UNIVERSIDADE DO VALE DO RIO DOS SINOS
ÁREA DE EXATAS E TECNOLÓGICAS
PROGRAMA INTERDISCIPLINAR DE PÓS-GRADUAÇÃO EM
COMPUTAÇÃO APLICADA

Flexibilizando Graus de Colaboração, Segurança e Privacidade na Descoberta de Serviços

por

EDUARDO MOSCHETTA

Dissertação submetida a avaliação como requisito parcial para a obtenção do grau de Mestre em Computação Aplicada

Orientador: Prof Dr. Marinho Pilla Barcellos

São Leopoldo, março de 2008

CIP — CATALOGAÇÃO NA PUBLICAÇÃO

Moschetta, Eduardo

Flexibilizando Graus de Colaboração, Segurança e Privacidade na Descoberta de Serviços
/ por Eduardo Moschetta. — São Leopoldo: Área de Exatas e Tecnológicas da UNISINOS, 2008.

64 f.: il.

Dissertação (mestrado) — Universidade do Vale do Rio dos Sinos. Área de Exatas e Tecnológicas Programa Interdisciplinar de Pós-Graduação em Computação Aplicada, São Leopoldo, BR–RS, 2008. Orientador: Barcellos, Marinho Pilla.

I. Barcellos, Marinho Pilla. II. Título.

Em primeiro lugar, agradeço a Deus, por ter me dado inúmeras forças ao longo desses dois anos de pesquisa, quando dividi meus dias entre o trabalho de tempo integral e um mestrado praticamente noturno. Nem por isso deixei de fazer um trabalho de qualidade, pois Ele me deu perseverança, paciência e vontade de abdicar de minhas horas de lazer à noite e fins de semana ao lado de meus amigos e família. Agradeço à minha família e minha esposa, pela sua habitual compreensão e auxílio nas horas mais difíceis. E um agradecimento especial ao meu orientador, que foi fundamental neste trabalho, com seu grande conhecimento técnico, experiência e profissionalismo. Através dele, foi possível atingir um bom nível de maturidade para o trabalho de pesquisa e para minha pessoa, como pesquisador.

Sumário

Lista de Figuras

Resumo

Este trabalho apresenta *Flexible Secure Service Discovery* (FSSD), um protocolo para a descoberta de serviços em sistemas ubíquos. Seu projeto é centrado no compromisso entre os níveis de colaboração, segurança e privacidade que os participantes desejam na descoberta. A abordagem proposta oferece gerenciamento de confiança, além de mecanismos de controle de exposição e de acesso descentralizados. As propriedades do protocolo foram avaliadas através de simulações, variando-se os níveis de segurança e privacidade do sistema para demonstrar que a abordagem proposta lida adequadamente com o compromisso em relação à colaboração entre pares.

Palavras-chave: Descoberta de serviços, Controle de exposição, Rede de confiança.

TITLE: "FLEXIBLE COLLABORATION, SECURITY AND PRIVACY IN SERVICE DISCOVERY SYSTEMS"

Abstract

This work presents *Flexible Secure Service Discovery* (FSSD), a protocol for service discovery in ubiquitous systems. Its design is centered at the tradeoff among the levels of collaboration, security and privacy desired by the participants. The proposed approach provides trust management, in addition to descentralized mechanisms to control the exposure and access to the service information. The protocol properties were evaluated with simulation, by varying both security and privacy levels of the system in order to demonstrate that the proposed approach properly addresses the tradeoff regarding peer collaboration.

Keywords: Service discovery, Exposure control, Trust network.

Capítulo 1

Introdução

A descoberta de serviços foi introduzida em sistemas distribuídos com o intuito de reduzir o custo de administração na provisão e no uso de serviços da rede. Ela permite a detecção automática de dispositivos e serviços, os quais são anunciados através de protocolos e formatos de dados conhecidos. Com o advento da computação ubíqua, observado principalmente na proliferação de uma variedade de dispositivos computacionais e no uso ubíquo de redes sem fio, a descoberta de serviços se torna imprescindível. O nível de transparência que ela oferece entre o sistema e o usuário é uma característica importante para a obtenção de sistemas o mais independentes possível da intervenção humana em sua configuração, previstos pela computação ubíqua.

Um dos grandes desafios em ambientes ubíquos é como obter propriedades desejáveis de uma infra-estrutura de rede ou de sistema (como escalabilidade, segurança, fácil administração, etc) sem muitas vezes haver a infra-estrutura propriamente dita [Edwards, 2006]. Em outros casos, a mesma estará presente, porém limitada a um determinado número de usuários por meio de mecanismos de autenticação e autorização. A formação de redes *ad hoc* permite contornar o problema de infra-estrutura de rede para a descoberta de serviços [Chakraborty et al., 2006]. Usuários ou dispositivos desses e do ambiente (doravante denominados **pares**) podem colaborar nas tarefas de anúncio e descoberta de serviços, tal como propagando anúncios ou consultas de serviços aos seus vizinhos da rede, verificando se um serviço anunciado atende a uma consulta recebida, entre outras.

Entretanto, sistemas movidos pela colaboração entre pares devem lidar com a possível presença de pares mal-intencionados, cujos objetivos incluem obter vantagens por conta de outros pares e corromper o funcionamento do sistema. Em ambientes sem garantias de uma infra-estrutura de segurança fixa, fica difícil a autenticação de serviços/consultas e a implantação de controle de acesso. Além destas questões de segurança, a descoberta de serviços leva a problemas de privacidade: a troca de mensagens necessária para a mesma implica a exposição de informações sensíveis como identidade, perfil do participante, etc. Na ausência de segurança e privacidade, pares podem limitar a sua predisposição a colaborar, comprometendo assim a eficácia da descoberta de serviços no ambiente.

1.1 Motivação

Parte dos trabalhos existentes na área de descoberta de serviços são propostas orientadas a redes *ad hoc*, e portanto em contexto similar, tais como [Chakraborty et al., 2006] e [Lenders et al., 2005]. Todavia, esses trabalhos não consideram questões de segurança e privacidade, por decisão de projeto. De fato, prover segurança e privacidade em redes *ad hoc* não é uma tarefa trivial, visto que estas não podem depender de recursos geralmente encontrados em infra-estruturas de rede fixa, tais como servidores de PKI (*Public-Key Infrastructure*) e de controle de acesso.

No mesmo sentido, outros trabalhos (como [Czerwinski et al., 1999] e [Zhu et al., 2005b]) apresentam soluções para segurança e privacidade na descoberta de serviços em um contexto mais favorável: redes corporativas ou domínios administrados pelo próprio usuário, prevendo a colaboração entre pares sob um mesmo domínio administrativo. As soluções de segurança propostas em [Almenárez and Campo, 2003] e [Wishart et al., 2005] podem ser aplicadas em redes *ad hoc*, porém os mecanismos apresentados são empregados somente *após* a descoberta ter sido realizada. Como mencionado anteriormente, as mensagens trocadas *durante* a descoberta expõem informações sensíveis do usuário, colocando em risco sua privacidade.

A segurança e privacidade na descoberta de serviços para redes *ad hoc* é um tema desafiador, porém pouco explorado na literatura, o que contrasta com sua importância para o estágio atual da computação ubíqua. Em um cenário ideal de ambiente ubíquo, pares colaborariam entre si para obter uma descoberta de serviços eficaz, que assim refletisse a capacidade e os recursos do ambiente e dos usuários que ali se encontram. Entretanto, sem os devidos mecanismos de segurança e privacidade, pares podem estar menos predispostos a colaborar na descoberta de serviços. Entre fatores que contribuem para isso, destacam-se:

- Transparência [Satyanarayanan, 2001]: a computação ubíqua visa tornar a exploração de ambientes, dispositivos e serviços "invisível". Na prática, uma aproximação razoável para invisibilidade seria o mínimo de distração para o usuário. O alto nível de transparência almejado requer que o usuário se exponha mais ao sistema (e aos demais usuários), colocando em risco sua privacidade [Sackmann et al., 2006].

- Incerteza [Cahill et al., 2003]: à medida que a computação ubíqua é incorporada no cotidiano dos usuários, os mesmos irão se deparar com situações onde as interações envolvem elementos de incerteza. Por exemplo, utilizar um serviço anunciado em um ambiente nunca visitado antes é um fator de risco para o usuário.

1.2 Objetivos e Contribuição

Um dos principais objetivos deste trabalho é investigar o compromisso (*tradeoff*) entre colaboração, segurança e privacidade na descoberta de serviços para redes *ad hoc*. Como será discutido na Seção 3.2, é praticamente impossível desenvolver um sistema que obtenha o melhor dos três aspectos. Isso talvez explique porque trabalhos relacionados até o momento não propuseram soluções nesse sentido.

Outro objetivo secundário desta dissertação é apresentar uma revisão das principais propostas na área de descoberta de serviços que lidam com pelo menos um destes aspectos.

A principal contribuição deste trabalho é a proposta de um protocolo para **descoberta de serviços flexível** em ambientes ubíquos. O protocolo, denominado FSSD (*Flexible Secure Service Discovery*), tem como principal característica permitir que usuários ajustem o grau de colaboração em função dos níveis de segurança e privacidade desejados. Nesse contexto, o compromisso entre os três aspectos deixa de ser um problema no projeto do sistema, e torna-se um ajuste que reflete as necessidades dos usuários em tempo de execução. Essas necessidades podem ser momentâneas, podem variar em diferentes ambientes, podem ser relativas a determinados serviços, etc. A flexibilidade obtida consiste em poder alterar dinamicamente o balanço entre estes três aspectos.

A solução proposta emprega mecanismos conhecidos, tais como gerenciamento de confiança [Jösang et al., 2007] (que permite mitigar a ausência de uma infra-estrutura de segurança fixa) e criptografia de chave pública para criar canais seguros entre pares que possuem uma relação de confiança mútua. O trabalho introduz dois mecanismos adicionais: um para o controle de exposição, que gerencia a quantidade de informações sensíveis sendo propagadas em anúncios e consultas de serviços; e um mecanismo de casamento (*matching*) *in-network*, no qual pares intermediários verificam se cliente e provedor estão autorizados a interagirem, sem que ambos se exponham de forma prematura. Esses quatro mecanismos, cerne do FSSD, são descentralizados, tendo em vista o foco do trabalho em redes *ad hoc*.

Com a finalidade de avaliar o protocolo, outro objetivo deste trabalho consiste na implementação de um protótipo do FSSD em um ambiente de simulação. A avaliação será dirigida principalmente por métricas que permitem avaliar os efeitos no ajuste do compromisso por parte dos usuários. Visto que não existem trabalhos semelhantes ao presente, não serão realizados experimentos comparativos entre FSSD e outros protocolos.

O restante deste documento encontra-se organizado como segue. O Capítulo 2 apresenta uma revisão bibliográfica da área de descoberta de serviços, focando em desafios desta área na computação ubíqua e discutindo trabalhos relacionados. O Capítulo 3 descreve o projeto do FSSD, tratando desde os cenários alvo e requisitos para sua construção, até uma descrição de sua arquitetura, incluindo um exemplo ilustrativo de seu funcionamento. No Capítulo 4, discute-se o modelo de simulação do protocolo e os resultados obtidos através de experimentos com o mesmo. Por fim, o Capítulo 5 tece considerações finais e uma agenda para trabalhos futuros.

Capítulo 2

Descoberta de Serviços

Este capítulo oferece uma síntese da área de descoberta de serviços. Primeiramente, será apresentada a terminologia adotada no restante do trabalho, facilitando a comparação entre este e trabalhos relacionados. Na seqüência, serão discutidos desafios para a descoberta de serviços na computação ubíqua, principalmente aqueles que dizem respeito a questões de segurança e privacidade. Por fim, são apresentados trabalhos relacionados que exploram o uso de redes *ad hoc* e mecanismos de segurança e privacidade; estes aspectos formam a base do desenvolvimento do presente trabalho.

2.1 Terminologia

Sistemas de descoberta de serviços foram inicialmente concebidos com o propósito de localizar instâncias de serviços que atendam aos requisitos de um cliente, com a mínima sobrecarga possível de configuração. Um serviço pode ser qualquer entidade de hardware ou software que pode ser utilizada por clientes. Também podem ser armazenados e providos por uma série de periféricos, dispositivos, computadores, entre outros equipamentos. Uma vez obtida sua localização (por exemplo, um endereço IP e uma porta) o serviço encontrado pode ser utilizado pelo cliente, ou então pode haver uma etapa de autenticação e autorização quando é verificado se o cliente pode acessar o mesmo. A etapa de descoberta geralmente envolve duas entidades: **provedor**, que anuncia serviços; e **cliente**, que procura por serviços. Uma terceira entidade (**diretório**) também é comumente utilizada, como será comentado a seguir.

Em linhas gerais, a descoberta de serviços resolve o problema de **associação** entre dispositivos de um ambiente ou sistema [Kindberg and Fox, 2002]. Geralmente esse estágio é antecedido pela fase de **iniciação** e sucedido pela fase de **interação**. Na primeira fase, são definidos os parâmetros necessários para um dispositivo se integrar a uma rede ou sistema de descoberta. Uma vez associados, clientes e serviços podem interagir dado um modelo comum de interoperabilidade. Quanto maior a padronização na especificação destes serviços, maior será o grau de associação. Redes institucionais com escopo administrativo são exemplos de cenários caracterizados pelo alto grau de associação entre clientes e serviços providos pela rede.

É possível encontrar na literatura referências à "descoberta de recursos", muito embora "descoberta de serviços" seja mais adequado para o presente trabalho. Um recurso é algo que pode ser especificado e alocado de forma quantitativa

(por exemplo, número de processadores e tamanho de memória) em função da necessidade de utilização, enquanto que um serviço deve ser compreendido como algo disponibilizado por um provedor [Lima et al., 2007]. Além de recursos e serviços, outras categorias de objeto para descoberta vieram a ser suportadas ao longo da evolução dos sistemas de informação, a fim de atender às necessidades das comunidades que as criaram. Em 1983, por exemplo, o problema de gerenciamento de nomes frente ao crescimento de usuários da ARPAnet levou à criação do DNS, sistema de resolução de nomes atualmente implantado na Internet.

Existe uma gama de trabalhos na área de descoberta de serviços. Em [Lima et al., 2007], os autores separam esses trabalhos em três categorias principais: aqueles que são aplicados a redes fixas, a redes sem fio de um salto e a redes sem fio de múltiplos saltos (MANETs). Embora cada categoria conduza a princípios de projeto diferentes, é possível obter uma taxonomia para classificar os sistemas de descoberta de serviços existentes. Ainda em [Lima et al., 2007], os autores definem esta taxonomia através de uma compilação de trabalhos relacionados como [Zhu et al., 2005a], [Marin-Perianu et al., 2005] e [Mian et al., 2006]. Os principais aspectos dessa classificação, aplicados diretamente ao presente trabalho, são reproduzidos a seguir:

- **Arquitetura**: pode ser centralizada ou descentralizada, dependendo da existência de diretórios na infra-estrutura de descoberta. Diretórios são componentes desta infra-estrutura que armazenam informações sobre serviços e suas disponibilidades, com base em anúncios enviados na rede. Além do registro e descoberta, diretórios podem oferecer outras funcionalidades, como autenticação e autorização para a descoberta de serviços do repositório [Czerwinski et al., 1999]. Mais de um diretório pode ser utilizado em uma infra-estrutura, seja para fins de escalabilidade, seja para associar um domínio para cada diretório. Estes podem ser organizados de forma par-a-par (P2P) ou de forma hierárquica. Por outro lado, em protocolos que não dependem de diretórios, serviços e clientes são responsáveis por processar todo tipo de requisições e anúncios.

- **Escopo**: pode ser baseado na topologia da rede, influenciado pelo papel do usuário, dirigido por informações de contexto ou uma combinação dos mesmos. A primeira é a forma mais comum, onde redes locais (LANs) e redes sem-fio de um salto (topologias geralmente empregadas) definem a forma de propagação e o alcance lógico das mensagens de descoberta. Uma premissa nesse caso é que clientes, serviços e diretórios pertencem a um mesmo domínio administrativo, como uma casa, um ambiente corporativo ou provedor à rede sem-fio metropolitana. Em outros casos, protocolos de descoberta de serviços suportam um conjunto de domínios como escopo possível da descoberta, e assim permitem que o usuário tenha influência na definição, em uma granularidade mais fina, de quais domínios deseja que façam parte do escopo final. Esse é um exemplo de escopo influenciado pelo papel do usuário. Informações de contexto em alto nível, tais como informações de tempo e espaço, também podem auxiliar na definição do escopo da descoberta. Como identificado por Kindberg [Kindberg and Fox, 2002], o significado de "aqui", ao representar a posição espacial de um usuário, torna-se uma importante ferramenta para a descoberta de serviços baseada em contexto.

- **Gerenciamento da informação de serviço**: o método de consulta utilizado pode ser entendido como um processo de busca atrelado a um casamento (*matching*) entre as requisições de descoberta (demandas), ou simplesmente **consultas**, e as descrições de serviços locais e remotos (ofertas), estas últimas divulgadas através de **anúncios** ou registradas em diretórios. O algoritmo de casamento utilizado representa uma função que aceita como entrada a demanda e um conjunto de descrições de ofertas, gerando como resultado o subconjunto das ofertas que satisfazem a demanda especificada. As funções de comparação empregadas pelo algoritmo de casamento podem variar entre comparação de atributos, comparação semântica (geralmente fazendo uso de padrões como XML) ou dependente da linguagem de programação. No último caso, as estruturas da linguagem são utilizadas para definir consultas e anúncios de serviços.

- **Mecanismos de requisição e anúncio de serviços**: abordagens para a troca de informações na descoberta de serviços podem ser baseadas em requisições ou anúncios, às vezes descritas como comunicação ativa e passiva, ou *pull* e *push*, respectivamente. Na primeira abordagem, clientes agem somente quando querem requisitar determinado serviço. Nesse caso, enviam uma mensagem de consulta, que é respondida por serviços que atendam aos requisitos informados na mensagem. Na segunda abordagem, serviços anunciam sua disponibilidade e demais informações relacionadas através de mensagens periódicas destinadas a toda ou parte de uma rede. Clientes interessados permanecem em modo passivo, esperando pela chegada destes anúncios e aprendendo sobre estes serviços. Um terceiro componente, o diretório ou **negociador** (*broker*), pode coletar tais anúncios com vistas a oferecer um repositório de informações de serviço aos pares da rede, que por sua vez podem direcionar consultas de serviços ao mesmo.

- **Armazenamento**: informações de serviços, divulgadas em anúncios periódicos ou em resposta a consultas, são armazenadas em repositórios centralizados ou descentralizados. A primeira abordagem corresponde ao uso de diretórios, enquanto que a segunda assume que cada dispositivo da rede possui seu próprio repositório local, onde armazenam informações de serviços que disponibilizam, bem como de serviços anunciados por outros. A abordagem descentralizada pode ainda ser subdividida em "cooperativa" e "não-cooperativa", dependendo se cada par atua de forma independente dos demais quanto ao armazenamento. Em outras palavras, no primeiro caso os dispositivos mantêm informações parciais sobre os serviços da rede, enquanto no segundo armazenam informações sobre *todos* os serviços da rede, buscando manter uma visão global do sistema. A versão cooperativa geralmente é mais atrativa, pois se restringe o armazenamento em função de critérios como espaço disponível, sobrecarga etc.

- **Validade**: independente da abordagem de armazenamento utilizada, as informações têm sua validade representada em *soft-state* ou *hard-state*. Na primeira forma (comumente empregada em armazenamento descentralizado) a validade da informação é especificada no corpo da mensagem de anúncio e precisa ser atualizada periodicamente pelo seu provedor antes que expire, o que tornaria o serviço inalcançável. Caso as informações sejam mantidas em *hard-*

state, elas só serão removidas se o provedor do serviço solicitar explicitamente a sua remoção, ou então for constatada a indisponibilidade do serviço, ao se tentar utilizá-lo.

- **Seleção dos serviços**: visando lidar com o conjunto de resultados provenientes da descoberta realizada, é necessária uma etapa de seleção, a qual pode ser manual ou automática. No primeiro caso, é concedido ao usuário controle total sobre os resultados da consulta, permitindo que esse navegue sobre a lista resultante de serviços e escolha aquele que considerar mais adequado. Na seleção automática, em contraste, o protocolo de descoberta também é responsável pela seleção de uma única instância do serviço, realizada através de mecanismos que comparam os atributos requisitados pelo usuário com a capacidade anunciada pelos serviços candidatos.

- **Suporte à mobilidade**: em arquiteturas de armazenamento descentralizadas, uma preocupação adicional é assegurar que as informações de serviços se encontram atualizadas, principalmente considerando cenários de mobilidade de serviços e clientes. Para tanto, três abordagens são utilizadas: atualização das informações de serviços, que pode ser pró-ativa (anúncios periódicos e uso de armazenamento *soft-state*) ou reativa (disparada por alterações na topologia ou outros eventos, gerados por protocolos de roteamento em MANETs, por exemplo); controle de anúncios, através do emprego de medidas como alteração da taxa ou diâmetro dos anúncios; e uso de redes *overlay* com algoritmos que visam manter sua estrutura, mediante a mobilidade. Grande parte dos protocolos depende de infra-estrutura fixa para seu funcionamento, o que caracteriza um fator limitante de suporte à mobilidade.

