Flexibilizando Graus de Colaboração, Segurança e Privacidade na Descoberta de Serviços em Ambientes Ubíquos

Eduardo Moschetta[1], **Marinho P. Barcellos**[2]
Rodolfo Stoffel Antunes[1], **Giovani Facchini**[1]

[1]UNISINOS – Universidade do Vale do Rio dos Sinos
Av. Unisinos, 950 – São Leopoldo, RS – CEP 93.022-000

[2]PUCRS – Pontifícia Universidade Católica do Rio Grande do Sul
Av. Ipiranga, 6681, Prédio 32 – Porto Alegre, RS – CEP 90.619-900

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 system security and privacy levels in order to demonstrate that the proposed approach properly addresses the tradeoff regarding peer collaboration.*

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 utiliza 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.*

1. Introdução

A descoberta de serviços é um recurso importante para sistemas distribuídos, pois elimina a fase de configuração explícita de serviços da rede. No contexto da computação ubíqua, sua aplicação é fundamental, por viabilizar a integração entre dispositivos do ambiente e tornar as interações mais espontâneas [8]. Um dos grandes desafios nestes ambientes é como obter propriedades desejáveis de uma infra-estrutura para descoberta de serviços – como escalabilidade, segurança, fácil administração, etc. – sem muitas vezes haver a infra-estrutura de rede e de segurança propriamente dita [6] (*firewall*, autoridade certificadora, etc).

Nesse contexto, é importante que pares colaborem nas tarefas de anúncio e descoberta de serviços para contornar a limitação da infra-estrutura. Entretanto, esse tipo de colaboração insere problemas de segurança e privacidade para os pares. Em ambientes ubíquos, por exemplo, não é possível assumir que pares conheçam recursos legítimos, nem mesmo que possuam acesso a um servidor de autenticação para avaliar sua legitimidade. Além disso, a troca de mensagens de anúncio e descoberta de serviços implica a exposição de informações sensíveis como identidade, perfil do par, etc. Na ausência de segurança e privacidade, pares podem limitar a sua predisposição a colaborar, comprometendo assim o desempenho da descoberta de serviços no ambiente.

Os trabalhos existentes na área de descoberta de serviços, tais como [4], [9], [1] e [18], não consideram no projeto de seus sistemas essa relação de compromisso (*tradeoff*) entre colaboração, segurança e privacidade. A principal contribuição deste trabalho é o projeto do FSSD (*Flexible Secure Service Discovery*), um protocolo de **descoberta de serviços flexível** para ambientes ubíquos. Sua principal característica é permitir que pares sempre colaborem, porém ajustando o nível de exposição para suas informações sensíveis. Redes de confiança são utilizadas em substituição à infra-estrutura fixa de segurança, e mecanismos para controle de exposição são empregados como uma política de privacidade do usuário que está anunciando ou buscando serviços.

O restante deste trabalho encontra-se organizado como segue. A Seção 2 aborda brevemente os trabalhos relacionados na área de descoberta de serviços. A Seção 3 define o problema tratado e os princípios que guiaram o projeto do FSSD, enquanto uma visão geral do protocolo e sua formalização são apresentadas nas Seções 4 e 5, respectivamente. A Seção 6 apresenta uma avaliação do protocolo, discutindo os principais resultados encontrados. A Seção 7 apresenta considerações finais e uma agenda para trabalhos futuros.

2. Trabalhos Relacionados

Segundo [17], há uma gama de trabalhos que se concentram em resolver os problemas ligados à descoberta de serviços. O estudo em [10] apresenta vários destes trabalhos, categorizando-os principalmente quanto ao tipo de rede em que foram projetados: redes fixas, redes móveis *ad hoc* de um salto ou de múltiplos saltos (MANETs). Os trabalhos relacionados a FSSD são principalmente aqueles que abordam questões de segurança e privacidade, bem como aqueles que utilizam a colaboração entre pares na descoberta de serviços para contornar a ausência de infra-estrutura de rede. Esta seção apresenta brevemente alguns desses trabalhos.

Os protocolos apresentados em [4] e [9] enfatizam a colaboração entre os pares em MANETs e não possuem mecanismos de segurança e privacidade. No primeiro trabalho, é proposto um protocolo de descoberta de serviços com encaminhamento seletivo baseado em grupos de serviços. A descrição de serviços em grupos viabiliza, entre outros aspectos, uma tabela de encaminhamento escalável e um casamento de serviços aproximado. O segundo trabalho propõe um modelo de descoberta baseado na física eletro-estática, onde a busca (carga negativa) vai ao encontro do serviço (carga positiva) utilizando como parâmetros de escolha do serviço que será mostrado ao cliente a distância em saltos e a capacidade do servidor (CoS).

