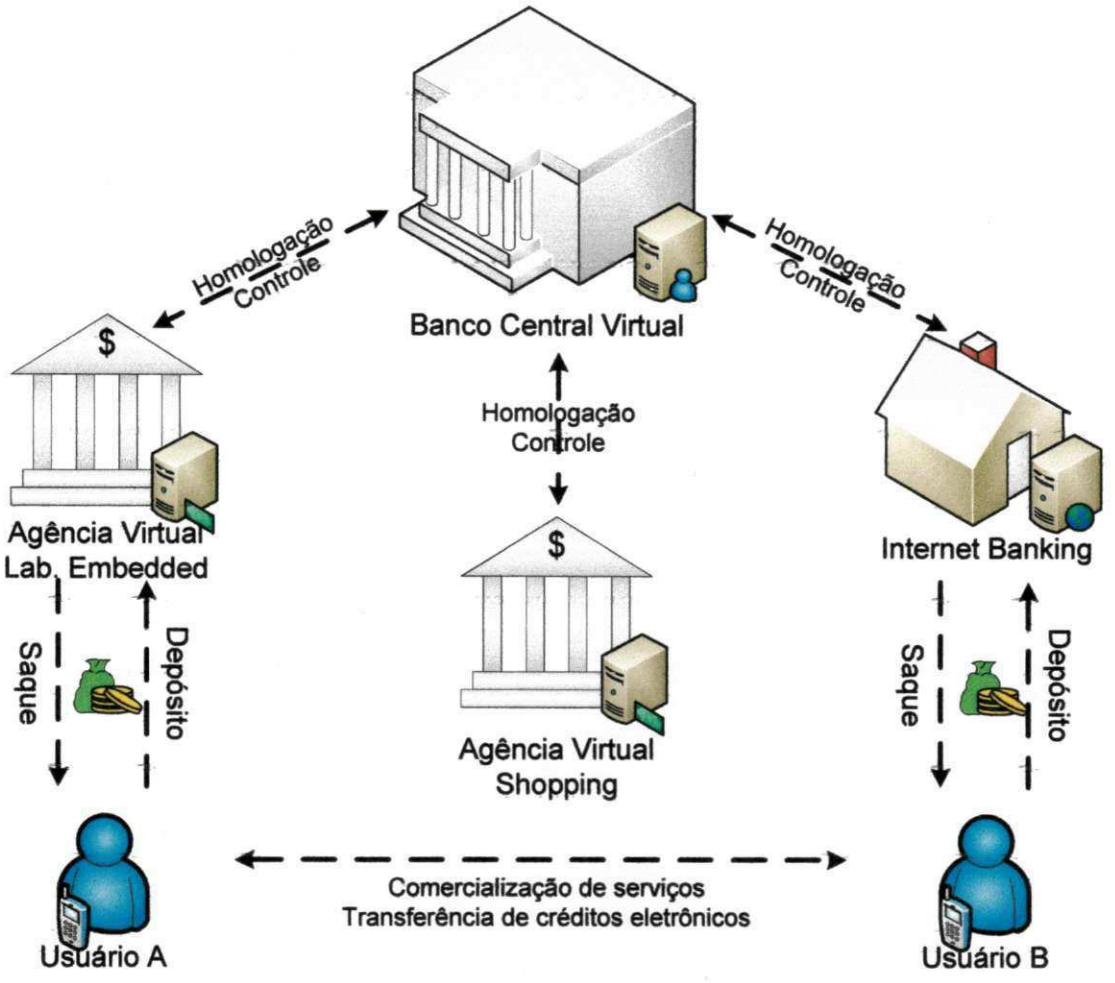


Figura 4.1: Visão geral arquitetura da infraestrutura

nessa infraestrutura é um serviço WEB; agências Virtuais também são componentes dessa infraestrutura, que são autorizadas pelo Banco Central Virtual a repassar e a receber dinheiro eletrônico em seu nome, abstraindo para o usuário as ações de saque e depósito que seriam efetuadas direto no Banco Central Virtual; o terceiro componente é a aplicação cliente, que participa desse cenário através do uso de uma e-Wallet instalada em um dispositivo móvel.

Portando uma e-Wallet, o usuário pode oferecer ou consumir serviços móveis disponíveis no ambiente em que ele se encontra. Um exemplo disso seria a disponibilização de um serviço de envio de mensagens SMS, que encaminha uma mensagem escrita no formato texto, para dispositivos celulares a partir da transferência de um arquivo. Desta forma, a aplicação servidora pode efetuar a bilhetagem do usuário consumidor e receber os créditos eletrônicos pelo serviço prestado durante a transação.

Ainda, os usuários podem realizar o saque de créditos eletrônicos, o depósito de créditos recebidos e a sincronização da aplicação para a atualização dos registros trocados e dados gerados. Os usuários também podem efetuar a transferência de créditos eletrônicos de forma análoga a um pagamento em dinheiro, realizado por duas pessoas motivada por uma prestação de serviço. Um crédito eletrônico é uma representação virtual do dinheiro real. O dinheiro virtual pode ser adquirido em uma Agência Virtual da mesma forma que a compra de um produto. A taxa de conversão entre o dinheiro real e o virtual não faz parte do escopo desse trabalho, por isso, é tomado como referência a conversão de um para um.

As atribuições, características e detalhamento dos componentes da arquitetura geral proposta neste trabalho são discutidos nas seções seguintes.

4.1.1 Uso de um sistema de Arquivos Criptografado

Para garantir a segurança do armazenamento dos dados nos dispositivos dos usuários da infraestrutura, é necessário a utilização de um repositório que não permita alteração de dados senão pelas rotinas sistêmicas desenvolvidas para isso. Além disso, esse repositório utilizado deve prover a integridade dos dados, e portanto, não pode ser fácil a "quebra" de sua segurança. Diante desses aspectos, foi escolhido um sistema de arquivos que oferece a criptografia de todos os registros que são armazenados nele.

O sistema de arquivos que oferece a criptografia utilizado é o eCryptfs[1] [35], um sistema de arquivos disponível nas distribuições do Linux que instala um sistema de arquivos virtual por cima de sistemas de arquivos UNIX, como o EXT3. Ele é um sistema de arquivos virtual que disponibiliza a criptografia de todos os registros armazenados nele. Ele tem as operações e funções básicas de um sistema de arquivos e a função de criptografia. A escolha pelo eCryptfs deve-se ao fato dele aceitar chaves de criptografia para autenticação.

Para criptografar os registros, o eCryptfs precisa de uma chave. Esta chave é uma chave criptografada com o algoritmo AES [18]. A infraestrutura mantém essa chave armazenada no Banco Central Virtual e não divulga nem distribui a nenhuma outra entidade abertamente. Porém essa chave é disponibilizada junto a biblioteca de desenvolvimento compilada no código fonte da biblioteca. Para aumentar a segurança contra quebra esta chave é obfuscada dentro do código. Mesmo assim, uma política da infraestrutura é a mudança periódica dessa

[1] https://launchpad.net/ecryptfs

chave e consequente atualização da versão da biblioteca.

É nesse sistema de arquivos criptografado que a maior parte das informações do sistema, no módulo Cliente, fica armazenado. No decorrer desse capítulo, é possível perceber mais claramente o uso do eCryptfs.

4.2 Banco Central Virtual

O Banco Central Virtual - BCV é a entidade do modelo que é responsável pela centralização e armazenamento de todas as informações da infraestrutura. Nele estão armazenados todos os dados cadastrais dos usuários do sistema, estão armazenadas todas as chaves de segurança utilizadas para criptografia tanto do sistema quanto dos usuários. Guarda também as informações e permissões de acesso das Agências Virtuais, componente que é descrito na seção seguinte. A Figura 4.2 ilustra os serviços que o Banco Central Virtual realiza na infraestrutura.

Uma das atribuições desse componente é disponibilizar serviços para os usuários e Agências Virtuais. Os serviços oferecidos diretamente aos usuários do sistema são aqueles oferecidos de forma semelhante por um Internet Banking, são eles: saque de créditos eletrônicos, depósito de créditos, consulta de saldo e histórico, sincronização da aplicação e atualização dos créditos. O saque e o depósito funcionam de modo similar as ações realizadas em um Banco físico, com a diferença de que o dinheiro eletrônico é guardado na e-Wallet [6] do usuário. A consulta de saldo e histórico também é similar as ações realizadas em um banco físico. A sincronização da aplicação é uma operação que faz a checagem da e-Wallet a fim de rastrear inconsistências nos dados, atualizar as chaves da aplicação, verificar a versão da biblioteca utilizada pelo aplicativo móvel e atualizar o dinheiro eletrônico. A atualização desse dinheiro é uma solução que força o usuário a manter-se periodicamente realizando esta ação. Dessa forma, ele garante que os créditos que ele porta em sua carteira virtual está sempre atualizado e reduz a probabilidade de que aquele crédito seja inválido. O detalhamento dessas operações são descritas na seção que apresenta as atribuições e características das Agências Virtuais. Já o detalhamento da utilização, controle das chaves de criptografia e assinatura digital são descritas nas subseções a seguir.

O Banco Central Virtual também é responsável pela emissão do dinheiro virtual utilizado

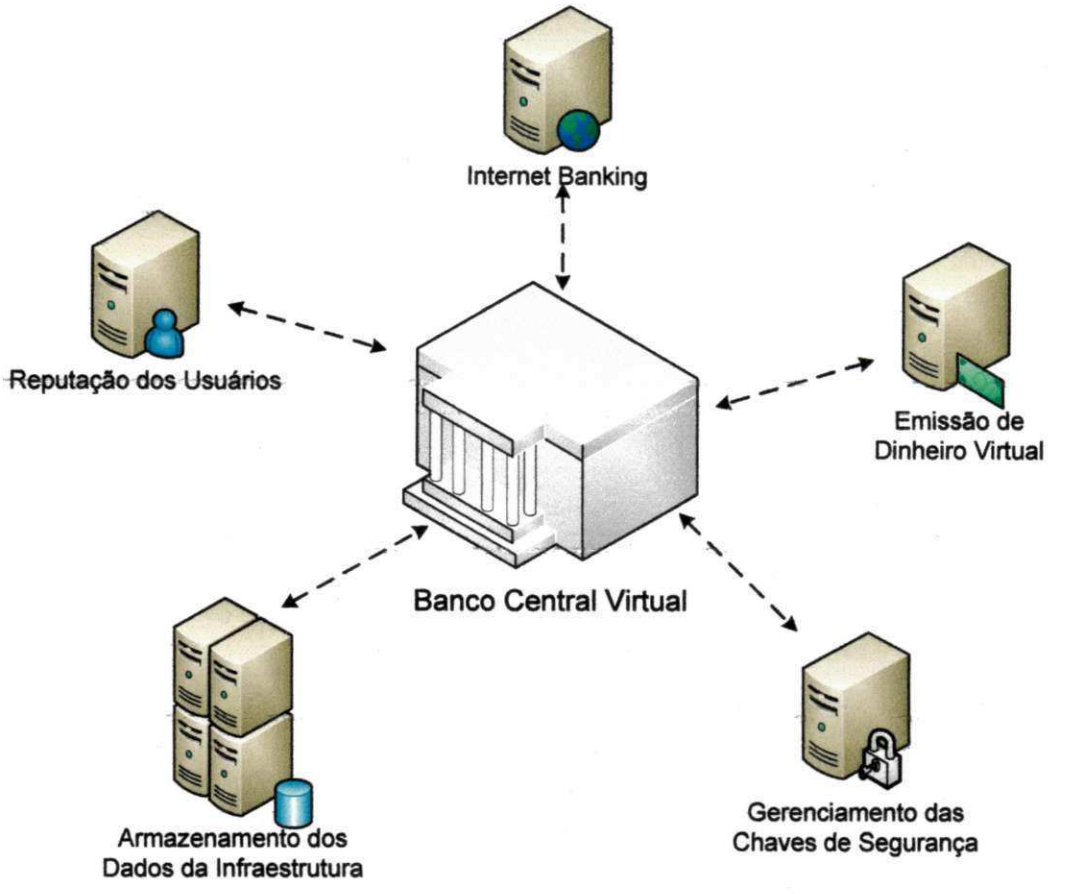


Figura 4.2: Atribuições do Banco Central Virtual

pelos usuários e pelo controle de reputação dos usuários. Essas duas características geridas por este componente são detalhadas nas subseções a seguir.

4.2.1 Dinheiro Virtual

O dinheiro virtual é a representação de valores monetários dentro do sistema. Esse dinheiro não é o mesmo que o dinheiro físico, mas pode ser uma representação eletrônica dele também. A nível de estrutura de dados a representação desse crédito virtual é um objeto que contém dois atributos, como mostra o quadro em evidência nomeado Dinheiro Virtual na Figura 4.3. É possível identificar na parte superior direita da Figura 4.3 que o dinheiro é um registro que contém um valor e uma data de validade. O valor é do tipo número real e a data de validade é do tipo data, composta por ano, mês e dia.

