Um controle de associações resistente a ataques Sybil para a disseminação segura de conteúdo da IoT

Danilo Evangelista, Eduardo da Silva, Michele Nogueira, Aldri Santos

Universidade Federal do Paraná - Instituto Federal Catarinense

1 Introdução

- A necessidade por serviços personalizados e autônomos tem possibilitado o desenvolvimento da Internet das Coisas (IoT).
- IoT permite que objetos estejam conectados com as pessoas em qualquer momento e lugar.
- IoT proporciona conforto e bem estar.
- Disseminação de conteúdo é a base da IoT.
- Segurança dos dados?

1 Introdução

- Dentre as possíveis ações maliciosas, o estudo destaca o ataque Sybil.
  - Atacante Sybil forja identidades para ter acesso à rede e a disseminação de dados.
  - Atacante busca recursos não autorizados, infligindo confidencialidade e privacidade dos usuários.
- Qualidade dos serviços afetada.
- Segurança dos dados é comprometida.

1 Introdução

- Origem do nome:
  - Nome proposto por Brian Zill em um artigo publicado em 1 de janeiro de 2002.
  - Livro Sybil de Flora Reta Schreiber.
    - Livro retrata o estudo de uma mulher com transtorno dissociativo de identidade.

1 Introdução

- Três possíveis técnicas para detectar ataques Sybil:
  - Baseadas nas características da rede.
  - Criptografia.
  - Relacionamento entre vizinhos.

1 Introdução

- Três possíveis técnicas para detectar ataques Sybil:
  - Baseadas nas características da rede:
    - Nós e RSS.
    - Mobilidade.
    - Não é considerado eficiente contra ataque Sybil.

1 Introdução

- Três possíveis técnicas para detectar ataques Sybil:
  - Criptografia:
    - Uso de par de chaves simétricas e assimétricas.
    - Necessita de constante atualização do par de chaves assimétricas.
    - Sobrecarga da rede.

1 Introdução

- Três possíveis técnicas para detectar ataques Sybil:
  - Relacionamento entre vizinhos:
    - Considera as opiniões sobre um nó emitidas pelos vizinhos.
    - Nó malicioso.

1 Introdução

- SA²CI – *Sybil Attack Association Control for IoT*
  - *Middleware* que atua entre Rede e Aplicação.
  - Criptografia de curvas elípticas.
    - Distribuição de chaves a baixo custo computacional.
    - Criação de canais seguros entre dispositivos heterogêneos.
  - Aplica funções não clonáveis (PUF).
    - Funções extraídas do hardware dos dispositivos.

2 Trabalhos Relacionados

- As técnicas empregadas na literatura geralmente são ineficazes à IoT.
- Estudam o uso de redes em geral.
- IoT requer soluções leves, dinâmicas e eficientes.

2 Trabalhos Relacionados

- Lightweight Sybil Attack Detection (LSD) [Abbas et al. 2013].
  - Solução leve e dinâmica, emprega a técnica de características da rede.
  - Um conjunto de dispositivos verifica uma nova associação na rede.
  - Um dos participantes armazena o RSS e a identidade em uma tupla.
  - Abordagem falha. Ignora a irretratabilidade das identidades.

2 Trabalhos Relacionados

- Curvas elíplticas [Mahalle et al. 2012, Chatzigiannakis et al. 2011]
  - Promove um canal seguro de comunicação.
  - Baixo custo para gerar pares de chaves.
  - Garantia da identidade dos dispositivos.
    - Recibo de identidade.
      - Função não clonável (PUF) [Choden Konigsmark et al. 2014, Zheng and Potkonjak 2014].
      - Recibo de identidades [Wu et al. 2008].

3 Mecanismo contra Ataque Sybil - SA²Ci

- Modelo da rede e do ataque
  - Camada de Rede
    - Encaminhamento de dados entre nós.
  - Camada de Aplicação
    - Troca de chaves.
  - Trabalha com nós com ou sem restrição de recursos.

