GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

POLI - Escola Politécnica
COPPE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro

Controle de Acesso Auto-Organizável e Robusto Baseado em Nós Delegados para Redes Ad Hoc

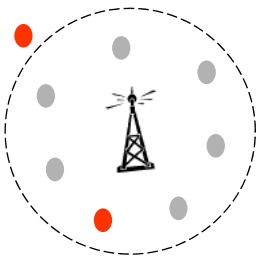
Natalia Castro Fernandes e Otto Carlos M. B. Duarte

VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais
Gramado, setembro de 2008

Introdução

GTA / UFRJ

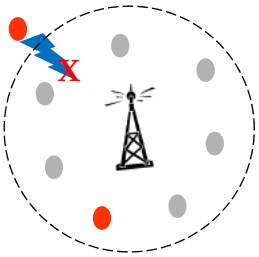
- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas



Introdução – Redes Ad Hoc

GTA / UFRJ

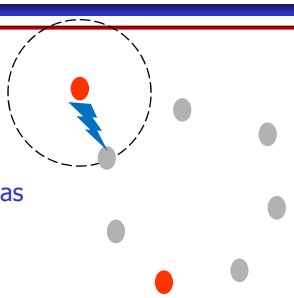
- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas



Introdução

GTA / UFRJ

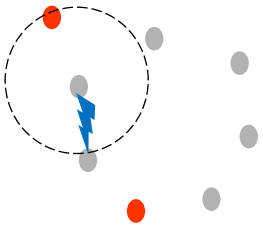
- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas
    - Roteamento colaborativo
      - Múltiplos saltos
    - Conectividade intermitente



Introdução

GTA / UFRJ

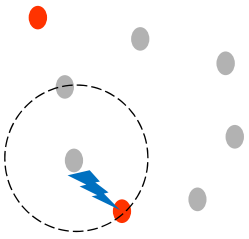
- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas
    - Roteamento colaborativo
      - Múltiplos saltos
    - Conectividade intermitente



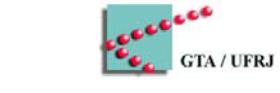
Introdução

GTA / UFRJ

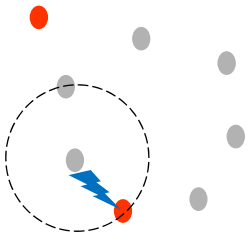
- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas
    - Roteamento colaborativo
      - Múltiplos saltos
    - Conectividade intermitente



Introdução



- Redes ad hoc
  - Características
    - Ausência de infra-estrutura
      - Disponibilidade de serviços não garantidas
    - Roteamento colaborativo
      - Múltiplos saltos
    - Conectividade intermitente
  - Segurança
    - Vulnerabilidades
      - Roteamento
        - Ausência de colaboração
        - Ações maliciosas



Autenticação em Redes Ad Hoc

- Autenticação
  - Prova da identidade
  - Identificação correta da origem das mensagens
- Autoridade certificadora
  - Registro de identidades
  - Emissão de certificados
  - Tratamento da lista de revogações

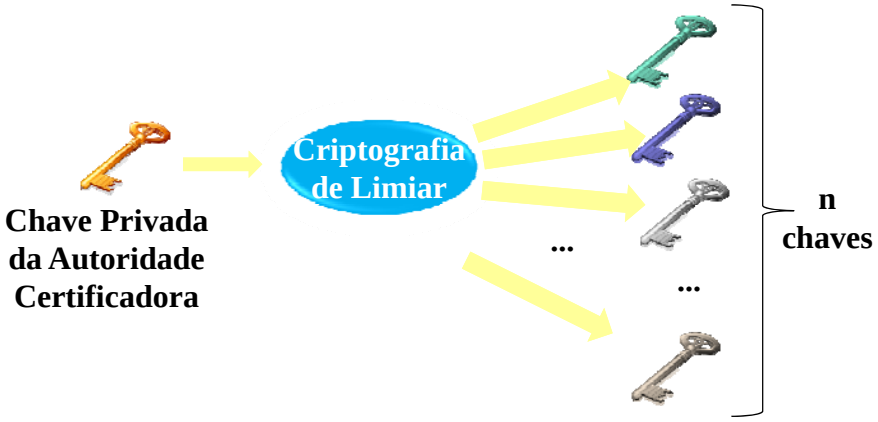
Autenticação em Redes Ad Hoc

- Autenticação
  - Prova da identidade
  - Identificação correta da origem das mensagens
- Autoridade certificadora
  - Registro de identidades
  - Emissão de certificados
  - Tratamento da lista de revogações

Redes ad hoc
↓
Ausência de infra-estrutura
↓
Ausência de administrador

Autoridades Certificadoras Distribuídas

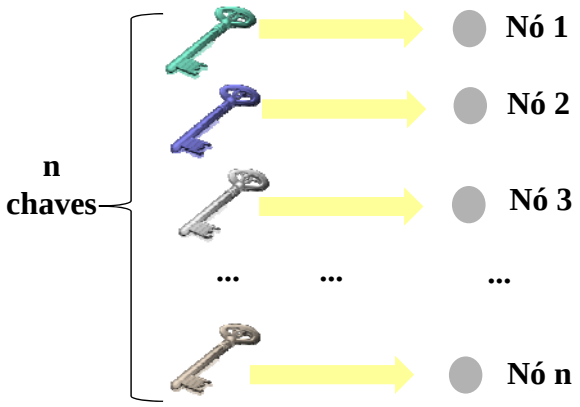
- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