No sistema, esse dinheiro virtual é assinado com uma chave de criptografia, a chave

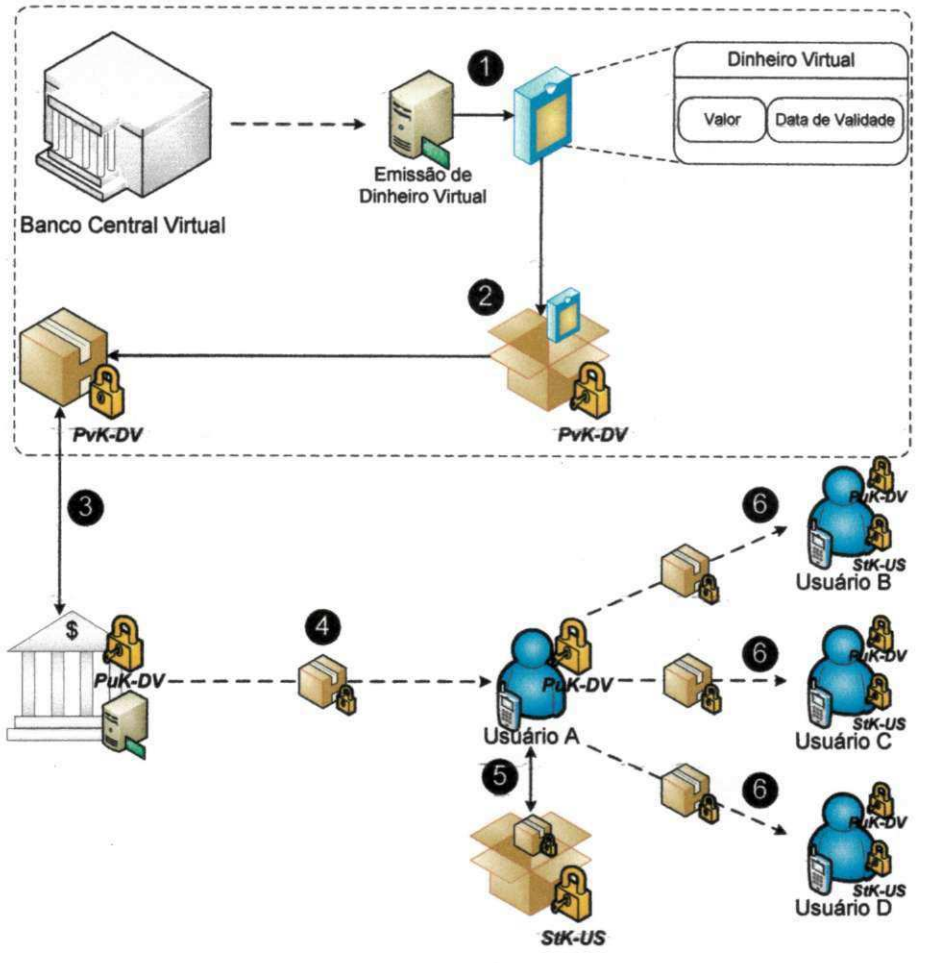


Figura 4.3: Cenário de emissão e distribuição do dinheiro virtual

privada de assinatura de dinheiro virtual (PvK-DV). A correspondente chave pública (PuK-DV) dessa chave privada é distribuída junto a biblioteca de desenvolvimento e deve fazer parte das aplicações móveis que oferecerem o suporte a bilhetagem. Portanto deve ser de conhecimento de todos da infraestrutura a chave pública de assinatura de dinheiro virtual. É possível verificar na Figura 4.3 o cenário de emissão e distribuição de um dinheiro eletrônico. Este esquema garante que os aplicativos reconheçam a validade do dinheiro virtual devido a assinatura realizada com a PvK-DV, que é de posse apenas do Banco Central Virtual. Como todos os aplicativos com suporte a bilhetagem possuem a PuK-DV, elas verificam a nível de *software* a validade de um crédito eletrônico recebido. Caso alguém tente decriptar um crédito com a chave pública e tentar replicar esse crédito indeterminadamente, esse dinheiro falso perde a validade para o sistema. A primeira rotina de checagem do dinheiro eletrônico verifica sua validade, isto é, é executada uma função de descriptografia

daquele registo com a PuK-DV. O retorno dessa função só é positiva caso o crédito eletrônico verificado tenha sido assinado com a respectiva chave privada da PuK-DV, a chave PvK-DV. Tal chave é mantida de forma segura pelo Banco Central Virtual e não é distribuída a nenhum outro componente da arquitetura. Em caso de divulgação da chave PvK-DV, o Banco Central Virtual deve imediatamente realizar a mudança dessa chave e comunicar a todos os usuários do sistema, através dos veículos de comunicação em massa disponíveis como redes sociais, correio eletrônico, SMS, entre outros, a troca da chave e disponibilizar a nova chave pública para atualização.

A seguir serão detalhadas mais algumas características do dinheiro eletrônico.

Validade do dinheiro virtual

Um dos recursos oferecidos na arquitetura geral do sistema é a possibilidade de checagem da validade de um crédito eletrônico. Quando o registro eletrônico de um crédito é gerado, ele contém o valor e uma data de validade. Esta data de validade faz parte do dinheiro virtual. Este mecanismo de validade de uma cédula virtual serve para que os usuários verifiquem periodicamente a situação do dinheiro de sua carteira eletrônica [6]. Os objetivos de impor uma data de validade ao dinheiro virtual são a redução de riscos na troca de cédulas emitidas a muito tempo e o estímulo a sincronização dos usuários com a infraestrutura. Uma cédula eletrônica que tem sua validade considerada expirada pela aplicação pode representar um risco maior de ter sofrido alguma alteração, como um ataque de *multi-spending* explicado na subseção a seguir. Na prática, esse recurso oferece ao usuário um mecanismo de verificação de idade da cédula virtual. Quanto mais distante for a validade de uma cédula virtual, comparada a data corrente de uma transação, significa que aquele crédito foi emitido ou atualizado a pouco tempo. Isso pode representar para o usuário mais conforto ou segurança, já que uma aplicativo móvel com suporte a bilhetagem pode utilizar este recurso para não aceitar dinheiro virtual com a data de validade vencida, visando a redução de riscos. Este recurso pode ser utilizado de outras formas pelos aplicativos móveis, como ,por exemplo, para comparação da idade de cédulas virtuais de diferentes usuários como forma de decisão por qual consumidor deve ser atendido primeiro por um provedor de serviços móveis.

Para a infraestrutura, o intuito desse recurso é análogo a imposição que as operadoras de telefonia móvel fazem aos seus clientes pré-pagos. A operadora de Telefonia aplica validade

aos créditos comprados por um cliente para obrigá-lo constantemente a comprar mais créditos, caso contrário seus créditos ficam retidos pela operadora até a próxima recarga. Neste trabalho a validade do dinheiro virtual tem como objetivo para a infraestrutura, forçar os usuários a atualizar o maior números de vezes seus aplicativos móveis. Dessa forma, o sistema se mantém atualizado, com a base de dados de reputação dos usuários também atualizados, além de facilitar possíveis atualizações de *software*, como chaves de segurança utilizadas na infraestrutura e outros registros.

Multi-spending

No trabalho de Ching e Kreft em [6], o conceito de *Multi-spending* é tratado como uma forma ilegal e fora dos padrões de uma infraestrutura de bilhetagem. O *Multi-spending* é considerado um ataque ao sistema. É a possibilidade de repassar a mesma cédula virtual mais de uma vez a diversos usuários do sistema. Sendo assim, um usuário praticante do *Multi-spending* pode repassar aquela cédula virtual indeterminadamente.

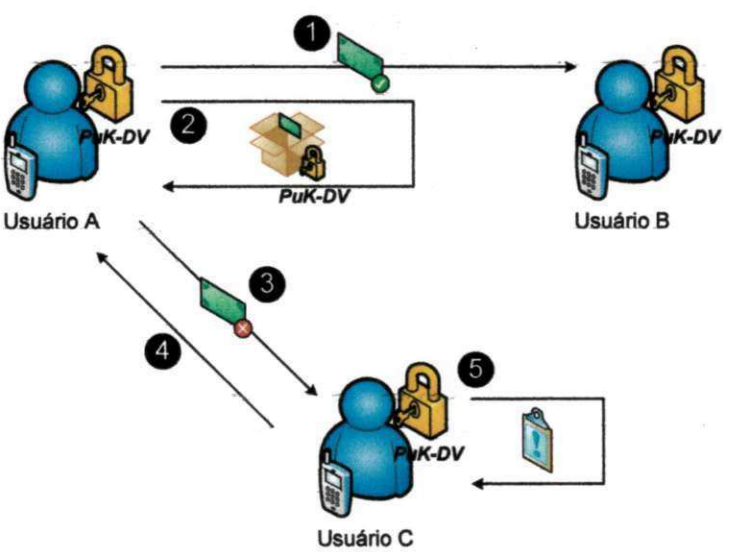


Figura 4.4: Exemplo de *Multi-spending*

Para evitar este problema a infraestrutura proposta nesse trabalho utiliza um mecanismo de invalidade da cédula virtual após seu repasse. Ao invés de a aplicação transferir o crédito na forma de recortar e enviar, ela transfere na forma de copiar e enviar. Para solucionar possíveis ataques de *Multi-spending*, a aplicação, automaticamente após o envio da cédula virtual, invalida esse dinheiro no dispositivo que executou o repasse. O processo para

invalidar uma cédula também é baseada em chaves de criptografia. Assim que a cédula é enviada, o *software* aplica nela uma criptografia com a chave pública PuK-DV. Então, quando o usuário for tentar repassar novamente essa cédula, será impossível de restaurar seu estado inicial sem a respectiva chave privada. O único componente da arquitetura que possui essa chave é o Banco Central Virtual. Portanto não é mais possível reutilizar uma cédula virtual repassada adiante.

A Figura 4.4 ilustra o processo de invalidação do dinheiro virtual e uma tentativa de ataque por *Multi-spending*. Na Figura 4.4 é possível perceber que após o repasse da cédula virtual (passo 1), a aplicação do usuário A criptografa a cédula com a chave pública de assinatura de dinheiro virtual em seu dispositivo (passo 2). Ao tentar reenviar a mesma cédula (passo 3), dessa vez para outro usuário, a estrutura eletrônica do dinheiro não é mais uma estrutura válida para o sistema. Portanto, quando o usuário C reconhece que o dinheiro que estão tentando repassar para ele é falso, ele cancela a transação (passo 4) e registra na base de dados do seu dispositivo que o Usuário A tentou realizar um *Multi-spending* (passo 5). Na próxima sincronização de aplicativo do usuário C, o sistema será atualizado com os dados da tentativa do ataque.

Se o aplicativo móvel foi desenvolvido para que a transferência dos créditos eletrônicos seja realizada antes, após ou durante o consumo do serviço, a verificação do ataque de *Multi-spending* não sofre alterações. Cabe ao desenvolvedor optar pela melhor forma de utilizar a verificação de *Multi-spending* em seus aplicativos.

Rastreamento e Auditoria

Quando um crédito eletrônico é repassado para o próximo usuário, é também enviado a informação de rastreamento daquele crédito. O rastreamento do dinheiro é composto por uma fila de elementos. Cada elemento contém um código *hash* correspondente ao identificador de cada usuário que utilizou o dinheiro. Essa lista de identificadores representa o histórico da cédula virtual. Cada vez que o dinheiro é repassado adiante, o aplicativo deve guardar essa informação. Na próxima sincronização esses dados são enviados ao Banco Central Virtual. Diante das informações do histórico do dinheiro virtual o BCV pode rastrear os usuários que receberam e repassaram a cédula. Assim, quando for detectado alguma inconsistência de dados, ou detectado tentativas de ataque ao sistema, esse esquema de

rastreamento serve como ferramenta de auditoria de dados para investigar quais usuários manipularam as cédulas marcadas como problemas.

4.2.2 Reputação

O serviço de reputação oferecido pelo Banco Central Virtual serve para classificar os usuários em termos de confiabilidade e restrição. Esse serviço oferece duas funções: a função de pontuação dos usuários e a função de serviço de proteção aos usuários. Todas as informações de reputação dos usuários ficam armazenadas no Banco Central Virtual e são disponibilizadas às Agências Virtuais por um serviço de consulta. Essas informações também são disponibilizadas para que os usuários possam carregá-las em suas aplicações. Com esses dados é possível identificar se alguém está marcado no sistema com restrições ou se um usuário possui um ranqueamento alto o que demonstra, por exemplo, que ele é considerado confiável para a infraestrutura.

A identificação de um usuário por outro é feita através de uma comparação de códigos *hash* de identificadores de usuários. Os valores desses identificadores são conhecidos apenas pelo Banco Central Virtual. O Banco disponibiliza e distribui apenas o código *hash* dos identificadores para avaliação da reputação. Além disso, cada usuário guarda em seu sistema de arquivos criptografado, o valor real de seu identificador na infraestrutura. Mesmo assim, essa informação não fica acessível de forma plana para ele. Quando ele envia sua identificação para comparações, ela trafega codificada. A Figura 4.5 ilustra o cenário de distribuição de um ID de um usuário que possui uma restrição no sistema. Por exemplo, o usuário é avaliado pelo sistema como um perigo e por isso recebe um marcação negativa para que outros usuários não transacionem com ele. Os passos destacados na Figura 4.5 são enumerados a seguir:

- No passo 1 ilustra-se o cadastro do usuário no sistema e a geração do seu identificador. A representação da identificação deste usuário é um número inteiro. Um exemplo da numeração utilizada é a concatenação do ano corrente com uma sequência numérica de tamanho definido. A Figura 4.5 ilustra esse exemplo.

- O passo 2 destaca a execução do algoritmo de codificação utilizado para gerar o *mesasge digest* do identificador do usuário. Existem vários algoritmos de *hashing*

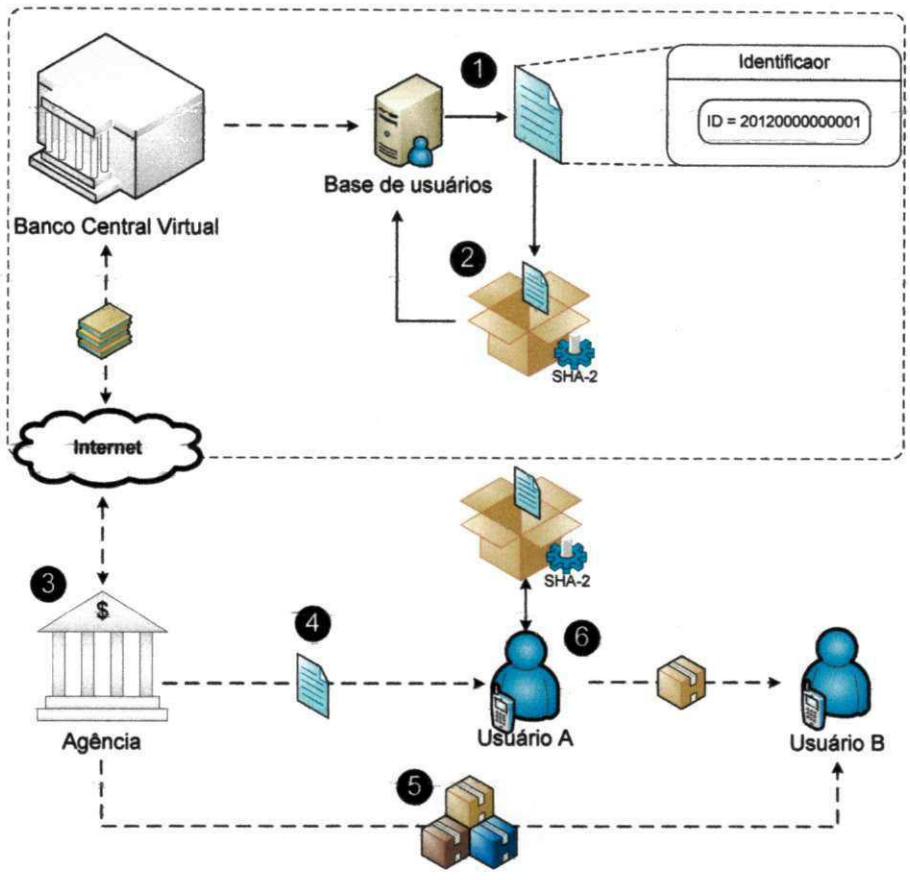


Figura 4.5: Cenário de distribuição e disponibilização de identificadores de usuários

disponíveis. Um algoritmo de *hashing* transforma uma palavra ou chave em um código. A partir deste código considera-se que é praticamente impossível conhecer a palavra utilizada para sua geração. Um exemplo de algoritmo de *hashing* é o SHA [19] que a partir do identificador do usuário pode gerar códigos *hash* de até 512 bits. Na Figura 4.5 é possível identificar que o algoritmo de codificação utilizado foi o SHA.

- O passo 3 trata dos serviços disponibilizados pelo Banco Central Virtual às Agências Virtuais. Serviços de consulta e distribuição dos códigos *hash* dos identificadores dos usuários do sistema e um serviço de tunelamento de distribuição do identificador (plano, sem codificação) para o respectivo usuário.

- O passo 4 demonstra uma sincronização de aplicativo realizada por um usuário junto a uma Agência Virtual. Nesta etapa o usuário recebe o seu ID na infraestrutura e armazena o dado no sistema de arquivos criptografado. Esse processo é realizado na

fase de instalação e configuração do aplicativo móvel.