3 Mecanismo contra Ataque Sybil - SA²Ci

- Modelo da rede e do ataque
  - A rede IoT é composta por um conjunto n de nós.
    - N={N1, N2,...Nn}.
    - NL.
    - Ns.
  - Restrições
    - Nkdc
    - Nmov

3 Mecanismo contra Ataque Sybil - SA²Ci

- Modelo da rede e do ataque
  - Transmissão sem fio padrão 802.15.4.
  - Canal assíncrono sujeito a perda de pacotes.

3 Mecanismo contra Ataque Sybil - SA²Ci

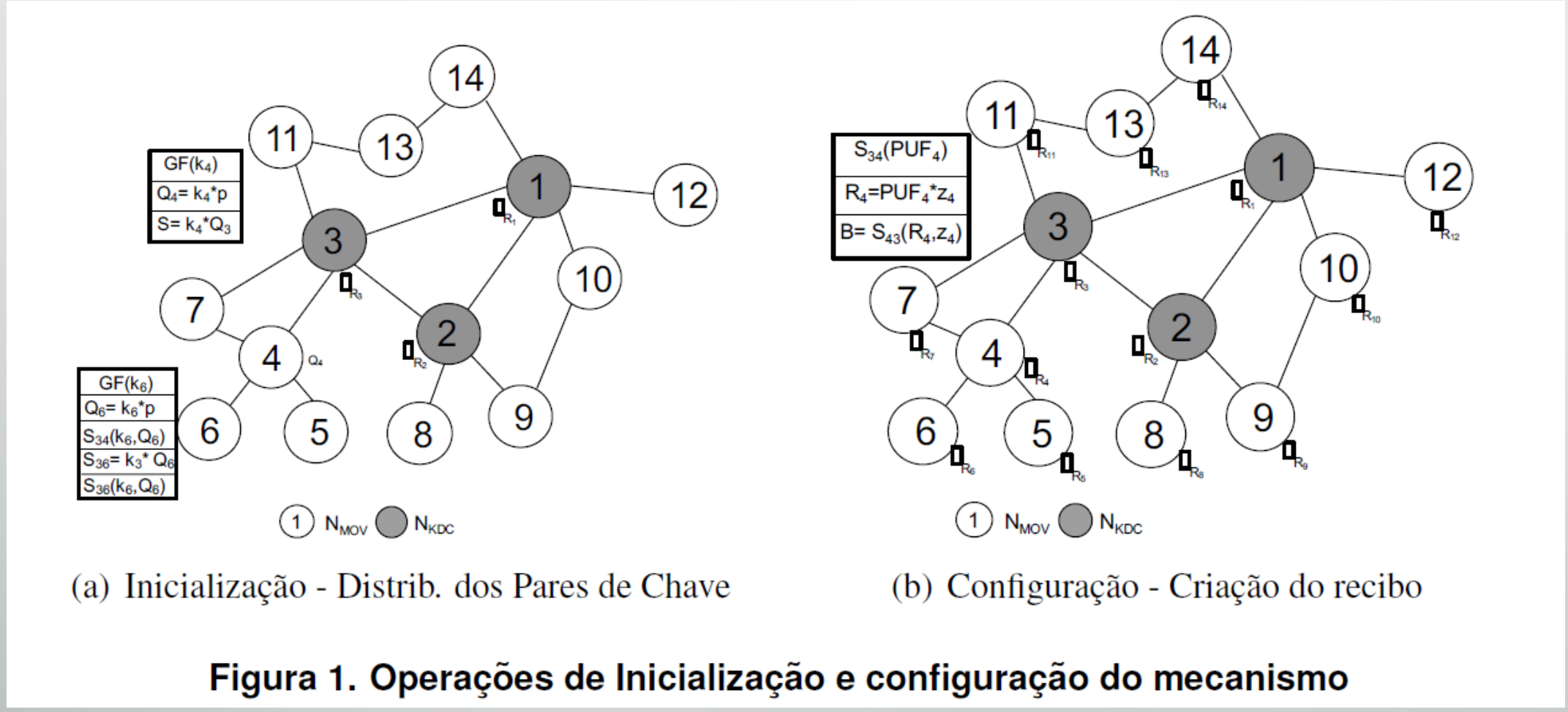
- Modelo da rede e do ataque
  - Ataque Sybil
    - Um nó adversário cria ou rouba identidades de nós legítimos.
    - Duas formas de ataque:
      - Churn.
      - Múltiplas identidades.