GTA / UFRJ

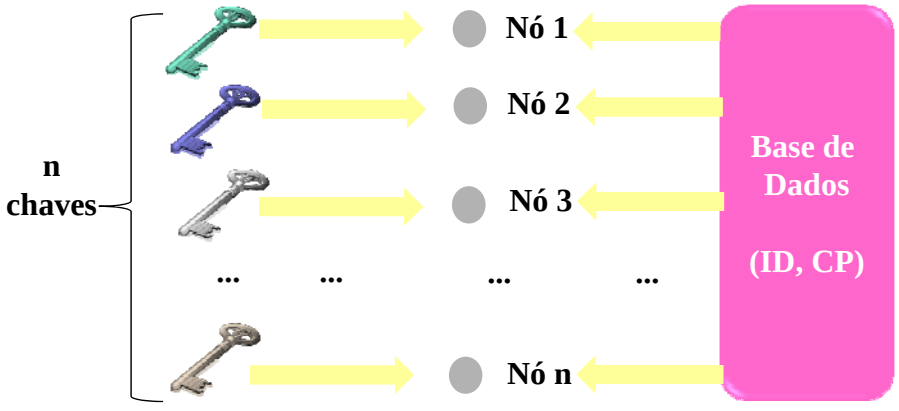
- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

GTA / UFRJ

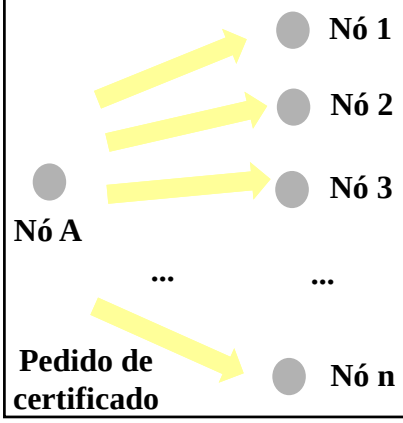
- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

GTA / UFRJ

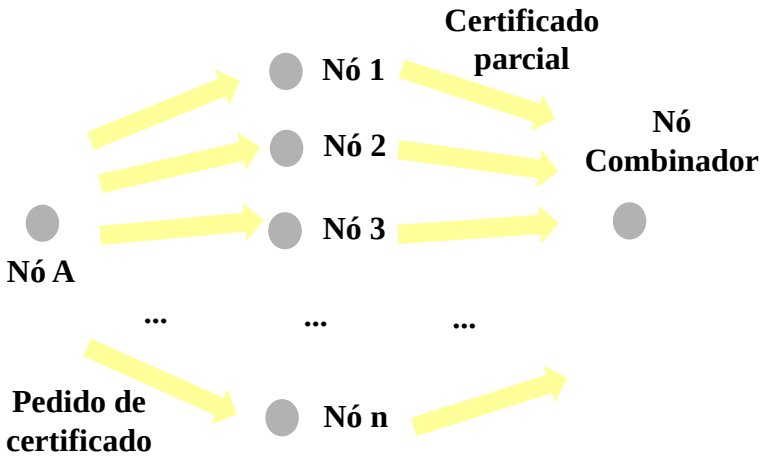
- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