- O passo 5 também demonstra uma sincronização de aplicativo realizada por um usuário. Só que nesta etapa, o usuário recebe uma lista de identificadores codificados (Passo 2). Cada elemento dessa lista representa um usuário. Além disso, cada elemento tem as informações de reputação do respectivo usuário: informações de pontuação e status do serviço de proteção ao usuário.

- O passo 6 exemplifica a execução de uma verificação que um provedor de serviços realiza dos dados de reputação que o consumidor tem armazenado em seu dispositivo sem poder de alteração. Cabe aos usuários o julgamento da reputação de outros usuários. É oferecido a todos, a pontuação de cada usuário no sistema e seu status do Serviço de Proteção ao Usuário. É também decisão de cada usuário realizar transações com outras pessoas que não constam registros de sua reputação na base de dados do dispositivo.

Pontuação de Usuários

O esquema de pontuação oferecido é semelhante ao esquema utilizado pelas aplicações WEB de comércio eletrônico, como o caso do Mercado Livre. Nesse *site* a reputação dos vendedores é baseado nas qualificações recebidas (positivas ou negativas) e pela quantidade de vendas concretizadas ou canceladas. Neste trabalho o esquema de pontuação é controlado pelo Banco Central Virtual, que qualifica os usuários baseado apenas na quantidade de transações realizadas com sucesso, isto é, se o recurso foi entregue ou não. O aplicativo do usuário consumidor, após a finalização da transação e pagamento pelo consumo do recurso, devolve para o provedor uma confirmação da transação. Esta confirmação é armazenada localmente no dispositivo do provedor do recurso. Posteriormente durante uma sincronização de aplicativo, essa informação é minerada por uma Agência ou pelo Banco virtual que atualiza o cadastro do usuário e consequentemente sua reputação na infraestrutura. Portanto o crescimento da quantidade de confirmações positivas registradas em nome de um usuário, aumentam sua pontuação.

Uma das etapas da sincronização é o *download* dessas informações de pontuação, que calculados pelo Banco Central servem para os usuários como uma ferramenta de decisão.

Esta ferramenta auxilia o consumidor ou provedor no momento da decisão em aceitar ou não uma transação, baseado no julgamento a partir da pontuação que o sistema informa. Sendo assim, as aplicações podem agregar mais esta funcionalidade no momento da bilhetagem dos serviços móveis.

Serviço de Proteção ao Usuário

O Serviço de Proteção ao Usuário - SPU, funciona semelhante ao Serviço de Proteção ao Crédito - SPC disponibilizado pelo SPC Brasil[2]. O SPC Brasil disponibiliza às empresas um serviço de consulta por CPF que informa se o dono do CPF está negativado ou não no sistema do SPC. Diante dessa informação as empresas podem negar a oferta de crédito aos clientes que se apresentam negativados no sistema do SPC Brasil. A base de dados desse sistema é centralizado e fica sobre a responsabilidade do SPC Brasil.

Para oferecer um serviço semelhante na infraestrutura apresentada neste trabalho algumas adaptações foram realizadas. A primeira adaptação realizada foi a criação de uma lista de usuários e sua situação no sistema, armazenados exclusivamente pelo Banco Central Virtual. Para evitar que todos os usuários carreguem toda a base com as informações de usuários negativados, ou a base com todos os usuários não negativados, a infraestrutura oferece às aplicações, o registro da reputação (SPU) de cada usuário para armazenamento em seu próprio dispositivo, no sistema de arquivos criptografado. Dessa forma, obrigatoriamente todas as vezes que um usuário consumidor requisitar um serviço é possível para o servidor verificar se o requisitante está ou não negativado junto ao SPU. Ainda, a infraestrutura garante que não é possível alterar o registro que contém as informações de SPU do usuário a não ser através de uma ação de sincronização de aplicação explicado na seção de agências virtuais. Para acessar o registro de SPU pode ser utilizado uma senha de criptografia conhecida apenas pela infraestrutura e consequentemente pela biblioteca de desenvolvimento. Esta chave está compilada junto ao código fonte de forma obfuscada para evitar sua quebra. Esta solução evita o consumo excessivo do espaço físico de armazenamento nos dispositivos.

De posse do registro do SPU do usuário consumidor, os aplicativos móveis podem oferecer a verificação de um usuário e seu registro do SPU. Cabe ao usuários a decisão

[2]http://www.spcbrasil.org.br/

de realizar transações, e portanto, o sistema não oferece nenhuma restrição baseada nas informações disponíveis pelo SPU, mas sim, uma ferramenta de decisão para as aplicações com suporte a bilhetagem. Esta ferramenta é disponibilizada para que os desenvolvedores de aplicações com suporte a bilhetagem façam o uso ou não dela.

4.3 Agências Virtuais

Uma Agência Virtual - AV, é um componente da infraestrutura que representa o Banco Central Virtual. É uma entidade autorizada pelo BCV a representá-lo junto aos usuários do sistema. Para tornar-se uma dessas agências, a entidade deve seguir as especificações de segurança exigidas pelo BCV. Essas especificações são todas fundamentadas na teoria da segurança da informação. Não faz parte do escopo do trabalho detalhar toda a especificação de segurança de rede e dados que uma Agência Virtual deve adotar. Esse assunto é apontado como um trabalho futuro.

As Agências Virtuais são entidades cadastradas junto ao BCV com o direito de disponibilizar alguns serviços do BCV: saque, depósito, consulta a saldo e histórico, e sincronização de aplicativo. Todas essa operações são determinadas e controladas pelo BCV. Uma AV assume o papel de provedora desses serviços, mas a agência funciona como uma ponte entre as requisições dos usuários e as respostas do BCV. Entretanto, as Agências Virtuais adquirem duas características que as diferenciam de uma ponte de dados apenas: elas auxiliam a infraestrutura adquirindo um papel de nó, de uma rede distribuída de informações de reputação de usuários e funcionam como uma casa de câmbio, capaz de repassar e receber dinheiro virtual com a particularidade de que elas não cobram taxas nem recebem nada por isso. Sendo assim, usuários que sacam e depositam em Agências Virtuais estão trocando cédulas virtuais diretamente com essas Agências. Posteriormente as Agências executam uma sincronização com o Banco Central Virtual, exportando e importando os dados necessários. Dessa forma, diversas entidades podem se candidatar a se tornarem uma Agência Virtual, shoppings, estações de metrô, bares, universidades, laboratórios de pesquisa, até mesmo pessoas físicas com acesso à Internet.

Os objetivos de uma Agência Virtual para a infraestrutura são: evitar a sobrecarga de requisições ao BCV, utilizando uma AV como representante oficial do BCV; além disso,

disponibilizar recursos de *hardware* e *software* para uma rede de informações distribuídas que é a rede de informações que contém todos os dados com as reputações dos usuários do sistema; ainda, representar o BCV junto aos usuários nas operações de saque e depósito, adquirindo papel de um correspondente bancário. A Figura 4.1 ilustra o esquema de distribuição de nós da infraestrutura, mostrando também a interação entre Agência Virtual e Banco Central Virtual e a interação de uma AV com usuários.

O Banco Central Virtual disponibiliza uma Agência Virtual diferente das demais, um *Internet Banking*. Esse componente funciona como as aplicações WEB disponibilizadas pelos Bancos físicos. O *Internet Banking* é uma interface gráfica para os serviços oferecidos pelo Banco Central Virtual, destinado aos usuários do sistema. Esses serviços são os mesmos de uma Agência Virtual, além do cadastro de usuários.

Os usuários precisam efetuar uma autenticação para poder utilizar as funcionalidades do *Internet Banking* do sistema. Para isso ele precisa cadastrar chaves de acesso junto ao BCV. É utilizado um esquema de chaves pública e privada. O usuário deve gerar essas chaves e disponibilizar a chave pública para os componentes da infraestrutura. A criptografia das mensagens é realizada com uma chave simétrica. Essa chave simétrica é trocada de forma segura utilizando a Infraestrutura de chave pública e privada - PKI [13] para codificar a chave de sessão compartilhada entre o usuário e o *Internet Banking*.

4.3.1 Operações

Nesta subseção são detalhados os fluxos das operações realizadas por uma Agência Virtual. As operações que elas podem realizar são: Saque de dinheiro virtual, depósito, consultas de saldo e histórico e efetuar a sincronização de aplicativo do usuário. Todas as operações devem ser acessadas pelos usuários através da requisição a uma agência virtual. Em seguida, as agências, dependendo da operação, como saque e depósito, podem responder direto ao usuário e somente depois se comunicar com o BCV, ou funcionam como uma ponte direta de comunicação entre o usuário e o BCV, que é o componente que centraliza o controle e acesso aos dados do sistema.

Saque

O saque de dinheiro virtual é a ação de retirada de créditos da conta do usuário na infraestrutura para o seu dispositivo. Para que esta ação seja realizada com sucesso, o usuário deve ter saldo o suficiente, ou não poderá realizar o saque. A Figura 4.6 mostra o fluxo de uma operação de saque realizado em uma AV.

A requisição por saque é iniciada pelo usuário. Uma requisição pode ser iniciada a qualquer instante desde que o usuário possua comunicação com uma agência virtual. Uma requisição de saque é uma mensagem que contém as seguintes informações: valor para retirada e identificação do usuário. A identificação do usuário é realizada por sua autenticação junto a infraestrutura. Para efetuar a autenticação o dispositivo deve enviar a identificação do usuário e ele deve informar uma senha para realização de operações. A mensagem é criptografada com uma chave privada que o usuário porta em seu dispositivo para garantir o não repúdio das mensagens emitidas por ele. Esse processo é básico para o início de todas as operações.

Logo após a requisição de saque e autenticação do usuário, a agência carrega as informações dele. Caso não conste seus dados na base de dados da Agência, ela precisará requisitar esses dados ao BCV e aguarda a atualização da sua base para continuar o processo de saque. Logo em seguida, de posse dos dados do usuário, é realizada a verificação de pendências que envolvam o usuário em questão. Essas pendências são verificadas e resolvidas através de auditoria, processo explicado na sincronização de aplicativo. Caso o usuário possua alguma pendência ele não poderá realizar saques de créditos até que a auditoria seja realizada e sua situação de pendência seja alterada. Então o processo é terminado e cabe ao usuário realizar uma sincronização de aplicativo para resolvera pendência.

Sem pendências de usuário, a agência verifica se ele possui saldo o suficiente para realizar uma retirada no valor requisitado. Caso tenha saldo o suficiente a retirada é liberada, caso contrário, uma mensagem de saldo insuficiente é gerada e encaminhada de volta para o dispositivo do usuário. A mensagem de saldo insuficiente também informa o saldo disponível, para o caso de o usuário desejar sacar uma quantia menor, dessa forma, uma nova requisição deverá ser iniciada. Após a verificação de saldo do usuário, a agência também verifica se ela tem cédulas virtuais o suficiente para repassá-las para o usuário. Em caso

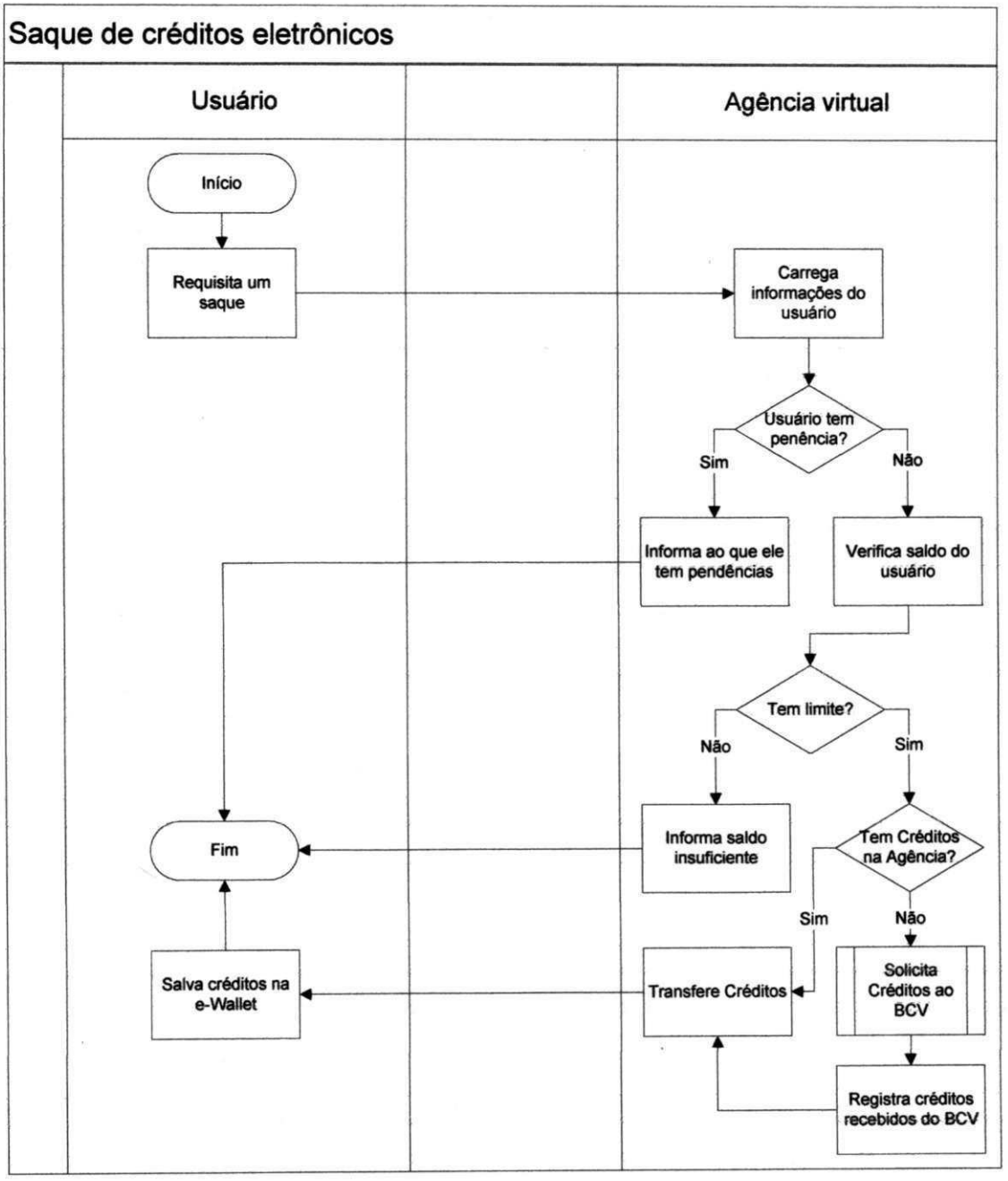


Figura 4.6: Fluxo de interação entre usuário e Agência para realização de um saque

positivo, realiza o repasse de imediato, caso contrário, solicita mais cédulas ao BCV para repassar ao usuário. Com a etapa de verificação de saldo concluída e de posse de dinheiro virtual o suficiente para concluir o saque, a AV transfere o crédito para a carteira eletrônica do usuário.