Os protocolos apresentados em [5], [1] e [16] empregam mecanismos de segurança na descoberta de serviços. O primeiro trabalho introduz o Ninja SDS, um protocolo para redes com infra-estrutura fixa, adequado para redes com controle administrativo forte. Ninja SDS utiliza três unidades centrais para prover segurança na descoberta, incluindo autorização e autenticação. Certificados e listas de controle de acesso são utilizados para autenticar clientes e verificar se os mesmos podem acessar uma informação de serviço, respectivamente. Em contraste, o segundo trabalho apresenta uma solução para MANETS utilizando modelos anárquicos de confiança com certificados digitais. O terceiro trabalho segue a linha do segundo, apresentando um protocolo que utiliza sistemas de reputação para manter, de forma distribuída, qual a reputação de um serviço.

O trabalho de Zhu [19] enfatiza uma abordagem para proteger a privacidade dos usuários e provedores. Nesse esquema, usuários e serviços se expõem progressivamente através de uma troca de mensagens compostas por filtros Bloom, utilizados para expor sumários de domínios e serviços procurados. Somente usuários destes domínios e

serviços poderão decodificar a mensagem e descobrir que o requisitante está pedindo seus serviços, satisfazendo assim critérios de privacidade. A exposição progressiva agrupa sumários de domínios e serviços procurados em um único sumário, e expõe parcelas deste interativamente até que seja detectado um par que satisfaça os critérios de domínio e serviços procurados, ou então a interação é abortada quando tais critérios não são detectados, impedindo assim a exposição do requisitante.

Como será explicado posteriormente, colaboração, segurança e privacidade são aspectos conflitantes em ambientes sem garantias de infra-estrutura fixa de rede e segurança. Nesse contexto, FSSD se diferencia dos demais trabalhos por oferecer um modelo flexível de descoberta de serviços, onde provedores e clientes podem ajustar o grau destes aspectos em tempo de execução, de acordo com suas necessidades. É importante ressaltar também que a segurança e privacidade são garantidas também na etapa de descoberta, ao contrário de protocolos como [1] e [16], que rodam sobre ambientes sem infra-estrutura de rede e segurança, porém utilizam mecanismos de segurança apenas para a seleção dos serviços descobertos.

3. Princípios de Projeto

No contexto de descoberta de serviços, o problema que este trabalho estuda é o compromisso entre a colaboração, segurança e privacidade. Esse compromisso é relevante em ambientes ubíquos onde a colaboração entre pares é necessária para contornar a limitação da infra-estrutura de rede e segurança, ao mesmo tempo em que a segurança e privacidade agem em detrimento da colaboração. Esse problema é definido em detalhes na Seção 3.1. A Seção 3.2 apresenta o modelo flexível de descoberta de serviços proposto pelo FSSD.

3.1. Compromisso entre Colaboração, Segurança e Privacidade

A descoberta de serviços é uma tarefa desempenhada de forma colaborativa entre pares de um ambiente ubíquo. Entretanto, é possível que existam pares mal-intencionados que buscam comprometer o funcionamento do sistema de descoberta de serviços. Além disso, o nível de incerteza nesses ambientes reduz o nível de segurança que anunciantes e clientes de serviços possuem no momento de interagirem. Conseqüentemente, isso também aumenta os riscos para a privacidade do usuário, haja visto que a colaboração na descoberta envolve informações sensíveis como identidade, perfil do usuário, entre outros [17]. Nesse contexto, é importante que a descoberta de serviços seja realizada de forma segura e prudente.

A presença de uma infra-estrutura fixa de rede e segurança no ambiente facilita a obtenção de segurança e privacidade, pois oferece recursos para a implantação de um *firewall*, acesso a autoridades certificadoras, entre outros mecanismos. Entretanto, essa premissa não é válida em computação ubíqua por duas razões: ou a infra-estrutura é inexistente ou a mesma é restrita a um conjunto de pares, sendo delimitada por um domínio administrativo. Logo, assumir uma infra-estrutura de segurança irá limitar a colaboração entre os pares da rede. Caso um gerenciamento de confiança descentralizado (tal como [7]) seja utilizado no sistema, o nível de colaboração pode ser proporcional ao nível de confiança que um par possui no outro. Em ambos os cenários, é possível observar a escolha ou 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 de informações de serviço tende a melhorar o desempenho da descoberta, porém

diminui a privacidade do usuário. O segundo compromisso corresponde à escolha entre **segurança e privacidade**, onde se define que tipo de informações são expostas para permitir a implantação de mecanismos de segurança. Expor informações como identidade, por exemplo [11], permite criar mecanismos de gerenciamento de confiança; em contrapartida, isso possibilita também que pares consigam associar um serviço ao seu dono, o que pode levar à perda de privacidade.