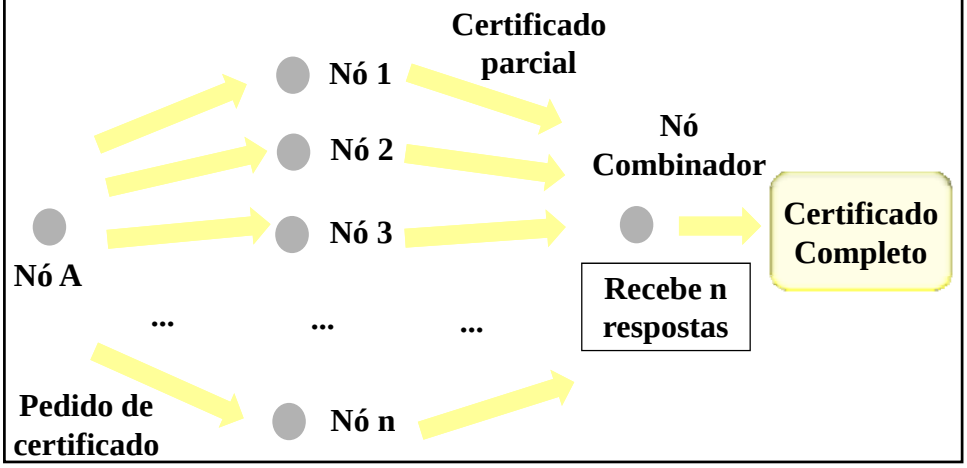
GTA / UFRJ

- Distribuição da função de autoridade certificadora



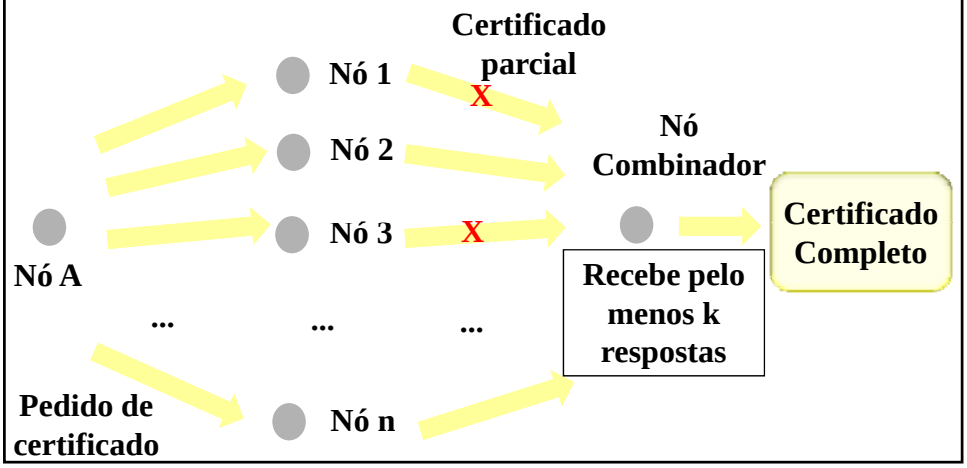
Autoridades Certificadoras Distribuídas

- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

- Distribuição da função de autoridade certificadora



Autoridades Certificadoras Distribuídas

- Desvantagens
  - Administrador *offline*
    - Escolha dos n nós
    - Controle de acesso
  - Disponibilidade dos k nós

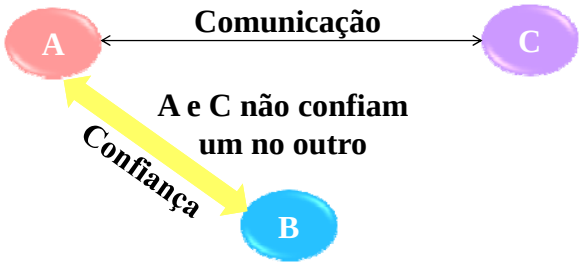
Autenticação por Cadeias de Certificado

- Autenticação baseada em cadeias de certificado

A e C não confiam um no outro

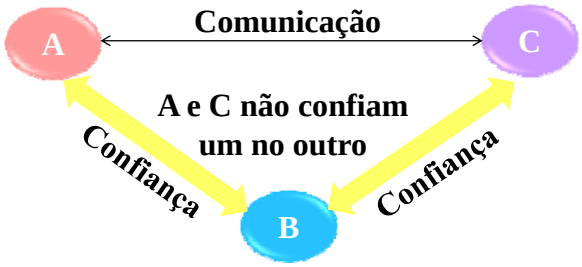
Autenticação por Cadeias de Certificado

- Autenticação baseada em cadeias de certificado



Autenticação por Cadeias de Certificado

- Autenticação baseada em cadeias de certificado



Autenticação por Cadeias de Certificado

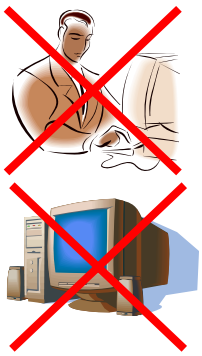
- Autenticação baseada em cadeias de certificado

Autenticação por Cadeias de Certificado

- Autenticação baseada em cadeias de certificado
  - Busca por cadeias de certificado em comum
- Vantagens
  - Ausência de administrador
  - Ausência de centralização
- Desvantagem
  - Inexistência de controle de acesso
    - Retorno de nós maliciosos à rede

Protocolo Proposto

- AMORA
  - Autenticação e MOnitoração em Redes Ad hoc
  - Características
    - Ausência de administrador e servidor



Protocolo Proposto

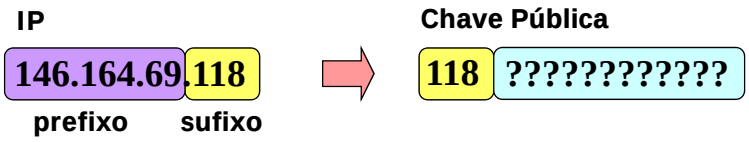
- AMORA
  - Autenticação e MOnitoração em Redes Ad hoc
  - Características
    - Ausência de administrador e servidor
    - Autenticação distribuída com controle de acesso
      - Cadeias de delegação

Protocolo Proposto

- AMORA
  - Autenticação e MOnitoração em Redes Ad hoc
  - Características
    - Ausência de administrador e servidor
    - Autenticação distribuída com controle de acesso
      - Cadeias de delegação
    - Certificação e monitoração do nós
      - Nós delegados