Depósito

O depósito de dinheiro virtual é a ação de transferir créditos do dispositivo do usuário para sua conta na infraestrutura. Para que esta ação seja realizada com sucesso, o usuário deve ter saldo o suficiente em seu dispositivo de cédulas virtuais válidas. A Figura 4.7 mostra o fluxo de uma operação de depósito realizado em uma AV.

Após a requisição de depósito e autenticação do usuário, a agência executa o carregamento das informações do usuário, como descrito na operação de saque. Na requisição de depósito o usuário já submete seus créditos eletrônicos. Em seguida a Agência avalia a validade dos créditos. Caso os créditos sejam reconhecidos como válidos, a AV efetua a operação de depósito, atualizando a base de dados com os dados de depósito do usuário. A reposta positiva para o usuário de que o depósito foi executado com sucesso, gera uma requisição ao aplicativo móvel. Essa requisição inicia o processo de invalidação dos créditos depositados no lado do dispositivo. Esse dinheiro virtual é invalidade pelo aplicativo utilizando o mesmo procedimento de assinatura da subseção *Multi-spending* de Dinheiro Virtual apresentado nesse capítulo.

Se as cédulas virtuais submetidas forem detectadas como cédulas falsas, a AV não prossegue com o depósito do dinheiro virtual. Ao invés disso, ela comunica o usuário que há cédulas falsas entre as enviadas e que por conta disso, é necessário a realização de uma sincronização de aplicativo. Na sincronização de aplicativo, o sistema fará o devido tratamento dessa inconsistência, como será explicado na subseção de sincronização de aplicativo a seguir.

Consulta

Além do saque e do depósito de dinheiro virtual o usuário pode efetuar consultas em sua conta na infraestrutura para verificar seu saldo e o histórico das operações realizadas. Para que esta operação seja realizada o usuário deve autenticar-se no sistema através de uma

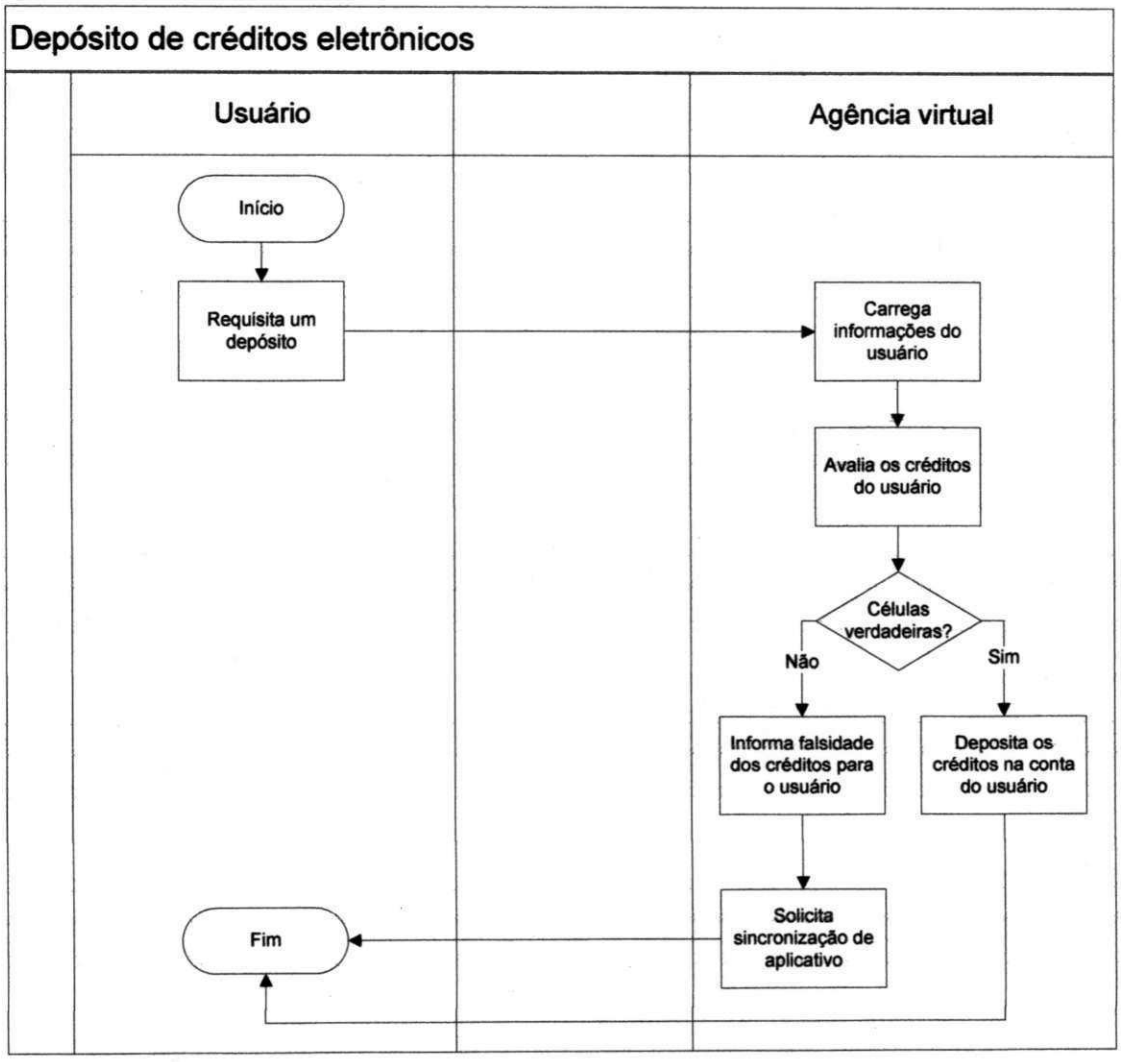


Figura 4.7: Fluxo de interação entre usuário e Agência para realização de um depósito

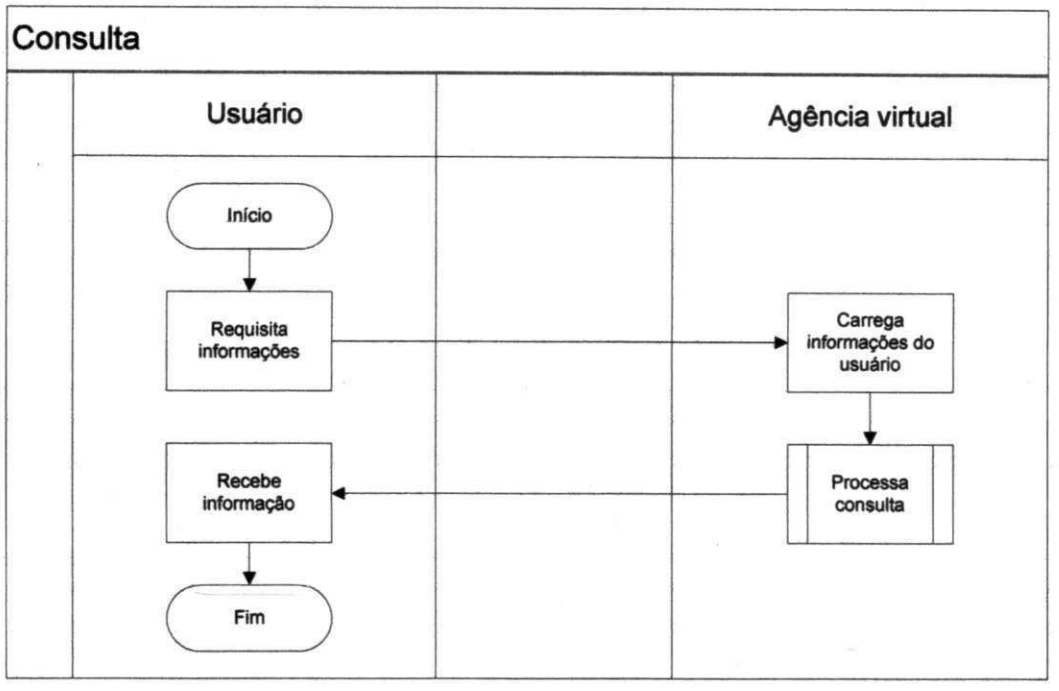


Figura 4.8: Fluxo de interação entre usuário e Agência para realização de uma consulta

Agência Virtual e requisitar uma das consultas disponíveis, saldo e histórico. A agência repassa as requisições de consulta do usuário para o BCV e por conta disso é o Banco Central quem o carrega as informações do usuário. O processamento da requisição da consulta também é repassado ao BCV. A requisição é encaminhada ao BCV, que realiza a operação e devolve a resposta para a agência. O processo da consulta termina com a devolução da resposta da consulta ao dispositivo do usuário. A Figura 4.8 ilustra a operação de consulta disponível nas Agências Virtuais.

Sincronização de Aplicativo

A sincronização de aplicativo é a operação de atualização geral do dispositivo. Esta operação não efetua saque, nem depósito, nem consulta. Ela atualiza o dispositivo exportando os dados gerados no aplicativo móvel através de transferência de dados para uma agência virtual. A Agência Virtual repassa as informações importadas dos usuários diretamente à base do BCV. A sincronização também exporta registros da infraestrutura para os aplicativos móveis. Alguns dos registros que o sistema disponibiliza para atualização dos usuários são: chave pública de assinatura PuK-DV, informações de reputação de usuários, novas versões

da biblioteca de desenvolvimento e atualização do dinheiro virtual.

Após a requisição da sincronização e autenticação do usuário, o sistema requisita a exportação dos dados do usuário para atualização de suas informações. Usuário envia os dados (nesta etapa todos os dados armazenados no dispositivo são enviados: informações de cédulas virtuais, rastreamento de cédulas, informações de reputação gerada pelas transações e o resultado de auditorias realizadas. Todas as informações enviadas pelos usuários são salvos na sua conta na infraestrutura.

A Figura 4.9 ilustra os passos do processo de sincronização de aplicativo. Uma das etapas do processo é a verificação da versão e integridade da biblioteca de desenvolvimento e da chave PuK-DV. Nessa etapa o sistema checa se as versões utilizadas são as mais atuais. Em caso negativo ele se prepara para atualizar o aplicativo móvel. A etapa seguinte é a etapa de atualização de dinheiro virtual. O pagamento pela bilhetagem de transações realizadas pelo usuário invalidam o dinheiro virtual na base de dados do dispositivo. Ele também recebe cédulas virtuais de outros usuários como pagamento por serviços providos. As cédulas virtuais recebidas e mesmo as não repassadas possuem uma data de validade. Cédulas com data de validade vencida podem ser rejeitadas dentro da infraestrutura e comparadas a outras cédulas com data de validade maior podem ser preteridas. Todos essas características que envolvem as cédulas eletrônicas justificam o incentivo a atualização do dinheiro virtual. O próximo passo do processo de sincronização serve para atualizar em todos os aspectos a carteira eletrônica do aplicativo móvel e todos os seus registros.

Durante a atualização do dinheiro virtual do usuário, o sistema verifica inconsistências nos dados, problemas detectados e salvos na área de reputação dos outros usuários e cédulas falsas. Caso algum desses problemas relacionados sejam encontrados, o sistema resgata os créditos válidos e verdadeiros, guarda na conta do usuário como se fosse um depósito e logo em seguida atualiza a reputação desse usuário com as inconsistências identificadas. Esse processo continua a invalidação do usuário. Esse recurso é executado pela AV da seguinte forma: é inserido uma informação na base de dados do dispositivo que diz ao aplicativo móvel que ele tem pendências e que só será liberado mediante uma sincronização novamente; essa nova sincronização serve para atualizar mais uma vez o dispositivo do usuário e caso não existam mais pendências contra ele essa marcação negativa será excluída da base de dados. O último passo da sincronização de um usuário que apresenta problemas termina com a

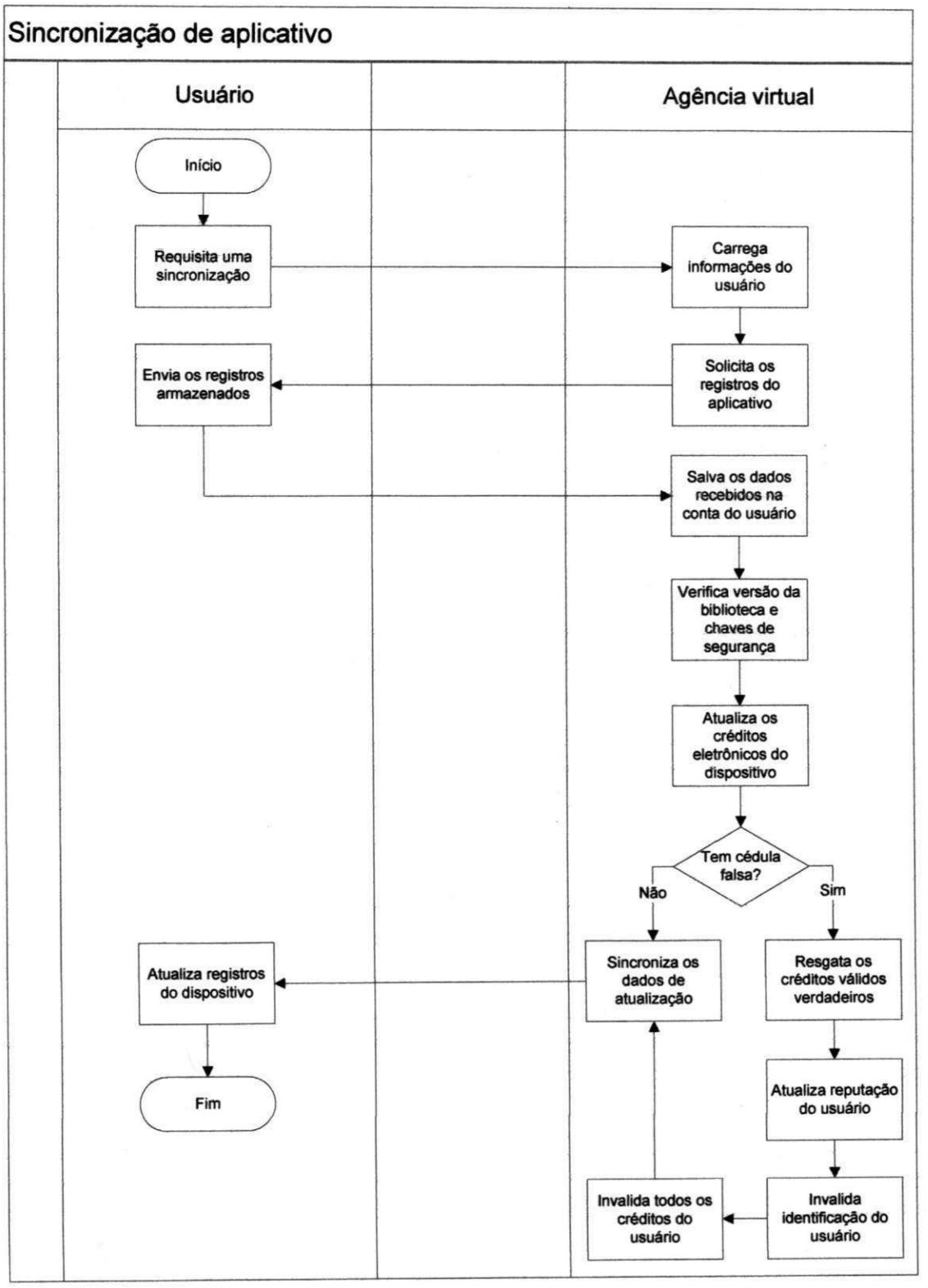


Figura 4.9: Fluxo de interação entre usuário e Agência para realização de uma sincronização de aplicativo

invalidação de todos as cédulas virtuais de sua *e-Wallet*. Ao final de todos essas verificações e tratamentos a agência sincroniza os dados com o dispositivo executando as atualizações necessárias. Os usuários que não apresentaram problemas durante a atualização das cédulas virtuais, passam imediatamente para a etapa de sincronização dos dados final com a Agência Virtual. Os registros no dispositivos são atualizados e o processo é terminado.