3.2. Modelo flexível de descoberta de serviços

Através de um modelo flexível de descoberta de serviços, provedores e clientes podem ajustar o grau de colaboração em função dos graus de segurança e privacidade exigidos para determinado serviço ou consulta. Basicamente, a idéia é: quanto maior o grau de segurança e privacidade exigido para determinado anúncio/consulta, menor será a exposição deste para os pares da rede e, conseqüentemente, menor será a colaboração do provedor/cliente para o sistema de descoberta. Essa flexibilidade é oferecida ao usuário através de um conjunto de parâmetros, que permitem também a escolha entre segurança e privacidade. O restante desta seção aborda os princípios de projeto definidos para o correto funcionamento desse modelo.

A comunicação entre pares, seja no envio de anúncios e consultas, seja no repasse dessas informações, deve ser realizada de forma segura mas sem depender de uma infraestrutura fixa de segurança. Isso é obtido com o uso de redes de confiança, onde pares se comunicam com seus vizinhos através de canais criptografados assimétricos. Portanto, a rede de confiança limita o fluxo possível de mensagens do FSSD na rede física subjacente. Cada canal é uma relação de confiança estabelecida entre dois pares, seguida de uma troca de chaves públicas entre os mesmos a fim de estabelecer o canal seguro. Assume-se que a distribuição de chaves públicas entre pares seja feita de maneira segura, através de estratégias como contato físico [14] ou contato visual [2].

Como mencionado anteriormente, o gerenciamento de confiança implica a exposição da identidade de cada par, levando à perda de privacidade do mesmo. Nesse contexto, o modelo de descoberta faz uso de duas identidade por par: uma **identidade forte**, para uso em transações seguras entre os pares e uma **identidade fraca**, para fins de gerenciamento de confiança. A primeira é um identificador persistente (endereço MAC), e portanto mais sensível na exposição.

Quanto maiores os riscos envolvidos no processo de descoberta, menor deve ser a exposição de informações sensíveis por um par. Nesse contexto, o presente modelo prevê diferentes níveis de visibilidade para um anúncio ou consulta de serviço. À medida que um anúncio/consulta é propagado pela rede de confiança, partes mais sensíveis dessa informação vão sendo suprimidas, pois os riscos à privacidade com sua exposição aumentam. Os riscos são maiores devido à **transitividade** das relações de confiança. Se Bráulio confia em Ana, que confia em Carlos, certamente o risco para Bráulio envolvido na exposição do anúncio do serviço a Carlos é maior do que à Ana. Quanto mais estreitas forem as relações de confianças, sejam diretas ou transitivas, maior será a visibilidade da informação ao longo do canal de propagação.

Por fim, é necessário evitar a exposição prematura de provedores e clientes até o momento em que o casamento é confirmado e ambas as partes desejam interagir. Para tanto, o modelo prevê dois tipos de casamento: local, realizado pelo provedor ou cliente; e *in-network*, feito por um par intermediário aos mesmos. No casamento local, uma das partes se expõe à outra de acordo com seu grau de risco aceitável. Já o casamento *in-network* possui uma etapa de autorização, onde o par intermediário verifica as **credenciais**

impostas no anúncio e na consulta, para então autorizar o casamento e notificar o provedor e o cliente. Por exemplo, se o anúncio do serviço de Bráulio não chegou a Carlos, e a consulta de Carlos àquele serviço não chegou a Bráulio, significa que estas informações não são visíveis aos mesmos. Entretanto, Ana recebeu ambas as informações, e pode autorizar o casamento caso Bráulio satisfaça as credenciais da consulta e Carlos satisfaça as credenciais do anúncio.

Cenários-alvos deste protocolo incluem ambientes ubíquos cuja infra-estrutura de rede e segurança é restrita a certos pares ou inexistente. Pares participam de uma sistema seguro de descoberta de serviços que contorna essas limitações do ambiente. Por exemplo, se Bráulio entra em um hospital, provavelmente ele não deseja expor os serviços que está procurando a todos os presentes. Quando Bráulio vai consultar seu laboratório de confiança, só deseja expor suas consultas a usuários daquele laboratório. No outro lado, a doutora Ana expõe a maioria dos seus serviços para médicos e funcionários do hospital, porém alguns outros poucos são expostos apenas às suas colegas de laboratório. Nesse sentido, a capacidade de ajustar os níveis de segurança e privacidade torna a colaboração mais atraente.

4. Visão Geral do Protocolo

FSSD é um protocolo de descoberta no nível de aplicação, sendo independente da rede física subjacente e dos protocolos de roteamento utilizados. A arquitetura do FSSD é constituída de três componentes principais: **gerenciamento de confiança**, responsável em coletar, distribuir e computar opiniões sobre pares da rede (como será explicado posteriormente, uma opinião é uma tupla confiança/certeza); **controle de exposição**, que controla a visibilidade de um anúncio ou consulta ao longo de sua propagação pela rede de confiança; e **mecanismo de casamento**, que suporta o casamento entre anúncios e consultas de forma local ou *in-network*.