Protocolo Proposto

- AMORA
  - Autenticação e MOnitoração em Redes Ad hoc
  - Características
    - Ausência de administrador
    - Autenticação distribuída com controle de acesso
      - Cadeias de delegação
    - Certificação e monitoração do nós
      - Nós delegados
    - Chaves assimétricas relacionadas ao IP

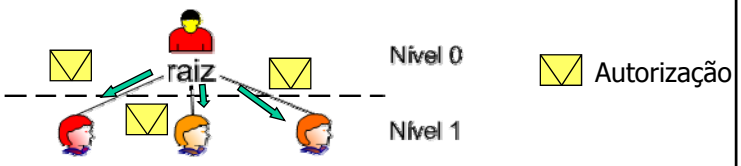


Cadeias de Delegação

- Ausência de administração centralizada
- Associação de confiança entre usuários
  - Estabelecimento *offline* anterior ou concomitante com o funcionamento da rede

Cadeias de Delegação

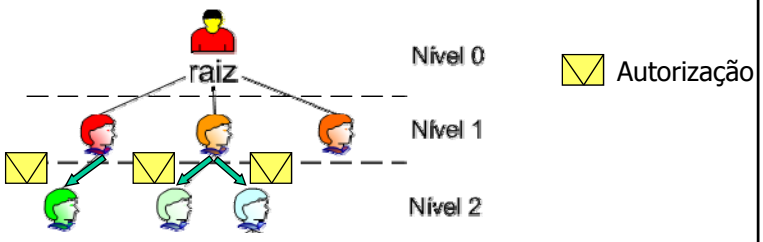
- Ausência de administração centralizada
- Associação de confiança entre usuários
  - Estabelecimento *offline* anterior ou concomitante com o funcionamento da rede



Cadeias de Delegação

GTA / UFRJ

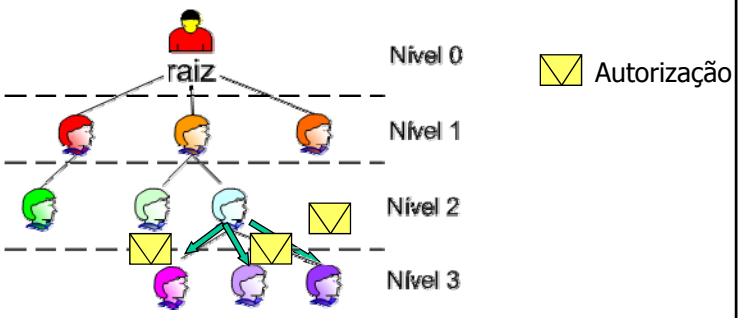
- Ausência de administração centralizada
- Associação de confiança entre usuários
  - Estabelecimento *offline* anterior ou concomitante com o funcionamento da rede



Cadeias de Delegação

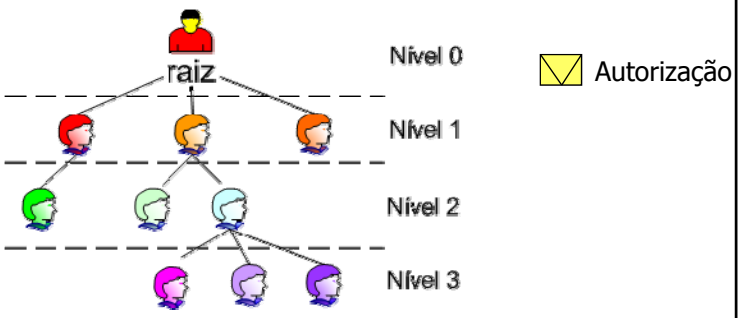
GTA / UFRJ

- Ausência de administração centralizada
- Associação de confiança entre usuários
  - Estabelecimento *offline* anterior ou concomitante com o funcionamento da rede



Cadeias de Delegação

- Ausência de administração centralizada
- Associação de confiança entre usuários
  - Estabelecimento *offline* anterior ou concomitante com o funcionamento da rede



Cadeias de Delegação

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	

Cadeias de Delegação

GTA / UFRJ

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	

Número máximo de filhos

Cadeias de Delegação

GTA / UFRJ

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	

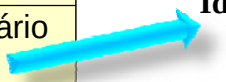
Identifica a cadeia de delegação

Cadeias de Delegação

GTA / UFRJ

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	



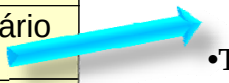
Identifica o usuário que autorizou a entrada

Cadeias de Delegação

GTA / UFRJ

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	



•Identifica o novo usuário
•Torna a autorização um documento público

Cadeias de Delegação

GTA / UFRJ

- Autorização

Filhos	ID autorização
Expiração da autorização	
Chave pública do usuário raiz	
Chave pública do usuário avô	
Chave pública do usuário pai	
Chave pública do usuário filho	
Assinatura do usuário pai	

Valida a autorização

Nós Delegados

GTA / UFRJ

- Emissão de certificados
- Monitoração de atividades
  - Revogação de acesso
- Tipos
  - Delegados de usuário (m_u)
    - Controle
      - Entrada de nós filhos
      - Uso da autorização
  - Delegados de nó (m_n)
    - Monitoração e exclusão de nós
- Decisões
  - Votação
    - Mínimo de k votos