4.4 Cliente

O cliente é o terceiro componente dessa infraestrutura como pode ser observado na Figura 4.1. O cliente se comunica com a infraestrutura através da interação com Agências Virtuais e também estabelece a comunicação com outros clientes através da oferta e consumo de recursos móveis. As operações que as aplicações cliente podem realizar com a infraestrutura já foram discutidas na seção que apresenta o Banco Central Virtual e as Agências Virtuais. Esta seção apresenta a parte da arquitetura P2P do trabalho, o funcionamento dessa arquitetura, o papel de cada componente, o meio de acesso de um aplicativo móvel à infraestrutura e o protocolo de comunicação desenvolvido para determinar o passo-a-passo da troca de mensagens entre dois aplicativos móveis.

De acordo com o Sommerville [32], um projeto de arquitetura envolve o estabelecimento de um *framework* básico que identifica os principais componentes de um sistema e as comunicações entre eles. A arquitetura da solução é baseada no modelo de comunicação ponto a ponto, descrita no capítulo de Fundamentação Teórica deste trabalho. Os dispositivos devem estabelecer uma conexão de rede entre si para o funcionamento do sistema, além de seguir um protocolo de comunicação. A Figura 4.10 ilustra a arquitetura em camadas de um cliente da infraestrutura de comercialização de serviços entre pares. Cada camada, verticalmente, oferece serviços para a camada superior e, horizontalmente, elas se comunicam, manipulando o mesmo tipo de dados. Ainda, cada camada só tem o conhecimento de sua camada inferior.

Na Figura 4.10 é possível visualizar a disposição das camadas da arquitetura do Cliente. O nível mais acima é a GUI, camada responsável peal interação direta com o usuário. Aqui estão disponíveis as formas de acesso do aplicativo móvel ao usuário, através das interfaces de interação disponíveis por cada dispositivo móvel, por exemplo, interface

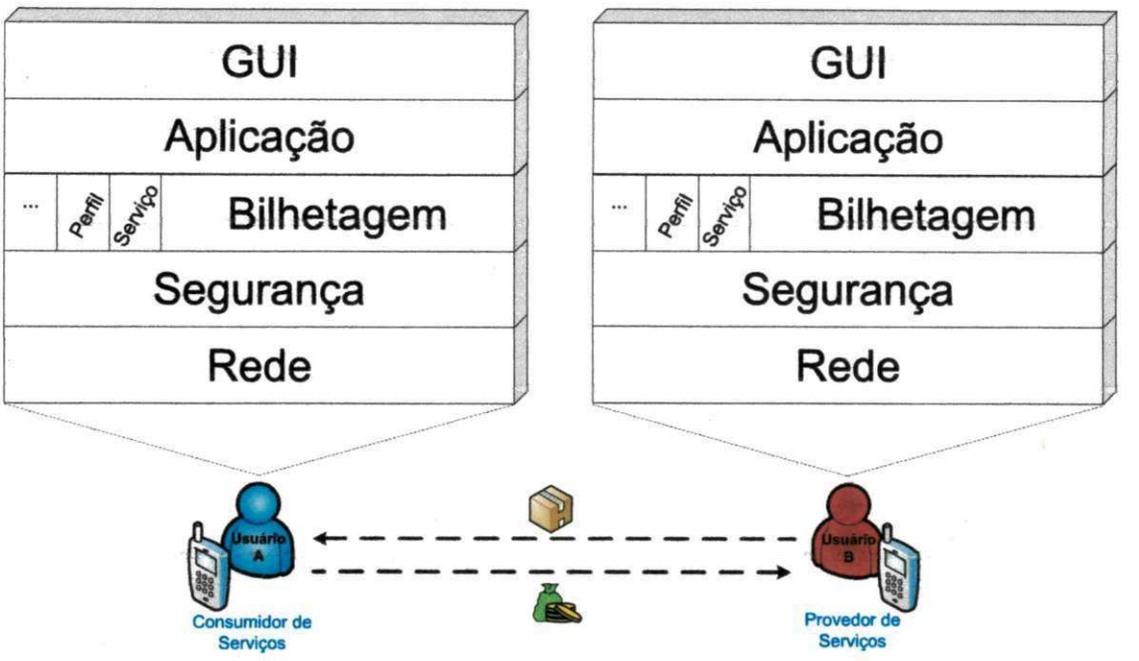


Figura 4.10: Arquitetura em camadas de uma aplicação Cliente

gráfica. Essa interface se comunica com a camada de Aplicação explorando e acessando todas as funcionalidades que o aplicativo móvel oferece. Cabe ao desenvolvedor determinar quais funcionalidades a aplicação tem. Um exemplo de aplicação é o envio de mensagens SMS para aparelhos celulares, como está descrito no estudo de caso desse trabalho. Funções como escrita de mensagens, envio de mensagens, transferência de mensagens, importação de modelos de mensagens, visualização de termos de bilhetagem, envio de termos de bilhetagem, entre outros, são exemplos de funcionalidades encaixadas na camada de aplicação. Uma mensagem enviada de um dispositivo consumidor para um dispositivo provedor de um serviço de envio de mensagens SMS, é tratada do mesmo formato, por exemplo formato texto plano, na camada de aplicação de cada um.

A camada de Bilhetagem contém a biblioteca de desenvolvimento distribuída pela infraestrutura aos desenvolvedores de aplicações móveis, que oferecem o suporte a bilhetagem de recursos e o acesso à infraestrutura. Ao longo deste capítulo foram apresentadas as funcionalidades que a infraestrutura oferece aos desenvolvedores de *software*, todas disponíveis na camada de bilhetagem da arquitetura. O envio do código de identificação de um usuário consumidor é comparado com a base de reputação de um

usuário provedor na camada de bilhetagem e a partir dessa comparação, a camada oferece, por exemplo, o serviço de consulta ao SPU desse usuário consumidor. Está presente também na camada de bilhetagem todas as funções de interação com as Agências Virtuais, como por exemplo saque e sincronização de aplicativo.

A base de dados, acessível apenas através da biblioteca de desenvolvimento, que contém registros como: a chave pública PuK-DV; os registros de reputação dos usuários; as cédulas eletrônicas; e todos os demais registros do sistema disponíveis aos componentes Cliente; ficam armazenados em uma camada de segurança da arquitetura, representada por um sistema de arquivos criptografados, o eCryptfs. Todas essas informações são criptografadas com uma chave simétrica de criptografia que está obfuscada e compilada no código da biblioteca de desenvolvimento. Apenas com essa chave é possível descriptografar as informações nele armazenados. Além disso, essa chave simétrica é utilizada para encriptar as mensagens trocadas entre os usuários.

Finalmente, a camada de rede oferece a interface de rede utilizada pelos dispositivos dos usuários para o estabelecimento da comunicação. A tecnologia de rede utilizada varia de acordo com o aplicativo móvel e com o suporte do dispositivo às tecnologias de rede. Para a biblioteca de desenvolvimento e para o protocolo de comunicação estabelecido pela infraestrutura, a tecnologia de rede utilizada é transparente. Cabe a aplicação móvel identificar e consumir os serviços da camada de rede disponíveis por dispositivo.

A seguir serão detalhadas as características e funções da biblioteca de desenvolvimento e o protocolo de comunicação para o estabelecimento da comunicação entre pares de dois usuários clientes da infraestrutura de suporte a bilhetagem.

4.4.1 A Biblioteca de Desenvolvimento Mobbillib

A Biblioteca de Desenvolvimento é um conjunto de classes que cooperam entre si para oferecer aos desenvolvedores o acesso a toda a infraestrutura de bilhetagem deste trabalho. Ela foi denominada de Mobbillib, uma abreviatura para *Mobile Billing Library*. Essa Biblioteca contém as rotinas de *software* necessárias para o desenvolvimento de uma aplicação para dispositivos móveis com suporte a bilhetagem de recursos entre pares. Os aplicativos móveis com este tipo de suporte devem utilizar essa biblioteca em seus *softwares*. A Figura 4.11 ilustra um diagrama com a arquitetura da aplicação Cliente. Na Figura 4.11

também é possível observar a arquitetura interna em módulos da biblioteca.

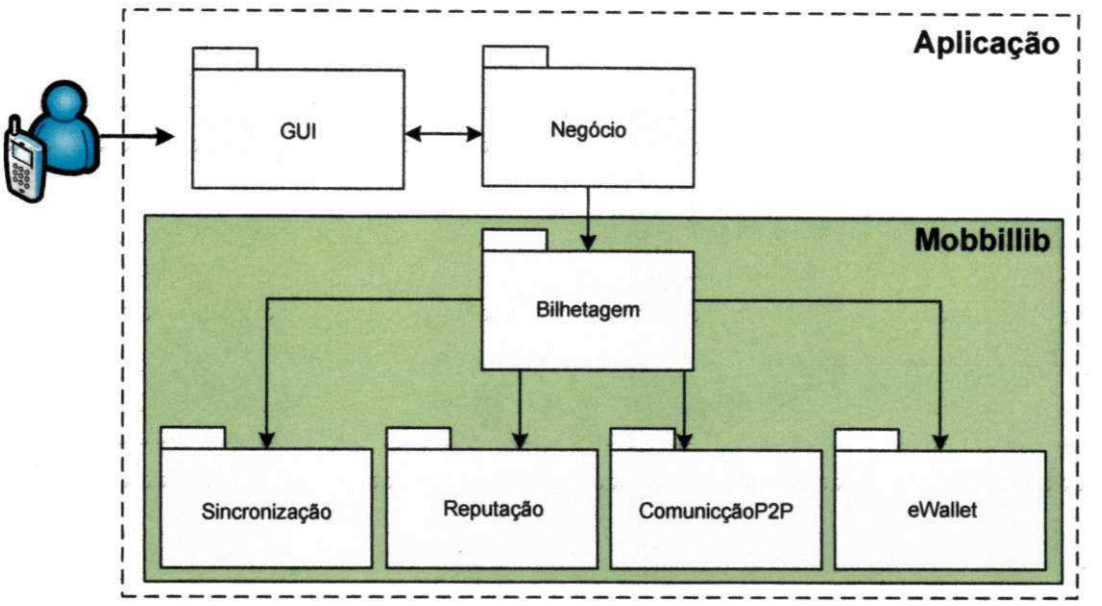


Figura 4.11: Arquitetura em módulos da biblioteca de desenvolvimento e *interface* de acesso

Interface Gráfica

O módulo da GUI é composto pelos elementos de interface gráfica da aplicação, os quais permitem a interação com usuário das funcionalidades oferecidas pelo aplicativo móvel. Esse módulo contém todas as telas do sistema que foram desenhadas pelos desenvolvedores de *software*. O módulo GUI que aparece na Figura 4.11 não é disponibilizado pela biblioteca Mobbillib. Cabe ao desenvolvedor da aplicação criar a interface gráfica dos aplicativo móvel.

Módulo de Negócio

Semelhante ao módulo GUI, o módulo de Negócio também é desenvolvido e distribuído apenas pelo desenvolvedor do aplicativo móvel. O módulo de Negócio contém as classes que vão consumir todos os serviços disponibilizados pela Biblioteca de Desenvolvimento. Este módulo contém as funcionalidades da aplicação, por exemplo, o *core* de funções de envio de mensagens SMS do serviço de envio de mensagens exemplificado no início deste capítulo. A interface de acesso a API da Mobbillib é consumida deste módulo.

Módulo de Bilhetagem

O módulo Bilhetagem é o que contém toda a API de acesso às funcionalidades da Biblioteca de Desenvolvimento. Esse módulo contém as classes que encapsulam as funções da biblioteca. É uma forma de padronizar o acesso e a utilização da Mobbillib.

Módulo de Sincronização

O módulo de sincronização contém todas as funcionalidades de sincronização de aplicativo e interação com as Agências Virtuais discutidos na subseção Operações desta seção Cliente. Este módulo oferece os seguintes serviços e operações: saque, depósito e consulta na AV; sincronização do aplicativo; atualização de todos os dados controlados pela biblioteca Mobbillib.

Módulo de Reputação

O módulo de reputação contém todas as informações dos usuários do sistema que foram baixados para o dispositivo. Este módulo controla o acesso e as alterações das informações de pontuação de usuários e do SPU. Ele pode ser requisitado pelo módulo de Sincronização ou pelo módulo de negócio da aplicação, mas sempre através de uma interface do módulo de Bilhetagem.

Módulo de ComunicaçãoP2P

O módulo de ComunicaçãoP2P contém as regras do protocolo de comunicação entre dois usuários para a comercialização de um recurso móvel. Este módulo é acessado todas a vezes que uma transação for iniciada. A descrição detalhada das regras e funções deste módulo são apresentadas na subseção a seguir, Protocolo de Comunicação.

Módulo da eWallet

O módulo da eWallet é módulo que contém todo o acesso, e controle de consulta e alteração dos dados e registros do dinheiro virtual. Ao longo do trabalho foram discutidos diversos aspectos do dinheiro virtual, desde a sua geração pelo Banco Central Virtual, passando pelo seu armazenamento no dispositivo, checagem de validade, invalidação, repasse de créditos,

até o depósito desse dinheiro. Todas as funcionalidades que acessam e alteram a carteira eletrônica do dispositivo, são controladas pelo módulo da eWallet. Nesse módulo também se encontra a chave simétrica de acesso ao sistema de arquivos criptografado.

4.4.2 Protocolo de Comunicação

O protocolo de comunicação desenvolvido normatiza as etapas, a ordem e as mensagens trocadas durante a comunicação entre dois usuários. Esse protocolo deve ser seguido durante a bilhetagem de um serviço móvel. O protocolo garante a ordenação das requisições e respostas, garante a integridade e confidencialidade das mensagens trocadas e a utilização da funcionalidade de bilhetagem por um recursos entre pares. A Figura 4.12 mostra uma representação do modelo de troca de mensagens do protocolo de comunicação e a ordem das requisições e respostas.

