

# Simulação de um Protocolo de Descoberta de Serviços Seguro e Flexível para Ambientes Ubíquos

Rodolfo Stoffel Antunes<sup>1</sup>  
Orientador: Dr. Marinho Pilla Barcellos<sup>2,3</sup>

<sup>1</sup> Universidade do Vale do Rio dos Sinos

<sup>2</sup> Universidade Federal do Rio Grande do Sul

<sup>3</sup> Pontifícia Universidade Católica do Rio Grande do Sul

1º de Setembro de 2008

## Introdução

## Protocolo FSSD

## Modelo de Simulação

## Resultados

## Introdução

- ▶ Computação móvel e ubíqua é cada vez mais comum
- ▶ Ambientes onde dispositivos anunciam e buscam serviços
- ▶ Descoberta de serviços se torna componente essencial: reduz o trabalho de configuração e favorece a espontaneidade
- ▶ Processo de descoberta: casamento do anúncio de um serviço com uma consulta por este serviço

## Introdução

- ▶ Soluções centralizadas não são adequadas à computação ubíqua
- ▶ Protocolos distribuídos dependem da corretude de dispositivos
- ▶ Divulgação de informações é necessária para a descoberta de serviços
- ▶ Informações devem ser protegidas por causa das questões de segurança
- ▶ Equilíbrio garante a descoberta segura e eficaz de serviços

### Objetivo

- ▶ Modelar, simular e avaliar o protocolo FSSD

## Flexible Secure Service Discovery

- ▶ Protocolo de descoberta de serviços em nível de aplicação
- ▶ Gerência de reputação limita a exposição de informações sensíveis
- ▶ Usuário tem a opção entre prudência ou colaboração

## Rede de Confiança

- ▶ Relação é uma tupla  $(t, c)$  que representa confiança e certeza
- ▶ Relações assimétricas
- ▶ Permitem estabelecer um canal seguro de comunicação

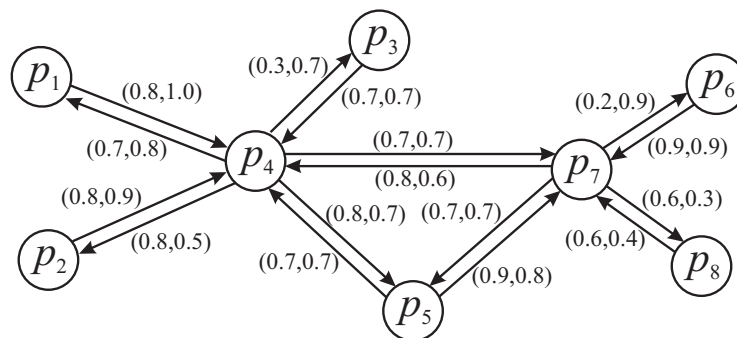
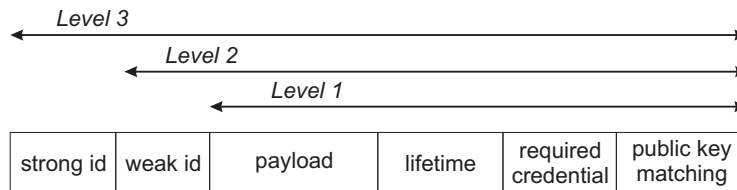


Figura: Rede de Confiança

## Controle de Exposição

- ▶ Mensagens de anúncio e consulta possuem informações que identificam usuários e serviços
- ▶ Informações possuem nível de sensibilidade, que varia de 1 a 3
- ▶ Cada nível possui um requisito mínimo de confiança
- ▶ Se o requisito não é atingido, a informação é suprimida



**Figura:** Service information record

## Modelo de Simulação

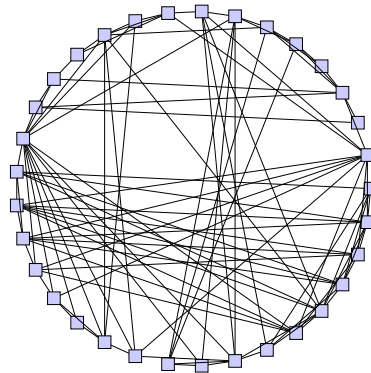
- ▶ Dinamicidade é característica de ambientes ubíquos
- ▶ Implementação em ambiente real permite análise completa
- ▶ Elevado número de variáveis mascara propriedades fundamentais do protocolo
- ▶ Simulação permite concentrar análise nestas propriedades
- ▶ Implementada como extensão ao *Simmcas*t