Nós Delegados

GTA / UFRJ

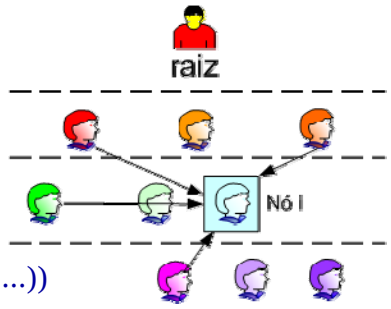
- Seleção
  - Suposição
    - Conhecimento da lista dos IPs dos nós ativos
  - Impossibilidade de nó selecionar seu grupo de delegados
    - Uso de funções *hash*
  - Delegados de nó

$$D_i = hash^i(IP)$$

  - Delegados de usuário

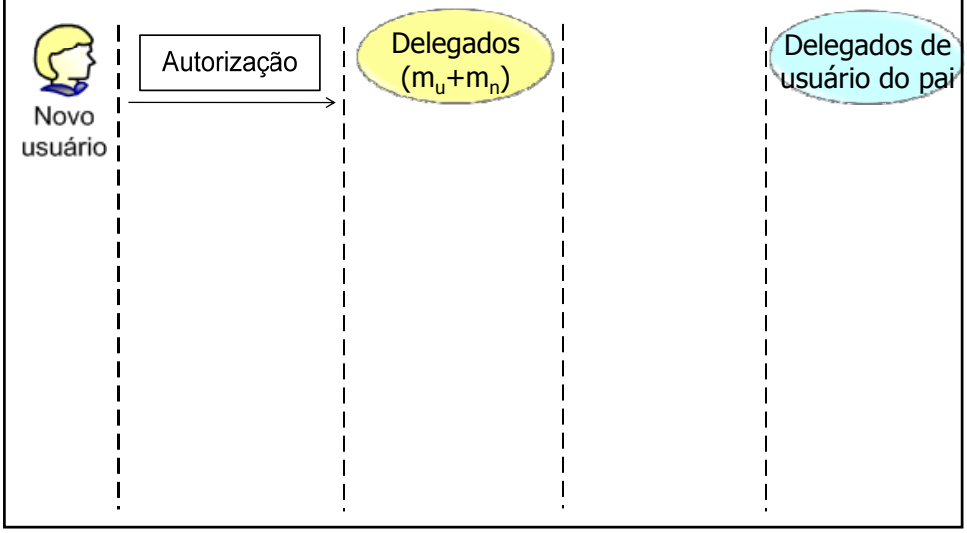
$$D_j = hash^j(Cp)$$

$$hash^k(X) = hash(hash(...hash(X)...))$$



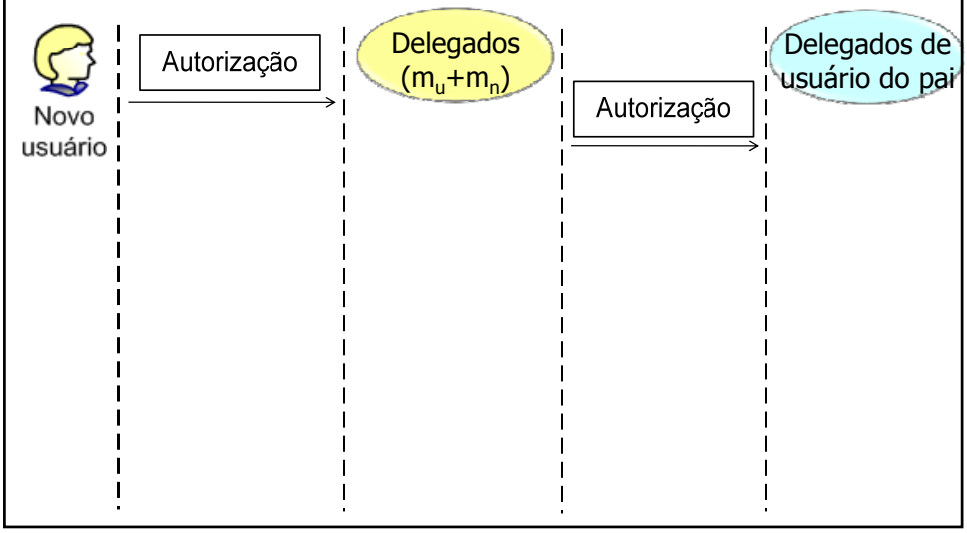
Entrada de Nós – Obtenção do Certificado