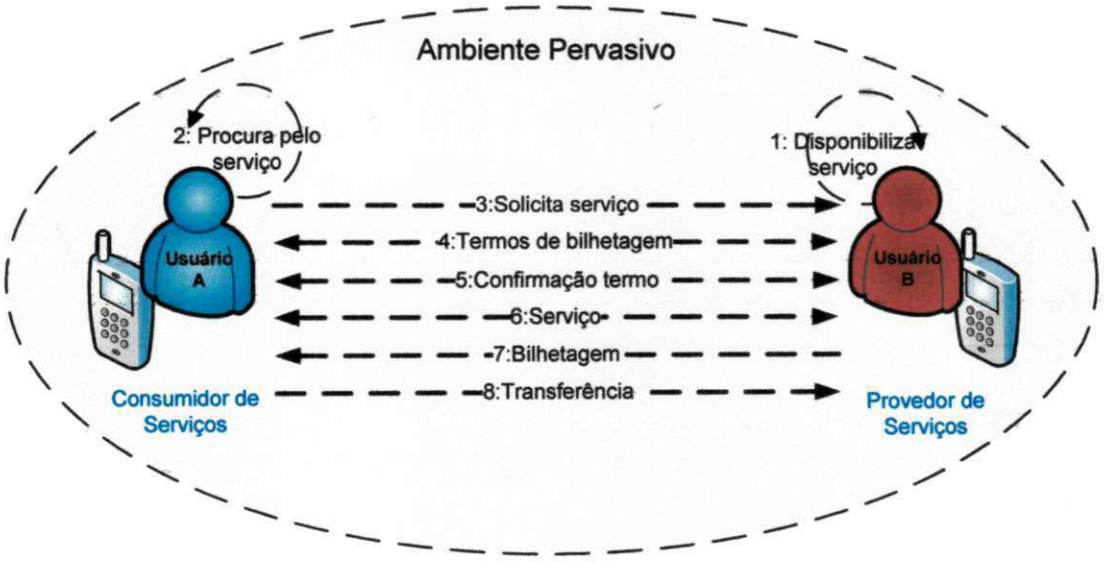


Figura 4.12: Representação da troca de mensagens do protocolo de comunicação

Na Figura 4.12 as setas representam as ações, ou passos, que as aplicações móveis devem adotar para o estabelecimento da comunicação. Inicialmente o usuário interessado em fornecer um serviço deve oferecê-lo em uma rede móvel para que seja possível sua detecção por outros usuários da rede (passo 1). Por sua vez, o usuário interessado em consumir um serviço deve procurá-lo na rede (passo 2). Diante da descoberta do serviço, o consumidor deve requisitar o fornecimento através do envio de uma mensagem de requisição (passo 3).

Nessa mensagem ele envia o tipo de serviço desejado e o código referente a sua identificação no sistema.

Após a análise da requisição e da avaliação da identificação do consumidor, o provedor do serviço, representado na Figura 4.12 como usuário B, pode aceitar ou não a requisição. Em caso afirmativo, os termos da bilhetagem são processados e enviados para o usuário consumidor (passo 4), representado na Figura 4.12 como usuário A. Esses termos então são reconhecidos pelo usuário A cabendo a ele a decisão pela aceitação ou não dos termos para o início do consumo do serviço.

O quinto passo do protocolo trata da confirmação dos termos de bilhetagem. Nessa etapa, os dois usuários devem trocar uma mensagem de confirmação da comercialização para dar início a transação. Ainda nesta quinta etapa, os usuários podem desistir da transação enviando uma mensagem para abortar a transação. Essa mensagem, de acordo com o protocolo, só pode ser enviada até o início da prestação do serviço. Interrupções externas como desligamento de um dos dispositivos, falha de bateria ou falha de rede, devem ser tratados pela aplicação, pois não é tratado pelo protocolo.

O passo 6, demonstra a prestação do serviço. Nesse momento o protocolo entra em estado de espera até a aplicação sinalizar o fim da prestação do serviço. Após essa sinalização é iniciado o processo de bilhetagem do serviço. Esse processo é representado pela seta de número 7 da Figura 4.12. Esse passo 7 trata de uma mensagem enviada ao usuário B (no caso, o consumidor) com a cobrança do serviço. A resposta dessa cobrança é a transferência das cédulas virtuais (passo 8). Nessa última etapa de transferência, ocorre o processo de repasse dos créditos para o usuário provedor do serviço e invalidação dos créditos no dispositivo do usuário consumidor, como foi descrito na subseção Dinheiro Virtual da seção Banco Central Virtual.

Para garantir a integridade e confidencialidade das mensagens trocadas na transação, as mensagens são todas assinadas com uma chave de criptografia simétrica, como a AES [18]. A chave simétrica utilizada pelos usuários para uma transação é trocada nas etapas 3 e 4 do protocolo. Na requisição, o usuário B envia uma sugestão de chave e o usuário A aceita. Os termos de bilhetagem já trafegam criptografados com essa chave simétrica. Antes disso, as mensagens são criptografadas com a chave simétrica que todo aplicativo móvel tem, que é distribuído junto a biblioteca de desenvolvimento compilada no próprio código. Ao final da

comunicação, a chave trocada nos passos 3 e 4 é descartada.

Finalizando, as aplicações móveis que oferecem o suporte a bilhetagem através da infraestrutura apresentada nesse trabalho, utilizam esse protocolo de comunicação para o estabelecimento de uma transação com comercialização de recursos móveis.

4.5 Conclusão

Neste capítulo foi apresentada a visão geral do projeto da infraestrutura de desenvolvimento de aplicações com suporte a Comercialização de recursos entre pares em ambientes pervasivos. Os componentes envolvidos (Banco Central Virtual, Agências Virtuais e os Clientes) na estrutura e os papéis desempenhados pelos mesmos foram apresentados como "caixas pretas", de modo a esclarecer como todo o sistema funciona. Em seguida, os três componentes foram detalhados e explicados separadamente. A prova de conceito e a validação da infraestrutura foram realizados por meio de um estudo de caso de um serviço de envio de mensagens SMS, que encaminha uma mensagem escrita no formato texto, para dispositivos celulares a partir da transferência de um arquivo, denominado ForwardSMS, o qual é discutido no capítulo 5.

Capítulo 5

Estudo de caso

Neste capítulo é apresentado o desenvolvimento de um estudo de caso para validar o suporte da infraestrutura à criação de aplicações para sistemas com suporte a bilhetagem de serviços móveis entre pares. Inicialmente, é apresentada a metodologia utilizada no estudo de caso, seguida de uma breve descrição do experimento e da configuração das aplicações cliente. Por fim os resultados obtidos com o desenvolvimento da aplicação para o estudo de caso.

5.1 Metodologia

A metodologia do experimento procedeu com uma revisão de literatura e uma prova de conceito sobre a hipótese de aplicabilidade do desenvolvimento de aplicativos móveis P2P que possam realizar a bilhetagem dos recursos disponíveis nos dispositivos móveis. Foi desenvolvida uma aplicação baseada nos conceitos apresentados nesse trabalho que simula a parte da arquitetura P2P da arquitetura geral da infraestrutura. Para elaboração da aplicação foi necessário verificar dentre os Trabalhos Relacionados qual tecnologia de rede melhor se adequaria para atender aos requisitos apresentados no Capítulo 4, qual plataforma utilizar e qual seria o objeto de estudo a ser solucionado até então não investigado pela comunidade científica.

A escolha da tecnologia de rede Bluetooth deve-se ao fato de que a aplicação foi desenvolvida em laboratório como um experimento e não percebeu-se a necessidade de explorar, pelo menos nessa fase inicial, uma tecnologia de longo alcance, já que o objetivo é provar a arquitetura e não a tecnologia de rede. Outro aspecto utilizado como comparativo,

foi a simplicidade de conexão. Desta forma, simulou-se o grau de segurança como sendo a chave trocada entre os usuários durante o estabelecimento de uma conexão Bluetooth. Além disso, o Bluetooth atende a todos os requisitos e características fundamentais para a escolha de uma tecnologia de rede no escopo desse experimento.

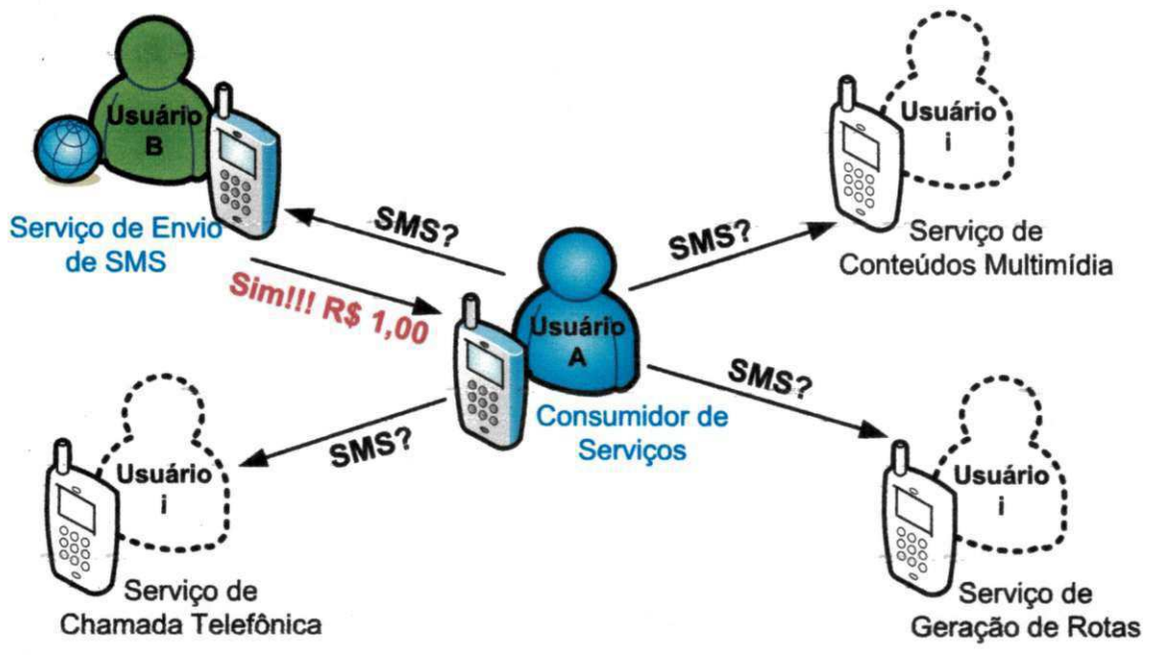


Figura 5.1: Possíveis aplicações de bilhetagem entre pares em ambientes pervasivos

A plataforma de desenvolvimento escolhida foi a plataforma Android[1], que se apresenta no mercado como uma das plataformas mais utilizadas no mundo. Foi escolhida a plataforma Android pelos seguintes fatores: é uma plataforma de desenvolvimento gratuita, reduzindo os custos da pesquisa; é uma plataforma que tem uma ampla documentação disponível[2], o que facilita o desenvolvimento de aplicações para esta plataforma; é baseada no Linux, o que herdou todo o Kernel, bem como suas diretivas de segurança, permitindo a inserção de diferentes níveis de segurança; diversos aparelhos móveis do mercado (com diversos recursos) adotam o Android como Sistema Operacional; possibilidade de instalação do eCryptfs; disponibilidade de dispositivos com diversos recursos para o oferecimento de serviços, como acesso a Internet, multimídia e vários outros recursos; e principalmente por

[1] www.android.com/

[2] http://developer.android.com/index.html

se enquadrar nas necessidades de uma aplicação cliente como descrito no Capítulo 4.

Para a escolha do cenário de estudo de caso a ser solucionado, foram analisados diversas aplicações de bilhetagem entre pares em ambientes pervasivos. A Figura 5.1 mostra alguns casos possíveis de aplicação do tema discutido neste trabalho. Na Figura 5.1 ainda é possível identificar algumas características discutidas nos capítulos anteriores, como a conexão entre dois usuários, o serviços que estão sendo oferecidos, os diferentes papéis dos atores no cenário e a etapa de transferência de créditos pelo consumo de um recurso. A Figura 5.1 exemplifica um usuário, A, que procura pela prestação de um serviço de acesso à Internet. Ele realizou uma busca na rede e verificou que são oferecidos quatro serviços: serviço de chamada telefônica, serviço de conteúdo multimídia, serviço de geração de rotas e por fim o serviço de acesso à Internet. Ao encontrar o serviço é mostrado nessa Figura o termo de bilhetagem para a transação.

Após a análise de possíveis cenários de aplicação do experimento, foi decidido que o estudo de caso seria a disponibilização de um serviço de envio de mensagens SMS entre dispositivos, no qual o dispositivo provedor oferece um serviço de envio de SMS através da retransmissão de pacotes de texto recebidos de outro aparelho móvel por Bluetooth.

5.2 Experimento

O experimento é o desenvolvimento de uma aplicação para dispositivos móveis que contém um módulo cliente (consumidor de recursos) e um módulo servidor (provedor de recursos), ambos distribuídos no mesmo *software*. O módulo servidor oferece serviços de envio de mensagens SMS e, portanto deve possuir conexão com uma rede de telecomunicação para realizar esta função, por exemplo, um chip habilitado de uma rede de telefonia. O servidor disponibiliza este serviço através de uma conexão Bluetooth que deve ser estabelecida com algum dispositivo cliente. O serviço disponibilizado possui uma configuração de bilhetagem previamente configurada para que durante a comercialização do recurso, os termos da cobrança sejam enviados para o cliente. Os termos de bilhetagem foram configurados da seguinte maneira e independente do tipo do usuário: deve ser cobrado do usuário $ 0,05 por cada kB de texto. A aplicação servidora recebe um arquivo texto no formato *properties*, interpreta os campos desse arquivo, que são o corpo da mensagem de texto, o título da

mensagem e o telefone de destino da mensagem, encapsula esses dados em um SMS e o envia para o destino (número e telefone informado no arquivo pelo consumidor do serviço). Este exemplo suporta apenas uma única conexão por vez, portanto não aceita múltiplas conexões.

O módulo cliente possui a interface gráfica para escrita da mensagem de texto (corpo da mensagem, título e telefone de destino), a escolha do dispositivo da rede, e outras interfaces apresentadas na seção de resultados. O usuário cliente após escrever a mensagem procura na rede o serviço de envio de mensagem SMS. Após a varredura na rede por dispositivos servidores e resposta de um usuário, o usuário consumidor inicia a transação com o usuário servidor. Após essa escolha o resumo dos termos da bilhetagem é mostrado ao usuário que opta por aceitar ou rejeitar os termos. Em caso de aceitação o arquivo texto é enviado ao provedor do serviço e logo após é realizada a transferência dos créditos e o devido débito do cliente e crédito do servidor.

Para esse experimento foi considerado que os dois dispositivos participantes da transação possuem cédulas virtuais o suficiente para a conclusão e pagamento do serviço. Além disso, foi considerado que a verificação das cédulas virtuais devem ser realizadas após a prestação do serviço. Como a tecnologia de rede utilizada foi a Bluetooth que tem um alcance pequeno, os usuários envolvidos estão localizados em um perímetro de alguns metros, portanto, facilmente um pode interpelar o outro quanto a possíveis interrupções da transação exatamente durante a fase da transferência dos créditos. Ainda assim, para esse primeiro experimento, foi esperado todo o tempo necessário para a conclusão da transação, isto é, até o final da transferência do dinheiro virtual.

Foi gerada um par de chaves pública e privada com a API Java Sign[3] da linguagem JAVA. Com esse par de chaves, foi possível realizar a criptografia do dinheiro virtual como descrito na seção Banco Central Virtual do Capítulo 4. O dinheiro foi assinado com a chave privada e salvo em um arquivo do tipo texto. Para realizar a verificação de saldo ou autenticidade do dinheiro bastava descriptografar o dinheiro com a chave pública que fora distribuída para os dois usuários.