## Modelo de Simulação

- ▶ Cada nodo representa um dispositivo que anuncia e busca serviços
- ▶ Nodos divididos em três classes de usuários:
  - $C_1$  Alta prudência: Usuário interessado em privacidade
  - $C_2$  Média prudência: Usuário com interesse misto
  - $C_3$  Baixa prudência: Usuário com interesse na descoberta
- ▶ Nodos interligados em uma topologia estrela, através de conexões TCP sem perdas
- ▶ Comunicação restrita pela rede de confiança do FSSD
- ▶ Simulação utiliza rede de confiança estática

## Rede de Confiança

- ▶ Rede de confiança com propriedades *small world*
- ▶ Cada aresta representa duas relações de confiança
- ▶ Valores das relações de confiança distribuídos uniformemente



**Figura:** Grafo de confiança gerado

## Modelo de Simulação

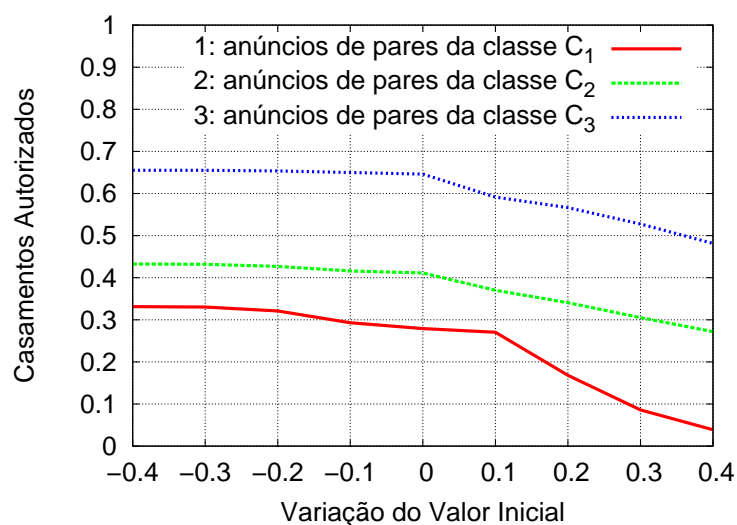
### Q1 Impacto dos requisitos de confiança na eficácia do protocolo

- ▶ Eficácia: razão entre número de pesquisas realizadas e resultados obtidos
- ▶ Variação dos requisitos de confiança utilizados pelos pares

### Q2 Impacto da topologia de confiança no processo de descoberta

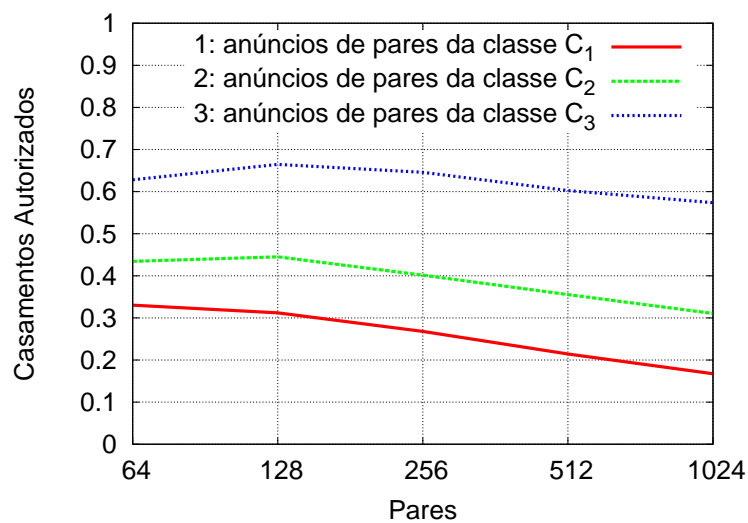
- ▶ Eficácia: razão entre número de pesquisas realizadas e resultados obtidos
- ▶ Variação do número de pares simulados

## Variação da Prudência



- ▶ Diferença constante entre as curvas demonstra influência da configuração dos requisitos de exposição

## Variação da Topologia




- ▶ Número de pares influencia na eficácia da descoberta, por causa da maior distância entre provedores e clientes

## Objetivo

- ▶ Modelar, simular e avaliar o protocolo FSSD

## Artigos Publicados

-  MOSCHETTA, E.; BARCELLOS, M.; ANTUNES, R. Flexibilizando Graus de Colaboração, Segurança e Privacidade na Descoberta de Serviços em Ambientes Ubíquos. XXVI Simpósio Brasileiro de Redes de Computadores (SBRC 2008).

## Trabalhos Futuros

- ▶ Diminuir o número de restrições da simulação
- ▶ Implementar o protocolo em ambiente real