GTA / UFRJ



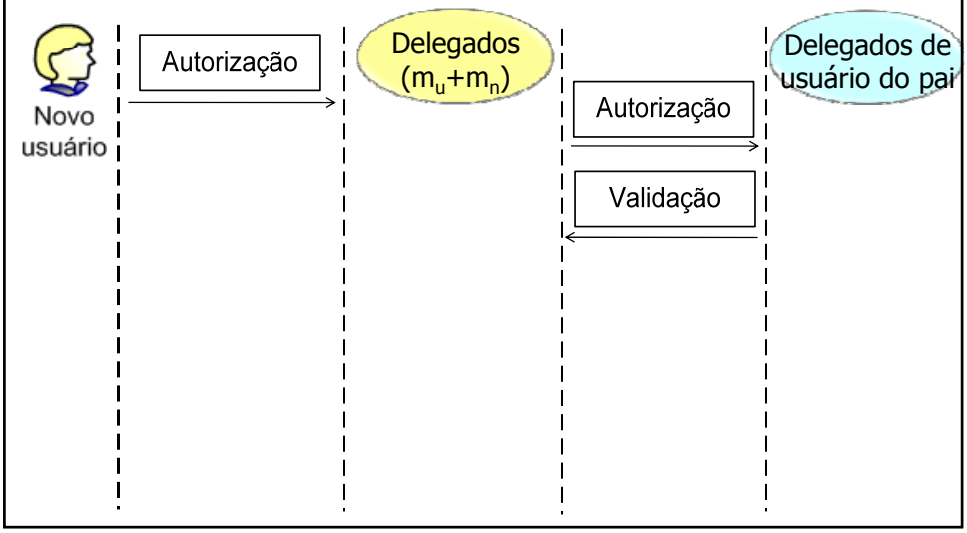
Entrada de Nós – Obtenção do Certificado

GTA / UFRJ

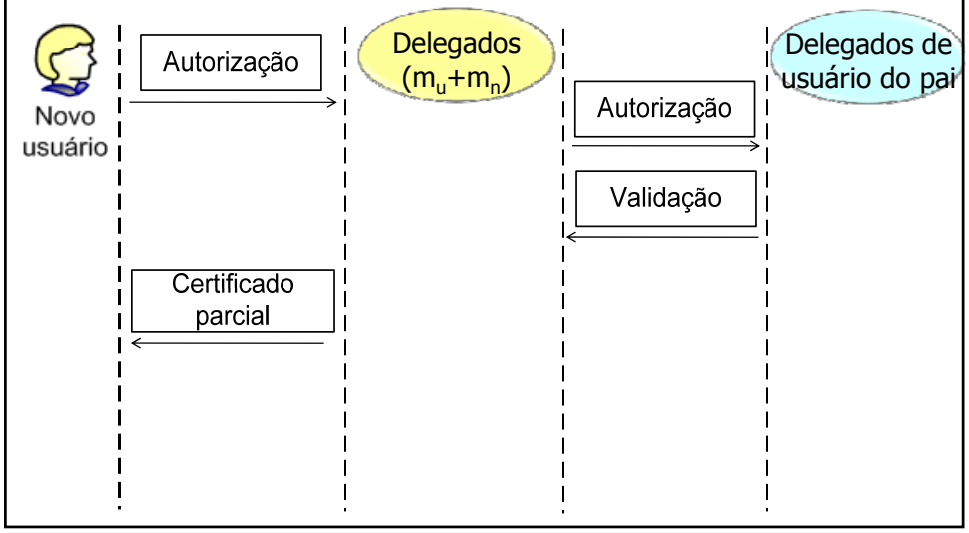


Entrada de Nós – Obtenção do Certificado

GTA / UFRJ



Entrada de Nós – Obtenção do Certificado



Certificados

- Certificado completo
  - Utilização dos serviços da rede
    - Apresentação para os nós na primeira conexão
  - Formação do certificado
    - Mínimo de k_u certificados parciais gerados por delegados de usuário
    - Mínimo de k_n certificados parciais gerados por delegados de nó

Certificado Parcial

ID autorização	Reservado
Chave pública do usuário raiz	
Chave pública do usuário pai	
Validade	
Chave pública do nó	
Chave pública do delegado	
Assinatura do delegado	

Certificados

- Certificado completo
  - Utilização dos serviços da rede
    - Apresentação para os nós na primeira conexão
  - Formação do certificado
    - Mínimo de k_u certificados parciais gerados por delegados de usuário
    - Mínimo de k_n certificados parciais gerados por delegados de nó

Certificado Completo

ID autorização	Reservado
Chave pública do usuário raiz	
Chave pública do usuário pai	
Validade	
Chave pública do nó	
Chave pública do delegado 1	
Assinatura do delegado 1	
...	
Chave pública do delegado k	
Assinatura do delegado k	

Exclusão de Nós

- Exclusão por ausência
  - Detectada pelas delegados ou nós monitorados
    - Troca de pacotes de teste
- Exclusão por mau comportamento
  - Indicada pelos delegados de nó
    - Delegados armazenam e processam informações recebidas
    - Mínimo de k_n votos para exclusão
      - Exclusão de todos os filhos

Monitoramento

- Delegados de nó
  - Cálculo da reputação (R)

$$R_i = R_{i-1} - 1 \longrightarrow \textbf{Ações maliciosas}$$

$$R_i = R_{i-1} + 1 \longrightarrow \textbf{t}_\textbf{a}\textbf{ s sem denúncias}$$