Esse experimento contou com dois aparelhos celulares, um Samsung Galaxy S[4] e um

[3]http://javasign.sourceforge.net/

[4]http://www.samsung.com/br/consumer/cellular-phone/cellular-phone/smartphones/GT-I9100LKLZTO/index.idx?pagetype=prd_detail\&tab=specification

Nexus one[5] com a aplicação ForwardSMS instalada em cada um deles, além da plataforma Android. A troca de créditos entre os dois aparelhos foi simulada da seguinte forma:

- Cada aparelho celular continha um arquivo criptografado com uma chave simétrica AES com o nome **creditos.txt**. Essa chave era a mesma para ambas as aplicações. Cada arquivo (o conteúdo também era criptografado) continha o valor de R$ 0,05 créditos dentro deles antes da comercialização do serviço dar início e uma data de validade a se vencer em sete dias. No início do envio da mensagem do usuário consumidor para o servidor existiu uma etapa que bloqueou estes arquivos para edição e exclusão, simulando algumas das propriedades do sistema de arquivos criptografado. Após o término da transferência, os arquivos foram desbloqueados e foi realizada uma subtração no valor do serviço do lado do usuário consumidor e uma adição no lado usuário servidor com o valor do serviço. Essa ação seguiu o processo de descriptografia do arquivo, transferência do crédito e invalidação do lado consumidor. Esses arquivos não podem ser alterados de forma alguma, pois estão assinados com uma chave que só quem conhece e os abre é a aplicação ForwardSMS, portanto não teve como o arquivo **creditos.txt** ser alterado. Portanto desta forma simulou-se o processo de transferência de créditos com as operações de crédito e débito nos dois dispositivos envolvidos.

5.3 Configuração do Aplicativo Cliente

A configuração do aplicativo Cliente segue a especificação da arquitetura da Figura 4.11 apresentada no Capítulo 4. Para o desenvolvimento da aplicação móvel foi implementada a arquitetura de acordo com o diagrama de arquitetura interna ilustrado na Figura 5.2. A Figura demonstra a implementação da arquitetura de camadas da Figura 4.11.

A camada de de visão determina a camada mais externa da aplicação, que contém a interface gráfica de interação entre o usuário e o programa e as funções as quais ele podem acessar. Nessa camada estão presentes as funcionalidade de preenchimento de mensagem, importação de modelo de mensagem, tela de visualização dos termos da bilhetagem, busca na rede por serviços e caixas de diálogo com os estados da transação. A camada controladora

[5]http://www.webcitation.org/5wvL9MTmm

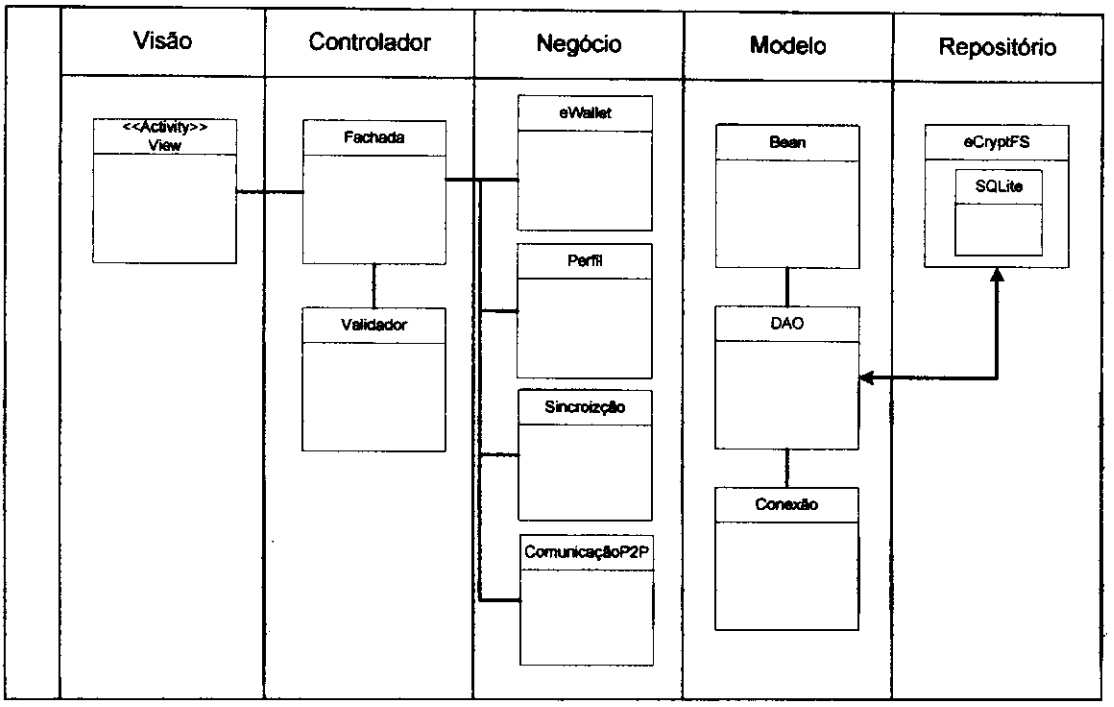


Figura 5.2: Arquitetura interna da aplicação Cliente

é responsável pela interface de funcionalidades e serviços do Sistema e pelas suas validações. Nela foram implementadas as fachadas para as funcionalidades do aplicativo e a classe de validação dos dados informados pelo usuário.

Ainda, a camada de negócio e a de modelo contém a implementação de todas as operações e unidades de trabalho do Sistema. As classes dessas camadas são consumidoras dos serviços providos pela biblioteca de desenvolvimento. É possível perceber na camada de Negócio da Figura 5.2 que foi desenvolvida uma classe representativa para cada módulo da biblioteca de desenvolvimento. As funcionalidades controladas e manipuladas nas classes dessas camadas são semelhantes as de mesmo nome da subseção que detalha a biblioteca Mobbillib do Capítulo 4. Como a biblioteca é acessada através do módulo de Bilhetagem, decidiu-se retirá-la do desenho da arquitetura interna da Figura 5.2.

Finalmente, a camada de repositório é a responsável pela persistência dos dados. Para a escolha da persistência dos dados foi escolhido um sistema de arquivos que suporta criptografia de dados, mas que nesse estudo de caso foi simulado como descrito na seção anterior e um SGBD para gerenciar o armazenamento de parte dos dados da aplicação. Para

o SGBD foi escolhido o SQLite, que dá suporte a diversas plataformas, inclusive Android. A quantidade de camadas de abstração do Sistema e a granularidade de cada uma delas é uma tarefa que posteriormente poderá ser redefinida ou refatorada com a continuidade deste trabalho.

5.4 Resultados

Após a realização do experimento, foi identificado que o usuário consumidor conseguiu escrever e enviar uma mensagem de texto com sucesso de seu aparelho celular através de um serviço de envio de SMS fornecido por outro celular. Foi identificado também que os termos de negociação do serviço foram devidamente apresentados e que após a aceitação dos termos por ambas as partes a transferência de créditos foi realizada corretamente do usuário consumidor para o usuário provedor do serviço. Além disso, foi identificado que a bilhetagem do serviço entre as duas partes envolvidas ocorreu em uma rede móvel que atendia aos requisitos de um ambiente pervasivo como explicado na seção de fundamentação teórica deste trabalho.

É também resultado do estudo de caso os seguintes pontos:

- Uma aplicação que oferece um serviço de envio de SMS e que cobra por esse serviço.
- Uma aplicação que envia um arquivo texto e que para enviar um SMS a partir desse arquivo deve consumir um serviço e pagar por ele.
- Um caso de sucesso de bilhetagem de um serviço de envio de SMS através de uma rede Bluetooth.
- Um caso de sucesso de crédito e débito de valores a partir de uma transferência de créditos eletrônicos.
- A oferta de uma nova forma de cobrança por recursos móveis sem a necessidade de conexão com a Internet durante a transação comercial.

Como resultado do experimento também é possível perceber algumas interfaces do Sistema que são apresentadas a seguir.

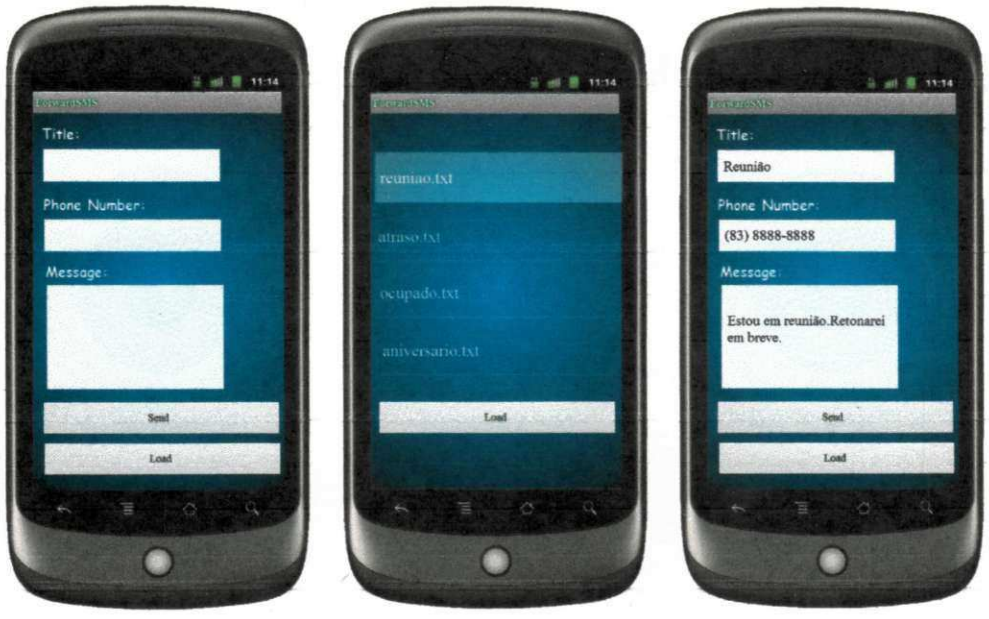
Figura 5.3: Tela de Abertura da Aplicação ForwardSMS

- Para demonstrar os conceitos aplicados nesse trabalho, foi criado o protótipo de uma aplicação denominada ForwardSMS, que tem como tela inicial a Figura 5.3. Basicamente esta é uma aplicação onde uma pessoa poderá enviar uma mensagem de texto do tipo SMS - Short Message Service através de um serviço disponibilizado por outra pessoa.

  É possível observar que esta é uma aplicação que possui uma interface simples, onde o usuário poderá preencher os dados de título, telefone de destino e mensagem de um SMS, como é visto na Figura 5.4(a). Outra opção dada ao usuário é a de carregar uma mensagem gravada no dispositivo. Para ter acesso a essa opção, ele irá pressionar o botão "load", e será mostrada uma tela com a listagem de mensagens previamente salvas, como pode ser observado na Figura 5.4(b).

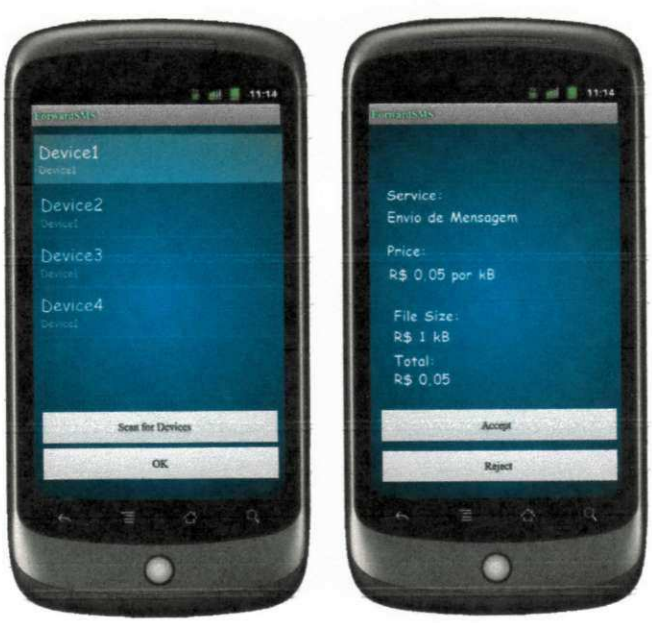
  Escolhida a mensagem, o conteúdo do arquivo texto será carregado no formulário de envio de SMS, como pode ser observado na Figura 5.4(c).

  Ao finalizar o preenchimento do formulário de envio de Mensagem, o usuário pressionará o botão "send"e então será exibida uma tela que lista os dispositivos disponíveis por Bluetooth para prover esse serviço, como pode ser observado na Figura 5.5(a). Escolhido o dispositivo provedor, serão exibidas para o usuário as



(a) Formulário para preenchimento (b) Tela de Escolha de Mensagens Pré-Definidas (c) Informações da Mensagem Preenchidas

Figura 5.4: Telas de envio de mensagem

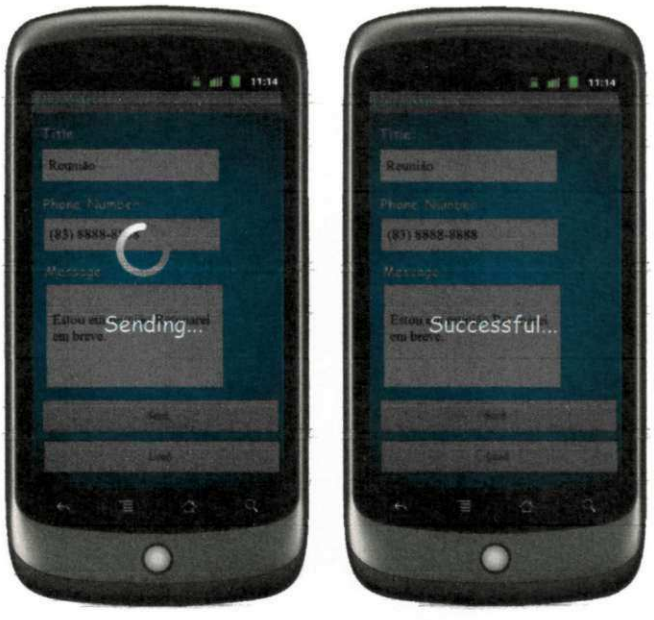


(a) Tela para escolha de um Dispositivo Provedor de Serviço

(b) Tela com as Informações sobre o Serviço Prestado

Figura 5.5: Etapa de escolha do dispoisitivo e negociação do serviço

informações relativas à cobrança do serviço. O resumo dessa cobrança é observado na figura 15. Como também pode ser observado na figura 5.5(b), o usuário pode aceitar esse dispositivo provedor ou rejeitá-lo, de acordo com a descrição da cobrança que é mostrada na tela. Caso aceite, a mensagem será enviada e caso rejeite a listagem de dispositivos disponíveis é novamente exibida para a escolha de outro provedor.



