Sec-SD: Descoberta Segura de Serviços em Redes Locais

Janaína Sutil Lemos[1], **Rafael Bohrer Ávila**[1], **Luiz Paulo Luna de Oliveira**[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950, Bloco 6B, São Leopoldo – RS – Brasil

janaina.lemos@gmail.com, lpluna@unisinos.br, rbavila@unisinos.br

Resumo. *Com a crescente popularização dos dispositivos móveis nos últimos anos, há uma necessidade cada vez maior de conectividade em rede e de serviços nas redes de computadores, onde o uso de tecnologias para descoberta de serviços simplifica a interação entre usuários e dispositivos e facilita as tarefas administrativas. Devido a grande diversidade de ambientes onde essas tecnologias podem ser utilizadas, surge também a necessidade de tratar as questões relacionadas a segurança. Neste trabalho é apresentado o Sec-SD, um sistema que combina tecnologias para descoberta de serviços em redes locais com mecanismos de segurança. A verificação do modelo apresentado é feita através de análise matemática.*

1. Introdução

Como consequência natural do interesse nas aplicações para encontrar de forma automática os recursos disponíveis em redes de computadores, pode-se constatar atualmente uma grande diversidade de tecnologias e sistemas dedicados à publicação, descoberta e utilização de serviços, que estão se tornando cada vez mais populares tanto para uso em redes de computadores convencionais como em redes móveis, como o Bluetooth[1]. Nesse contexto, surge também a preocupação com os aspectos relacionados a segurança, que variam de acordo com o ambiente e tem sido tema de diversas pesquisas. Um sistema seguro deve impedir que um cliente não autorizado tenha acesso a um determinado serviço e até mesmo que ele tome conhecimento da existência dos serviços oferecidos em certos casos, mas por outro lado, um usuário que tenha as credenciais corretas sempre deve obter informações sobre os serviços disponíveis e acesso aos mesmos. A necessidade de contemplar estes aspectos pode tornar o projeto de protocolos seguros uma tarefa bastante complexa.

Neste trabalho apresentamos o Sec-SD *(Secure Service Discovery)*, um sistema seguro para descoberta de serviços em redes locais que tem como caso uso o LP2P *(Local Peer-to-Peer Protocol)* [Rocha 2009], um sistema de compartilhamento peer-to-peer projetado para ambientes LAN. O Sec-SD faz uso de mecanismos de criptografia e autenticação, permitindo que a busca pelos peers e pelos conteúdos disponibilizados pelos mesmos seja realizada de forma automática, de modo que o usuário visualize somente os conteúdos para os quais ele possui acesso. Para validar o modelo, é apresentada uma análise matemática do mesmo.

2. Trabalhos Relacionados

Existe uma grande quantidade de trabalhos realizados com o objetivo de viabilizar a descoberta de serviços em redes de computadores e/ou de dispositivos móveis, como por

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

exemplo o Jini[2], o UPnP[3], o mDNS/DNS-SD e o OLSR-mDNS [Krebs et al. 2008], entre outros. As tecnologias mais relevantes do ponto de vista deste trabalho são descritas a seguir.

Desenvolvido por um consórcio de empresas fundado pela Microsoft, o UPnP possibilita a auto configuração de dispositivos e descoberta de serviços em pequenas redes, podendo ser utilizado em diversas plataformas. Sua arquitetura é composta por dispositivos controlados e pontos de controle e utiliza o SSDP (*Simple Service Discovery Protocol*) [Goland et al. 1999] para anunciar a presença de um dispositivo para os outros participantes da rede e para descobrir os serviços que estão disponíveis. Estas operações são feitas através do envio de mensagens em multicast, enquanto que as respostas são enviadas em unicast. Em relação a segurança, o modelo utilizado no UPnP provê mecanismos para proteger as mensagens de controle e respostas, contemplando aspectos como identificação, integridade, autenticação, autorização e privacidade [Ellison 2003].

Diferentemente do UPnP, o modelo PrudentExposure [Zhu et al. 2006] foi desenvolvido com foco nas características dos ambientes pervasivos e embora possa ser utilizado em outros ambientes, permite que a descoberta de serviços seja realizada somente de modo seguro. Sua arquitetura é composta por clientes, *User Agents*, diretórios e serviços e o processo de descoberta é composto pelas seguintes etapas: busca por domínios disponíveis, autenticação, seleção do serviço, troca de chaves de sessão e invocação do serviço. Já no caso do registro de um serviço, devem ser cumpridas apenas duas etapas: a busca pelo domínio e o registro propriamente dito.