Anúncios e consultas de serviços são doravante chamadas de **informações de serviço**, apresentando uma estrutura similar com os seguintes campos: identidade forte do provedor ou cliente, identidade fraca, descrição da informação de serviço, credencial de acesso e opinião sobre a informação de serviço. Os três primeiros são oferecidos por FSSD para prover diferentes **níveis de visibilidade**: no nível 3, todos os campos são expostos; no nível 2, a identidade forte é suprimida; e no nível 1, ambas as identidades são suprimidas. Os outros dois campos são utilizados para o casamento *in-network*, a ser descrito mais adiante.

O controle de exposição visa diminuir a visibilidade de um anúncio/consulta (informação de serviço) à medida que é propagado pela rede. Para tanto, ele depende de um parâmetro configurado pelo usuário, o **Grau Mínimo de Confiança para Exposição** (GMCE), que deve ser configurado para cada nível de visibilidade e pode ser diferente para cada anúncio e consulta, dependendo do risco que estes representam para seus usuários. O GMCE é utilizado para verificar se o provedor/cliente possui um grau de confiança mínimo com o próximo par na propagação do anúncio/consulta; esse grau de confiança pode ser direto ou transitivo. Caso não possua, campos são suprimidos e a informação de serviço é passada com o maior nível de visibilidade cujo GMCE é satisfeito pelo grau de confiança do provedor/cliente com o próximo par.

No casamento *in-network*, o anúncio/consulta recebido é casado com uma consulta/anúncio de outro par, armazenada em seu repositório local. Esse casamento é atrelado a um mecanismo de autorização, que verifica se as credenciais impostas no anúncio são atendidas pelo cliente e vice-versa. Caso positivo, uma mensagem de resposta

ao casamento é enviada ao provedor e cliente através de um mecanismo de *backtracing* (Seção 5.3). Esse mecanismo é necessário pois o par intermediário pode não possuir uma relação de confiança com provedor/cliente para enviar a mensagem de forma segura. A mensagem indica ao cliente que o casamento foi autorizado e contém informações para o mesmo contatar o provedor, incluindo uma chave pública e um identificador de grupo, para enviar a requisição de serviço ao provedor de forma multicast. Logo, a identidade do provedor não é exposta até o momento em que o mesmo aceitar a requisição do cliente.

O conteúdo das mensagens de anúncio e de consulta é formado da seguinte maneira: informação de serviço (com os campos pertinentes ao nível de visibilidade corrente); o GMCE para cada nível de visibilidade; e um rastro da mensagem de tamanho fixo, utilizado para evitar ciclos na propagação, limitar o número de saltos na propagação (no sentido de que um rastro cheio indica que o número máximo de saltos foi atingido) e *backtracing*. Um quarto tipo de mensagem, ainda não comentado, é a **recomendação**, utilizada para o gerenciamento de confiança. Visto que ela também é sujeita ao controle de exposição, seu conteúdo é similar ao da mensagem de anúncio/consulta, trocando-se a informação de serviço pela recomendação.

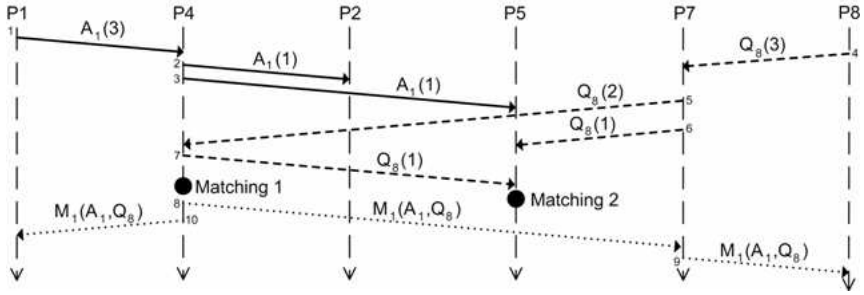

Figura 1. Diagrama de tempo

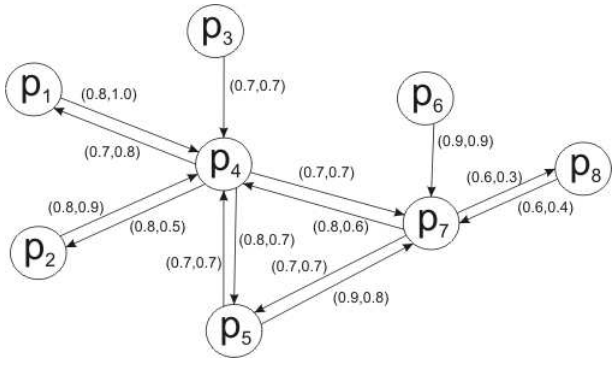

Figura 2. Exemplo de rede de confiança

O diagrama da Figura 1 ilustra o controle de exposição e o casamento *in-network* para um anúncio e uma consulta, onde nota-se três tipos de mensagens: consultas, anúncios e respostas ao casamento, representados respectivamente por Q, A e M. A rede de confiança utilizada no exemplo pode ser visualizada na Figura 2; conforme será explicado na seção seguinte, os pesos nas arestas representam confiança e certeza. p_1 e p_8 são provedor e cliente, respectivamente. É importante reforçar que essa rede não tem associação com a topologia física subjacente. A troca de mensagens ilustrada é descrita 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*.