(a) Mensagem sendo enviada (b) Mensagem enviada com sucesso

Figura 5.6: Telas de acompanhamento de envio da mensagem

Após todos os passos serem feitos, a mensagem é então enviada. Uma vez iniciado o processo de envio a tela formulário fica bloqueada para novas alterações e a palavra "sending"é exibida, como mostra a Figura 5.6(a). O *feedback* do aplicativo após o processo de envio, pode ser observado na Figura 5.6(b). Dessa forma ele pode saber se a mensagem foi enviada com sucesso ou não.

5.5 Conclusão

Neste capítulo foi apresentado um mecanismo de validação da infraestrutura desenvolvida expondo o desenvolvimento de um estudo de caso para um serviço de envio de mensagens SMS. O objetivo desse estudo de caso foi demonstrar como a infraestrutura pode ser

utilizada na comercialização de serviços móveis com fornecimento de estruturas de suporte à bilhetagem de recursos, apenas pela adoção de uma biblioteca de desenvolvimento nas aplicações móveis.

Capítulo 6

Considerações Finais

A motivação para esta pesquisa foi observada inicialmente após a investigação da literatura sobre dispositivos móveis, serviços móveis, ambientes pervasivos e bilhetagem de recursos. Foi visto pelo autor que diversas empresas estavam pesquisando a fundo sobre o tema, o comportamento e a aceitação de pessoas sobre o assunto. Percebeu-se que a área dos dispositivos móveis em geral está recebendo muita atenção do mercado de TI em todo o mundo. O número de diferentes tipos de dispositivos e a variedade de aplicações para estes aparelhos também só faz aumentar.

Após o levantamento do estado da arte da área de comércio eletrônico móvel, percebeu-se que grande parte dos estudos são voltados para a bilhetagem entre pares com a presença de uma entidade confiável e mediadora da transação, exigindo assim uma conexão com a Internet durante todo o período da transação entre os envolvidos na operação. Essa constatação foi a principal motivação encontrada para o desenvolvimento dessa pesquisa. Portanto o que o autor pretendeu desde o início da pesquisa foi verificar se a construção de aplicações que oferecem a bilhetagem de recursos móveis entre dois usuários seria possível em ambientes pervasivos sem a necessidade de conexão com a Internet durante a transação. Além disso, foi proposto um sistema que também tivesse a possibilidade de ser utilizado por dispositivos já lançados no mercado, facilitando o processo de adoção e disseminação da solução, ao contrário de outros autores [6] que ainda precisam que suas propostas sejam aceitas e construídas por fabricantes de *hardware*. A partir do resultado dessas discussões, surgiu a ideia de uma infraestrutura que oferecesse diversas funcionalidades de bilhetagem para o comércio eletrônico de serviços móveis através da adoção de uma biblioteca de

desenvolvimento que fornecesse um mecanismo de acesso a essa infraestrutura. Para provar esse conceito, um experimento que fosse todo desenvolvido em nível de *software*, isto é, sem a necessidade de uma adaptação de *hardware*, em uma plataforma já difundida no mercado, como foi o caso da escolha pelo Android.

A solução arquitetural proposta atendeu aos objetivos necessários apresentado no primeiro capítulo deste trabalho de pesquisa. A arquitetura é aplicável e extensível e pode ser aproveitada por outras aplicações de tal forma que o esperado do autor é que a solução de projeto encontrada para a divulgação e aceitação dessa infraestrutura, a biblioteca de desenvolvimento para aplicações com suporte a bilhetagem de serviços, seja experimentada e testada pela comunidade de desenvolvimento em diversas aplicações móveis.

A avaliação do experimento foi que ele atendeu aos requisitos estabelecidos no capítulo 5. Mesmo assim, o autor propõe a elaboração de um exemplo maior com outra tecnologia de rede, por exemplo, rede sem fio 802.11, que suporte maiores distâncias entre os usuários para poder avaliar outros aspectos do tema. Com um cenário desse, seria possível avaliar aspectos como: comercialização de serviços com a manutenção do anonimato dos usuários, já que eles não precisariam estar próximos para realizar negociações; diferentes serviços; utilizar um ponto de acesso para estabelecimento da rede; qualidade da conexão; tratamento de erros; outros possíveis ataques a solução; e muito mais.

Os resultados do experimento demonstram que a construção de aplicações com suporte a bilhetagem é possível e que desenvolvedores podem adaptar essa solução aos seus problemas. Por fim, o autor destaca os seguintes pontos de aprendizado:

- Conhecimento da área de dispositivos móveis;
- Diferentes tecnologias móveis;
- Estudo profundo do estado da arte de bilhetagem;
- Aplicação do processo científico e desenvolvimento de aplicativos móveis.

6.1 Contribuições

As principais contribuições deste trabalho são enumeradas a seguir:

- Arquitetura de uma infraestrutura que disponibiliza o suporte a bilhetagem de serviços móveis entre pares;
- Modelagem de um protocolo de comunicação P2P de bilhetagem de serviços;
- Disponibilização de uma Biblioteca de Desenvolvimento para acesso a infraestrutura de bilhetagem que pode ser utilizada nos mais diversos tipos de aplicação de comércio eletrônico móvel;
- Desenvolvimento de uma carteira eletrônica móvel com verificação *offline* de dinheiro virtual, totalmente a nível de *software*, para o suporte a bilhetagem de serviços móveis.

6.2 Trabalhos Futuros

A segurança da informação é uma preocupação de todos os sistemas de informação. A preocupação em um sistema da área financeira é ainda maior. Por isso, atualizações tecnológicas e a pesquisas por métodos de segurança cada vez mais seguros serão sempre preocupações desse trabalho. Um exemplo disso, seria a implantação de PKI na chave de autenticação do sistema de arquivos criptografado, eCryptfs, em substituição da chave simétrica. Outro exemplo seria a pesquisa por métodos matemáticos de obfuscação de código que dificulte ainda mais o processo de descompilação de código. Portanto, é interessante que o escopo desse trabalho seja sempre atualizado em vista de novas tecnologias de segurança aplicáveis ao trabalho.

O nível de detalhamento de funcionalidades e especificação dessas funcionalidades depende bastante do intuito do leitor. A nível de implementação do que foi apresentado nesse trabalho, seria interessante a redefinição ou detalhamento de alguns aspectos do trabalho, como: especificação dos requisitos necessários para que uma entidade se torne uma Agência Virtual; detalhamento de definições de cadastro de usuários e valor da chave de criptografia.

Do ponto de vista científico seria interessante novas avaliações da infraestrutura apresentada. Exemplo disso seria a comparação com outros trabalhos científicos. A realização de novos experimentos alterando a simulação da transferência de créditos virtuais, com a possibilidade de simulação de ataques também seria interessante. A validação do

experimento do estudo de caso com técnicas formais de validação é outro aspecto que pode ser abordado futuramente.

Por fim a extensão das funcionalidades da Mobbillib. A biblioteca é a porta para a infraestrutura. Da mesma forma que a infraestrutura é extensível, a biblioteca também deve ser. Portanto alterações e adição de funcionalidades como a verificação dos créditos eletrônicos, oferecendo a checagem das cédulas com mais uma etapa do protocolo de comunicação é uma nova funcionalidade que pode ser explorada futuramente. Outros aspectos da biblioteca de desenvolvimento , com o protocolo de comunicação, também podem ser revisados para melhorar o desempenho da comunicação e aumentar o nível de segurança dessa comunicação P2P.

Este trabalho ainda permite outros tipos de adaptação e a medida que as tecnologias avançam e os dispositivos agregam mais recursos, as aplicações de bilhetagem de serviços ganham novos formatos. Portanto esta pesquisa mostrou que o tema em questão é aplicável e promissor.

Bibliografia

[1] *IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Dezembro de 2007.

[2] Frank Adelstein, Sandeep KS Gupta, Golden Richard III, and Loren Schwiebert. *Fundamentals of Mobile and Pervasive Computing*. McGraw-Hill, 1st edition, 2004.

[3] Stephanos Androutsellis-Theotokis and Diomidis Spinellis. A survey of peer-to-peer content distribution technologies. *ACM Comput. Surv.*, 36:335–371, Dezembro de 2004.

[4] Rajesh Krishna Balan, Narayan Ramasubbu, Komsit Prakobphol, Nicolas Christin, and Jason Hong. mferio: the design and evaluation of a peer-to-peer mobile payment system. In *MobiSys '09: Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 291–304, New York, NY, EUA, 2009. ACM.

[5] Bo Begole. *Ubiquitous Computing for Business*. FT Press, 1st edition, 2011.

[6] Yen Choon Ching and Heinz Kreft. Faircash: Concepts and framework. *Next Generation Mobile Applications, Services and Technologies, International Conference on*, 0:269–274, 2008.

[7] Diane J. Cook, Juan C. Augusto, and Vikramaditya R. Jakkula. Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing*, 5(4):277–298, Agosto de 2009.

[8] Les Green e Linas Maknavicius. Secure billing for ubiquitous service delivery. In Burkhard Stiller e Peter Reichl e Bruno Tuffin, editor, *ICQT*, volume 4033 of *Lecture Notes in Computer Science*, pages 90–101. Springer, 2006.

[9] Rahul M. Godbole and Alwyn R. Pais. Secure and efficient protocol for mobile payments. In *Proceedings of the 10th international conference on Electronic commerce*, ICEC '08, pages 25:1–25:10, Nova York, NY, EUA, 2008. ACM.

[10] Rudinei Goularte. *Personalização e adaptação de conteúdo baseadas em contexto para TV Interativa*. Tese de Doutorado em Ciência da Computação e Matemática Computacional, Instituto de Ciências Matemáticas e de Computação - ICMC-USP. Universidade de São Paulo (USP) - São Carlos, 2003.

[11] Robert Grimm, Janet Davis, Eric Lemar, Adam Macbeth, Steven Swanson, Thomas Anderson, Brian Bershad, Gaetano Borriello, Steven Gribble, and David Wetherall. System support for pervasive applications. *ACM Trans. Comput. Syst.*, 22:421–486, Novembro de 2004.

[12] Jingzhi Guo and Angelina Chow. Virtual money systems: A phenomenal analysis. In *CECANDEEE '08: Proceedings of the 2008 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services*, pages 267–272, Washington, DC, EUA, 2008. IEEE Computer Society.

[13] Marko Hassinen, Konstantin Hyppönen, and Elena Trichina. Utilizing national public-key infrastructure in mobile payment systems. *Electron. Commer. Rec. Appl.*, 7:214–231, Julho 2008.

[14] Karen Henricksen and Jadwiga Indulska. A software engineering framework for context-aware pervasive computing. In *Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04)*, PERCOM '04, pages 77–86, Washington, DC, EUA, 2004. IEEE Computer Society.

[15] Karen Henricksen, Jadwiga Indulska, and Andry Rakotonirainy. Infrastructure for pervasive computing: Challenges. In *Workshop on Pervasive Computing INFORMATIK 01, Viena*, pages 214–222, 2001.

[16] Pan Hui, Onshun Chau, Xiaoshan Liu, and V.O.K. Li. A peer-to-peer jini architecture for pervasive multimedia. *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, 5:3160–3164 Vol. 5, Setembro de 2004.

[17] Ho Hui-Yi and Syu Ling-Yin. Uses and gratifications of mobile application users. In *Electronics and Information Engineering (ICEIE), 2010 International Conference On*, volume 1, pages V1–315 –V1–319, Agosto de 2010.

[18] Internet Engineering Task Force (IETF). The aes-cbc cipher algorithm and its use with ipsec. http://www.ietf.org/rfc/rfc3602 . Último acesso em Janeiro/2012.

[19] Internet Engineering Task Force (IETF). Us secure hash algorithms (sha and sha-based hmac and hkdf). http://tools.ietf.org/html/rfc6234 . Último acesso em Janeiro/2012.

[20] Prakash Iyer and Ulhas Warrier. Internetgatewaydevice:1 device template version 1.01, 2001. http://www.upnp.org/standardizeddcps/documents/upnp_igd_internetgatewaydevice

[21] Stamatis Karnouskos. Mobile payment: A journey through existing procedures and standardization initiatives. *IEEE Communications Surveys and Tutorials*, 6(1-4):44–66, 2004.

[22] H. Kreft and W. Adi. Wallet based e-cash system for secured multi-hop cash exchange. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pages 1 –5, Abril de 2008.

[23] Mario Massakuni Kubo. *FMMG: um framework para jogos multiplayer móveis*. Pós Doutorado em engenharia da computação e sistemas digitais, Escola Politécnica (EP) – Universidade de São Paulo (USP), 2006.

[24] Donggeon Lee, Seongyun Kim, Howon Kim, and Namje Park. Mobile platform for networked rfid applications. *Information Technology: New Generations, Third International Conference on*, 0:625–630, 2010.

[25] Vili Lehdonvirta, Hayuru Soma, Hitoshi Ito, Hiroaki Kimura, and Tatsuo Nakajima. Ubipay: conducting everyday payments with minimum user involvement. In *CHI '08: CHI '08 extended abstracts on Human factors in computing systems*, pages 3537–3542, Nova York, NY, EUA, 2008. ACM.

[26] Emerson Loureiro, Loreno Oliveira, and Hyggo Almeida. Improving flexibility on host discovery for pervasive computing middlewares. *MPAC '05: Proceedings of the 3rd international workshop on Middleware for pervasive and ad-hoc computing*, pages 1–8, 2005.

[27] Lorena Fernandes Maia. Infraestrutura para o desenvolvimento de aplicações baseadas em localização e orientadas a domínios. Dissertação de Mestrado em Ciência da Computação, Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Campina Grande - Campus I, 2011.

[28] Ulrike Meyer and Susanne Wetzel. A man-in-the-middle attack on umts. In *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, pages 90–97, Nova York, NY, EUA, 2004. ACM.

[29] Moon-Hee Park, Jin-Hyuk Hong, and Sung-Bae Cho. Location-based recommendation system using bayesian user's preference model in mobile devices. In Jadwiga Indulska, Jianhua Ma, Laurence Tianruo Yang, Theo Ungerer, and Jiannong Cao, editors, *UIC*, volume 4611 of *Lecture Notes in Computer Science*, pages 1130–1139. Springer, 2007.

[30] P. Pillai, Yim Fun Hu, and A. Lorelli. Universal plug and play based billing system for moving networks. In *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, pages 1–5, Setembro de 2006.

[31] M. Satyanarayanan. Pervasive computing: Vision and challenges. *IEEE Personal Communications*, 8:10–17, 2001.

[32] Ian Sommerville. *Software Engineering (7th Edition)*. Pearson Addison Wesley, 2004.

[33] Andrew S. Tanenbaum. *Redes de Computadores*. Elsevier, Rio de Janeiro, trad. 4 ed. edition, 2003.

[34] Mark Weiser. The computer for the 21st century. *Scientific American*, 265(3):66–75, Setembro de 1991.

[35] Kui Wu and Jingang Liu. Research and implementation of user data cryptographic mechanism based on vfs. In *FSKD*, pages 2557–2560. IEEE, 2011.

[36] John K. Zao, Yu-Chih Liu, Ming-Hsiao Yang, Sheng-Kun Li, Wei-Yu Chen, Ching-Wei Chen, Kuo-Chin Huang, Jwu-Sheng Hu, and Lun-Chia Kuo. Ubiquitous e-helpers: An upnp-based home automation platform. In *SMC*, pages 3682–3689. IEEE, 2007.