O conceito da infra-estrutura de descoberta é central para este trabalho. Basicamente, ela compreende a base de componentes de hardware e software que viabilizam a descoberta de serviços. Geralmente se encontra sobre uma infra-estrutura de rede (roteadores, pontos de acesso, protocolos de roteamento etc) que permite o envio de anúncios e consultas entre os pares por meio de uma rede fixa ou móvel. Entre essas duas infra-estruturas, é possível haver uma infra-estrutura de segurança, composta por entidades certificadoras, servidores para controle de acesso entre outros. A maioria dos sistemas de descoberta que suportam mecanismos de segurança e privacidade dependem de tal infra-estrutura, como será discutido a seguir. Por fim, em alguns casos, a infra-estrutura de descoberta compreende, além de aplicativos clientes para anúncio e consultas, o uso de diretórios.

2.2 Descoberta de Serviços na Computação Ubíqua

Em [Weiser, 1991], o autor levou à comunidade científica sua visão sobre o computador "invisível". Através dela, o computador iria se tornar uma ferramenta tão comum quanto um lápis, de tal forma que a presença da tecnologia seria transparente ao usuário e tornaria o uso da computação mais conveniente ao mesmo.

O trabalho [Satyanarayanan, 2001] foi um do pioneiros em propor desafios de pesquisa mais concretos em relação às idéias de Weiser. O artigo analisa as diferenças entre sistemas distribuídos, móveis e ubíquos, o que auxilia na tarefa

de projetar sistemas para computação ubíqua. No mesmo trabalho, são propostas quatro novas frentes de pesquisa no estudo desses sistemas: uso efetivo de espaços inteligentes (*smart spaces*); mínima distração possível aos usuários, que na prática, seria uma aproximação à invisibilidade prevista por Weiser; escalabilidade, não somente considerando a carga de processamento e comunicação, mas também a distância física entre as interações; e o mascaramento de condições diversas, tais como estrutura organizacional, que possam impedir a penetração uniforme da computação ubíqua na infra-estrutura fixa existente.

Duas características chave e intrínsecas de sistemas ubíquos são identificadas em [Kindberg and Fox, 2002]:

- **Integração entre dispositivos computacionais e objetos do mundo físico**. A integração entre *smart spaces* e dispositivos móveis de usuários é um bom exemplo da integração física almejada pela computação ubíqua. O principal objetivo é estender o mundo físico ao usuário, fornecendo-lhe serviços além daqueles providos pelas tecnologias digitais até então existentes. Nesse contexto, configurar o ar condicionado de acordo com o perfil do usuário é um bom exemplo dessa integração, enquanto que uma rede de laptops conectados através de uma malha sem fio não é um exemplo, dado que os usuários desses laptops têm acesso apenas à parte virtual do mundo (mais especificamente, a Internet).

- **Interoperabilidade espontânea entre componentes**. Por espontaneidade entende-se como a capacidade de componentes de lidarem com a dinâmica e imprevisibilidade característica de outros componentes, sejam estes serviços, clientes, recursos ou aplicações. Na computação ubíqua, a heterogeneidade ganha uma nova dimensão: além da variedade de dispositivos e tipos de informação, geralmente assumida em ambientes móveis, a funcionalidade provida por componentes do ambiente pode variar no tempo. Como postula Kindberg, esse conjunto altamente dinâmico de componentes deve ainda ser governado por invariantes bem definidas, com vistas a obter a interoperabilidade desejada.

Estas características possuem sérias implicações no projeto da infra-estrutura de software ubíquo. Segundo [Kindberg and Fox, 2002], o projeto de um sistema ubíquo é extremamente desafiador, pois deve atender às expectativas do usuário sob condições extremamente dinâmicas e imprevisíveis. Os usuários não vêem o mundo físico como um conjunto de ambientes computacionais, mas como um conjunto de lugares com semânticas culturais e administrativas diferentes. A descoberta de serviços, como cita a mesma referência, é um mecanismo fundamental no projeto destes sistemas. Ela exerce um papel de integrador espontâneo entre componentes, frente à heterogeneidade destes e de suas funcionalidades, mas que obedecem a um formato comum de interoperabilidade.

O restante desta seção está dividida em desafios para a descoberta de serviços segundo diferentes óticas. Na primeira parte, são apresentados desafios gerais, incluindo obtenção propriedades desejáveis de infra-estrutura para a descoberta, definição de escopo, entre outros. Na segunda e terceira partes, são discutidos desafios envolvendo as questões de segurança e privacidade, respectivamente. Antes de prosseguir, porém, é importante distinguir os termos privacidade e confidencialidade (um dos requisitos de segurança), que algumas vezes têm sido usado ambigüamente na literatura:

- **privacidade na informação:** segundo [Clarke, 2006], "é o interesse que um indivíduo tem em controlar, ou pelo menos influenciar significativamente, o uso de dados referentes a ele mesmo".

- **confidencialidade:** "é a obrigação legal de indivíduos com a posse de informações que adquirem sobre outros, especialmente no curso de tipos particulares de relacionamento entre eles" [Clarke, 2006]. Uma definição mais adotada no contexto de sistemas computacionais de segurança é "a proteção dos dados contra a exposição não-autorizada" [Stallings, 2005].

2.2.1 Desafios gerais para a descoberta de serviços

Alguns trabalhos na literatura têm apontado desafios de longo prazo para o desenvolvimento de sistemas ubíquos. Esta seção se concentra em desafios diretamente relacionados à descoberta de serviços, que incluem os aspectos de integração de sistemas ubíquos com indivíduos e ambientes [Zhu et al., 2005a], infra-estrutura necessária [Edwards, 2006] e interoperabilidade e espontaneidade entre componentes de ambientes ubíquos [Kindberg and Fox, 2002].

A integração entre sistemas ubíquos e indivíduos é um grande desafio e está longe de ser solucionado nos sistemas de descoberta existentes. Esses sistemas se concentram na interoperabilidade entre aplicações e dispositivos, prevêem interações apenas entre componentes tradicionais de um sistema de descoberta (aplicativos clientes, serviços ou diretórios) e, devido a estes e outros fatores, requerem usuários com conhecimento especializado para sua configuração (como aquele executado por administradores da rede de uma corporação, por exemplo). Em acréscimo, assume-se papéis de usuários bem definidos: administradores da rede, que definem a infra-estrutura de descoberta e a terminologia utilizada (nome, atributos, etc) para descrever estes serviços; e usuários normais da rede, que utilizam aplicativos clientes para realizar a descoberta. Na computação ubíqua, entretanto, usuários potencialmente possuem duplo papel (podem ser tanto clientes como provedores), o que aumenta o problema de usabilidade, ao demandar de usuários a habilidade de configurar serviços providos e aplicativos clientes.

A integração entre sistemas ubíquos e ambientes é igualmente desafiadora, e mais recente, pois representa uma visão diferente no plano de serviços. Protocolos existentes foram projetados para executarem sobre LANs ou redes sem fio de múltiplos saltos. Porém, o escopo de serviços na computação ubíqua assume semânticas diferentes: muitos ambientes ubíquos são mais bem definidos por limites físicos, localização e outras informações de contexto, o que é difícil de representar com escopos baseados em LANs e MANETs [Kindberg and Fox, 2002, Zhu et al., 2005a]. Outra característica importante nessa integração é o significado de "aqui" [Kindberg and Fox, 2002]; através deste, usuários podem limitar a descoberta aos serviços mais próximos dos mesmos. Tanto "aqui" como espaços físicos constituem-se em artifícios para fornecer uma construção de escopo mais compreensível aos seus usuários. Serviços que estão sujeitos a este tipo de escopo são mais conhecidos como "serviços de ambiente" [Herrmann et al., 2005].

Ao contrário de ambientes corporativos, onde indivíduos podem fazer uso de uma infra-estrutura de segurança para acesso a recursos e serviços, em ambientes ubíquos essa dependência não escala de forma satisfatória. Nestes ambientes, não existe necessariamente uma infra-estrutura [Edwards, 2006], e mesmo se uma está presente, o acesso à mesma pode ser restrito devido a questões não-técnicas como

estrutura organizacional e modelo de negócios [Satyanarayanan, 2001]. Estes fatores impedem uma penetração uniforme da computação ubíqua em ambientes diversos, que por outro lado seria possível graças a uma infra-estrutura em comum. Nesse contexto, o desafio compreende o projeto de sistemas de descoberta que exibam propriedades desejadas de uma infra-estrutura (tais como escalabilidade, robustez, segurança e facilidade de administração) sob os mais diversos cenários de ambiente, incluindo os dois supracitados.

Além dos aspectos de infra-estrutura e integração, é reconhecida também a importância da interoperabilidade e espontaneidade em ambientes ubíquos. Visto que todo usuário é um provedor de serviços em potencial, aumenta-se a exigência de formatos comuns de interoperabilidade; caso contrário, provedores podem, em um caso extremo, descrever serviços utilizando terminologias diferentes e utilizando protocolos de descoberta incompatíveis entre si. A espontaneidade, por sua vez, deve refletir nos componentes do sistema as alterações que diriam respeito à disponibilidade, comportamento ou confiança dos componentes. Tais mudanças são comuns em ambientes ubíquos em função da dinâmica graças à mobilidade, colaboração entre pares, etc. O suporte à mobilidade e a dinâmica presente nas requisições e anúncios de serviços (apresentados na Seção 2.1) são fundamentais nesse aspecto.

2.2.2 Desafios em segurança para a descoberta de serviços

Em [Zhu et al., 2005a] são discutidos vários desafios em segurança para descoberta de serviços em computação ubíqua. O restante dessa seção reproduz os principais desafios discutidos no artigo.

Ao contrário de redes corporativas, cenários ubíquos não podem valer-se sempre de um escopo estruturado através de domínios administrativos, protegido por firewall e gerenciado por usuários especializados (isto é, administradores de rede). Assim como é difícil definir o escopo de um ambiente ubíquo, como comentado anteriormente, conseqüentemente se torna difícil também definir o escopo de um serviço deste ambiente. Sem um escopo definido, os mecanismos de segurança sob esse serviço devem ser disponibilizados pelo seu provedor, o que muitas vezes pode não estar de acordo com os mecanismos providos pelo ambiente em si. Por outro lado, quando se consegue definir o escopo de um ambiente (através de mecanismos conscientes de localização, por exemplo), os serviços sob o mesmo não serão necessariamente gerenciados por um único usuário.

Outro problema é ausência de domínio administrativo ou a existência de múltiplos em um ambiente ubíquo, o que limita (ou dificulta) o compartilhamento de informações relacionadas à segurança tais como chave pública, credenciais, entre outras. Em muitos casos, também não será possível ter conhecimento prévio sobre pares e serviços providos. Logo, uma das primeiras perguntas que vem à tona é: como verificar se um par ou serviço é legítimo, antes de concretizar uma interação entre provedor e cliente [Zhu et al., 2005a]? Legitimidade, nesse caso, se refere tanto à presença de credenciais válidas quanto ao acesso privilegiado, correspondendo às etapas de autenticidade e autorização, respectivamente.

Além da legitimidade, a qualidade de um serviço anunciado também deveria ser apurada, especialmente em ambientes dinâmicos e incertos como os previstos pela computação ubíqua, onde componentes são potencialmente transientes [Wishart et al., 2005]. Uma possível solução é o emprego de sistemas de

confiança ou de reputação [Jösang et al., 2007], que são mais adequados para redes *ad hoc*. Nesses sistemas, participantes expressam suas opiniões sobre serviços/pares através de votos, divulgando-os pela rede. Esta informação pode ser consolidada em um servidor central ou em cada participante, refletindo então a qualidade do serviço/par na perspectiva dos pares que têm interagido com o mesmo. Trabalhos como [Almenárez and Campo, 2003] fazem uso de sistemas de confiança para contornar a ausência de uma PKI centralizada, oferecendo assim uma abordagem anárquica para testar a legitimidade de pares.

Por fim, a construção de novos mecanismos de segurança para a descoberta de serviços deve ser centrada no usuário. É necessária a criação de ferramentas inteligentes que levem em conta o perfil e papel do usuário no momento da descoberta, e não apenas características da aplicação e do dispositivo que o usuário está utilizando. Como exemplo, usuários que utilizam um mesmo dispositivo, em diferentes momentos, devem ser capazes de descobrir diferentes serviços em um mesmo ambiente, dependendo de seus perfis e credenciais de acesso. Essas ferramentas também devem ser capazes de gerenciar as informações de segurança para o usuário e utilizá-las de forma conveniente ao mesmo. Nesse sentido, alguns exemplos que podem melhorar a usabilidade durante a descoberta de serviços incluem o fornecimento automático de credenciais sob diferentes domínios [Zhu et al., 2006] e interfaces que permitem selecionar as informações a serem expostas em anúncios e consultas (a ser discutido a seguir).

2.2.3 Desafios em privacidade para a descoberta de serviços

A questão da invisibilidade na computação ubíqua, discutida em [Satyanarayanan, 2001], requer o projeto de sistemas que oferecem alto nível de transparência para seus usuários. A descoberta de serviços exerce papel fundamental nesse aspecto, como discutido anteriormente; entretanto, seu uso leva à exposição de informações sensíveis de provedores e clientes. Estas informações compreendem desde a "presença do usuário" (a qual pode ser inferida pelos endereços de enlace e de rede utilizados nas mensagens de descoberta, ou por tecnologias como RFID (*Radio-Frequency Identification*) e GPS (*Global Positioning System*)) até dados mais sensíveis, como identidades e a intenção do usuário, capturadas pelas mensagens de descoberta [Zhu et al., 2005a, Carminati et al., 2005].

Restringir o envio de informações sensíveis apenas a entidades legítimas mitiga, porém não resolve, o problema de privacidade. Nesse caso, a legitimidade de um par expressa a condição de poder utilizar a informação para qualquer fim, seja para armazenamento próprio ou para acessar um determinado serviço que está representado na informação. Não é possível, por exemplo, indicar quais as operações que podem ser realizadas com a informação recebida, muito menos garantir que o conjunto de operações possíveis seja realmente obedecido.

Segundo Clarke [Clarke, 2006], proteção de privacidade é o processo de encontrar equilíbrios adequados entre a privacidade e interesses conflitantes. Por exemplo, os interesses privados de uma pessoa podem conflitar com outros interesses seus, como é o caso da obtenção de serviços personalizados [Sackmann et al., 2006]. Nesse caso, informações como identidade do usuário, localização, rastreamento de suas atividades, entre outras, podem ser empregadas para personalizar um determinado serviço. Isso gera um compromisso entre privacidade e personalização, que deve ser tratado pelo próprio usuário, isto é, o mesmo deve decidir se libera tais

informações em benefício de uma maior personalização.

Uma tecnologia que será valiosa para a proteção de privacidade em computação ubíqua é **protocolos de etiquetagem** (*labeling protocols*) [Ackerman and Mark, 2004]. Protocolos, ou linguagens, dessa categoria incluem P3P (*Platform for Privacy Preferences Project* [W3, 2006]), EPAL (*Enterprise Privacy Authorization Language* [Ashley et al., 2003]) e XACML (*eXtensible Access Control Markup Language* [Oasi, 2005]). Seu principal propósito é a publicação de políticas de privacidade do requisitante, que governam a transmissão de dados privados do usuário durante sua interação com o primeiro. Um exemplo prático de P3P é dado a seguir: empresas publicam em seus *websites* declarações de políticas de privacidade (propostas P3P), que são carregadas pelo navegador de Internet do usuário e comparadas com suas preferências de privacidade. Caso as declarações atendam às preferências definidas, o navegador aceita a transferência do conteúdo privado do usuário.

O protocolo P3P sofre de duas limitações principais [Ashley et al., 2003]: problemas com usabilidade, dado que existe uma terminologia pré-definida para especificar políticas de privacidade; e a ausência de mecanismos que permitem garantir o seguimento da política de privacidade. Estas limitações são resolvidas pelos outros dois protocolos, EPAL e XACML. De qualquer forma, os mecanismos que garantem o seguimento de uma política são difíceis de serem implantados em um ambiente ubíquo, por necessitarem de um domínio administrativo bem definido.

Em [Langheinrich, 2001], o autor descreve seis princípios a serem utilizados no desenvolvimento de soluções que protejam a privacidade em computação ubíqua: (1) notificação e exposição, (2) escolha e consentimento, (3) anonimidade e pseudo-anonimidade, (4) proximidade e localidade, (5) segurança adequada e (6) acesso e recurso. Em resumo, o autor considera o primeiro o mais importante, pois através dele, a coleta de informações sensíveis é notificada ao usuário, que então tem consciência sobre sua atual exposição ao sistema. Os três primeiros princípios são difíceis de serem concebidos na prática; uma possível solução é utilizar os conceitos de proximidade e localidade, mesmo que isso leve a pequenos ajustes de cunho social. Por exemplo, usuários consentem com a coleta de seus dados sensíveis somente se o dono do mecanismo coletor se encontra no mesmo ambiente físico. Já o princípio de segurança vem antes de qualquer questão sobre privacidade, visto que serviços como autenticação e confidencialidade na comunicação são fundamentais para protocolos e política de privacidade. Por fim, o princípio de acesso e recurso é mais utilizado no mundo jurídico. Entretanto, pode-se ter facilitadores no mundo digital, como por exemplo, utilizar propostas P3P com assinaturas digitais, o que garante o não-repúdio no caso de disputas judiciais.

2.3 Trabalhos Relacionados

Esta seção apresenta os protocolos e sistemas de descoberta de serviços mais relevantes no contexto deste trabalho. A área de descoberta é bastante segmentada, muito devido aos diferentes tipos de topologias de rede existentes, que demandam sistemas de descoberta específicos. Em [Lima et al., 2007], é feita uma revisão bibliográfica desses sistemas para redes fixas, redes móveis de um salto e redes móveis de múltiplos saltos. Outros exemplos incluem a descoberta de serviços na Internet (Web Services) e redes celulares. Este trabalho foca na revisão de sistemas de

descoberta existentes que apresentam soluções para redes *ad hoc*, por serem propícias para ambientes ubíquos, ou naqueles que empreguem mecanismos de segurança e privacidade para ambientes ubíquos. Ao final desta seção, é realizada uma discussão envolvendo os trabalhos do último grupo, destacando suas limitações frente aos problemas de segurança e privacidade já discutidos na Seção 2.2.

2.3.1 Descoberta de serviços para redes *ad hoc*

Todos os protocolos apresentados nesta seção operam sobre uma rede de múltiplos saltos (MANETs). No protocolo GSD (*Group-Based Service Discovery*) [Chakraborty et al., 2006], serviços são categorizados segundo uma hierarquia de grupos; por exemplo, uma impressora a laser pertence ao grupo de impressoras, que pertence ao grupo de periféricos e etc. Pares anunciam periodicamente seus serviços aos vizinhos dentro do alcance da comunicação sem fio, os quais armazenam estas informações no seu repositório local em *soft-state* e as repassam adiante até um número máximo de saltos especificado pelo protocolo. A mensagem de anúncio também carrega uma lista de grupos de serviços dos quais o par anunciante tem conhecimento. Esta informação adicional é utilizada pelo encaminhamento seletivo empregado por GSD, cujo funcionamento é exemplificado a seguir: uma consulta a uma impressora a laser é encaminhada a pares que oferecem serviços relativos a mesma ou que conhecem vizinhos que oferecem um serviço do grupo de impressoras; no pior caso, quando nenhuma das condições é satisfeita, a consulta é enviada via broadcast. Uma vez realizado o casamento, uma resposta à consulta é enviada pela rota reversa que a consulta percorreu. A detecção de falhas na rota reversa leva o protocolo a transmitir a resposta via o protocolo de roteamento AODV (*Ad hoc On-demand Distance Vector*).

A idéia central no projeto de FTA (*Field Theoretic Approach*) [Lenders et al., 2005] é a analogia com campos eletrostáticos da Física: um serviço é visto como uma carga positiva, que gera um campo sobre a rede, e as requisições de serviço representam uma carga negativa, que são atraídas pelo serviço, em função do gradiente de campo gerado. Assim como GSD, é empregado um mecanismo de encaminhamento seletivo, que direciona a consulta aos pares que possuem o maior gradiente de campo para o tipo de serviço procurado (isto é, à região com maior probabilidade de se encontrar determinado serviço). Isso requer que pares troquem periodicamente entre si valores de gradiente para tipos de serviços conhecidos; esses valores são somados em cada par, formando o gradiente final que é utilizado pelo encaminhamento seletivo. Um valor de gradiente, também chamado de potencial, é calculado como sendo a capacidade da instância do serviço (CoS), que representa a carga do mesmo, dividida pela distância (em saltos) entre o par e a instância do serviço. Exemplos de CoS incluem a largura de banda de um serviço de *gateway* para Internet ou a velocidade de impressão para serviços oferecidos por impressoras.