O mDNS (*Multicast DNS*) [Cheshire and Krochmal 2010b] e o DNS-SD (*DNS based Service Discovery*) [Cheshire and Krochmal 2010a] fazem uso de operações e tipos de dados tradicionais do DNS e, combinados, permitem a descoberta e anúncio de serviços no enlace local. Estas tecnologias permitem que o acesso aos serviços seja feito através de nomes amigáveis e que eventuais mudanças nos endereços IP e/ou portas onde os serviços são disponibilizados ocorram de forma transparente para o usuário. Entre as ferramentas que utilizam estas tecnologias, podem ser citados o Bonjour[4] e o Avahi[5]. Ao contrário dos protocolos apresentados anteriormente, o mDNS não oferece nenhum mecanismo de segurança.

Nas tecnologias estudadas foram identificados diversos aspectos desejáveis no funcionamento do Sec-SD. Porém, tais características são encontradas isoladamente nos protocolos, criando a necessidade de combinar tecnologias já existentes com o desenvolvimento de mecanismos específicos para obter o comportamento desejado no sistema.

3. Sec-SD

O Sec-SD tem como caso de uso o LP2P *(Local Peer-to-Peer Protocol)*, um sistema de compartilhamento P2P para uso em redes locais que emprega uma abordagem descentralizada e escalável [Rocha 2009]. O LP2P combina as características específicas destes ambientes, como as altas taxas de transmissão e a baixas latências de comunicação com

[2]http://www.jini.org
[3]http://www.upnp.org
[4]http://developer.apple.com/mac/library/documentation/Cocoa/Conceptual/NetServices/Introduction.html
[5]http://avahi.org

os aspectos comumente encontrados nas redes P2P, como por exemplo os métodos utilizados para busca de conteúdos e formação de base de conhecimento. Este sistema está em desenvolvimento e prevê módulos para gerenciamento de mensagens, segurança, gerenciamento das informações relacionadas a reputação dos participantes da rede, uso de mecanismos de recompensa e o Sec-SD para descoberta de serviços. Para obter melhor aproveitamento da largura de banda, as mensagens de controle do protocolo para compartilhamento P2P (como por exemplo, adição e remoção de conteúdos) são enviadas em multicast.

Quando utilizado em conjunto com o LP2P, o Sec-SD integra funcionalidades de anúncio e descoberta de serviços a este sistema, permitindo que a descoberta dos peers e dos conteúdos disponibilizados pelos mesmos ocorra de forma automática. Os arquivos ofertados pelos nodos são organizados em *compartilhamentos*, que são os serviços providos pelo LP2P. No momento da criação de um compartilhamento o usuário tem a opção de configurar se seu conteúdo é aberto ou restrito.

O fato de o Sec-SD permitir que a descoberta de serviços seja realizada com ou sem o uso de mecanismos de segurança o torna apto para ser utilizado em diferentes ambientes. Entre os possíveis cenários de uso do Sec-SD, pode ser citada uma combinação de NFS (*Network File System*) com IPSec [Kent and Atkinson 1998a] [Kent and Atkinson 1998b]. O IPSec oferece mecanismos para criptografia e autenticação, enquanto que o Sec-SD permite a descoberta dos compartilhamentos e obtenção da chave criptográfica. Para cada compartilhamento NFS pode ser atribuída uma senha de acesso, fazendo com que cada usuário visualize somente as pastas para as quais ele possui as credenciais corretas. Da mesma forma, um compartilhamento sem senha pode ser acessado por todos os usuários da rede.

Entre as características desejáveis no Sec-SD, está a facilidade de uso do sistema que inclui, entre outros aspectos, a apresentação de informações importantes para a escolha de um ou outro serviço. Entre as tecnologias estudas, o mDNS e o DNS-SD, descritos na sessão 2, mostraram-se mais adequados e por esse motivo, serão utilizados no protótipo do Sec-SD através da ferramenta Avahi. Dois tipos de serviços distintos são utilizados para designar os compartilhamentos abertos e os compartilhamentos restritos, o *open-lp2p* e o *confidential-lp2p*, respectivamente. Os provedores anunciam seus conteúdos abertos no momento em que ingressam na rede e respondem todas as requisições por este tipo de conteúdo, retornando uma listagem com os nomes dos seus compartilhamentos.