  - Limiar de votação
    - R<L → nó malicioso
    - L variável
      - Impedimento de criação de filhos maliciosos
        - » A cada exclusão de filhos → Punição de todos os ascendentes

-

Monitoramento

- Delegados de nó
  - Cálculo da reputação (R)

$$R_i = R_{i-1} - 1$$

$$R_i = R_{i-1} + 1$$

  - Limiar de votação
    - R<L → nó malicioso
    - L variável
      - Impedimento de criação de filhos maliciosos
        - » A cada exclusão de filhos → Punição de todos os ascendentes

Análise Matemática

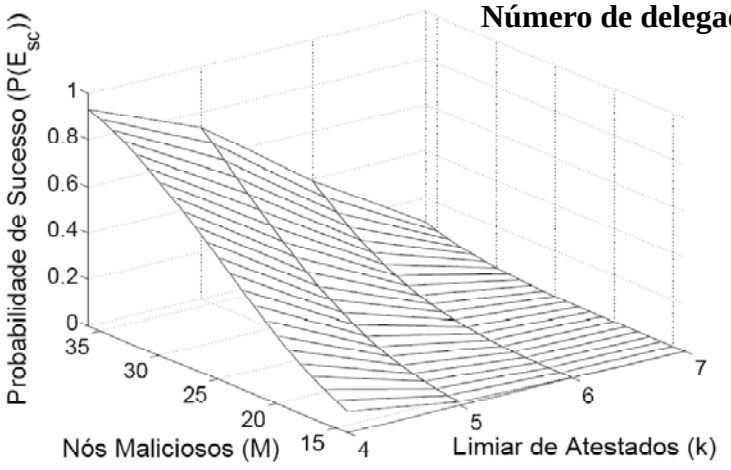
- Casos analisados
  - Sucesso de conluio na votação
    - Robustez a (k_u + k_n) nós maliciosos
    - Tentativa de revogação de certificado de nó não-malicioso

Se $m < M$ e $(N-1-M) \geq (m-k)$

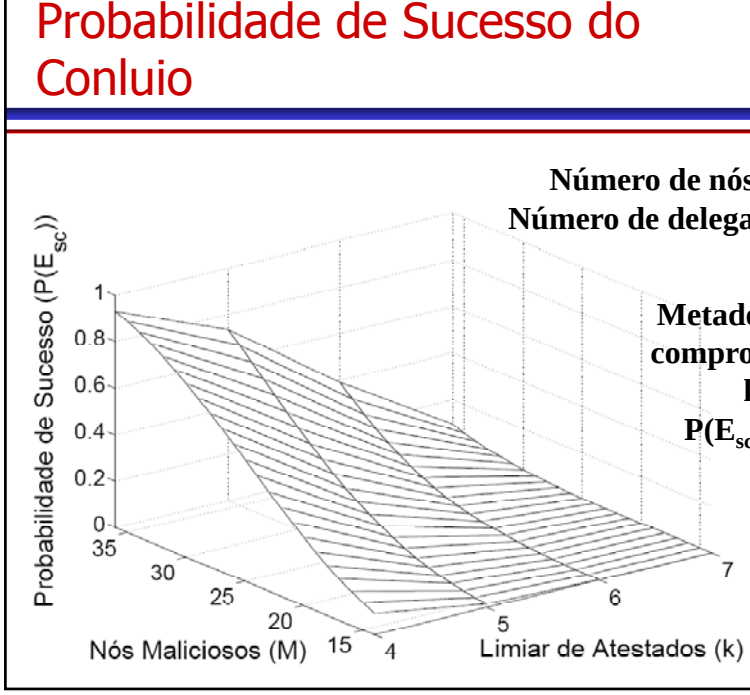
$$P(E_{sc}) = \frac{C_k^M \cdot C_{m-k}^{N-1-M} + C_{k+1}^M \cdot C_{m-k-1}^{N-1-M} \cdots C_m^M \cdot C_{m-m}^{N-1-M}}{C_m^{N-1}}$$

Probabilidade de Sucesso do Conluio

Número de nós (N)= 50
Número de delegados (m) = 7



Probabilidade de Sucesso do Conluio

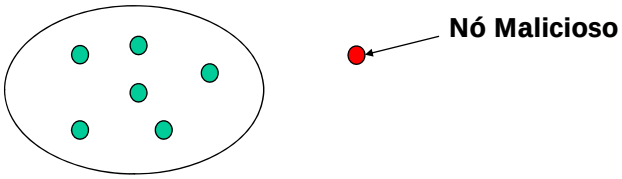


Número de nós (N)= 50
Número de delegados (m) = 7

Metade da redes comprometida → k=7
$P(E_{sc})$=0,005

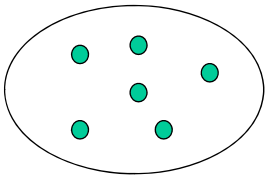
Falsificação de Certificados

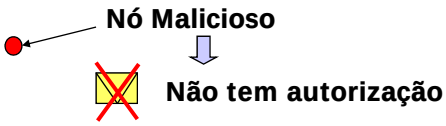
- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado



Falsificação de Certificados

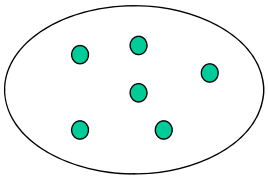
- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado





Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado



Falsificação de Certificados

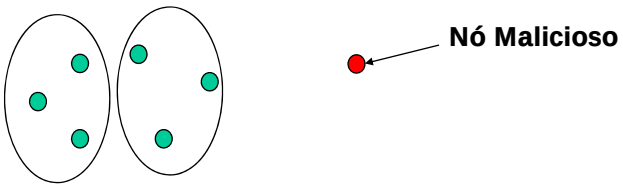
- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado

Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado

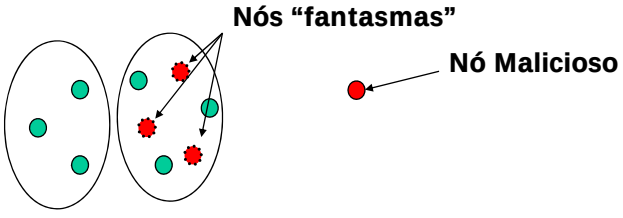
Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado



Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado



Falsificação de Certificados

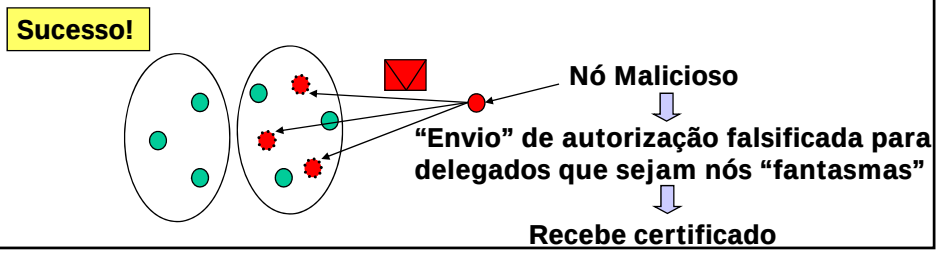
- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado

Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado

Falsificação de Certificados

- AMORA
  - Ausência de verificação de todos os saltos da cadeia
  - Verificação apenas da validade da autorização
  - Falsificação do certificado



Falsificação de Certificados

- Formação de nós "fantasmas"
  - Probabilidade de não-detecção de ausência de nó após partição - $P(E_a)$
    - Ausência de pacotes de testes
      - Ausência
        - » Nó
        - » Delegados de nó e usuário
        - » Nós monitorados
        - » Novos nós monitorados

          Reorganização dos conjuntos de delegados

Falsificação de Certificados

- Formação de nós "fantasmas"
  - Probabilidade de não-detecção de ausência de nó após partição - $P(E_a)$
    - Ausência de pacotes de testes
      - Ausência
        - » Nó
        - » Delegados de nó e usuário
        - » Nós monitorados
        - » Novos nós monitorados
          - Reorganização dos conjuntos de delegados
- Supondo
  - Número de delegados =7
  - Número de nós na rede (N) =50
  - Número de nós na partição (P) =N/7~7

$\Rightarrow P(E_a) \approx 10^{-8}$

Falsificação de Certificados

- Formação de nós "fantasmas"
  - Probabilidade de não-detecção de ausência de nó após partição - $P(E_a)$
    - Ausência de pacotes de testes
      - Ausência
        - » Nó
        - » Delegados de nó e usuário
        - » Nós monitorados
        - » Novos nós monitorados
          - Reorganização dos conjuntos de delegados
- Supondo
  - Número de delegados =7
  - Número de nós na rede (N) =50
  - Número de nós na partição (P) =N/7~7

$\Rightarrow P(E_a) \approx 10^{-8}$

$\Downarrow$

Desprezível

Conclusões

- Redes ad hoc
  - Controle de acesso distribuído
    - Autorização
    - Autenticação
    - Monitoração e exclusão de nós maliciosos
  - Dificuldades
    - Ausência de administrador centralizado
    - Impedimento de entrada de nós maliciosos
- Sistema proposto
  - Administrador distribuído
    - Cadeia de delegação
  - Certificação, monitoramento e exclusão de nós
    - Delegados

Conclusões

- AMORA
  - Robusto contra a entrada de nós maliciosos
    - Baixa probabilidade de sucesso de conluio mesmo com metade da rede comprometida
    - Impossibilidade de falsificação de certificado por nó externo
  - Alta disponibilidade
    - Ausência de pontos centrais
    - Flexibilidade na inicialização
    - Tratamento de partições
  - Auto-organizável e flexível
    - Adequação às características das redes ad hoc

POLI - Escola Politécnica
COPPE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro

Controle de Acesso Auto-Organizável e Robusto Baseado em Nós Delegados para Redes Ad Hoc

Natalia Castro Fernandes e Otto Carlos M. B. Duarte

VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais
Gramado, setembro de 2008