Segundo os autores, a solução é proposta para resolver dois requisitos importantes em MANETs: seleção ótima de um serviço, na presença de múltiplos provedores, e a robustez diante da mobilidade inerente de MANETs. Considerando um cenário com múltiplos provedores e instâncias de serviços com cargas homogêneas, os fatores que acabam impactando no encaminhamento seletivo são: a menor distância entre pares e instâncias, por ser inversamente proporcional ao potencial; e a quantidade de instâncias contabilizadas no gradiente final de cada

par, o que indica um maior potencial da região. Esse encaminhamento é feito em prol da robustez, pois um número maior de provedores em uma região aumenta a probabilidade de encontrar o serviço, diante de cenários de mobilidade. Provedores de uma região não selecionada no encaminhamento podem reverter esse quadro caso aumentem a CoS de seus serviços, o que pode tornar o encaminhamento em prol da seleção ótima de serviços.

Allia [Ratsimor et al., 2004] é um arcabouço que prevê o uso de agentes configuráveis por meio de políticas locais. Segundo os autores, o uso destas garante, entre outras coisas, a adaptabilidade dos agentes, em tempo de execução, às características do ambiente. Grande parte dos elementos da descoberta (*cache*, encaminhamento, anúncio e diretório, por exemplo), podem ser configurados a partir de políticas. Pares podem especificar estratégias de armazenamento de informações de serviço e de encaminhamento de requisições, quando os serviços procurados não são encontrados no repositório local. O repositório local é preenchido com anúncios advindos de pares que formam a "aliança" de um par. Tanto os pares que compõem a aliança, bem como aqueles que podem receber as requisições encaminhadas, são declarados na política local. Dos trabalhos apresentados nesta seção, Allia é o único que prevê o emprego de mecanismos de segurança: pares podem incluir na política restrições como controle de acesso e verificação de credenciais.

Em [Varshavsky et al., 2005] é proposta uma arquitetura *cross-layer*, com mecanismos de descoberta de serviços atrelados a protocolos de roteamento. Nessa abordagem, a difusão das requisições e anúncios de serviços depende do protocolo de roteamento adotado. Por exemplo, com uma abordagem de descoberta ativa e o uso de protocolos de roteamento reativos, como *Dynamic Source Routing* (DSR) e *Ad hoc On-Demand Distance Vector* (AODV), requisições são propagadas fazendo-se o broadcast de mensagens modificadas de descoberta de rota. Com uma abordagem de descoberta passiva e protocolos de roteamento pró-ativos, como o *Destination Sequence Distance Vector* (DSDV), as tabelas de rota devem ser estendidas com informações de serviço. Outro aspecto que depende do protocolo de roteamento é o suporte à mobilidade, frente à necessidade de manter as informações sobre serviços consistentes para a descoberta. Por exemplo, a indisponibilidade de serviços pode ser inferida mediante uma quebra de rota detectada.

Konark [Helal et al., 2003] é o único dos protocolos apresentados nessa seção que realiza o armazenamento de informações de forma cooperativa. Na abordagem empregada, os pares procuram manter uma visão global dos serviços oferecidos na rede gerenciando seu repositório local e compartilhando o mesmo com outros pares. Para reduzir a sobrecarga de mensagens que tal abordagem implica, o conteúdo dos anúncios de serviços corresponde à diferença (*delta*) entre as informações de serviço que o par conhece e daqueles que os outros pares anunciam. O objetivo dessa estratégia é compartilhar o conhecimento da visão global de serviços disponíveis, com a máxima convergência, gerando a menor sobrecarga possível na rede.

2.3.2 Descoberta de serviços com segurança e privacidade

O Ninja SDS (*Service Discovery Service*) [Czerwinski et al., 1999] foi um dos primeiros protocolos de descoberta de serviços a lidar com problemas de segurança no seu projeto. Entretanto, o mesmo é inadequado para computação ubíqua, sendo seu foco redes corporativas. Informações sensíveis são expostas apenas a diretórios centrais, chamados de servidores SDS, os quais podem ser organizados

de forma hierárquica. Ambas as estratégias de descoberta (ativa e passiva) estão presentes, sendo que anúncios e consultas de serviços devem necessariamente ser enviadas a estes servidores, utilizando um canal seguro até os mesmos. Antes de armazenar as informações de serviço, o servidor SDS autentica provedores e clientes; no caso de uma consulta, o servidor ainda verifica se o cliente é autorizado a descobrir o serviço procurado. Isso satisfaz requisitos de privacidade em um ambiente corporativo, muito embora informações sensíveis necessariamente ainda sejam expostas ao servidor central.

Os mecanismos de autenticação e autorização mencionados anteriormente dependem de outros dois componentes do sistema SDS: autoridade certificadora (CA) e gerenciador de capacidades (*capabilities*). O primeiro componente emite certificados que provam a legitimidade de um "principal"; o segundo gera e publica uma lista de capacidades, assinadas pelo mesmo, que provam que um principal é autorizado a acessar determinado serviço. Um principal é uma descrição que identifica um ou mais conjuntos de dispositivos ou usuários, os quais devem responder pelo mesmo (isto é, serem capazes de decodificar mensagens codificadas destinadas a este principal). Além de mecanismos de segurança e privacidade, SDS visa obter uma solução eficiente nos aspectos de alcance geográfico e escalabilidade. SDS emprega sumários de informações de serviços para diminuir a sobrecarga com o encaminhamento de requisições de serviços entre servidores SDS de uma hierarquia. Sumários correspondem a filtros *Bloom*, que representam um conjunto de informações em uma série de bits. Ao realizar uma operação AND binária entre um sumário de anúncios e um de consultas, um resultado diferente de zero indica que pelo menos um serviço procurado foi encontrado.

PrudentExposure [Zhu et al., 2006] oferece um sistema de descoberta de serviços com segurança e privacidade para computação ubíqua, visando cenários onde usuários desejam descobrir serviços na vizinhança. Os elementos envolvidos na descoberta são: clientes, serviços, diretórios locais e agentes de usuário. Diretórios locais e serviços que nele se registram devem pertencer ao mesmo par, com a finalidade de se obter privacidade. Além disso, ambos devem estar associados a um único domínio. Já o agente de usuário auxilia o cliente na tarefa de descoberta, com a provisão automática de identidades de domínio para cada domínio conhecido. PrudentExposure assume que essas identidades sejam previamente trocadas entre provedores e clientes antes de se realizar a descoberta. No modelo lá proposto, a requisição de um serviço é antecedida por uma etapa de reconhecimento de domínios, onde o agente do usuário envia um sumário broadcast (filtro *Bloom*) com as identidades de domínios conhecidos e apenas diretórios que encontram no sumário a identidade do domínio ao qual estão associados respondem a esse sumário. Isso indica se o cliente está autorizado a enviar requisições de serviço a um determinado domínio. Mecanismos adicionais são providos para diminuir a taxa de falsos positivos nesta etapa, visto que os sumários podem ser facilmente forjados.

Em um trabalho posterior [Zhu et al., 2005b], os autores identificaram duas falhas de privacidade com a abordagem existente: clientes e provedores sempre expõem sua presença com a etapa de reconhecimento de domínios; o cliente expõe sua requisição de serviço a todos os domínios reconhecidos. No centro desses dois problemas, está um dilema: quem se expõe primeiro? Se provedores expõem identidades e serviços disponíveis primeiro, o cliente pode abordar apenas os provedores necessários; se o cliente se expõe primeiro, o provedor pode determinar se o mesmo é legítimo, para então expor sua presença e serviços disponíveis. Na

tentativa de resolver esse dilema, os autores propõem a exposição progressiva de identidades, requisições e serviços disponíveis, mesclando a etapa de reconhecimento de domínios com a requisição de serviços. À medida que estas informações vão progressivamente sendo expostas por ambas as partes, aumenta-se o grau de confiança na autorização do cliente bem como pode-se detectar um acesso não autorizado mais cedo. Caso o último cenário ocorra, apenas uma parte da informação foi exposta, o que impede de inferir com certeza sobre o conteúdo íntegro dessas informações.

[Trabelsi et al., 2006] propõe uma extensão ao protocolo WS-Discovery para proteger informações sensíveis ao longo do processo de descoberta. Este protocolo não utiliza diretórios, porém prevê o uso de *proxies* para estender a descoberta além da rede local. A abordagem de descoberta é híbrida: provedores anunciam serviços através de mensagens *Hello* e clientes enviam suas requisições através de mensagens *Probe*, que são respondidas com mensagens *Probe Match* quando ocorre o casamento. Os autores propõem proteger as informações sensíveis presentes nas duas últimas mensagens. Para tanto, utiliza-se ABE (*Attribute-based Encryption*), uma variante de IBE (*Identity-based Encryption*). O conjunto de atributos do serviço que o cliente está interessado (tipo e escopo, na implementação atual) formam a chave pública utilizada para a criptografar as partes sensíveis da mensagem *Probe*. No caso da mensagem *Probe Match*, é utilizada a identidade do provedor como chave pública. Somente pares que provam possuir tais atributos têm a respectiva chave privada para decodificar a mensagem, a qual é gerada por um PKG (*Public Key Generator*) confiável. Dessa forma, pares somente se expõem àqueles com quem querem interagir, o que aumenta o nível de privacidade.

Em [Buford et al., 2006], é proposto um mecanismo federativo de descoberta de serviços, onde anúncios e requisições de serviços são enviadas somente aos pares que pertencem a um grupo em comum. Pares são habilitados a entrar no grupo somente se possuem um conjunto de credenciais que satisfazem os critérios definidos pelo dono do grupo. Qualquer par pode ser dono de um grupo, podendo também determinar a visibilidade do mesmo a demais pares. Um grupo público pode ser descoberto por qualquer par, enquanto que um privado necessita ser acessado por vias de configuração. Os autores comentam que esta abordagem preserva a privacidade dos usuários, visto que as informações sensíveis serão expostas somente a pares que possuem as devidas credenciais. Entretanto, os critérios são definidos pelo dono do grupo, logo os demais pares não tem controle sobre sua privacidade.

Carminati et al [Carminati et al., 2005] propõem o uso de políticas locais de privacidade que devem ser adotadas por diretórios de serviços em arquiteturas Web Services, o que permite que provedores e clientes identifiquem os propósitos da coleta de suas informações sensíveis, bem como as regras que limitam seu uso, exposição e o tempo de retenção. No caso de anúncios e consultas (que obrigatoriamente irão passar pelo diretório) os autores apresentam três estratégias que apóiam a imposição de privacidade no comportamento dos diretórios. Uma estratégia é um mecanismo que regula o acesso do diretório a informações de provedores e clientes expostas nas mensagens de anúncio e consulta. Sua desvantagem é que depende de uma entidade confiável por todas as partes (uma CA, por exemplo). Outra estratégia, que contorna essa limitação, é o uso de *hashes* nas partes sensíveis dos anúncios e consultas. O casamento é realizado através de valores de *hash*, prevenindo que o diretório possa inferir sobre o conteúdo sensível.

Os protocolos apresentados em [Almenárez and Campo, 2003,

Wishart et al., 2005, Ali et al., 2005] exploram o uso de redes de confiança/reputação entre pares na descoberta de serviços. No primeiro trabalho, pares lidam com uma lista de pares confiáveis, com os respectivos graus de confiança que compartilham com cada um. Essa informação é utilizada com o intuito de restringir o armazenamento de informações de serviço em seu repositório local: somente anúncios advindos de pares confiáveis são armazenados. Isso torna a descoberta progressivamente segura, à medida que serviços de pares com má reputação vão sendo descartados. Na mesma linha, o segundo e o terceiro trabalhos fazem uso da confiança apenas para a posterior seleção dos serviços descobertos. Nenhum desses trabalhos, entretanto, utiliza a confiança/reputação para proteger as informações de serviço durante o processo de descoberta.

2.3.3 Discussão

Os trabalhos apresentados na seção anterior possuem certas limitações (algumas já abordadas na Seção 2.2) em relação à segurança e privacidade na descoberta de serviços para computação ubíqua. A dependência de uma infra-estrutura de segurança, CAs ou PKGs, é o principal aspecto negativo, pois a sua ausência inibe a colaboração segura entre pares. O uso de credenciais ou chaves geradas por PKGs mitiga esse problema, pois não é necessária a conexão permanente com essa infra-estrutura para viabilizar autenticação e autorização de clientes. Credenciais podem ser alteradas sempre que o provedor precisar criar ou alterar uma regra de autorização para seus serviços; chaves de PKGs são geradas sempre que um novo serviço deve ser anunciado. Embora sejam operações esporádicas, a expectativa é que sejam mais freqüentes em ambientes ubíquos, o que aumentaria o impacto da ausência de infra-estrutura de segurança. Os principais argumentos são a dinâmica de ambientes ubíquos e o fato de que todo usuário é um potencial provedor de serviços.

A dependência com chaves previamente distribuídas, como é o caso em [Zhu et al., 2006], inibe a colaboração entre pares que não se conhecem. Para efetuar a descoberta nesses casos é necessário que provedores e clientes estabeleçam alguma forma de confiança. Tal estratégia é mais adequada para ambientes corporativos ou domésticos, onde as partes são conhecidas e a distribuição de chaves pode ser facilmente realizada por contato direto [Stajano and Anderson, 1999] ou contato visual [Capkun et al., 2006]. Uma alternativa seria o uso de redes de confiança e relações transitivas tal que pares pudessem estabelecer um grau de confiança em função de um par intermediário (ou pares) em comum. Como mencionado anteriormente, os trabalhos [Almenárez and Campo, 2003, Wishart et al., 2005, Ali et al., 2005] seguem essa linha, porém exploram apenas parcialmente essa solução pois não a utilizam para proteger informações sensíveis ao longo da descoberta.

Grande parte dos trabalhos apresentados codificam informações sensíveis visando a privacidade. Por exemplo, [Zhu et al., 2006] e [Czerwinski et al., 1999] utilizam sumários para expressar anúncios e consultas; [Trabelsi et al., 2006] codifica informações empregando atributos de serviços como uma chave pública; [Carminati et al., 2005] propõe uma estratégia de anúncios e consultas de serviços com valores em *hash*. Em geral, o formato final da informação nessas abordagens assume a existência de um vocabulário específico e adotado por todos os pares, para fins de interoperabilidade. Em computação ubíqua, é improvável que a

existência de apenas um formato universal para descrição e consulta de serviços; essa limitação diminui a eficácia da descoberta. O mais adequado nesse caso é o emprego de estruturas semânticas [Chakraborty et al., 2006, Ali et al., 2005], mas até o momento não existe na literatura um sistema de descoberta para computação ubíqua que tenha agregado mecanismos de segurança e privacidade com tais estruturas.

Revogação de chaves também é um problema enfrentado pela maioria dos trabalhos, sendo reconhecido e discutido em [Zhu et al., 2006, Trabelsi et al., 2006]. Esta é uma funcionalidade importante em sistemas de segurança, principalmente em ambientes ubíquos, quando decisões prematuras sobre determinados pares são feitas por conta do maior nível de incerteza desses ambientes. Redistribuir novas chaves de segurança, invalidando dados criptografados com chaves antigas, é uma abordagem possível, porém difícil de ser concretizada com sucesso em cenários de mobilidade.

Outro problema causado por essas decisões prematuras é a perda de privacidade em situações de risco. Quanto maior a incerteza de um ambiente, maior é o risco associado com a exposição do usuário. Este fator deve ser levado em consideração no momento da descoberta, muito embora às vezes a exposição seja ainda necessária. Os trabalhos listados limitam-se a explorar a privacidade como o problema de garantir que apenas partes autorizadas tenham acesso às mensagens de anúncios e requisições trocadas. Porém, esse nível de proteção é insuficiente para garantir a privacidade da informação [Clarke, 2006]: uma vez transmitidas as informações, seus donos perdem o controle sobre sua disseminação subseqüente. O uso de políticas de privacidade através de P3P, como proposto em [Carminati et al., 2005], auxilia no sentido de publicar como se dará o manuseio da informação sensível coletada, embora isso não seja uma garantia que a política será realmente adotada [Langheinrich, 2001].

Capítulo 3

Projeto do FSSD

O projeto do FSSD é centrado no compromisso entre os aspectos de colaboração, segurança e privacidade para a descoberta de serviços em ambientes ubíquos. A Seção 3.1 apresenta exemplos de cenários alvo para a descoberta de serviços que envolvem os três aspectos e servem de inspiração para o projeto do FSSD. A definição do problema, isto é, do referido compromisso, é realizada na Seção 3.2. As Seções 3.3 e 3.4 apresentam o protocolo, descrevendo o modelo de descoberta proposto e sua arquitetura. A formalização do protocolo é descrita na Seção 3.5, seguida de detalhes de implementação na Seção 3.6. A Seção 3.7 finaliza o capítulo, com uma discussão sobre as principais características apresentadas pelo protocolo.

3.1 Cenários Alvo

Os cenários almejados por este trabalho são aqueles em que a descoberta de serviços não pode ser realizada com garantias de uma infra-estrutura de segurança fixa, a qual suportaria o uso de certificados, controle de acesso etc. Tal limitação pode estar relacionada a aspectos institucionais, como por exemplo, a existência de um domínio administrativo restrito a funcionários de uma empresa. Nesse contexto, na solução adotada por FSSD, os pares devem colaborar para obter propriedades de segurança e privacidade no processo de descoberta [Zhu et al., 2005a].

Um exemplo é a utilização de sistemas ubíquos em hospitais, os quais têm sido explorados pela comunidade científica por serem ambientes de intensa colaboração entre profissionais [Hansen et al., 2006]. Hospitais podem ser ambientes complexos, compostos por várias unidades que lidam com serviços e usuários diferentes. Bráulio, por exemplo, é um paciente do laboratório de exame de sangue, com o qual possui uma boa relação de confiança mediante visitas passadas; as demais unidades são desconhecidas ao mesmo. Ele possui chaves de segurança que permitem a comunicação segura com dispositivos e serviços do laboratório. O laboratório, por outro lado, encontra-se sob o domínio administrativo do hospital, o que protege as comunicações entre dispositivos e funcionários do mesmo. O hospital ainda possui uma infra-estrutura de descoberta sob esse domínio, sendo utilizada por todas as suas unidades.

Consideramos agora o papel da descoberta de serviços nesse cenário. O laboratório oferece uma série de serviços a funcionários e pacientes autorizados, caso de Bráulio (através das chaves de segurança mencionadas). Entretanto, se

Bráulio precisa descobrir novos serviços, digamos relacionados a um laboratório de radiologia, como fazer isso de forma segura e prudente, sem depender da infra-estrutura de segurança do hospital? Sem prudência na exposição de suas consultas, Bráulio estaria colocando em risco sua privacidade, pois tanto pacientes como outras unidades do hospital poderiam receber as mesmas.

A solução adotada neste trabalho explora comportamentos exibidos em redes de relacionamentos. Se Bráulio possui um canal de comunicação seguro com o primeiro laboratório, ele inicialmente expõe sua consulta através desse canal. Esta consulta é associada a uma política de privacidade declarada por Bráulio, que requer que o laboratório suprima sua identidade da mensagem de consulta antes de propagar a mesma a outras unidades do hospital. Baseado no seu grau de confiança com o laboratório, Bráulio tem relativa certeza que o último irá fazer o uso devido da informação recebida, seja no armazenamento ou repasse da informação. Fazendo isso, o laboratório estará preservando a identidade de Bráulio. Na perspectiva do hospital, o recebimento de uma consulta sem a identidade do requisitante é digamos aceitável, dado que é proveniente de uma de suas unidades. Logo, o serviço procurado pode ser anunciado a Bráulio através do mesmo canal por onde foi enviada a consulta. Após interações com tal serviço, é possível então que Bráulio aumente sua rede de relacionamentos, incluindo chaves de segurança para acessar serviços do laboratório de radiologia.

Independentemente do fato de existir uma infra-estrutura de descoberta, usuários podem desejar muitas vezes interagir de maneira mais informal. O mecanismo de segurança PGP [Stallings, 2005], por exemplo, viabiliza a criação de redes P2P seguras, onde certificados de chaves públicas emitidos pelos próprios pares são utilizados para verificar a legitimidade entre os mesmos. O grau de confiança que um par tem sobre uma chave pública é determinado a partir dos graus de confiança depositados nos emissores dos certificados que atestam a legitimidade dessa chave. Essas redes P2P (também conhecidas como redes sociais) são exploradas neste trabalho para obter-se uma descoberta de serviços controlada. Deve ser possível, por exemplo, que Ana e Mercedes, colegas no laboratório de exame de sangue, possam trocar serviços entre si de forma privada.

Através dos cenários apresentados, é possível identificar a importância dos aspectos de colaboração entre pares, segurança e privacidade na descoberta de serviços. Como será discutido na próxima seção, é difícil conciliar o melhor dos três aspectos em ambientes sem infra-estrutura de descoberta compartilhada entre provedores e clientes.