5. Formalização do Protocolo

A rede de confiança considerada em FSSD é um grafo direcionado, onde vértices são usuários/dispositivos da rede e um arco ponderado de i para j corresponde à opinião do par p_i sobre o par p_j, definida como $L(i, j)$. Uma opinião consiste de dois números: a confiança t_{ij} (*trust*), tal como uma estimativa baseada em evidências locais ou recomendações de outros pares; e a certeza c_{ij} (*confidence*), ou exatidão, sobre t_{ij}. Ambos os números podem assumir um valor no intervalo $[0, 1]$. Além da opinião $L(i, j)$, p_i deve ter também a chave pública de p_j para poder transmitir algo ao mesmo; essa chave é representada por $PK(i, j)$.

Este modelo de confiança é semelhante ao proposto em [15], 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. Uma opinião transitiva é calculada usando operadores de concatenação e consenso; um exemplo de implementação destes é descrito na referência citada. 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 $L^1(i, k)$ e $L^2(i, k)$ opiniões de p_i sobre p_k, adquiridas através de diferentes pares intermediários, temos $L(i, k) = L^1(i, k) \oplus L^2(i, k)$. Ambos os operadores são associativos e comutativos, sendo que $\oplus$ é distribuído sobre $\otimes$.

No controle de exposição, os parâmetros de GMCE para o nível de visibilidade $v = 1, 2, 3$, definidos para a informação de serviço (anúncio/consulta) ou recomendação x, são representados através de $GMCE_x^v$. $GMCE_x^v = (t_{min}, c_{min})$ define os valores de confiança e certeza necessários. Considerando que o par p_i deseja enviar um anúncio x a p_k; este é apto a receber o anúncio no nível de visibilidade v se e somente $\exists PK(k, i)$ e $L(i, k) \geq GMCE_x^v$, ou $t_{ij} \geq t_{min} \wedge c_{ij} \geq c_{min}$. Se p_k deseja propagar x para p_j, teríamos a condição $L(i, j) \geq GMCE_x^v$, onde $L(i, j)$ é uma opinião transitiva.

Tabela 1. Tabela de símbolos

$L(i, j)$: opinião de p_i sobre p_j	t_{ij} e c_{ij}: confiança e certeza de p_i sobre p_j
v: nível de visibilidade	x: informação de serviço ou recomendação
$GMCE_x^v$: GMCE do nível de visibilidade v para x	t_{min} e c_{min}: confiança e certeza mínima necessária
$\otimes$ e $\oplus$: operadores de concatenação e consenso	$PK(i, j)$: chave pública de p_j publicada a p_i

5.1. Gerenciamento de confiança

Os mecanismos de controle de exposição e casamento propostos pelo FSSD dependem do gerenciamento de confiança. Integrar o gerenciamento de confiança ao protocolo em vez de utilizar um mecanismo ortogonal é uma escolha de projeto, que traz como benefício a

possibilidade de submeter recomendações de outros pares ao mecanismo de controle de exposição. Com o gerenciamento de confiança integrado, FSSD garante que informações sensíveis, como a identidade fraca, não estarão sendo expostas a pares quaisquer por mecanismos ortogonais. Embora tenha seu próprio gerenciamento de confiança, FSSD emprega algoritmos conhecidos da literatura.

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 evidências seja menos sujeita a falsas acusações e, portanto, mais exata. Quando a opinião sobre um par está presente em ambas as tabelas, a opinião consolidada é calculada da seguinte forma: $L(i,k) = L^l(i,k) \times W^l + L^r(i,k) \times W^r$, 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. Deve-se ter $W^l + W^r = 1$ e $W_l \geq W_r$.

5.2. Controle de exposição

O Algoritmo 1 apresenta o algoritmo de controle de exposição empregado por p_c, que recebeu x e deve decidir se propaga a mesma, baseando-se nos valores $GMCE_x^v$ definidos por p_i (provedor, cliente ou par que enviou uma recomendação). Se pares não possuem um grau mínimo de confiança para receber informações sensíveis, campos devem ser suprimidos (linhas 4 e 7) ou a informação não deve ser mais propagada (linha 10). O algoritmo para o envio inicial de um anúncio ou consulta, assumindo de p_c para p_j, é mais simples: ele consiste da linhas 2 do algoritmo. Caso a condição falhe, a informação de serviço não é enviada a p_j.