A fim de evitar a exposição de informações confidenciais na descoberta de compartilhamentos restritos, os participantes que possuem esse tipo de conteúdo não enviam anúncios espontâneos. Ao invés disso, eles aguardam o recebimento de requisições e na presença das mesmas verificam se o cliente está apto a acessar o serviço. As credenciais para acesso aos compartilhamentos devem ser repassadas somente aos interessados e através de um meio seguro, cuja escolha é responsabilidade dos usuários do sistema e está fora do escopo desse trabalho. Da mesma forma, para impedir que um usuário autorizado continue tendo acesso a um determinado compartilhamento é necessário substituir as credenciais, procedimento realizado pelos outros usuários que tem acesso ao compartilhamento.

3.1. Descoberta do serviço *confidential-lp2p*

Um usuário que cria um compartilhamento seguro atribui a ele um nome e uma senha, tornando-se então o primeiro participante do grupo que possui acesso ao mesmo. Ao liberar o acesso para outros usuários da rede LP2P, ele divulga para os mesmos o nome e a senha, que servirão para que um membro do grupo possa descobrir outros membros na rede, uma vez que compartilhamentos restritos não são anunciados de forma espontânea. Um cliente com acesso a um determinado compartilhamento seguro que ingressa na rede LP2P procura por outros participantes do grupo enviando requisições multicast para o serviço *confidential-lp2p*, com o objetivo de obter uma chave de grupo, que será utilizada mais tarde para visualizar a listagem dos arquivos presentes no compartilhamento.

A requisição para um compartilhamento seguro é composta pelo tipo de serviço *confidential- lp2p*, o hash do nome do compartilhamento concatenado com a senha de acesso ao mesmo e com um *time-stamp*, que é empregado com o objetivo de prevenir ataques causados pela repetição de mensagens capturadas de forma indevida. Para permitir a verificação da mensagem por parte do receptor, o *time-stamp* também é enviado em claro na requisição. Após o envio da requisição o cliente aguarda um determinado tempo (da ordem de segundos) e se não receber nenhuma resposta, ele envia novamente a requisição. Se ainda assim não obtiver respostas, o peer conclui que não há mais nenhum participante do grupo na rede e gera ele mesmo a chave de grupo, que será válida por um determinado período de tempo. Por outro lado, se já existirem outros membros do grupo na rede, cada um deles determinará através de uma probabilidade P_p se deve processar (e responder, se for o caso) a requisição. Esta probabilidade é proporcional ao número de compartilhamentos que um participante possui e é aplicada com o objetivo de evitar um aumento excessivo do tráfego em ambientes com muitos nodos.

Durante o processamento de uma requisição um peer verifica se possui pelo menos um compartilhamento seguro e se não possuir, descarta a mensagem. Do contrário, ele extrai o hash e o *time-stamp* da mensagem. Posteriormente, ele gera um hash do nome de cada um dos seus compartilhamentos seguros com a respectiva senha e com o *time-stamp* recebido e compara o resultado com o hash extraído da requisição. Se ele possuir o compartilhamento buscado deverá responder em unicast ao potencial cliente. A resposta é composta pelo hash do nome do compartilhamento concatenado com a senha do mesmo e com um novo *time-stamp*. Também são enviados o novo *time-stamp* e o *time-stamp* anterior em claro. Se receber mais de uma resposta, o cliente escolhe apenas um peer para se comunicar, ignorando todas as outras respostas recebidas. Se a resposta recebida estiver correta, ele assume que o provedor realmente possui o compartilhamento buscado e solicita a chave de grupo. O provedor analisa a solicitação e pede a chave pública do cliente, que então envia a sua chave pública. Esta será utilizada pelo provedor para criptografar a chave de grupo. O cliente, por sua vez utilizará a sua chave privada para descriptografar a informação recebida e a partir desse momento, ele pode visualizar o conteúdo do compartilhamento. A listagem do conteúdo de um compartilhamento, a seleção do(s) arquivo(s) desejado(s) e o estabelecimento de chaves de sessão para acesso aos mesmos são feitos através do protocolo LP2P. Por outro lado, se após o cálculo de P_p um peer determinar que não deve processar uma requisição e após algum tempo ele receber novamente a solicitação, a probabilidade P_p assume valor 1. Todas as requisições recebidas ficam armazenadas por um período de tempo, para que a máquina possa identificar quando se trata de uma repetição de uma solicitação. A Figura 1 mostra o processo