3.2 Colaboração vs Segurança vs Privacidade

Um dos principais desafios na descoberta de serviços ubíqua é a obtenção de propriedades desejáveis de uma infra-estrutura fixa de rede ou sistema (tais como escalabilidade, segurança, privacidade, fácil administração etc.) sem depender da mesma [Edwards, 2006]. Este trabalho persegue o referido desafio ao explorar a colaboração entre pares como uma alternativa a essa infra-estrutura, objetivando obter uma descoberta eficaz e com propriedades de segurança e privacidade. Por colaboração, nesse contexto, entende-se a disposição de pares a anunciar e consultar serviços, bem como contribuir para o funcionamento do protocolo de descoberta de serviços.

Contudo, a segurança e privacidade não podem ser consideradas apenas como propriedades finais para usuários da descoberta (tais como permitir que o usuário possa determinar que pares são autorizados a receber anúncios dos seus serviços, por exemplo). Sistemas movidos pela colaboração entre pares são passíveis de ataques onde pares mal-intencionados buscam corromper o funcionamento do sistema ou apenas beneficiar-se do mesmo sem retribuir na mesma proporção. Esse problema deve ser tratado com mecanismos adicionais de segurança que permitem identificar e excluir pares maliciosos do sistema. Mecanismos de privacidade também devem ser considerados, haja visto que a colaboração na descoberta envolve a exposição de informações sensíveis como identidade, perfil do usuário, entre outros [Zhu et al., 2005a].

Sistemas de confiança, tais como PGP e outros sistemas citados em [Jösang et al., 2007], podem ser empregados para lidar com ataques de pares mal-intencionados. A essência destes sistemas é a colaboração dos pares no cálculo da confiança sobre cada par, o que possibilita a identificação de pares maliciosos. Em geral, possuem componentes para: coleta de opiniões sobre comportamento dos pares; consolidação destas opiniões e cálculo de um escore final, o qual expressa confiança sobre um par; e mecanismos de incentivo e punição. Sistemas de confiança empregam mecanismos onde pares votam entre si, o que introduz uma série de ataques possíveis, tais como traição, coluio, egoísmo, entre outros [Marti and Garcia-Molina, 2006]. Diminuir a suscetibilidade de sistemas a estes ataques é um importante requisito e tema de uma quantidade de trabalhos na área de gerenciamento de confiança.

Considerando as ameaças de ataques no sistema de confiança, faz sentido pares adotarem estratégias de colaboração segundo os níveis de segurança exigidos pelos mesmos. Nesse contexto, uma solução é limitar a colaboração entre pares em função do grau de confiança compartilhado entre os mesmos. Por exemplo, quanto menos exigente e seletivo for Bráulio, maior poderá ser o número de pares com quem pode colaborar. Este cenário exemplifica a escolha e o compromisso entre **colaboração ou segurança**.

A questão de privacidade na exposição de informações de serviço leva a outros dois compromissos no projeto de sistemas de descoberta. O primeiro, **colaboração ou privacidade**, diz respeito ao nível de exposição que um par assume. Uma maior exposição dessas informações tende a aumentar a eficácia da descoberta, isto é, um número maior de informações aumenta a probabilidade de casamento. Por outro lado, o grau maior de exposição diminui a privacidade do usuário. O segundo compromisso corresponde à escolha entre **segurança e privacidade**, na qual define-se que tipo de informações pessoais devem ser empregadas para a implementação dos mecanismos de segurança. Expor informações como identidade, por exemplo [Marti and Garcia-Molina, 2006], é indispensável para sistemas de confiança. Em contrapartida, também possibilita que votos de pares possam ser identificados, fazendo com que estes virem alvos potenciais de ataques objetivando inibir seus votos [Singh and Liu, 2003].

A Figura 3.1 resume o problema definido, onde o diagrama conta com dois triângulos. Os três lados do triângulo de cima compreendem os três compromissos supracitados. Uma forma de lidar com os diferentes compromissos é possibilitar que o usuário defina um balanço entre os aspectos envolvidos, de acordo com suas necessidades (a próxima seção apresenta uma solução nestes moldes). Como regra geral, quanto maior a colaboração entre pares na descoberta, maior será sua eficácia,

porém maior também serão os riscos envolvidos com segurança e privacidade (a relação inversa também é aplicável).

FIGURA 3.1 – Compromissos entre colaboração, segurança e privacidade

3.3 Princípios de Projeto

Após a discussão anterior (sobre os compromissos entre colaboração, segurança e privacidade envolvidos na descoberta de serviços), nota-se que é praticamente impossível obter um sistema que exiba o melhor dos três aspectos em ambientes sem garantias de uma infra-estrutura de segurança. Ao invés de um protocolo que priorize um ou dois dos aspectos apresentados, este trabalho propõe um modelo flexível, onde o próprio usuário ajusta o balanço entre eles. O cerne dessa flexibilização é o conceito da distribuição de anúncios e consultas com **diferentes níveis de visibilidade**, que são necessárias devido à privacidade exigida pelo usuário e as **diferentes relações de confiança** deste com seus pares vizinhos.

Nesse contexto, anúncios de serviços são enviados de forma prudente, respeitando configurações de segurança e privacidade do provedor. Da mesma forma, clientes que não recebem anúncios para os serviços procurados podem transmitir consultas, também de forma prudente e parametrizada. O suporte a diferentes níveis de visibilidade é importante para preservar a privacidade do usuário ao longo da exposição de seus anúncios e consultas de serviços. Basicamente, cada anúncio/consulta é composta por um conjunto de campos, que variam no grau de privacidade exigido pelo provedor/cliente (identidade e descrição do anúncio/consulta são exemplos de campos). À medida que a informação é propagada pela rede, os campos mais sensíveis (como identidade) são suprimidos, diminuindo a visibilidade da informação. O principal fator que determina a redução da visibilidade é o grau das relações de confiança entre os pares envolvidos na propagação. Quanto mais estreitas forem as relações de confiança em um canal de propagação, maior será a visibilidade do anúncio/consulta ao longo desse canal, ou seja, mais campos serão expostos para um número maior de pares.

Anúncios e consultas podem ser casadas localmente (ou seja, pelo cliente que procura o serviço anunciado ou pelo provedor que fornece o serviço consultado, respectivamente), ou por pares intermediários. No segundo caso, também chamado de casamento *in-network*, é também realizada um etapa de autorização, pois o fato do cliente e provedor não terem recebido o anúncio e a consulta indica que não compartilham um canal de propagação com relações de confiança estreitas o bastante. Entende-se essa autorização como verificar se é possível "abrir uma exceção" para o cliente que não recebeu o anúncio do serviço procurado. Essa

autorização é feita com base nas credenciais (condições) impostas pelos anúncios e consultas de serviços. Caso o cliente seja autorizado, o anúncio é enviado ao mesmo, mas preservando a identidade física do provedor. É importante relembrar que FSSD se limita à descoberta de serviços, portanto, em ambos os casos, o acesso ao anúncio de um serviço não significa que o cliente está habilitado a utilizar o mesmo. Isso de fato compete à etapa de interação entre provedor e cliente [Kindberg and Fox, 2002].

Os compromissos definidos na seção anterior se encaixam no projeto do FSSD da seguinte forma:

- o ajuste nos níveis de visibilidade e credenciais de anúncios e consultas representa o compromisso entre colaboração e privacidade;
- o grau de confiança de um par sobre outros pares define o compromisso entre colaboração e segurança; e
- o emprego de duas identidades (descritas a seguir) para cada par na descoberta, cuja visibilidade pode ser ajustada, expressa o compromisso entre segurança e privacidade.

Em todos os casos, existe uma relação de "perda e ganho", a ser ajustada de acordo com as necessidades do usuário. Seguindo princípios básicos nessas configurações, como será discutido na próxima seção, pares conseguem obter uma boa relação entre segurança, privacidade e eficácia da descoberta de serviço (devida à colaboração).

FSSD prevê que pares possuam duas identidades: uma para uso em transações seguras entre pares e outra para fins de gerenciamento de confiança. A primeira, chamada de **identidade forte**, é composta por um identificador persistente do par (endereço MAC), enquanto que a segunda, **identidade fraca**, é um id qualquer, gerado pelo próprio par. A identidade forte possui adicionalmente uma chave pública associada, publicada a pares com quem um par deseja se comunicar de forma segura. Uma das vantagens obtidas com esse esquema é possibilitar a pares resguardarem suas identidades físicas no gerenciamento de confiança, o que os previne de virarem alvos de futuras retaliações [Singh and Liu, 2003].

Todavia, a maior vantagem obtida com o uso de duas identidades está na criação de dois níveis de visibilidade de anúncios/consultas: um com apenas a identidade fraca, e outro com ambas. Em geral, a identidade fraca atrela um anúncio ou consulta somente ao grau de confiança sobre o provedor/cliente e não à sua identidade física, como acontece com a identidade forte. Nesse contexto, o uso da identidade fraca preserva a privacidade do usuário. Exceções incluem cenários onde pares puderam associar, de alguma forma, as duas identidades (através de interações passadas onde ambas eram expostas, por exemplo). Para esses casos, uma solução é trocar a identidade fraca, mas com o custo de perder parte da confiança obtida na rede.

As chaves públicas associadas às identidades fortes são utilizadas para obter-se um modelo anárquico de PKI, como proposto pela ferramenta PGP [Stallings, 2005]. Nesse contexto, a autenticação é realizada par-a-par. Assume-se nesse caso que as chaves públicas são trocadas de maneira segura entre pares, seja através de estratégias de contato físico [Stajano and Anderson, 1999], contato visual mediante a mobilidade [Capkun et al., 2006] ou por meio de um terceiro par, que é confiável aos outros dois. O terceiro caso imita o comportamento social de indivíduos,

onde interações passadas são recomendadas a outros indivíduos [Jösang et al., 2006]. No cenário do hospital, por exemplo, Ana pode recomendar a Bráulio outros laboratórios, o qual decidirá se aceita as respectivas chaves públicas baseando-se na sua confiança depositada em Ana.

As propriedades do protocolo são resumidas a seguir, com base na terminologia apresentada na Seção 2.1:

- **Arquitetura da descoberta**: descentralizada, sem a existência de diretórios.
- **Escopo da descoberta**: limitada primeiramente pela topologia física subjacente. Considerando a rede física com pares remotos correntemente alcançáveis pelo par local, o escopo será adicionalmente limitado pela rede de confiança. O ajuste dos níveis de visibilidade de anúncios e consultas também ajuda a definir o escopo da descoberta.
- **Gerenciamento da informação de serviço**: atrelado a um mecanismo de casamento, o qual pode ser efetuado por pares intermediários em comum ao provedor e cliente do serviço em questão. O algoritmo de casamento executa uma simples comparação entre os tipos dos serviços anunciados e procurados. A qualidade do casamento não é o foco deste trabalho.
- **Mecanismos de requisição e anúncio de serviços**: abordagem híbrida, baseada em consultas e anúncios propagados para pares de uma rede de confiança. Nesse trabalho, a consulta é diferenciada da requisição, pois são utilizadas em diferentes etapas: a primeira é empregada na descoberta, enquanto que a segunda é resultado direto da descoberta, sendo utilizada como parte da seleção de serviços.
- **Armazenamento**: repositórios descentralizados, mantidos por todos os pares de forma cooperativa. Um repositório compreende as informações disponíveis em cada anúncio e consulta recebida pelo par.
- **Validade**: informações de serviço (anúncios e consultas) mantidas de forma *soft-state*.
- **Seleção dos serviços**: não prevista, é assumida como sendo manual.
- **Suporte à mobilidade**: combinação do uso de informações *soft-state* e anúncios periódicos de serviços.

Algumas semelhanças podem ser encontradas entre elementos do FSSD e soluções de trabalhos relacionados. De forma complementar ao proposto em [Almenárez and Campo, 2003, Wishart et al., 2005, Ali et al., 2005], adota-se sistemas de confiança para guiar a descoberta de serviços de forma segura e prudente. A exposição prudente de informações de serviço, proposta em [Zhu et al., 2005b], é realizada sob um controle de exposição baseado na confiança entre pares, e não se assume que provedores e clientes conheçam previamente uma chave de domínio para interagirem. Anúncios e consultas de serviços são encaminhadas seletivamente, como proposto em [Chakraborty et al., 2006, Lenders et al., 2005]; entretanto, o encaminhamento ocorre de acordo com as restrições impostas no controle de exposição definido pelo usuário.

O principal diferencial do FSSD em relação aos demais trabalhos é a flexibilidade na descoberta de serviços, discutida nesta seção em termos do suporte a diferentes níveis de visibilidade, do uso de uma rede de confiança e do emprego de um mecanismo de casamento *in-network*. A seguir, os elementos aqui discutidos são apresentados em um nível maior de detalhes.

3.4 Arquitetura do Protocolo

Em FSSD, anúncios e consultas são expressas em mensagens com diferentes níveis de visibilidade. As informações contidas nestas mensagens são armazenadas no repositório local de cada par envolvido na propagação, comparadas com informações já armazenadas para verificar a possibilidade do casamento e então encaminhadas para os próximos pares de uma rede de confiança, utilizando a chave pública destes para criptografar as mensagens que lhes são destinadas. O encaminhamento da mensagem está sujeito a um mecanismo de **controle de exposição**, que suprime campos da mensagem sempre que o próximo par não possui um grau de confiança necessário para continuar propagando a mensagem com o atual nível de visibilidade. Outro mecanismo importante é o **casamento *in-network***, o qual permite obter casamentos em pares intermediários, sem que clientes e provedores se exponham. Ambos os mecanismos dependem do gerenciamento de confiança, que é basicamente um sistema de confiança descentralizado onde pares trocam opiniões entre si.

De uma forma geral, o processo de descoberta de serviços descrito acima reflete os princípios de projeto definidos na seção anterior. Usuários podem influenciar boa parte do processo através de parâmetros nos anúncios/consultas e colaborando no gerenciamento de confiança, o que indica o alto grau de flexibilidade provido por FSSD. Os elementos deste processo são apresentados a seguir.

3.4.1 Informações de serviço

Anúncios e consultas de serviços são doravante também chamados de **informações de serviço**. Ambos são codificados de maneira similar, através de um registro que possui os seguintes campos:

- identidade forte do provedor/cliente;
- identidade fraca do provedor/cliente;
- descrição da informação;
- credenciais de acesso para o casamento *in-network*; e
- opinião sobre a informação de serviço.

A descrição da informação é o único campo onde anúncios e consultas se diferem. Entre vários dados, este campo inclui o tipo do serviço anunciado e seus atributos (para anúncios) ou o tipo de serviço e atributos procurados (para consultas). A descrição do anúncio, em particular, contém os dados necessários que habilitam um cliente a enviar uma requisição criptografada ao provedor do serviço anunciado. Estes dados resumem-se a um IP multicast e uma chave pública, presumindo assim que a rede subjacente suporta IP multicast. Esse IP é oferecido ao invés do endereço do provedor tendo em vista preservar sua privacidade.

O uso de identidades forte e fraca já foi discutido anteriormente. A identidade fraca é importante pois permite ao provedor/cliente preservar a sua privacidade, ao mesmo tempo em que pares que recebem o anúncio/consulta possam associar um grau de confiança com a informação recebida. Já a identidade forte aumenta os riscos com a perda de privacidade do par, pois expõe seu endereço de rede. Em casos onde a identidade fraca não é exposta, é possível ainda obter uma opinião aproximada sobre a informação de serviço recebida através do último campo da mesma. Essa opinião reflete o grau de confiança sobre o canal por onde a informação foi propagada (Seção 3.6.1). As credenciais de acesso são empregadas pelo mecanismo de casamento *in-network*, como explicado adiante.

É importante ressaltar que uma maior visibilidade representa uma maior exposição de informações sensíveis para o usuário. Os níveis de visibilidade providos por FSSD são descritos a seguir:

1. **Exposição da informação de serviço**: nesse nível, são expostos os campos de descrição da informação, credenciais de acesso e opinião sobre a informação. É o nível que oferece maior privacidade ao provedor/cliente, porém, no ponto de vista de outros pares que recebem a informação, não permite nenhum vínculo entre a informação de serviço e o par que a gerou. Logo, não é possível prever a qualidade dos anúncios/consultas com base na confiança sobre os provedores/clientes.

2. **Exposição da informação de serviço e identidade fraca**: a informação de serviço é atrelada a uma identidade fraca, o que permite pares vincularem a primeira a um grau de confiança fornecido pelo gerenciamento de confiança. Dessa forma, é possível descobrir se o anúncio ou consulta é proveniente de pares com boa confiança, por exemplo. A identidade fraca pode prover um grau suficiente de privacidade ao provedor/cliente ao mesmo tempo em que possibilita a outros pares conhecerem a confiança sobre ele.

3. **Exposição da informação de serviço e identidades**: a informação de serviço é ligada a ambas as identidades, o que expõe de forma mais sensível a privacidade do usuário e facilita sua identificação na rede. Por outro lado, essa exposição é necessária para um cliente inicialmente enviar uma consulta ou um provedor enviar um anúncio, pois ele vai expor de qualquer forma sua identidade física na comunicação com o próximo par. Como será apresentado adiante, uma informação de serviço nesse nível é limitada aos pares com quem o provedor/cliente possui uma relação de confiança e um canal seguro para comunicação.

3.4.2 Parâmetros do usuário

Os parâmetros do usuário podem ser definidos para cada anúncio e consulta de serviço de forma independente, possibilitando assim refletir diferentes compromissos exigidos entre eficácia (devida à colaboração), segurança e privacidade para cada um. O usuário pode influenciar o escopo da descoberta em três momentos, através dos seguintes parâmetros:

- **Envio unicast do anúncio/consulta**: o provedor/cliente pode definir quais vizinhos de sua rede de confiança que receberão o anúncio/consulta diretamente do mesmo.

- **Propagação do anúncio/consulta**: configura-se o grau de confiança mínimo que pares devem possuir para receber o anúncio/consulta em um determinado nível de visibilidade.

- **Casamento *in-network***: define-se as credenciais necessárias para a etapa de autorização.

A possibilidade de limitar o envio de uma informação de serviço a um número de vizinhos da rede de confiança é opcional, muito embora ofereça um acréscimo ao grau de privacidade obtido com o nível de visibilidade 3. Em muitos casos, as relações de confiança boas são construídas sob diferentes contextos, logo não faz sentido expor uma informação sensível a todas elas. No cenário do hospital, por exemplo, Bráulio utiliza a relação de confiança com o laboratório de exame de sangue para obter serviços do laboratório de radiologia pois, naquele momento, não possuía outra forma de fazer isso de forma segura. Uma vez que tenha construído uma relação de confiança com o segundo laboratório, não é mais necessário expor suas consultas destinadas a este através do primeiro laboratório.

FIGURA 3.2 – Níveis de visibilidade e os respectivos graus de confiança necessários (exemplo)

Os parâmetros pertinentes à etapa de propagação são utilizados pelo mecanismo de controle de exposição. O grau de confiança mínimo para exposição (doravante chamado de GMCE) para um nível de visibilidade limita a exposição desse nível apenas para pares que compartilham um grau de confiança maior que o parâmetro definido pelo usuário. A Figura 3.2 mostra um exemplo de configuração destes parâmetros, em um espaço de valores entre 0 e 1. GMCE $= 0,75$ para o nível de visibilidade 2, por exemplo, permite a exposição de identidades fracas somente aos pares com quem o provedor/cliente tem um grau de confiança maior ou igual a $0,75$.

As credenciais de acesso podem ser das mais diversas. Na área de segurança, credenciais são consideradas muitas vezes como sendo qualificações atestadas por alguma fonte confiável, tal como uma entidade certificadora (por exemplo, um médico é atestado de sua profissão através de uma credencial assinada por uma entidade certificadora). Neste trabalho, não é imposta nenhuma limitação quanto ao uso de tais credenciais. Entretanto, como já comentado, quando pares não têm acesso a uma infra-estrutura de segurança, é difícil verificar propriedades como autenticação e autorização, muito embora mecanismos como PGP podem mitigar esse problema. Para não depender apenas deste tipo de credenciais, FSSD também emprega **credenciais quantitativas**, que basicamente correspondem ao grau mínimo de confiança que o par intermediário, o qual realizou o casamento, deve possuir no cliente da consulta e no provedor do anúncio casados. Isso torna a descoberta mais flexível e menos dependente da infra-estrutura de segurança.

3.4.3 Topologia da rede e mensagens

FSSD visa sua aplicação em redes móveis, de um ou múltiplos saltos. Sobre essa rede física, FSSD considera uma topologia lógica, formada pelas relações de confiança compartilhadas entre os pares da rede. A Figura 3.3 ilustra um exemplo de topologia formada por relações de confiança; conforme será explicado na Seção 3.5, os pesos nas arestas representam confiança e certeza. Cada arco da topologia indica um canal seguro entre dois pares, possível através do compartilhamento de chaves públicas e identidades fortes entre os mesmos. Todas as mensagens previstas pelo protocolo devem ser enviadas de forma segura; logo, a topologia lógica restringe o fluxo possível de mensagens entre os pares. Nessa abordagem, pares recebem uma mensagem, decodificam com a chave pública do par origem e, caso seja necessário propagá-la, codificam com sua própria chave privada. É importante observar que um arco na topologia lógica pode corresponder a uma rota envolvendo vários pares na topologia subjacente. Contudo, a premissa é que esses pares não são capazes de decodificar as mensagens, pois são criadas com chaves públicas cuidadosamente distribuídas (através de abordagens já discutidas na Seção 3.3).