Algorithm 1 Par p_c decide se propaga x para $\forall p_j : \exists(L(i,j) \wedge PK(i,j))$

1: $p_s \leftarrow$ par que enviou x {não necessariamente p_i}
2: $msg \leftarrow$ mensagem que carrega x
3: **if** $msg.identidadeForte$ é visível $\wedge\ msg.GMCE^3 > L(c,j)$ **then**
4: Suprime identidade forte
5: **end if**
6: **if** $msg.identidadeFraca$ é visível $\wedge\ msg.GMCE^2 > L(c,j)$ **then**
7: Suprime identidade fraca
8: **end if**
9: **if** $msg.GMCE^1 > L(c,j)$ **then**
10: Descarta propagação
11: **end if**
12: msg.opInfo $= msg$.opInfo $\otimes L(c,s)$
13: $msg.GMCE^v = msg.GMCE^v / L(c,j)$ para $v = 1,2,3$

Além da decisão de propagar ou não, o algoritmo atualiza dois campos importantes na mensagem a cada novo salto de propagação: a opinião sobre a informação de serviço ou recomendação recebida (linha 12), que representa a opinião transitiva do canal por onde a mensagem foi propagada, e o GMCE (linha 13) definido por p_i. Tendo em vista aumentar a exatidão da opinião sobre x, emprega-se o operador $\oplus$ para combinar a opinião sobre x com base em várias cópias do mesmo recebidas via canais alternativos. A fórmula utilizada para atualizar $GMCE$ corresponde ao inverso do operador $\otimes$: conforme x é propagada, o valor de GMCE aumenta (ou seja, fica mais restrito). O efeito é o

mesmo de se incluir na mensagem o valor de $GMCE_x^v$ original e $L(i, c)$, para o próximo par definir se pode propagar a informação. Entretanto, expor $L(i, c)$ em cada mensagem é uma perda de privacidade desnecessária, pois permite pares saberem o quanto outros confiam neles.

5.3. Casamento *in-network*

Sendo x_i^a o anúncio do provedor p_i e x_j^q a consulta do cliente p_j ao serviço anunciado por p_i, um par intermediário p_c que recebe ambos vai autorizar p_j a receber o anúncio de p_i somente se: a identidade fraca de p_j esteja exposta (x_j^q.idFraca); a opinião sobre a consulta 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.

A Figura 3 ilustra diferentes cenários de autorização. Abaixo de cada cenário estão os elementos envolvidos no controle de acesso para cada par. No cenário A, não há casamento. No cenário B, o casamento *in-network* ocorre, porém 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 que m verifique, em nome do cliente, se p é credenciado a prover tal serviço. Apesar da situação desigual, fica a cargo do cliente decidir se inicia uma requisição a p. No cenário D, a autorização não é necessária, pois ambos expõem a informação de serviço um ao outro.

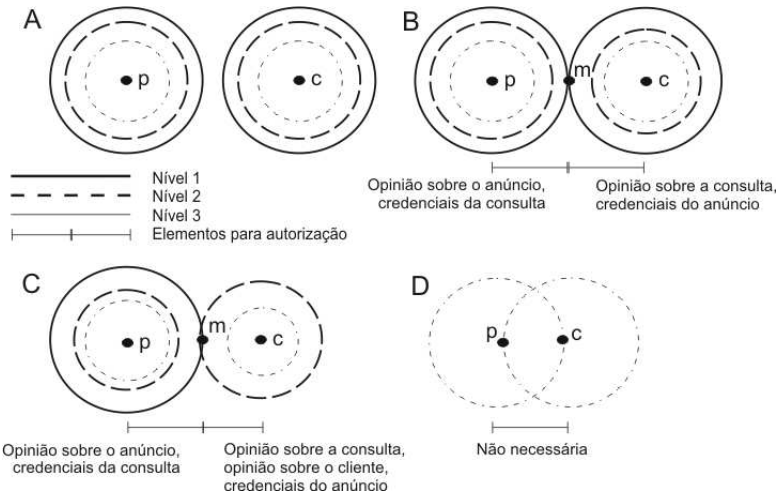

Figura 3. Cenários de controle de exposição, casamento e autorização

Por fim, é importante notar que respostas ao casamento são enviadas sem expor as identidades do provedor e do cliente, 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 iniciar a propagação da resposta pelo caminho inverso, criptografando a resposta com a chave pública da informação de serviço (presente na descrição); logo, só o cliente e provedor podem decodificar a resposta. Dessa forma, tal mecanismo satisfaz os requisitos de anonimidade do cliente e provedor.