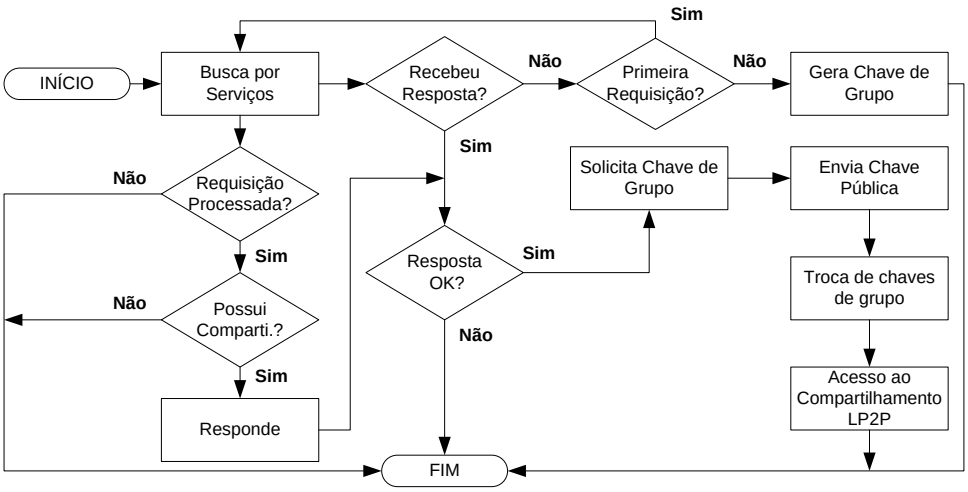

Figura 1. Processo de descoberta do serviço *confidential-lp2p*.

de descoberta do serviço *confidential-lp2p*.

4. Avaliação do Sistema

Nesta seção é apresentada uma análise matemática do Sec-SD, onde é avaliado o impacto causado pelo tráfego das mensagens de descoberta na rede, com o objetivo de identificar possíveis gargalos em ambientes com grande número de nodos e de compartilhamentos confidenciais.

4.1. Propriedades Matemáticas do Sec-SD

Conforme foi descrito anteriormente, cada nodo que ingressa na rede procura por cada um dos compartilhamentos secretos que ele possui com o objetivo de obter a chave de grupo enviando requisições em multicast. Nesse processo de descoberta não ocorrem falsos negativos, isto é, sempre que um usuário solicitar um compartilhamento para o qual ele possui as credenciais, ele irá obter acesso ao mesmo. Quanto aos falsos positivos, para uma entidade que não possui as devidas credenciais acessar um compartilhamento secreto é necessário que a mesma gere um hash idêntico ao produzido pela entrada do nome do compartilhamento, senha e o *time-stamp*. A aplicação deste parâmetro tem o objetivo de evitar ataques produzidos pela captura e repetição indevida de mensagens.

As requisições são processadas pelos outros peers com probabilidade P_p e respondidas em unicast. Desta forma, o tráfego de mensagens de descoberta é influenciado pelo número de participantes da rede e pela quantidade de compartilhamentos secretos que cada um possui. Além disso, a probabilidade P_p é aplicada com o intuito de reduzir o quantidade de respostas enviadas em unicast. O tráfego de mensagens de descoberta M em um ambiente dado por:

$$M = NSP_r$$

Onde N é a quantidade de participantes da rede, S é o número médio de compartilhamentos secretos por participante e P_r é a probabilidade de um nodo processar uma requisição e possuir o compartilhamento solicitado, ou seja, de o nodo efetivamente poder responder a requisição. O parâmetro P_r abrange a probabilidade P_p de o nodo processar