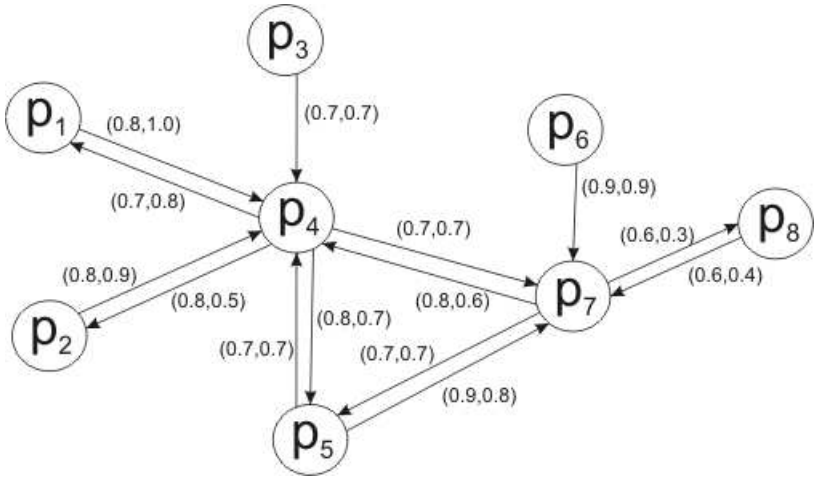


FIGURA 3.3 – Exemplo de rede de confiança

FSSD prevê quatro tipos de mensagens:

- **mensagem de anúncio**: inclui no seu corpo todos os campos suportados na informação de serviço mais os parâmetros de visibilidade (isto é, valores de GMCE) e o rastro da mensagem (a ser explicado a seguir). É necessário incluir os parâmetros de visibilidade para permitir que outros pares possam realizar o controle de exposição em nome do provedor/cliente.
- **mensagem de consulta**: idem ao anterior.
- **mensagem de resposta ao casamento**: gerada após o casamento autorizado, é enviada tanto ao provedor como ao cliente em questão. Inclui a descrição do anúncio ou da consulta no nível de visibilidade 1, dependendo se é destinada ao cliente ou provedor, respectivamente, bem como os resultados da autorização, que indicam se ambos ou apenas um deles obteve autorização.

- **mensagem de recomendação**: pode conter as identidades forte e fraca, e necessariamente um campo para recomendações sobre outros pares. É utilizada pelo gerenciamento de confiança, a fim de pares poderem trocar opiniões entre si. Também contém o rastro da mensagem.

Uma mensagem de anúncio ou consulta carrega inicialmente a informação de serviço com visibilidade total (isto é, nível 3). Mensagens sob o nível 3 não podem ser propagadas, pois a identidade forte é vinculada a um canal de comunicação seguro entre dois pares. Portanto, esse nível de visibilidade é restrito aos vizinhos de um par na topologia lógica. Nesse caso, o GMCE do nível 3 é utilizado apenas para filtrar os vizinhos que receberão os anúncios e consultas do par. Tal limitação é importante pois viabiliza ao provedor/cliente um controle maior sobre os pares com quem está expondo sua privacidade. No momento que o vizinho encaminha a mensagem a outros pares, esta já deve carregar a informação com visibilidade reduzida. A mensagem de recomendação, de forma similar, também é imposta ao mesmo mecanismo de controle de exposição, como explicado a seguir.

Considerando que um casamento realizado pelo par intermediário tenha sido autorizado, uma mensagem de resposta ao casamento é sempre enviada ao provedor e cliente pelos canais de propagação por onde vieram. Isso é possível graças a um mecanismo de *backtracing* (descrito na Seção 3.6.3), o qual é necessário pois o par intermediário pode não conhecer as identidades fortes do provedor e cliente. O conteúdo dessa mensagem é ainda codificado com a chave pública presente dentro da descrição do anúncio/consulta, tendo em vista um canal confidencial até o provedor/cliente.

O rastro da mensagem é um campo com tamanho limitado, utilizado para guardar os endereços MAC dos pares por onde passou a mensagem. Logo, o número de endereços que o campo pode suportar determina o número máximo de saltos que a mensagem pode ser propagada. Além de objetivar uma melhor escalabilidade na troca de mensagens de anúncio, consulta e recomendações, o rastro é utilizado também em outro dois aspectos: detecção de ciclos na propagação de mensagens e *backtracing*.

3.4.4 Principais componentes

Os principais componentes do FSSD são: gerenciamento de confiança, mecanismo pelo qual pares computam valores de confiança sobre outros pares; controle de exposição, o qual determina a visibilidade de uma informação de serviço ao longo de sua propagação, segundo parâmetros definidos pelo usuário; e casamento *in-network*, o qual realiza uma etapa de autorização sempre que ocorre um casamento no par intermediário ao provedor e cliente. Essa seção limita-se a explorar brevemente o funcionamento de cada componente; detalhes da implementação de cada um são apresentados na Seção 3.6.

O gerenciamento de confiança é integrado ao protocolo FSSD, ao invés de depender de um mecanismo ortogonal. A principal razão por trás dessa decisão de projeto é submeter as mensagens de recomendação ao controle de exposição. Dessa forma, FSSD garante que os mesmos princípios de privacidade utilizados para a exposição prudente de informações de serviço sejam aplicados também na exposição de opiniões entre os pares. Para tanto, utiliza-se os mesmos níveis de visibilidade de informações de serviço para as opiniões trocadas entre os pares. Essas opiniões, por sua vez, são formadas sobre as identidades fracas do sistema, podendo ser

baseadas em evidências diretas (uso de serviços, por exemplo) ou recomendações de outros pares. Cada par possui seu próprio repositório de opiniões, o que caracteriza um sistema de confiança descentralizado [Jösang et al., 2007]. No estado atual do trabalho, as opiniões são apenas subjetivas, podendo ter qualquer valor associado pelo par.

O controle de exposição tem como principal propósito diminuir a visibilidade de uma informação de serviço (ou opinião) na medida em que o risco com sua exposição aumenta. Tal risco está diretamente associado ao número de saltos que a mensagem é propagada (na topologia lógica), bem como as relações de confianças entre os pares associados aos saltos realizados. À medida que a mensagem é propagada, seus campos podem ser suprimidos para refletir a redução de visibilidade da informação carregada. Este controle é executado em cada par antes de propagá-la, com base nos parâmetros de visibilidade (valores de GMCE, Seção 3.4.2), definidos pelo usuário.

O armazenamento de informações de serviço e de opiniões ocorre em todos os pares que participam de sua propagação. As informações de serviço são armazenadas no repositório local de cada par, independente do nível de visibilidade que possuem. Pares podem receber a mesma informação de serviço através de diferentes canais de propagação, porém com níveis de visibilidade diferentes. Nesse caso, armazena-se a informação com sua maior visibilidade conhecida. As recomendações não são armazenadas, mas sim processadas pelos pares a fim de consolidar sua lista de opiniões locais.

A autorização implementada pelo mecanismo de casamento *in-network* complementa o controle de exposição, no sentido de tornar uma informação de serviço visível a pares que não a receberam por causa das restrições do controle de exposição. Essa etapa de autorização compreende verificar se o cliente atende às credenciais impostas no anúncio, bem como se o provedor atende às credenciais impostas na consulta. Uma vez que são utilizadas credenciais quantitativas, a autorização depende de o anúncio e consulta estarem com nível de visibilidade 2, dando acesso aos graus de confiança sobre o provedor e cliente. Além disso, o campo de opinião sobre a informação de serviço é empregado a fim de validar o uso da identidade fraca para obter o grau de confiança correspondente. Se o provedor/cliente é autorizado, recebe uma resposta ao casamento, contendo a consulta/anúncio correspondente no nível de visibilidade 1, o que preserva suas identidades até o momento da requisição e provisão do serviço, respectivamente.

A Figura 3.4 ilustra diferentes cenários de controle de exposição e de acesso. Os cenários estão organizados em ordem crescente de "proximidade" entre cliente e provedor. Abaixo de cada cenário estão os elementos envolvidos no controle de acesso para cada par, quando o casamento *in-network* é aplicável. No cenário A, não há casamento, pois não há um par intermediário alcançável por ambos, em termos de controle de exposição. No cenário B, a autorização falha, pois não existem identidades fracas expostas. No cenário C, m tem acesso à identidade fraca de c, o que permite determinar se o mesmo é autorizado a acessar o anúncio. Caso positivo, uma resposta ao casamento é enviada a c. Esse cenário, todavia, não permite verificar se p é credenciado a prover tal serviço (isto é, se atende às credenciais impostas na consulta). Apesar da situação desigual, fica a cargo do cliente decidir se inicia uma requisição a p. No cenário D, não existe autorização pois os pares já receberam a informação.

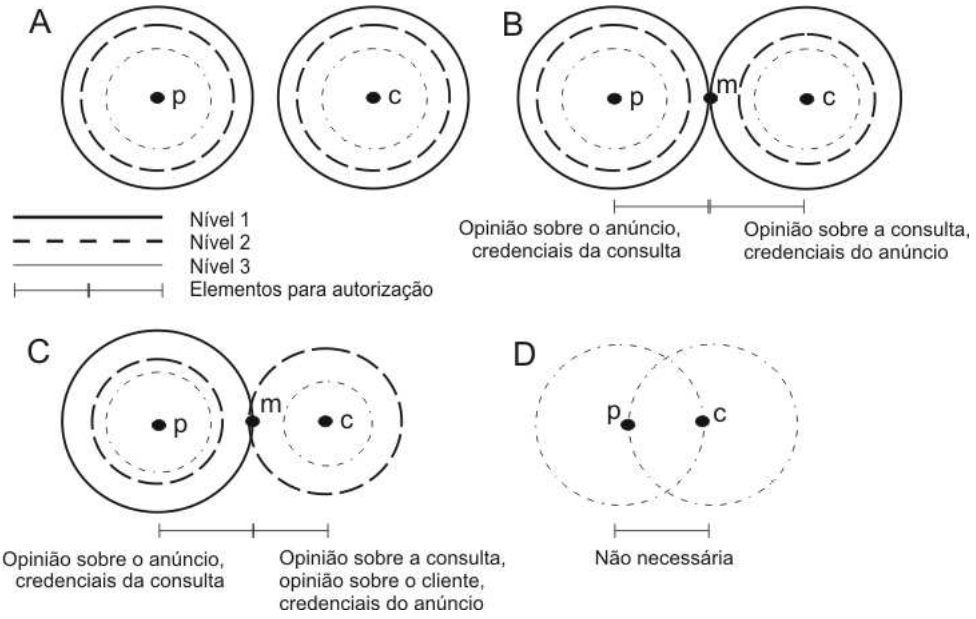


FIGURA 3.4 – Cenários de controle de exposição e de acesso

3.4.5 Exemplo ilustrativo

O diagrama da Figura 3.5 ilustra o comportamento dos componentes do FSSD para um anúncio e uma consulta, onde pode-se notar os três tipos de mensagens: consultas, anúncios e respostas ao casamento, representados respectivamente por Q, A e M. A rede de confiança utilizada no exemplo é a mesma definida na Figura 3.3; p_1 e p_8 são provedor e cliente, respectivamente.

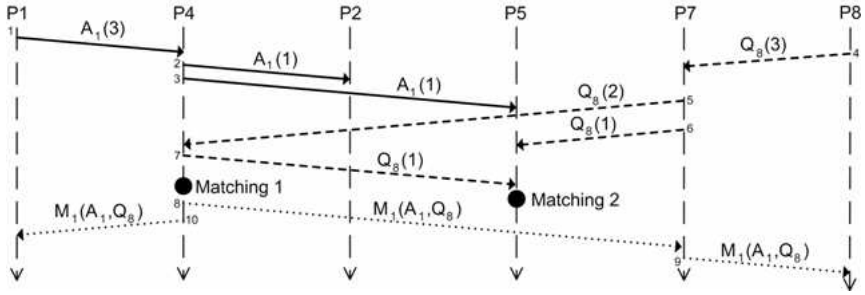


FIGURA 3.5 – Diagrama de tempo

O processo de descoberta ilustrado é descrito a seguir:

1-3: p_1 anuncia o serviço para p_4 (1), que propaga o mesmo para p_2 e p_5 (2 e 3), porém suprimindo as identidades forte e fraca;

4-6: p_8 envia a consulta para p_7 (4), que é propagada para os pares p_4 (5) – sem identidade forte – e p_5 (6) – sem ambas as identidades.

7 : par p_4 propaga ainda o anúncio para p_5, suprimindo a identidade fraca (7).

...: ocorre o casamento *in-network* nos pares p_4 e p_5, com base no anúncio e consulta recebidos.

8-10: o controle de acesso falha no par p_5, porém é realizado com sucesso em p_4, que então envia uma resposta ao casamento para o cliente p_8 (8) e o provedor p_1 (10). A resposta a p_8 deve passar por p_7 (9), uma vez que p_4 não conhece o endereço MAC de p_8. Esse caso ilustra o funcionamento do mecanismo de *backtracing*.

3.5 Formalização do Protocolo

Essa seção formaliza os componentes da arquitetura, parâmetros e outros elementos envolvidos no modelo de descoberta de serviços proposto. No gerenciamento de confiança, serão descritos a opinião e operadores que combinam múltiplas opiniões, bem como o conceito da rede de confiança. No controle de exposição, será formalizado o conceito de visibilidade da informação e será apresentada uma representação interna deste no protocolo, mais adequada para os mecanismos do FSSD. No casamento *in-network*, serão brevemente abordadas as credenciais de acesso, as quais são basicamente campos da informação de serviço. As definições aqui apresentadas serão úteis para a compreensão da próxima seção, que apresenta detalhes da implementação do FSSD.

O principal elemento do gerenciamento de confiança é a opinião (sobre um par, para não confundir com opinião sobre a informação de serviço), representada por $L(i, j)$, onde lê-se: opinião de p_i sobre o par p_j. Uma opinião consiste de dois números, $L(i, j) = (t_{ij}, c_{ij})$: a confiança t_{ij} (*trust*), tal como uma estimativa baseada em evidências locais ou recomendações de outros pares; e a certeza c_{ij} (*confidence*), sobre t_{ij}. O valor de certeza também corresponde à exatidão do valor de confiança associado; um valor alto de certeza indica que o p_i tem interagido com p_j por um longo tempo, logo o valor de confiança construído é mais preciso. Tanto confiança quanto certeza podem assumir um valor no intervalo $[0, 1]$. Até aqui, foi mencionado apenas o grau de "confiança", porém subentende-se nesse caso, e no restante do documento, que o valor de "certeza" também esteja associado.

No presente modelo de descoberta, uma opinião $L(i, j)$ pode tornar-se uma **relação de confiança** $L'(i, j)$, quando existe uma troca de identidades fortes e chaves públicas entre p_i e p_j para o estabelecimento de um canal de comunicação seguro entre os mesmos. As relações de confiança definem a rede de confiança, já apresentada neste capítulo. A rede de confiança é um grafo direcionado, onde vértices são pares e um arco de i para j corresponde à opinião de p_i sobre p_j. Seguindo o pressuposto acima, todos estes arcos são relações de confiança. Pode-se notar que elas não são simétricas, o que indica que pares podem possuir opiniões diferentes um do outro, porém tendo sido suficientes para estabelecer a relação de confiança entre eles.

O modelo de confiança considerado é semelhante ao proposto em [Theodorakopoulos and Baras, 2006], porém aqui a coleta de opiniões não é apenas local, mas também baseada em recomendações de outros pares. O uso de recomendações cria um nível de transitividade no gerenciamento de confiança, onde pares podem obter informações de outros com quem ainda não tenham interagido. Essa é uma propriedade importante para FSSD e seu mecanismo de controle de

exposição. Por exemplo, se Bráulio recebe uma opinião de Ana sobre Mercedes, tem-se uma relação transitiva do tipo Bráulio → Ana → Mercedes. Essa relação também é mensurável, o que viabiliza o controle de exposição para além dos pares vizinhos de um par.

A opinião transitiva é calculada usando operadores de concatenação e consenso; exemplos de implementação destes operadores são apresentados em [Theodorakopoulos and Baras, 2006]. O operador de concatenação $\otimes$ combina opiniões e recomendações, tal que $L(i,k) = L(i,j) \otimes L(j,k)$, gerando assim a opinião transitiva de p_i sobre p_k. Já o operador de consenso $\oplus$ combina opiniões transitivas sobre um mesmo par. Considerando $L^1(i,j)$ e $L^2(i,j)$ opiniões de p_i sobre p_j, adquiridas através de diferentes pares intermediários, temos $L(i,j) = L^1(i,j) \oplus L^2(i,j)$. Ambos operadores são associativos e comutativos, e o operador $\oplus$ é distribuído sobre $\otimes$, o que permite que sejam combinados. A definição considerada para esses operadores, no presente trabalho, é reproduzida a seguir:

$$(t_{ik}, c_{ik}) \otimes (t_{kj}, c_{kj}) = (t_{ik}t_{kj}, c_{ik}c_{kj})$$

$$(t^1_{ij}, c^1_{ij}) \oplus (t^2_{ij}, c^2_{ij}) = \begin{cases} (t^1_{ij}, c^1_{ij}), \text{ se } c^1_{ij} > c^2_{ij} \\ (t^2_{ij}, c^2_{ij}), \text{ se } c^1_{ij} < c^2_{ij} \\ (t^*_{ij}, c^1_{ij}), \text{ se } c^1_{ij} = c^2_{ij}, \text{ onde } t^*_{ij} = max(t^1_{ij}, t^2_{ij}) \end{cases}$$

Uma informação de serviço é representada por $X_i^{a|q}$, onde $a|q$ expressa um (a) anúncio ou (q) consulta e i indica o provedor ou cliente. Relembrando, a informação de serviço possui cinco campos, listados a seguir com os respectivos nomes utilizados para referência-los dentro da informação: identidade forte (*idForte*), identidade fraca (*idFraca*), descrição (*desc*), credenciais de acesso (*cred*) e opinião sobre a informação de serviço (*opInfo*). Os mesmos nomes são utilizados para referenciar esses campos nas mensagens de anúncio e consulta. Tendo em vista facilitar a representação, campos não visíveis dentro da mensagem e informação de serviço são iguais a *null*; por exemplo, X_i^a.idForte = null indica que a identidade forte de p_i não está exposta no seu anúncio a.

No controle de exposição, os parâmetros de GMCE para cada nível de visibilidade da informação de serviço são representados através de R^r_x, onde $r \in \{1,2,3\}$ é o nível de visibilidade e x é a informação de serviço. $R^r = (t_{min}, c_{min})$ define os valores de confiança e certeza necessários: considere que o par p_i deseja enviar um anúncio x a p_k; este é apto a receber o anúncio no nível de visibilidade r se e somente se $L'(i,k) \geq R^r_x$. Se p_k deseja propagá-lo para p_j, teríamos $\exists L'(k,j)$ e $L(i,j) \geq R^r_x$, onde $L(i,j)$ é uma opinião transitiva.

A próxima seção aborda aspectos de implementação do FSSD. Os algoritmos a serem apresentados utilizam muitos dos símbolos aqui introduzidos. Para facilitar a posterior leitura, a Tabela 3.1 resume todos os símbolos dessa seção.

3.6 Aspectos de Implementação

Os aspectos de implementação para cada componente de FSSD são descritos a seguir.

TABELA 3.1 – Tabela de símbolos

$L(i,j)$	Opinião de p_i sobre p_j
$L'(i,j)$	Relação de confiança de p_i com p_j
t_{ij}	Confiança de p_i sobre p_j
c_{ij}	Certeza de p_i sobre t_{ij}
$\otimes$ e $\oplus$	Operadores de concatenação e consenso
t_{min} e c_{min}	Valores mínimos de confiança e certeza
R^r	GMCE para o nível de visibilidade r
$X_i^{a\|q}$	Informação de serviço – (a) anúncio ou (q) consulta – cujo provedor ou cliente é p_i

3.6.1 Gerenciamento de confiança

Cada par mantém duas **tabelas de confiança**: uma baseada em evidências locais, e outra baseada em recomendações. A tabela de evidências locais é enviada por p_i como sua recomendação a outros pares. Uma vez que o envio desta recomendação é sujeito ao controle de exposição, a expectativa é que a coleta de opiniões se torne menos sujeita a falsas acusações e, conseqüentemente, mais exata [Marti and Garcia-Molina, 2006], além de proteger a privacidade do par. Ao receber uma recomendação de p_j, p_i atualiza sua tabela baseada em recomendações, combinando as opiniões existentes com as recém-recebidas. Para tanto, primeiro é utilizado o operador $\otimes$, para gerar opiniões transitivas baseadas nas recomendações de p_j; em um segundo momento, emprega-se o operador $\oplus$, para combinar as opiniões existentes com as transitivas calculadas no primeiro passo. O segundo operador é utilizado também quando pares atualizam a tabela de evidências diretas.