6. Avaliação do protocolo

Um protótipo do protocolo proposto foi implementado e então avaliado usando o simulador de protocolos de rede Simmcast [13], com foco nas características do controle de exposição e do casamento *in-network*. A Seção 6.1 descreve o modelo de simulação, incluindo parâmetros, cenários e métricas utilizadas. Os principais resultados encontrados são discutidos na Seção 6.2.

6.1. Modelo de 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 [12] 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 [3] foi utilizado para gerar cenários com 100 pares. 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 uma distribuição uniforme com valores no intervalo $[0,7; 1,0]$, e se mantêm estáticos ao longo da simulação. Nesse contexto, assume-se um gerenciamento de confiança eficaz, com uma etapa de convergência nos valores de confiança, e foca-se a avaliação nos demais componentes de FSSD, que são controle de exposição e casamento *in-network*. O valor de certeza (c_{ij}) é ignorado na presente avaliação, pois assume-se essa etapa de convergência, o que produzirá relações de confiança estáticas. 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 v deve ser definido como (t_{min}, t_{min}).

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 6 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. 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. A simulação roda um tempo suficiente para que as métricas coletadas convirjam, ou seja, quando novas mensagens de anúncio e consulta não afetam os resultados até então coletados.

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 diferente para um determinado nível de visibilidade. 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. Para diferenciar este parâmetro de anúncios e consultas, adota-se $GMCE_a^v$ e $GMCE_q^v$, respectivamente.

As métricas de avaliação consideradas neste trabalho foram: a **taxa de casamento**, que mede o número de casamentos entre serviços anunciados e consultas aos mesmos; e a **taxa de efetividade do casamento**, que representa o número desses casamentos onde o *cliente* recebeu o *anúncio*, seja por meio do controle de exposição ou pelo mecanismo de casamento *in-network*. Estas métricas permitem avaliar o compromisso entre a visibilidade da informação de serviço e a colaboração na descoberta de serviços. De um modo geral, os resultados esperados são aqueles que comprovam que um ajuste no GMCE de determinado nível, com intuito de refletir necessidades de segurança e privacidade, afetam de forma proporcional o desempenho da descoberta no sistema: quanto maior a visibilidade, menor a segurança e privacidade, porém melhor é desempenho da descoberta.

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 serviço de p_i 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 o cliente 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.

6.2. Resultados

Observa-se que nos resultados apresentados nesta seção, a variação do GMCE para consultas, $GMCE_q^v$, é expressa no eixo x dos gráficos. Isso significa que, se a variação do nível v estiver sendo medida, todos os pares possuirão o mesmo $GMCE_q^v$ (com exceção do nível 3, que é igual a $GMCE_a^3$). No caso dos anúncios, essa variação acontece com a introdução de um conjunto de **classes de privacidade** no modelo da simulação. Essas classes possuem diferentes valores $GMCE_a^v$ para os níveis de visibilidade. Cada par é alocado a uma destas classes durante a simulação. A configuração de cada classe pode ser conferida na legenda da Figura 4. 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 1, 2 e 3 são mais prudentes na exposição da identidade forte em seus anúncios ($GMCE_a^3 \in [0,9; 1.0]$). Quanto às credenciais impostas no anúncio, assume-se que possuem o mesmo valor do $GMCE_a^1$ da classe; as credenciais impostas nas consultas são desconsideradas, pois a taxa de efetividade do casamento considera apenas o caso onde o cliente foi autorizado no casamento *in-network*.

As Figuras 4 e 5 mostram o compromisso entre o grau de privacidade exigido pelo usuário para níveis de visibilidade 1 e 2, respectivamente, e o desempenho da descoberta. Ambos os gráficos foram extraídos de experimentos com $GMCE_q^2 = GMCE_q^1$, que é determinado por um ponto no eixo x, e $GMCE_q^3 = GMCE_a^3$, que é dado pela classe de privacidade. A primeira igualdade não compromete os experimentos, pois não existe uma correlação entre $GMCE_q^2$ e $GMCE_q^1$ que afete os resultados de cada métrica.