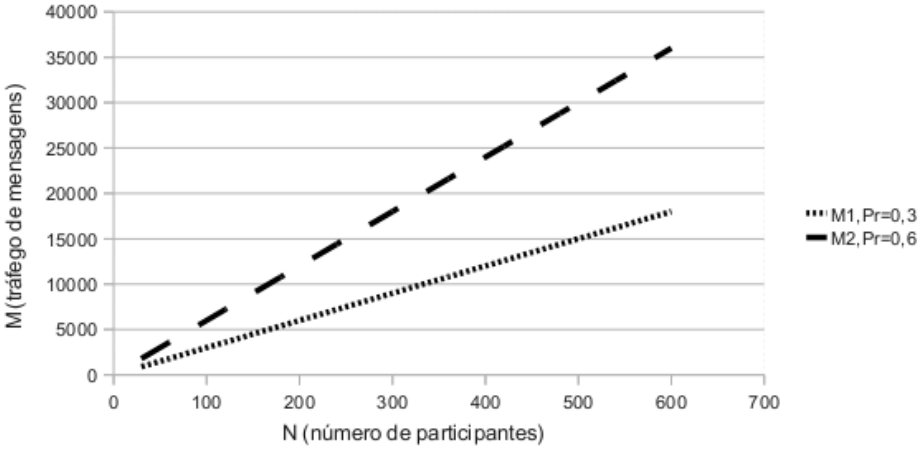

Figura 2. Tráfego de mensagens de descoberta M em função do número de participantes N.

a requisição e leva em conta o fato de que em um ambiente real o participante pode possuir ou não o conteúdo solicitado. Para a análise do tráfego de mensagens de descoberta na rede, trataremos P_r como uma constante. Serão avaliados os dois cenários descritos a seguir, que compreendem a variação do número de participantes na rede e a variação do número médio de compartilhamentos confidenciais por participante, respectivamente. Em ambos os casos, o tempo médio de processamento de uma requisição, T_p é proporcional ao tempo gasto no cálculo de um hash MD5 de 128 bits e na comparação de duas *strings*. Para obter uma estimativa deste tempo, foi utilizado o software *Md5sum* em uma plataforma Intel Core 2 Duo com 3GHZ. Observou-se então que o tempo t_p gasto para a realização destas duas operações foi em média $1ms$. Assim, T_p é dado por:

$$T_p = S.t_p$$

4.1.1. Variação da quantidade de participantes na rede

Neste cenário, são mantidos fixos o número médio de compartilhamentos confidenciais por participante S e a probabilidade P_r, cujos valores são mostrados abaixo. O gráfico correspondente ao tráfego de mensagens em função do número de participantes na rede é mostrado na Figura 2.

$S = 100, P_r = 0.3$

$S = 100, P_r = 0.6$

$30 <= N <= 600$

Neste cenário, observou-se que com a probabilidade de um participante processar a requisição e possuir o conteúdo solicitado P_r fixada em 0.3, o tráfego de mensagens de descoberta apresenta valores aceitáveis. Por exemplo, com 300 participantes, cada um disponibilizando em média 100 compartilhamentos confidenciais (uma quantidade alta em se tratando de um ambiente local) são trocadas aproxidamente 9000 mensagens de descoberta. Considerando que o ingresso deste número de participantes ocorra em um intervalo 30 minutos, seriam trocados em média 300 pacotes por minuto. Da mesma forma,

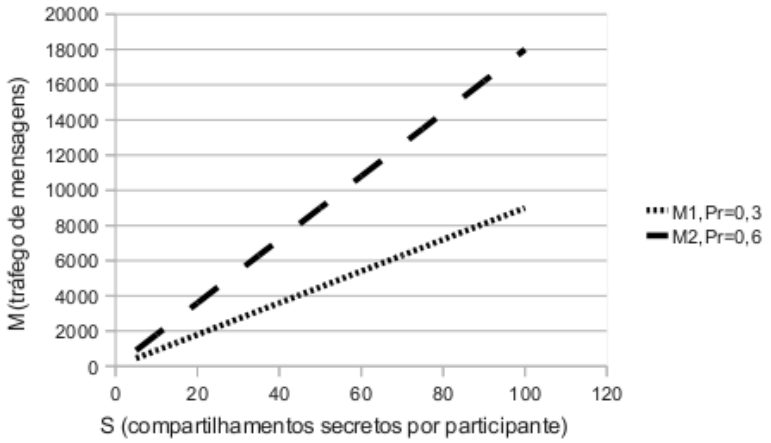

Figura 3. Tráfego de mensagens de descoberta M em função do número médio de compartilhamentos secretos por participante S.

quando ingressam 600 nodos neste mesmo intervalo de tempo, trafegariam aproximadamente 600 pacotes por minuto. Por outro lado, com $P_r = 0.6$, um número elevado de mensagens de resposta é enviado desnecessariamente, uma vez que o peer que enviou a requisição escolherá somente um participante para se comunicar e obter a chave de grupo.