O gerenciamento dessas tabelas considera o fator mobilidade, implementando assim a aplicação periódica de um fator de envelhecimento nas opiniões existentes. Isso faz com que a certeza sobre a opinião reduza ao passar do tempo, afetando principalmente aqueles pares que não costumam se interagir freqüentemente. O envelhecimento também diminui a probabilidade de ataques de traição [Feldman et al., 2004], onde pares comportam-se bem por um período de tempo, mudando um tempo depois o seu comportamento.

Os mecanismos de controle de exposição e de acesso dependem do gerenciamento de confiança. A principal interface entre estes componentes é o fornecimento de opiniões sobre identidades fracas aos dois mecanismos. Quando a opinião sobre um par está presente em ambas as tabelas, a opinião consolidada é calculada através da fórmula a seguir, onde L^l é a opinião na tabela de evidências locais, L^r é a opinião na tabela de recomendações e W^l e W^r são os respectivos pesos das opiniões. Estes pesos são parâmetros do usuário, devendo respeitar os seguintes critérios: $W^l + W^r = 1$ e $W_l \geq W_r$. Caso a opinião não esteja em nenhuma das tabelas de confiança do par, o gerenciamento de confiança retorna um resultado vazio ao controle de exposição ou de acesso, visto que não existe um mecanismo para consulta de opiniões em outros pares.

$$L(i,k) = L^l(i,k) \times W^l + L^r(i,k) \times W^r$$

3.6.2 Controle de exposição

O Algoritmo 1 descreve o controle de exposição empregado pelo par p_c, que recebe uma informação de serviço $X_i^{a|q}$, e deve decidir se propaga a mesma para p_j, baseando-se nos valores de GMCE (ou R_x^r, como definido na Seção 3.5) determinados por p_i, o qual é o provedor ou cliente que gerou a informação de serviço. Se o par p_j não possui um grau de confiança mínimo para receber as informações sensíveis de determinado nível de visibilidade, campos devem ser suprimidos (linha 8) ou a informação não deve ser mais propagada (linha 11), pois não há níveis menores de visibilidade. Como explicado anteriormente, a identidade forte é removida na propagação, por estar atrelada ao canal de comunicação entre p_i e p_c. A única forma de p_j conhecer a identidade forte de p_i é através do estabelecimento de uma relação de confiança com o mesmo.

FSSD prevê o estabelecimento de relações de confiança através de pares intermediários, entretanto sua especificação não detalha como essa operação deve ser feita. Algumas restrições são especificadas, principalmente para garantir que o algoritmo obedeça aos princípios de privacidade do FSSD. O par intermediário deve interceder de tal forma a não expor a privacidade de um par ao outro, até que ambos concordem com o estabelecimento da relação de confiança. Como dito anteriormente, essa forma de estabelecimento de relações de confiança pode ser uma propriedade importante para a publicação segura de identidades fortes e chaves públicas entre os dois pares.

Algorithm 1 Par p_c decide se propaga $X_i^{a|q}$ para todo par p_j, onde $\exists L'(c,j)$

1: $p_s \leftarrow$ par que enviou $X_i^{a|q}$ {não necessariamente p_i}
2: $msg \leftarrow$ mensagem recebida que carrega $X_i^{a|q}$
Require: $\exists L'(c,j)$
3: **if** msg.idForte $\neq$ null $\wedge\, msg.R^3 \leq L'(c,j)$ **then**
4: Permite criar relação de confiança entre p_i e p_j por meio de p_c
5: **end if**
6: msg.idForte = null {Suprime identidade forte}
7: **if** msg.idFraca $\neq$ null $\wedge\, msg.R^2 > L'(c,j)$ **then**
8: msg.idFraca = null {Suprime identidade fraca}
9: **end if**
10: **if** msg.desc $\neq$ null $\wedge\, msg.R^1 > L'(c,j)$ **then**
11: **return false** {Não propaga}
12: **end if**
13: **return true**

O algoritmo empregado para iniciar um anúncio ou consulta é uma versão simplificada deste último: p_i envia um anúncio/consulta para p_j se e somente se existe uma relação de confiança entre ambos ($\exists L'(i,j)$) e o grau de confiança é suficiente para a exposição do nível 3 ($msg.R^3 \leq L'(i,j)$). Entretanto, como mencionado na Seção 3.4.2, FSSD permite um nível adicional de parametrização, onde o provedor/cliente determina os próximos pares que podem receber o anúncio/serviço de forma manual, sobrepondo o controle de exposição no primeiro salto.

Antes de realizar qualquer modificação na mensagem com relação à supressão de informações, o par a armazena no seu repositório; em seguida, atualiza algumas

informações na mensagem utilizadas para o controle de exposição. O Algoritmo 2 descreve estas operações. As atualizações sobre a mensagem correspondem às linhas 4 e 10: na primeira, é atualizada a opinião sobre a informação de serviço, que reflete a opinião sobre o canal transitivo pelo qual a mensagem é propagada; na segunda, atualiza-se os valores de GMCE embutidos na mensagem para cada nível de visibilidade. A fórmula utilizada para atualizar o GMCE corresponde ao inverso do operador $\otimes$: conforme a informação é propagada, o GMCE aumenta. O efeito é o mesmo de se incluir na mensagem o GMCE original do par p_i para cada nível de visibilidade e $L(i, c)$, para o próximo par definir se pode propagar a informação de serviço. Contudo, expor $L(i, c)$ em cada mensagem é uma perda de privacidade desnecessária, pois permite que p_c saiba o quanto p_i confia nele.

Algorithm 2 Par p_c armazena $X_i^{a|q}$ e prepara a mesma para propagação

1: $p_s \leftarrow$ par que enviou $X_i^{a|q}$ {não necessariamente p_i}
2: $msg \leftarrow$ mensagem recebida que carrega $X_i^{a|q}$
3: $rep_c \leftarrow$ repositório local de p_c
4: msg.opInfo $= msg$.opInfo $\otimes L(c, s)$
5: **if** msg.idFraca $\neq null \wedge \exists L(c, i)$ **then**
6: $\quad rep_c.X_i^{a|q}$.opInfo $= L(c, i)$
7: **else**
8: $\quad rep_c.X_i^{a|q}$.opInfo $= rep_c.X_i^{a|q}$.opInfo $\oplus msg$.opInfo
9: **end if**
10: $msg.R^r = msg.R^r / L'(c, j)$ para $r = 1, 2, 3$

A opinião sobre a informação, $X_i^{a|q}$.opInfo, também é atualizada no repositório local de p_c. Caso a identidade fraca de p_i é acessível e é possível obter uma opinião sobre p_i através dessa identidade (com o gerenciamento de confiança), então a opinião sobre a informação de serviço se resume a $L(c, i)$ (linha 6). Caso contrário, é utilizada a própria opinião embutida na mensagem, msg.opInfo (linha 8). Para aumentar a precisão da opinião sobre a informação nesse segundo caso, emprega-se o operador $\oplus$, para combinar os valores de msg.opInfo presentes em várias cópias de $X_i^{a|q}$, advindas por caminhos alternativos.

3.6.3 Casamento *in-network*

Considerando um casamento entre X_i^a e X_j^q realizado pelo par intermediário p_c, o cliente p_j é autorizado a acessar X_i^a se e somente se: a identidade fraca de p_j esteja exposta (X_j^q.idFraca $\neq null$); a opinião sobre a informação de serviço X_j^q, e conseqüentemente sobre a identidade fraca exposta na mesma, for suficiente em relação à credencial de acesso imposta em X_i^a (X_j^q.opInfo $\geq X_i^a$.cred); e se a opinião de p_c sobre p_j, baseada na identidade do último, atende à credencial de acesso ($L(c, j) \geq msg$.cred). Trocando X_i^a por X_j^q, tem-se o controle de acesso executado para o provedor p_i, onde o par intermediário verifica se o mesmo atende à credencial imposta em X_j^q.

Por fim, é importante notar que respostas ao casamento são enviadas sem expor as identidades dos donos de X_i e X_j (p_i e p_j), por meio de um mecanismo de *backtracing*. Mensagens de anúncios e consultas possuem um rastro (*trace*) embutido, excluindo a identidade do provedor ou cliente, para garantir sua

privacidade. Através deste rastro, o par p_m consegue propagar a resposta pelo caminho inverso, criptografando a resposta com a chave pública da informação de serviço (presente na descrição); logo, só o dono da informação pode decodificá-la. Dessa forma, tal mecanismo satisfaz os requisitos de anonimidade do cliente e provedor, além de evitar que estes se exponham um ao outro sem antes avaliar os benefícios e implicações envolvidas. Os pares que recebem uma mensagem de resposta ao casamento sabem que devem propagá-la pelo caminho inverso por onde veio o anúncio/consulta. Para fins de escalabilidade, ao invés de guardar todo o rastro no seu repositório local, cada par armazena apenas o par que lhe antecede no rastro. O rastro é guardado juntamente com um sumário *digest* da informação de serviço, para poder identificá-lo no momento do *backtracking*.

3.7 Discussão

Com FSSD, pares limitam seus anúncios e consultas em função dos graus de privacidade e segurança exigidos. O grau de segurança é dado pelas relações de confiança compartilhadas com outros pares. Uma questão importante é o problema do *bootstrapping*: o que acontece quando o usuário encontra-se em um novo ambiente, sem infra-estrutura de descoberta, ou de segurança, e não possui nenhuma relação de confiança para iniciar uma descoberta de serviços segura e prudente? Até onde sabemos, não existe na literatura um sistema que resolva completamente o problema do *bootstrapping* em um ambiente sem infra-estrutura de segurança. Em [Feldman et al., 2004], é proposta uma estratégia adaptativa, onde pares calculam uma probabilidade estimada de ser atacado pelo próximo estranho, e decide confiar no mesmo baseado nessa probabilidade. Entretanto, quando o problema tratado é a privacidade do usuário, não é viável depender de um sistema baseado em probabilidades.

O projeto do FSSD assume como premissa que usuários desejam ter segurança e privacidade ainda mais em ambientes estranhos, o que os levará a criar pelo menos uma relação de confiança antes de começarem a interagir com outros pares. Isso não é re-engenharia social: é comum em nosso dia-a-dia entrar em um ambiente desconhecido e se direcionar inicialmente a algum indivíduo que trabalhe no local. Através dele, "toma-se conhecimento" de vários serviços oferecidos naquele local. Da mesma forma, isso pode acontecer no modelo de descoberta proposto por FSSD. A partir de uma relação de confiança, pode-se interagir com a mesma, fortalecer essa relação e então confiar nela quando deseja obter outras relações de confiança. Esse é o caso do cenário de Bráulio obtendo serviços do laboratório de radiologia através de outro laboratório. Explorar o uso de dispositivos ubíquos também auxilia na obtenção de relações de confiança, como é o caso de cartões inteligentes. Um par poderia, por exemplo, obter uma associação segura com algum ambiente através de suas credenciais presentes no cartão.

A questão da usabilidade é um ponto crítico em sistemas ubíquos. FSSD oferece vários parâmetros que podem influenciar a descoberta de serviços. Entretanto, esta flexibilidade não é vista como um empecilho para um bom grau de usabilidade; pelo contrário, ela viabiliza a construção de soluções inteligentes sobre o protocolo de descoberta, que capturam o perfil e preferências do usuário, relativas à privacidade e segurança, e refletem isso como parâmetros na descoberta de serviços. As relações de confiança e o manuseio do sistema de confiança (através

de votos, por exemplo) também não são consideradas fatores limitantes à usabilidade dos sistemas. Associação de graus de confiança a usuários e serviços é cada vez mais um processo social, já presente em muitos sistemas comerciais e da Internet.

Um outro aspecto importante é a relação entre a topologia lógica e a rede fixa subjacente, conforme explicado a seguir. Os cenários considerados até então presumem que pares podem comunicar-se (através de rede fixa ou sem fio). Esse fator afeta o projeto de FSSD em termos de eficiência, devendo guiar a forma como deve ser realizada a comunicação entre os pares da topologia lógica. Como a topologia lógica tende a aumentar a medida que novas relações de confiança são estabelecidas, é possível que a mesma fique muito maior que a topologia física visível ao par em um dado instante. Portanto, pode ser necessário ao par saber quais vizinhos na topologia lógica são alcançáveis na topologia física.

Outras questões a serem investigadas no futuro incluem a revogação de chaves (isto é, o problema de invalidar uma chave de segurança e distribuir uma nova, porém a um conjunto alterado de pares) e a eficácia do gerenciamento de confiança.

Capítulo 4

Avaliação do Protocolo

O capítulo anterior apresentou a proposta do protocolo para descoberta de serviços FSSD. Para investigar o funcionamento do protocolo e suas propriedades básicas, foi implementado um protótipo em Java, valendo-se do ambiente de simulação Simmcast [Muhammad and Barcellos, 2002]. A simulação do protocolo foi empregada então para medir o impacto dos parâmetros configurados pelo usuário, relativos aos graus de privacidade exigidos, em métricas de descoberta. O presente capítulo descreve como essa avaliação foi realizada com o protótipo do FSSD e tece considerações sobre a eficácia do protocolo. A avaliação permite "validar" o principal diferencial de FSSD, que é a flexibilidade oferecida quanto aos compromissos entre colaboração, segura e privacidade.

Primeiramente, descreve-se o modelo da simulação considerado, com premissas, parâmetros de entrada e métricas estabelecidas (Seção 4.1). Na seqüência (Seção 4.2), os principais resultados são apresentados, permitindo tirar várias conclusões a respeito das características fundamentais do FSSD, bem como estabelecer os próximos passos para a avaliação do protocolo. A Seção 4.3 encerra o capítulo com uma discussão e as principais conclusões.

4.1 Modelo da Simulação

Os experimentos foram conduzidos empregando-se um conjunto de pares organizados em uma topologia física em estrela, simulando um canal de broadcast entre os mesmos. Acima desta topologia física, existe uma rede de confiança entre os pares, exibindo propriedades de *small-world*. Trabalhos como [Mtibaa et al., 2007] mostram que estas propriedades se aplicam também a redes *ad hoc* e portanto são adequadas para a simulação do FSSD. O algoritmo para geração de topologias expressando redes de confiança descrito em [Capkun et al., 2002] foi utilizado para gerar cenários com N pares. A Figura 4.1 ilustra um exemplo de topologia *small-world* gerada por esse algoritmo. Para obter-se valores estatisticamente confiáveis, os experimentos foram repetidos com várias topologias geradas aleatoriamente segundo o algoritmo. Considerando as topologias geradas, na média o diâmetro da rede foi 6, e o grau médio dos pares oscilou entre 6 e 9, com média 8.

Os valores dos arcos da topologia lógica (ou seja, das relações de confiança) são inicializados segundo distribuições de probabilidade (Seção 4.1.2) e se mantêm estáticos ao longo da simulação. Nesse contexto, assume-se um gerenciamento de confiança eficaz e foca-se a avaliação nos demais componentes de FSSD, que são

controle de exposição e casamento *in-network*. Visto que as relações de confiança são estáticas, o valor de certeza pode ser ignorado na presente avaliação. Dessa forma, ele é igual ao valor de confiança, ou seja, uma opinião $L(i, j)$ é igual a tupla (t_{ij}, t_{ij}). Da mesma forma, o valor de GMCE para o nível de visibilidade r, R^r, é definido como (t_{min}, t_{min}).

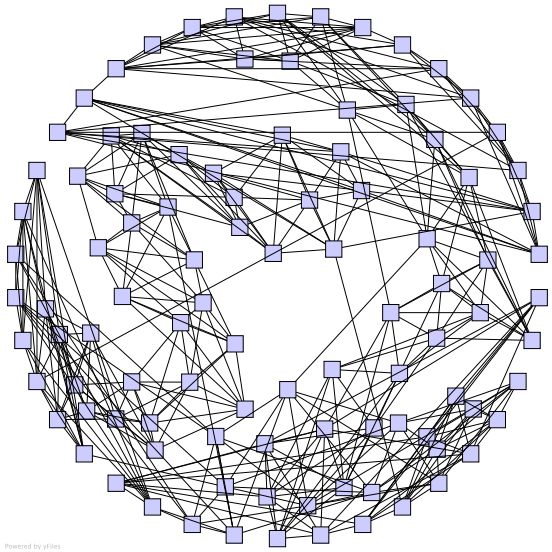


FIGURA 4.1 – Exemplo de topologia *small-world* gerada

Quanto à descoberta de serviços, é assumido um cenário simples, onde pares são clientes de um serviço (ou seja, que procuram esse serviço em um dado momento) e potencialmente provedores de outro serviço durante a simulação. Presume-se um conjunto de serviços, representado por S. Estes serviços podem ser oferecidos por mais de um par, sendo alocados uniformemente aos mesmos; uma parcela dos pares não oferecerá nenhum serviço. Cada par também deve estar associado ao serviço que irá consultar durante a simulação. Essa associação segue uma distribuição Zipf, a qual declara, no contexto da descoberta de serviços, que serviços mais conhecidos devem ser consultados com mais freqüência. Observa-se que o vínculo de um par com o serviço provido e o serviço consultado é estático. As mensagens de anúncio são enviadas de forma periódica, enquanto que as mensagens de consulta são transmitidas segundo uma distribuição exponencial.

Os experimentos foram divididos em duas partes. Na primeira, considerou-se apenas pares bons e relações de confiança estreitas entre os mesmos. Na segunda parte, o gerador de topologia foi modificado para associar uma parcela da rede a pares ruins. Nesse caso, foi determinado um modelo de ataque simples, onde pares ruins estabelecem relações de confiança altas entre si e opinam sobre pares bons de forma maliciosa. Os resultados obtidos permitem mostrar o impacto dos pares ruins nos aspectos de colaboração e privacidade.

O objetivo a cada execução é coletar as métricas da simulação com a variação da visibilidade dos anúncios e consultas. Cada experimento é dividido em múltiplas rodadas, nas quais é executada a simulação com um GMCE (grau mínimo de confiança para exposição, definido na Seção 3.4.2) diferente para um determinado nível de visibilidade. Como mencionado anteriormente, o GMCE para um nível de visibilidade determina se um par pode receber uma dada informação de serviço neste nível. São executadas múltiplas repetições de cada rodada, com sementes aleatórias distintas, computando-se uma média para a curva que representa o impacto da variação de GMCE. No restante do texto, GMCE pode ser encontrado também na forma de sua representação formal, R^r. Para diferenciar este parâmetro de anúncios e consultas, adota-se R^r_a e R^r_q, respectivamente.

4.1.1 Métricas

As métricas de avaliação consideradas neste trabalho foram: **taxa de casamento**, que mede o número de casamentos entre serviços anunciados e consultas ao mesmo; **taxa de efetividade do casamento**, que representa o número de casamentos onde o cliente recebeu o anúncio, seja por meio do controle de exposição ou pelo mecanismo de casamento *in-network*; e **taxa de exposição** de informações de serviço, em termos de números de pares que as recebem e são capazes de decodificá-las, tomando assim conhecimento sobre as mesmas. Na primeira e segunda métricas, é avaliado o aspecto da colaboração para obter eficácia na descoberta, porém em detrimento à privacidade dos pares. A terceira métrica mede o custo dessa colaboração, em termos da exposição de informações que comprometem a privacidade do provedor e cliente. De um modo geral, as métricas permitem estudar o compromisso entre os aspectos de colaboração e privacidade na descoberta de serviços, através da variação do GMCE de cada nível de visibilidade para anúncios e consultas.

A taxa de casamento e de efetividade do casamento são definidas a seguir. Seja Q_s o conjunto de consultas ao serviço $s \in S$, $q_{is} \in Q_s$ a consulta de p_i ao serviço s e a_{is} o anúncio de p_i sobre o serviço s. A taxa de casamento de p_i é o número de casamentos encontrados do tipo (a_{is}, q_{js}) (onde p_j pode ser qualquer par, com exceção de p_i), dividido por $|Q_s|$. Em outras palavras, é a porcentagem dos pares que procuram e encontram seu serviço sobre o número total de pares que o procuram. A taxa de efetividade do casamento de p_i utiliza um cálculo similar: é o número de casamentos do tipo (a_{is}, q_{js}), onde p_j obteve acesso a a_{is}, dividido por $|Q_s|$. Essa última é no máximo igual à primeira, pois desconsidera casamentos *in-network* onde o cliente não atende às credenciais impostas pelo anúncio. Pares que não oferecem serviços possuem ambas as taxas iguais a zero e são desconsiderados da média final. Já a taxa de exposição de p_i é calculada para consultas e um determinado nível de visibilidade; basicamente, corresponde ao número de pares que tomam conhecimento sobre a mesma no nível de visibilidade em questão.