O principal resultado da Figura 4 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 $GMCE_q^1$, 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

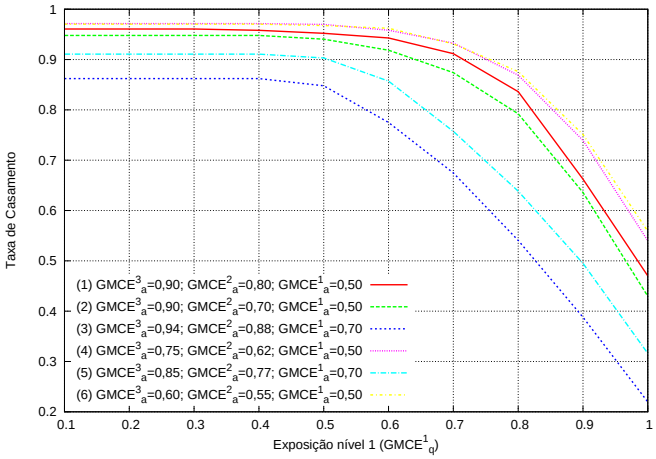

Figura 4. Impacto da variação do nível 1 de visibilidade

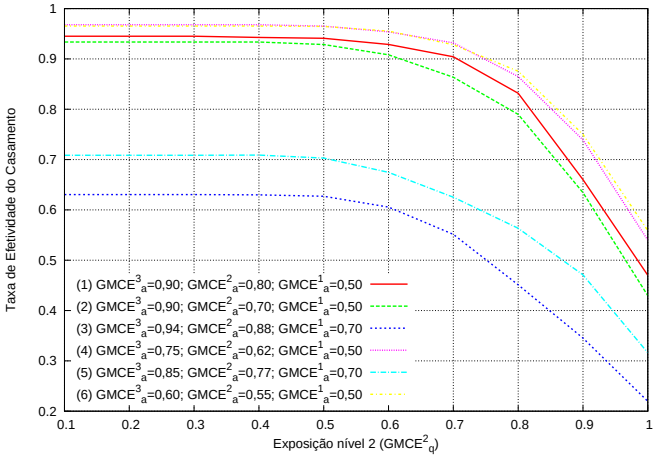

Figura 5. Impacto da variação do nível 2 de visibilidade

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, é possível obter altas taxas de casamento com grau de prudência médio ($GMCE^1_q = 0,5$).

A efetividade do casamento também obedece a relações semelhantes com o GMCE do nível de visibilidade 2. Observa-se, na Figura 5, que quanto menor o $GMCE^2_q$ (ou seja, menor prudência), 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 principalmente 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 expõem suas consultas com $GMCE^2_q = 0,8$ e provedores expõem anúncios com $GMCE^1_a = 0,8$, onde $0,8$ representa um grau de prudência alto.

Outro resultado importante é que pares não necessitam expor de forma demasiada suas identidades fortes tendo em vista contribuir mais para o desempenho da descoberta no sistema. Todas as classes apresentaram taxas de casamento efetivo entre 90% e 100%,

com $GMCE_a^3$ variando entre $0,60$ e $0,90$, excetuando-se as classes 3 e 5, onde o principal fator da baixa taxa é $GMCE_a^1$, e não $GMCE_a^3$. Essa propriedade é relevante porque permite a pares resguardarem sua identidade física, sem abrir mão da colaboração.

7. Conclusões

Este artigo apresentou FSSD, um protocolo para descoberta de serviços em ambientes ubíquos que permite que pares contornem a limitação da infra-estrutura 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, controle de exposição e mecanismo de casamento *in-network*, utilizados para viabilizar o compromisso entre colaboração, segurança e privacidade. Até onde se sabe, 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 rede e de segurança. Muitos cenários ubíquos possuem uma, 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 classes de experimentos, em particular um estudo sobre o impacto do gerenciamento de confiança e a existência de pares mal-intencionados na rede. Além disso, uma análise de desempenho do protocolo também é desejável, visto que o mesmo é destinado ao uso em dispositivos ubíquos, os quais muitas vezes possuem várias restrições computacionais. Por fim, é imperativo investigar o impacto da rede física subjacente no funcionamento e desempenho deste protocolo.

Referências

[1] F. Almenarez, A. Marin, D. Diaz, and J. Sanchez. Developing a model for trust management in pervasive devices. In *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on*, pages 5 pp.+, 2006.

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

[3] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux. Small worlds in security systems: an analysis of the pgp certificate graph. In *Proceedings of the ACM New Security Paradigms Workshop*, 2002.

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

[5] Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, Anthony D. Joseph, and Randy H. Katz. An architecture for a secure service discovery service. In *Mobile Computing and Networking*, pages 24–35, 1999.

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

[7] Audun Josang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, 43(2):618–644, March 2007.

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

[9] V. Lenders, M. May, and B. Plattner. 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, 2005.

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

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

[12] A. Mtibaa, A. Chaintreau, and Massoulie. Diameter of opportunistic mobile networks. In *ACM SIGCOMM CoNext 07*, December 2007.

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

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

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

[16] Ryan Wishart, Ricky Robinson, Jadwiga Indulska, and Audun Jøsang. Superstringrep: reputation-enhanced service discovery. In *CRPIT '38: Proceedings of the Twenty-eighth Australasian conference on Computer Science*, pages 49–57, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc.

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

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

[19] Feng Zhu, Wei Zhu, Matt W. Mutka, and Lionel Ni. 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, 2005. IEEE Computer Society.