4.1.2. Variação do número do número médio de compartilhamentos confidenciais por participante

Agora, fixamos a quantidade de participantes S e a probabilidade P_r, cujos valores são mostrados a seguir. O gráfico obtido para o tráfego de mensagens em função do número médio de compartilhamentos por participante é mostrado na Figura 3.

$N = 300, P_r = 0.3$

$N = 300, P_r = 0.6$

$5 <= S <= 100$

Com a variação do número médio de compartilhamentos secretos disponibilizados por cada participante, considerando-se um ambiente com 300 nodos, também foram obtidos resultados satisfatórios com $P_r = 0.3$, com 150 pacotes por minuto no caso médio e 300 para pacotes por minuto no caso de cada nodo possuir 100 compartilhamentos. Em relação ao tempo de processamento T_p, são gastos aproximadamente 100 ms quando um peer possui 100 compartilhamentos confidenciais considerando-se a plataforma utilizada.

Observa-se então que é necessário ajustar o valor de P_r com um valor baixo para garantir um bom desempenho da rede mesmo na presença de muitos participantes e/ou compartilhamentos confidencias. Como no ambiente real não é possível prever o número de nodos que irão possuir um determinado compartilhamento e de fato, responder uma requisição, é de grande importância a aplicação da probabilidade P_p, que no funcionamento do Sec-SD determina se um participante deve ou não processar uma requisição recebida. Este parâmetro é calculado em função do número de compartilhamentos confidenciais que cada peer possui para a primeira requisição enviada e automaticamente

assume valor 1 no recebimento de uma repetição da solicitação, para evitar que um participante fique sem resposta quando poucos nodos estiverem na rede, mesmo que algum deles possua o conteúdo solicitado.

5. Considerações Finais

O Sec-SD é um sistema para anúncio e descoberta segura de serviços em redes locais que permite, no caso de uso apresentado, que o usuário configure para cada compartilhamento se o conteúdo do mesmo é aberto ou restrito. Tal característica faz com que o este sistema possa ser utilizado em diferentes ambientes e em conjunto com diferentes aplicações. Em relação a análise do tráfego gerado pelas mensagens de descoberta, o modelo apresentou baixa taxa de mensagens por minuto mesmo em ambientes com muitos nodos e/ou com grande quantidade de compartilhamentos confidenciais, devido ao fato de que cada participante que recebe uma requisição aplica uma probabilidade para determinar se deve ou não processar a mensagem. Como trabalhos futuros, estão previstos a implementação do Sec-SD e ainda, o desenvolvimento de um segundo nível de segurança para o sistema, que torne possível a identificação dos usuários de forma individual, uma vez que o mecanismo de autenticação utilizado neste modelo permite que um participante seja identificado como sendo pertencente a um determinado grupo.

Referências

Cheshire, S. and Krochmal, M. (2010a). DNS-Based Service Discovery. Internet Draft, Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-cheshire-dnsext-dns-sd-06.

Cheshire, S. and Krochmal, M. (2010b). Multicast DNS. Internet Draft, Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-cheshire-dnsext-multicastdns-11.

Ellison, C. (2003). UPnP security ceremonies. UPnP Forum. http://www.upnp.org/specs/sec/UPnP-sec-UPnPSecurityCeremonies-v1.pdf.

Goland, Y., Cai, T., Leach, P., Gu, Y., and Albright, S. (1999). Simple Service Discovery Protocol/1.0. Internet Draft, Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-cai-ssdp-v1-03.

Kent, S. and Atkinson, R. (1998a). RFC 2401: Security Architecture for the Internet Protocol. Internet Engineering Task Force (IETF).

Kent, S. and Atkinson, R. (1998b). RFC 2402: IP Authentication Header. Internet Engineering Task Force (IETF).

Krebs, M., Krempels, K.-H., and Kucay, M. (2008). Service discovery in wireless mesh networks. In *IEEE Wireless Communications and Networking Conference (WCNC) 2008*, Las Vegas, NV, USA.

Rocha, E. (2009). LP2P: Sistema Peer-to-Peer para Redes Locais. White Paper. Programa Interdisciplinar de Pós-Graduação em Computação Aplicada - Universidade do Vale do Rio dos Sinos, São Leopoldo, RS, Brasil.

Zhu, F., Mutka, M., and Ni, L. (2006). A private, secure, and user-centric information exposure model for service discovery protocols. In *IEEE Transactions on Mobile Computing*, volume 5, Piscataway, NJ, USA.