Os resultados esperados são resumidos a seguir:

- as taxas de casamento e de efetividade do mesmo devem decrescer de forma proporcional ao aumento do GMCE dos níveis de visibilidade 1 e 2, respectivamente. Quanto mais exposta for a informação do serviço, maiores são as chances de obter um casamento; já a efetividade está relacionada também à exposição do anúncio/consulta com as identidades fracas do provedor/cliente,

para aumentar as chances de um cliente obter acesso ao anúncio em casamentos *in-network*;

- a variação do GMCE para o nível 3 deve implicar uma maior distribuição inicial do anúncio/consulta pelo provedor/cliente aos seus pares vizinhos na rede de confiança. Um valor menor de GMCE (ou seja, menor prudência na exposição) também contribui para aumentar ambas as taxas relativas ao casamento;

- a taxa de exposição deve seguir o comportamento das taxas de casamento, ou seja, ela deve decrescer à medida que aumenta-se o GMCE.

4.1.2 Parâmetros

A Tabela 4.1 apresenta os principais parâmetros da simulação do FSSD, com os respectivos valores utilizados.

TABELA 4.1 – Tabela de parâmetros

# de pares (N)	100
# categorias de serviço ($\|S\|$)	6
# repetições	5
# rodadas para cada repetição	20
diâmetro máximo de uma mensagem	3 saltos
Opiniões entre pares bons-bons	Distribuição uniforme [0,7;1,0]
Opiniões entre pares bons-ruins	Distribuição uniforme [0,0;0,3]
Opiniões entre pares ruins-ruins	Distribuição uniforme [0,3;1,0]
Opiniões entre pares ruins-bons	Distribuição uniforme [0,0;0,7]
GMCE para envio de recomendações	$R^1 = R^2 = R^3 = 0,7$
Peso das recomendações	0,4
Peso das evidências locais	0,6
Fator de envelhecimento	0,0

A eficácia do gerenciamento de confiança possui impacto nos demais componentes de FSSD, porém sua avaliação foge ao escopo desta dissertação, devendo a mesma ser realizada futuramente como parte de um estudo mais amplo. Portanto, uma série de parâmetros pertinentes ao gerenciamento de confiança é utilizada para abstrair parte do seu funcionamento durante a simulação. As opiniões iniciais entre os pares são relativas às arestas da rede de confiança gerada. Seus valores de confiança e certeza são gerados seguindo as distribuições descritas na presente tabela, dependendo se os vértices da aresta são bons ou ruins. Note que pares ruins reservam uma margem para estabelecer boas opiniões sobre pares bons e más opiniões sobre pares ruins; esta é uma forma de obter ataques de comportamento alternado [Marti and Garcia-Molina, 2006].

A tabela de evidências diretas do par é inicializada com suas opiniões iniciais e mantida de forma estática durante toda a simulação. A tabela de recomendações é inicializada da mesma forma, porém as opiniões existentes são atualizadas com as recomendações recebidas de outros pares. Nestes experimentos, o fator de envelhecimento é configurado para zero de maneira a desativá-lo; seu uso demandaria alimentar o sistema com evidências após interações e uso de serviços, o que foge ao escopo deste trabalho.

4.2 Principais Resultados

Os principais resultados obtidos com a presente avaliação são comentados a seguir.

4.2.1 Visibilidade da informação x eficácia na descoberta

Esta subseção apresenta resultados relativos às métricas taxa de casamento e de sua efetividade. As mesmas são empregadas para demonstrar a eficácia da descoberta, em função dos parâmetros de visibilidade definidos pelos pares em seus anúncios e consultas de serviços. Como discutido em outras seções, essa relação define o compromisso entre os aspectos de colaboração e privacidade. O resultado das métricas é determinado pelos valores de GMCE para anúncios e consultas dos pares da rede, bem como dos graus de confiança compartilhados entre os mesmos.

Os graus de confiança são definidos pelo gerador da topologia, e sua evolução no sistema compete ao gerenciamento de confiança, portanto não serão discutidos nesses resultados. A variação do GMCE para consultas, R_q^r, é expressa no eixo x dos gráficos. No caso dos anúncios, essa variação acontece com a introdução de um conjunto de **classes de privacidade** no modelo da simulação. Essas classes, resumidas na Tabela 4.2, possuem diferentes valores para R_a^r entre os níveis de visibilidade. Por conveniência, assume-se que as credenciais impostas em cada anúncio (coluna 5) possuem o mesmo valor que o R_a^1 da classe. Cada par é alocado a uma destas classes durante a simulação. É importante observar que, em uma determinada simulação, pares da rede irão compartilhar o mesmo valor de R_q^r (com exceção do nível 3, como será explicado adiante), enquanto que pares da classe irão possuir o mesmo valor de R_a^r para os três níveis de visibilidade.

TABELA 4.2 – Classes de privacidade para anúncios de serviços

Descrição	R_a^3	R_a^2	R_a^1	Credenciais
Classe 1	0,90	0,80	0,50	0,50
Classe 2	0,90	0,70	0,50	0,50
Classe 3	0,94	0,88	0,70	0,70
Classe 4	0,75	0,62	0,50	0,50
Classe 5	0,85	0,77	0,70	0,70
Classe 6	0,60	0,55	0,50	0,50

Pode-se interpretar uma classe de privacidade como sendo um tipo de perfil do usuário, no papel de provedor de serviços. Por exemplo, pares das classes 3 e 5 são mais prudentes na exposição de seus anúncios ($R_a^1 = 0,7$), enquanto que aqueles das demais classes são menos prudentes ($R_a^1 = 0,5$). Outro exemplo são os pares que se comportam de forma prudente ao expor a identidade forte atrelada ao anúncio, caracterizados nas classes 1, 2 e 3.

Os gráficos a seguir apresentam uma curva para cada classe. Avalia-se o protocolo ao variar o GMCE tanto para anúncios como consultas, identificando correlações entre valores de GMCE para anúncios e consultas. Cada curva corresponde a uma interpolação de pontos, resultantes das diferentes rodadas da simulação. Considerando a métrica de taxa de casamento, por exemplo, um ponto de uma curva pode ser interpretado como a média de casamentos obtida com os pares da classe associada àquela curva, dado um valor de GMCE.

As Figuras 4.2 e 4.3 mostram o compromisso entre o grau de privacidade exigido pelo usuário para níveis de visibilidade 1 e 2, respectivamente, e a eficácia da descoberta. Na Figura 4.2(a), varia-se R_q^1 ao longo do eixo x e assume-se $R_q^2 = R_q^1$ e R_q^3 como uma medida de cada par, sendo igual ao R_a^3 da classe com a qual o par está vinculado. R_q^2 e R_q^1 podem assumir valores equivalentes nos experimentos pois não existe uma correlação entres eles que impacte nos resultados das métricas. Já R_q^3 está correlacionado com ambos, pois limita a distribuição inicial da consulta pelo cliente aos seus pares vizinhos. De forma similar, na Figura 4.3(a) é variado R_q^2 ao longo do eixo x, assumindo-se $R_q^1 = R_q^2$ e R_q^3 igual ao R_a^3 da classe. Ambos os gráficos são resultantes de simulações com pares bons apenas.

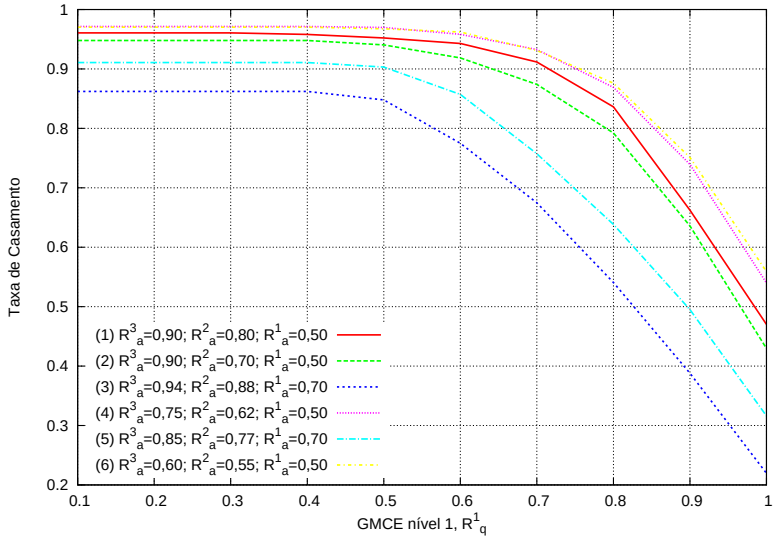
Esses experimentos foram ainda executados com valores diferentes de R_q^3, para expressar a variação do GMCE para o nível de visibilidade 3. As Figuras 4.2(b) e 4.3(b) apresentam os mesmos gráficos anteriores, porém com o valor original de R_q^3 menos $0,2$, o que caracteriza uma menor prudência na exposição das identidades fortes atreladas às consultas. Como discutido a seguir, uma exposição mais prudente nesse nível não representa muito ganho na eficácia da descoberta, o que significa que pares podem resguardar sua identidade física sem limitar a sua colaboração na descoberta.

O principal resultado da Figura 4.2(a) é a relação inversamente proporcional obtida entre os parâmetros de visibilidade e a taxa de casamento, como esperado. Isso permite validar o controle de exposição provido por FSSD como forma de usuários refletirem suas exigências de privacidade na descoberta de serviços. Quanto maior R_q^1, maior é a prudência na exposição das consultas, o que acaba diminuindo o número de casamentos realizados. As curvas exibem um comportamento similar: classes mais prudentes, como 3 e 5, obtêm uma taxa de casamento menor que as demais. É importante observar que a relação inversa mencionada não implica que uma taxa de casamento é alta somente se o valor de GMCE para o nível 1 é baixo. Conforme mostram as curvas da Figura 4.2(a) (e da maioria dos gráficos a seguir), é possível obter altas taxas de casamento com grau de prudência médio ($R_q^1 = 0,5$).

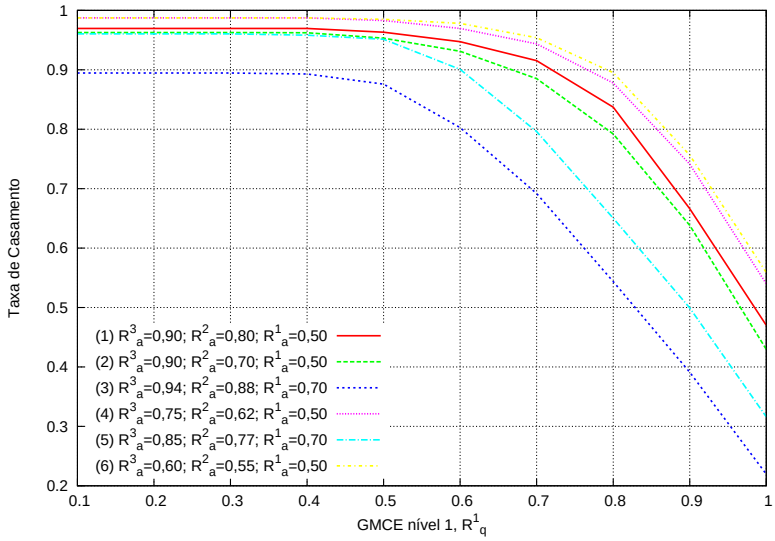
A efetividade do casamento também obedece a relações semelhantes com o GMCE do nível de visibilidade 2. Observa-se, na Figura 4.3(a), que quanto menor o R_q^2, maior é o número de casamentos efetivos realizados, particularmente devido à maior exposição das identidades fracas dos clientes (condição essencial para o casamento *in-network*). As classes 3 e 5 apresentam uma taxa menor devido às credenciais de acesso aos anúncios mais rígidas (0,7). Um ponto importante a ser destacado é o compromisso entre provedores e clientes: a curva 1, por exemplo, mostra que é possível obter taxas de casamento efetivo entre 80% e 90% quando clientes e provedores expõem suas consultas e anúncios com um grau mínimo de confiança igual a 0,8 para nível 2 ($R_q^2 = R_a^2 = 0,8$).

A variação de R_q^3 nas Figuras 4.2(b) e 4.3(b) mostra que a correlação entre o nível 3 e os níveis 1 e 2 é pequena, visto que não houve mudança significativa nas curvas de ambos os gráficos. Outro resultado importante, extraído destes e gráficos anteriores, é que pares não necessitam expor muito suas identidades fortes tendo em vista obter uma descoberta eficaz. Todas as classes apresentaram taxas de casamento efetivo entre 90% e 100%, com R_a^3 variando entre $0,60$ e $0,90$, excetuando-se as classes 3 e 5, onde a maior prudência está sobre R_a^1 e não R_a^3. Essa propriedade é relevante porque permite a pares resguardarem sua identidade física, sem abrir mão da colaboração na descoberta de serviços.

As Figuras 4.4 e 4.5 apresentam gráficos equivalentes àqueles das Figuras

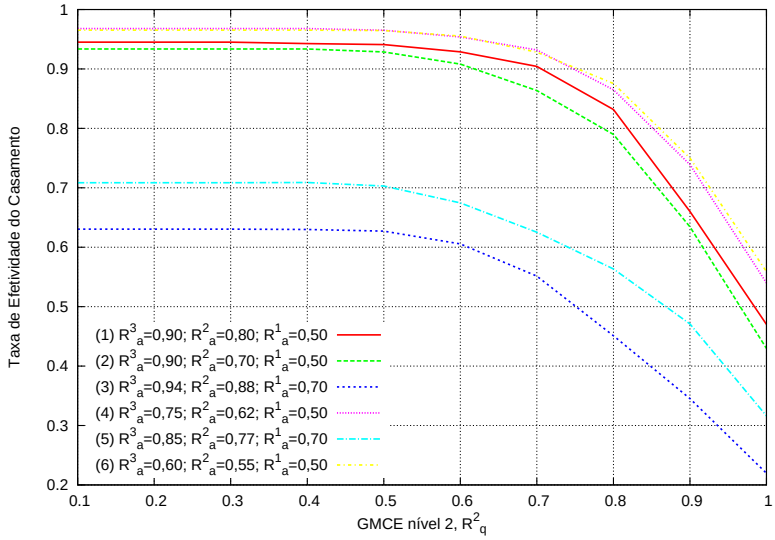


(a) Com menor visibilidade do nível 3

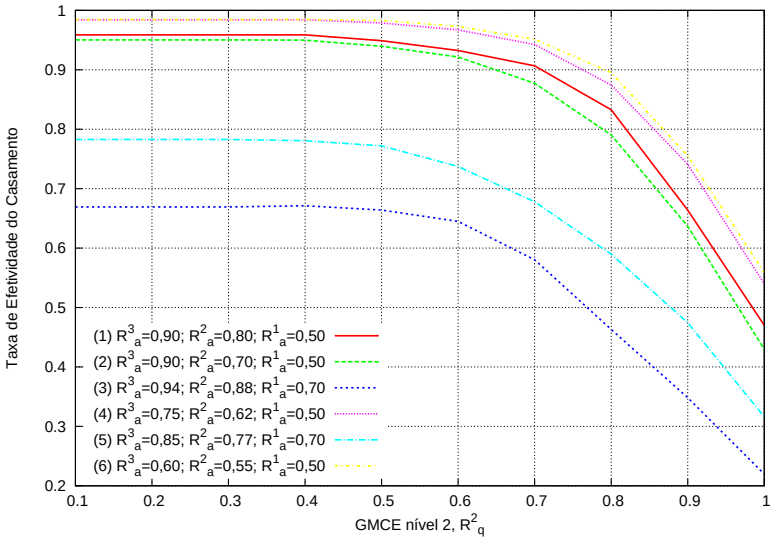


(b) Com maior visibilidade do nível 3

FIGURA 4.2 – Compromisso entre privacidade (nível 1) e eficácia na descoberta

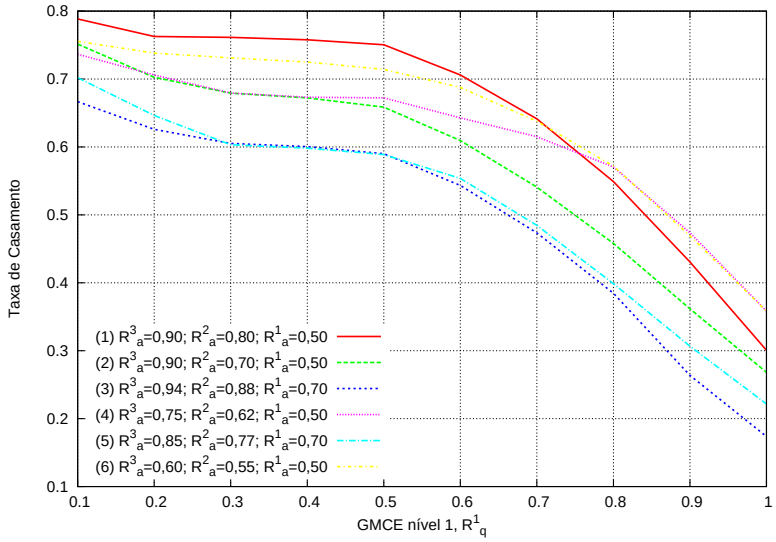


(a) Com menor visibilidade do nível 3

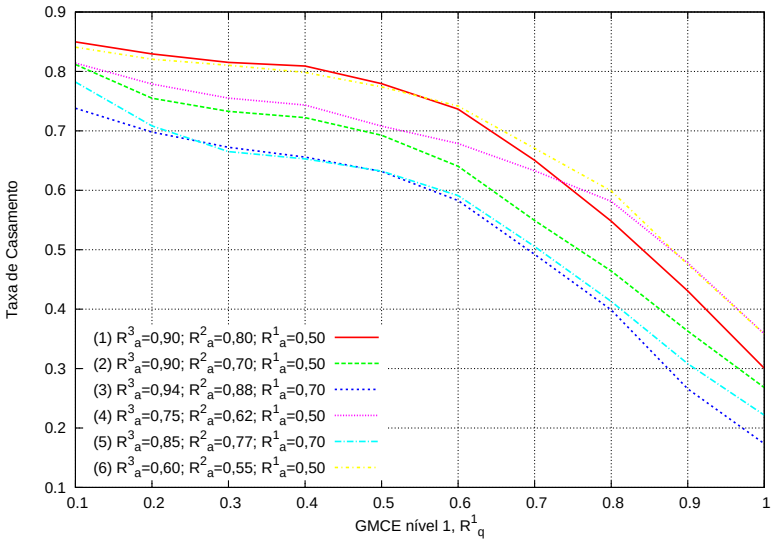


(b) Com maior visibilidade do nível 3

FIGURA 4.3 – Compromisso entre privacidade (nível 2) e eficácia na descoberta



(a) Com menor visibilidade do nível 3



(b) Com maior visibilidade do nível 3

FIGURA 4.4 – Compromisso entre privacidade (nível 1) e eficácia na descoberta – com pares ruins

4.2 e 4.3, porém resultantes de simulações com pares ruins na rede de confiança. Em geral, há uma diminuição de ambas as taxas relativas ao casamento, devido principalmente à redução do número de pares vizinhos a quem o cliente pode enviar suas consultas. Uma vez que pares maliciosos são detectados (através do gerenciamento de confiança), o controle de exposição se encarrega de excluí-los durante a propagação de anúncios e consultas. Na taxa de casamento efetivo, o impacto de pares maliciosos é maior, representando uma redução de 20% a 30% em todas as classes. A provável causa disso é o impacto no gerenciamento de confiança, pois sua eficácia depende do envio de recomendações entre pares, que serão mais limitadas devido ao maior controle de exposição no nível 3. Dessa forma, a probabilidade de obter opiniões sobre clientes é menor, o que influencia diretamente o controle de acesso utilizado pelo casamento *in-network*.

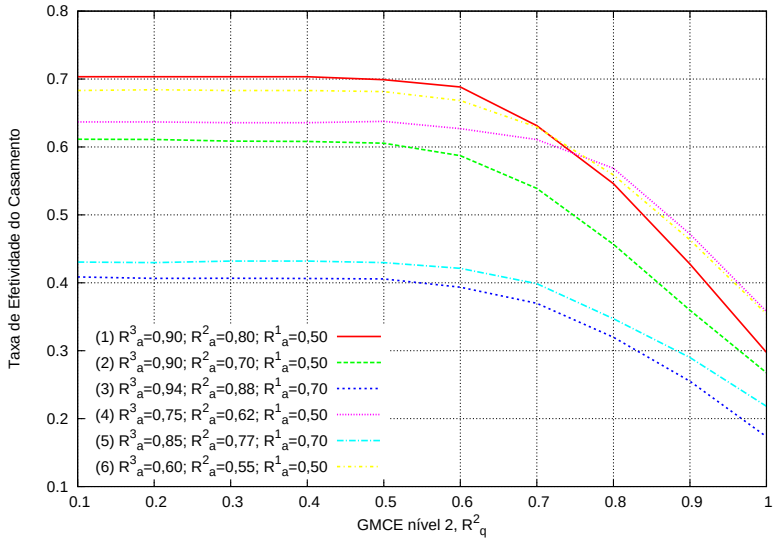
4.2.2 Visibilidade da informação x exposição

Os resultados da subseção anterior demonstraram os ganhos obtidos na descoberta de serviços com a maior exposição de informações sensíveis presentes nos anúncios e consultas. O objetivo desta subseção é mostrar o outro lado da descoberta, através do custo envolvido na exposição de informações de serviços, em termos do número de paresõ que tomam conhecimento sobre as mesmas por participar dos controles de exposição e de acesso. Essa métrica avalia exposição, quando deveria considerar privacidade para estudar o compromisso da mesma com colaboração. Por ora, privacidade é uma medida subjetiva, associada a cada indivíduo, logo é difícil ter uma métrica para avaliá-la. Por exemplo, um par pode considerar um nível de privacidade aceitável expor suas informações de serviço a um grande número de pares, porém limitar a poucos a associação com sua identidade forte. Além disso, o fato de pares serem confiáveis ou não também influencia na determinação do que pode ser exposto. Logo, a relação entre exposição e privacidade fica a cargo de cada par.

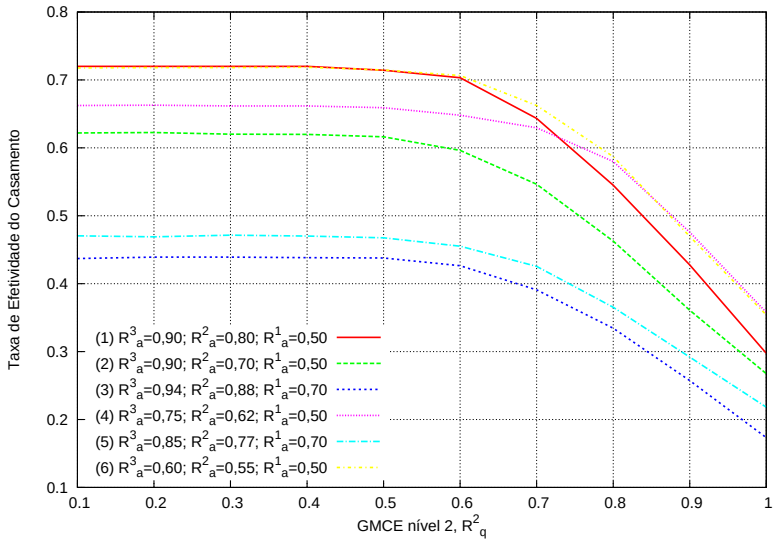
Neste trabalho, assume-se que quanto maior o número de pares que possuem a informação de serviço, e maior o nível de visibilidade da mesma, maior será a exposição de um par à rede. Os experimentos consideram apenas consultas enviadas por pares bons e a variação do nível de visibilidade 2 (R_q^2) para a obtenção dos resultados relativos à métrica. Mesmo assim, esses dados permitem fazer uma discussão paralela com os gráficos da subseção anterior.

A Figura 4.6 mostra os gráficos do cenário de exposição considerando pares bons (Figura 4.6(a)) e um misto de pares bons e ruins (Figura 4.6(b)). As duas primeiras curvas apresentam a média de pares que tomam conhecimento de consultas com nível de visibilidade 2, alternando R_q^3 entre as mesmas. As demais curvas, associadas ao nível 3, foram colocadas apenas como referência, pois não há uma variação de R_q^3 no gráfico para demonstrar seu impacto na métrica. Além disso, a exposição de consultas no nível 3 é limitada ao número de relações de confiança dos pares na rede, cuja média é 8 (conforme previamente comentado). A variação destas curvas a partir de $x = 0,7$ ocorre porque os valores de R_q^2 podem tornar-se maiores que R_q^3, o que não é um parâmetro válido do usuário.

É importante fazer um paralelo com os gráficos que demonstram a eficácia da descoberta em função de R_q^2. No cenário com pares bons, consultas com $R_q^1 = R_q^2 = 0,5$ e $R_q^3 = R_a^3$ produziram uma taxa de casamento efetivo entre 90% e 100% em provedores menos prudentes e entre 60% e 80% em provedores mais prudentes na

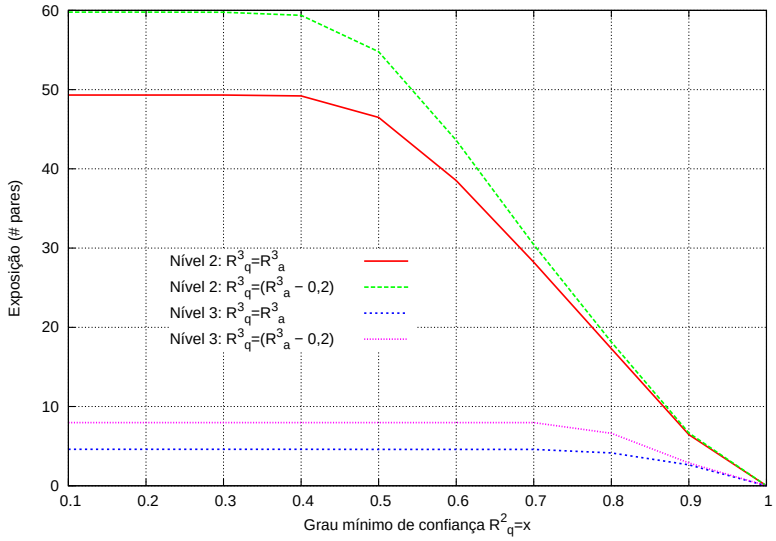


(a) Com menor visibilidade do nível 3

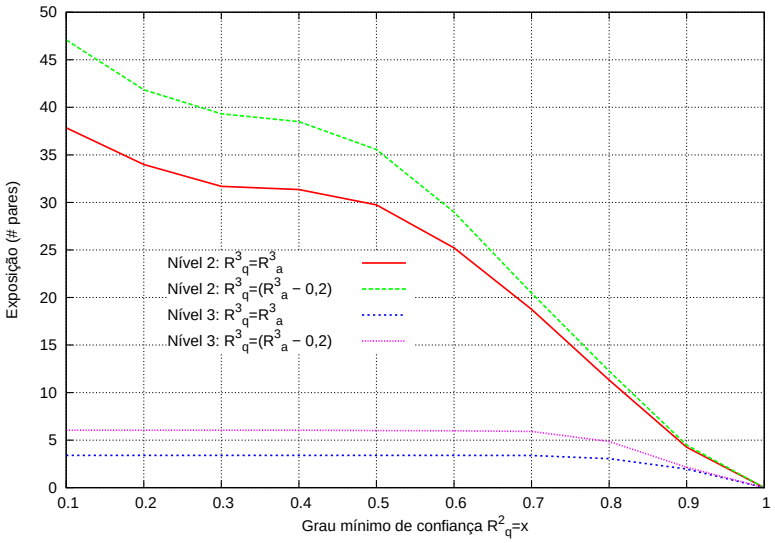


(b) Com maior visibilidade do nível 3

FIGURA 4.5 – Compromisso entre privacidade (nível 2) e eficácia na descoberta – com pares ruins



(a) Com pares bons apenas



(b) Com pares bons e ruins

FIGURA 4.6 – Exposição sob diferentes níveis de visibilidade das consultas

exposição de seus anúncios. Por outro lado, o custo associado com essa alta taxa de descoberta é uma maior exposição de nível 2, aproximadamente igual a 50% dos pares da rede, e 10% dos pares para o nível 3.

Com a existência de pares ruins, esse número cai aproximadamente 15%, o que corresponde ao número de pares ruins configurado na simulação. Experimentos adicionais mostraram que nenhuma consulta chega aos pares ruins, um resultado a ser destacado. Entretanto, tal resultado positivo depende de um gerenciamento de confiança eficaz, o que representa um (outro) desafio de pesquisa importante, e que (conforme previamente comentado) não foi tratado nesta dissertação. As distribuições utilizadas para gerar as opiniões entre os pares (Tabela 4.1) já assumem um gerenciamento de confiança eficaz pré-realizado *antes* do início das simulações.

4.3 Discussão

Os resultados desta avaliação permitiram "validar" os mecanismos de controle de exposição e de acesso, cujo principal propósito é refletir parâmetros de privacidade do usuário nas taxas de casamento e de sua efetividade. Foi possível demonstrar a influência de cada nível de visibilidade no compromisso entre colaboração e privacidade. O grau de privacidade foi limitado como sendo o grau de exposição de um par aos demais pares da rede. Resultados como a possibilidade de ter uma descoberta de serviços eficaz com pouca exposição da identidade física dos pares mostram que FSSD é adequado para muitos cenários de computação ubíqua que envolvem segurança e privacidade, já exemplificados na Seção 3.1.

Um ponto importante a considerar é o uso de um modelo "estático" de gerenciamento de confiança, no sentido que pares não obtêm opiniões baseadas em evidências diretas. O uso de tal modelo facilitou a interpretação dos resultados, pois as relações de confiança entre os pares possuíam um intervalo possível de valores e não mudava ao longo do tempo, o que permitia atribuir comportamentos do gráfico ao mecanismo de controle de exposição. Esse estudo seria mais complexo com relações de confiança dinâmicas. Por outro lado, admite-se que contemplar a dinâmica do gerenciamento de confiança nos experimentos forneceria resultados mais realistas.

Nesse contexto, um dos próximos passos neste trabalho é a definição de um modelo de simulação que permita capturar resultados para as métricas definidas considerando um gerenciamento de confiança de fato, com evidências diretas e recomendações. Além disso, o uso de modelos de ataques mais elaborados, como conluio, também são importantes para FSSD, pois permite validar seu controle de exposição frente a um número de pares não confiáveis. A avaliação de desempenho também é fundamental na computação ubíqua, pois existe um consenso na literatura e indústria que dispositivos ubíquos possuem recursos escassos de processamento e comunicação, o que requer o projeto de protocolos e aplicações eficientes.

Capítulo 5

Conclusões

Este trabalho apresentou FSSD, um protocolo para descoberta de serviços em ambientes ubíquos que possibilita a pares contornar a indisponibilidade de uma infra-estrutura de descoberta através da colaboração, ao mesmo tempo em que é guiado por um comprometimento com o grau de segurança e privacidade desejado pelo provedor ou cliente de um serviço. Os principais componentes do FSSD foram apresentados, que são o gerenciamento de confiança e os controles de exposição e de acesso, utilizados para viabilizar tal comprometimento. Até onde sabemos, não existe um sistema de descoberta de serviços que considera essas questões em seu projeto.

A avaliação preliminar do protocolo permitiu mostrar uma série de propriedades interessantes na descoberta de serviços, que formam o diferencial deste protocolo. Através destes experimentos, foi possível mostrar que é oportunístico aplicar um modelo flexível de descoberta de serviços considerando graus de colaboração, segurança e privacidade desejados, pois permite que o usuário os ajuste conforme sua necessidade e política de privacidade.

O uso do FSSD não é limitado a ambientes sem infra-estrutura de descoberta. Muitos ambientes ubíquos possuem a mesma, embora restrita a um número de usuários que pertencem a um domínio administrativo. Nesse contexto, FSSD pode ser combinado com a infra-estrutura existente de tal forma que usuários dentro do domínio possuem relações de confiança elevadas com os dispositivos controlados pelo domínio, enquanto usuários fora do mesmo possuem relações mais brandas. Dessa forma, é possível limitar o uso de certos dispositivos de acordo com o perfil de cada usuário que está inserido no ambiente.

Como trabalhos futuros, vislumbramos novas investigações com FSSD referentes principalmente à sua relação com a topologia física subjacente. É prevista também uma série de novos experimentos, para validar a relação dos mecanismos de controle de exposição e de acesso com o gerenciamento de confiança, bem como para avaliar o desempenho do protocolo em diferentes cenários de topologia física.

Bibliografia

[Ackerman and Mark, 2004] Ackerman and Mark (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal and Ubiquitous Computing*, 8(6):430–439.

[Ali et al., 2005] Ali, A. S., Ludwig, S. A., and Rana, O. F. (2005). A cognitive trust-based approach for web service discovery and selection. pages 12 pp.+.

[Almenárez and Campo, 2003] Almenárez, F. and Campo, C. (2003). Spdp: A secure service discovery protocol for ad-hoc networks. In *EUNICE 2003 9th Open European Summer School and IFIP Workshop on Next Generation Networks*, pages 213–218, Hungary, Budapest Balatonfred.

[Ashley et al., 2003] Ashley, P., Hada, S., Karjoth, G., Powers, C., and Schunter, M. (2003). Enterprise privacy authorization language (epal 1.2). Technical report, IBM.

[Buford et al., 2006] Buford, J., Celebi, E., and Frankl, P. (2006). Property-based peer trust in the sleeper service discovery protocol. In *COMPSAC '06: Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06)*, pages 209–214, Washington, DC, USA. IEEE Computer Society.

[Cahill et al., 2003] Cahill, V., Gray, E., Seigneur, J. M., Jensen, C. D., Chen, Y., Shand, B., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., Marzo, D., Bryce, C., Carbone, M., Krukow, K., and Nielson, M. (2003). Using trust for secure collaboration in uncertain environments. *Pervasive Computing, IEEE*, 2(3):52–61.

[Capkun et al., 2002] Capkun, S., Buttyan, L., and Hubaux, J.-P. (2002). Small worlds in security systems: an analysis of the pgp certificate graph. In *Proceedings of the ACM New Security Paradigms Workshop*.

[Capkun et al., 2006] Capkun, S., Hubaux, J. P., and Buttyan, L. (2006). Mobility helps peer-to-peer security. *IEEE Transactions on Mobile Computing*.

[Carminati et al., 2005] Carminati, B., Ferrari, E., and Hung, P. C. K. (2005). Exploring privacy issues in web services discovery/agencies. *Security & Privacy Magazine, IEEE*, 3(5):14–21.

[Chakraborty et al., 2006] Chakraborty, D., Joshi, A., Yesha, Y., and Finin, T. (2006). Toward distributed service discovery in pervasive computing environments. *Mobile Computing, IEEE Transactions on*, 5(2):97–112.

[Clarke, 2006] Clarke, R. (2006). Introduction to dataveillance and information privacy, and definitions of terms.

[Czerwinski et al., 1999] Czerwinski, S. E., Zhao, B. Y., Hodes, T. D., Joseph, A. D., and Katz, R. H. (1999). An architecture for a secure service discovery service. In *Mobile Computing and Networking*, pages 24–35.

[Edwards, 2006] Edwards, W. K. (2006). Discovery systems in ubiquitous computing. *Pervasive Computing, IEEE*, 5(2):70–77.

[Feldman et al., 2004] Feldman, M., Lai, K., Stoica, I., and Chuang, J. (2004). Robust incentive techniques for peer-to-peer networks. In *EC '04: Proceedings of the 5th ACM conference on Electronic commerceACM Press*, pages 102–111. ACM Press.

[Hansen et al., 2006] Hansen, T. R., Bardram, J. E., and Soegaard, M. (2006). Moving out of the lab: Deploying pervasive technologies in a hospital. *Pervasive Computing, IEEE*, 5(3):24–31.

[Helal et al., 2003] Helal, S., Desai, N., Verma, V., and Lee, C. (2003). Konark - a service discovery and delivery protocol for ad-hoc networks. volume 3, pages 2107–2113 vol.3.

[Herrmann et al., 2005] Herrmann, K., Muhl, G., and Jaeger, M. (2005). A self-organizing lookup service for dynamic ambient services. pages 707–716.

[Jösang et al., 2006] Jösang, A., Hayward, R., and Pope, S. (2006). Trust network analysis with subjective logic. In *ACSC '06: Proceedings of the 29th Australasian Computer Science Conference*, pages 85–94, Darlinghurst, Australia, Australia. Australian Computer Society, Inc.

[Jösang et al., 2007] Jösang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, 43(2):618–644.

[Kindberg and Fox, 2002] Kindberg, T. and Fox, A. (2002). System software for ubiquitous computing. *IEEE Pervasive Computing*, 1(1):70–81.

[Langheinrich, 2001] Langheinrich, M. (2001). Privacy by design – principles of privacy-aware ubiquitous systems. In Abowd, G. D., Brumitt, B., and Shafer, S., editors, *Ubicomp 2001 Proceedings*, volume 2201 of *Lecture Notes in Computer Science*, pages 273–291. Springer.

[Lenders et al., 2005] Lenders, V., May, M., and Plattner, B. (2005). Service discovery in mobile ad hoc networks: a field theoretic approach. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 120–130.

[Lima et al., 2007] Lima, L. S., Gomes, A. T. A., Ziviani, A., and Endler, M. (2007). Descoberta de serviços em redes de computadores (minicurso). *XXV Simpósio Brasileiro de Redes de Computadores*.

[Marin-Perianu et al., 2005] Marin-Perianu, R., Hartel, P., and Scholten, H. (2005). A classification of service discovery protocols. Technical Report TR-CTIT-05-25, Centre for Telematics and Information Technology, University of Twente, Enschede.

[Marti and Garcia-Molina, 2006] Marti, S. and Garcia-Molina, H. (2006). Taxonomy of trust: Categorizing p2p reputation systems. *Computer Networks*, 50(4):472–484.

[Mian et al., 2006] Mian, A. N., Beraldi, R., and Baldoni, R. (2006). Survey of service discovery protocols in mobile ad hoc networks. Technical report, Dipartimento di Informatica e Sistemistica "Antonio Ruberti", Università degli Studi di Roma "La Sapienza", Rome, Italy.

[Mtibaa et al., 2007] Mtibaa, A., Chaintreau, A., and Massoulie (2007). Diameter of opportunistic mobile networks. In *ACM SIGCOMM CoNext 07*.

[Muhammad and Barcellos, 2002] Muhammad, H. H. and Barcellos, M. P. (2002). Simulation group communication protocols through an object-oriented framework. In Sc, S., editor, *35th Annual Simulation Symposium, ANSS 2001*, volume 1, San Diego, USA. SCS.

[Oasi, 2005] Oasi, S. (2005). extensible access control markup language (xacml) version 2.0. Technical report.

[Ratsimor et al., 2004] Ratsimor, O., Chakraborty, D., Joshi, A., Finin, T., and Yesha, Y. (2004). Service discovery in agent-based pervasive computing environments. *Mob. Netw. Appl.*, 9(6):679–692.

[Sackmann et al., 2006] Sackmann, S., Strüker, J., and Accorsi, R. (2006). Personalization in privacy-aware highly dynamic systems. *Commun. ACM*, 49(9):32–38.

[Satyanarayanan, 2001] Satyanarayanan, M. (2001). Pervasive computing: vision and challenges. *Personal Communications, IEEE [see also IEEE Wireless Communications]*, 8(4):10–17.

[Singh and Liu, 2003] Singh, A. and Liu, L. (2003). Trustme: anonymous management of trust relationships in decentralized p2p systems. In *Peer-to-Peer Computing, 2003. (P2P 2003). Proceedings. Third International Conference on*, pages 142–149.

[Stajano and Anderson, 1999] Stajano, F. and Anderson, R. (1999). The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Security Protocols, 7th International Workshop Proceedings*, pages 172–194.

[Stallings, 2005] Stallings, W. (2005). *Cryptography and Network Security: Principles and Practices*. Prentice Hall, fourth edition.

[Theodorakopoulos and Baras, 2006] Theodorakopoulos, G. and Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):318–328.

[Trabelsi et al., 2006] Trabelsi, S., Pazzaglia, J.-C., and Roudier, Y. (2006). Secure web service discovery: Overcoming challenges of ubiquitous computing. In *ECOWS '06: Proceedings of the European Conference on Web Services*, pages 35–43, Washington, DC, USA. IEEE Computer Society.

[Varshavsky et al., 2005] Varshavsky, A., Reid, B., and de Lara, E. (2005). A cross-layer approach to service discovery and selection in manets. pages 8 pp.+.

[W3, 2006] W3, C. (2006). The platform for privacy preferences 1.1 (p3p1.1) specification. Technical report.

[Weiser, 1991] Weiser, M. (1991). The computer for the 21st century. *Scientific American*.

[Wishart et al., 2005] Wishart, R., Robinson, R., Indulska, J., and Jøsang, A. (2005). Superstringrep: reputation-enhanced service discovery. In *CRPIT '38: Proceedings of the Twenty-eighth Australasian conference on Computer Science*, pages 49–57, Darlinghurst, Australia, Australia. Australian Computer Society, Inc.

[Zhu et al., 2005a] Zhu, F., Mutka, M. W., and Ni, L. M. (2005a). Service discovery in pervasive computing environments. *Pervasive Computing, IEEE*, 4(4):81–90.

[Zhu et al., 2006] Zhu, F., Mutka, M. W., and Ni, L. M. (2006). A private, secure, and user-centric information exposure model for service discovery protocols. *Mobile Computing, IEEE Transactions on*, 5(4):418–429.

[Zhu et al., 2005b] Zhu, F., Zhu, W., Mutka, M. W., and Ni, L. (2005b). Expose or not? a progressive exposure approach for service discovery in pervasive computing environments. In *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, pages 225–234, Washington, DC, USA. IEEE Computer Society.