3 Mecanismo contra Ataque Sybil - SA²Ci

- Modelo da rede e do ataque
  - Churn
    - Um nó adversário possui apenas uma identidade falsa.
    - Busca promover o esgotamento de recursos.
  - Múltiplas Identidades
    - Um único atacante com várias identidades.

3 Mecanismo contra Ataque Sybil - SA²Ci

- Mecanismo de controle de associações para IoT – SA²CI
  - Nós sem restrição formam uma rede KDC de forma autônoma.
  - Formam uma curva elíptica e trocam as características.
  - Fase de configuração.
    - Emitem chaves públicas e privadas.
    - Nós computam suas PUF e enviam aos KDC.



(a) Inicialização - Distrib. dos Pares de Chave

(b) Configuração - Criação do recibo

Figura 1. Operações de Inicialização e configuração do mecanismo

3 Mecanismo contra Ataque Sybil - SA²Ci

- Configuração da rede
  - Visa estabelecer os pares de chaves entre Nmov e Nkdc.
  - Nkdc geram os pares de chaves para seus respectivos Nmov.
  - Nkdc gera um segredo para cada Nmov.
  - Nmov calcula seu PUF.
  - Nkdc cifra o recibo.

3 Mecanismo contra Ataque Sybil - SA²Ci

- Gerência de disseminação
  - Reassociação.
  - Pedido de nova associação.
    - Monitoram comportamento malicioso.
      - Entrar e sair da rede mudando de identidade.
      - Exibir múltiplas identidades.

4 Avaliação

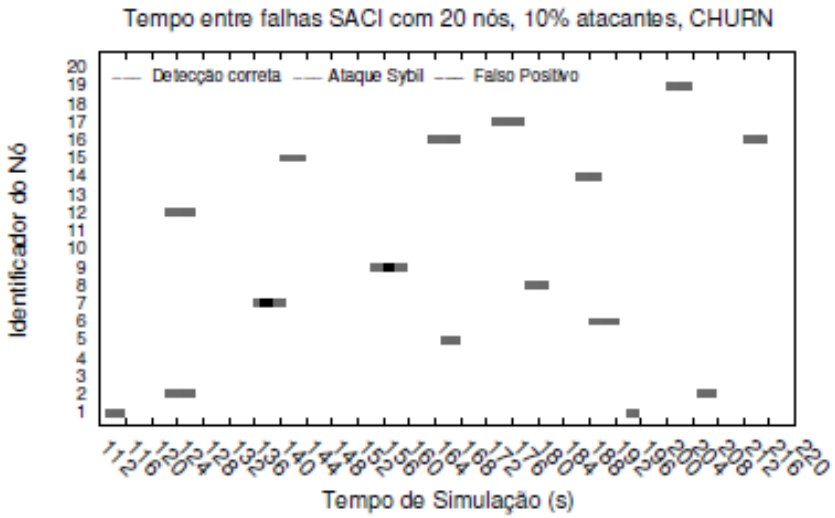
- SA²CI foi avaliado e comparado com LSD.
  - Implementados em um simulador NS3.
    - Funções PUF, medições de consumo, curvas elípticas.
  - Ataques Sybil.
  - Cenário Residencial.
  - Mensagens de 127 bytes.
    - 6LowPAN.
  - Nós atacantes com Id forjadas.
    - Churn e Múltiplas Identidades.

Tabela 1. Parâmetros dos Nós

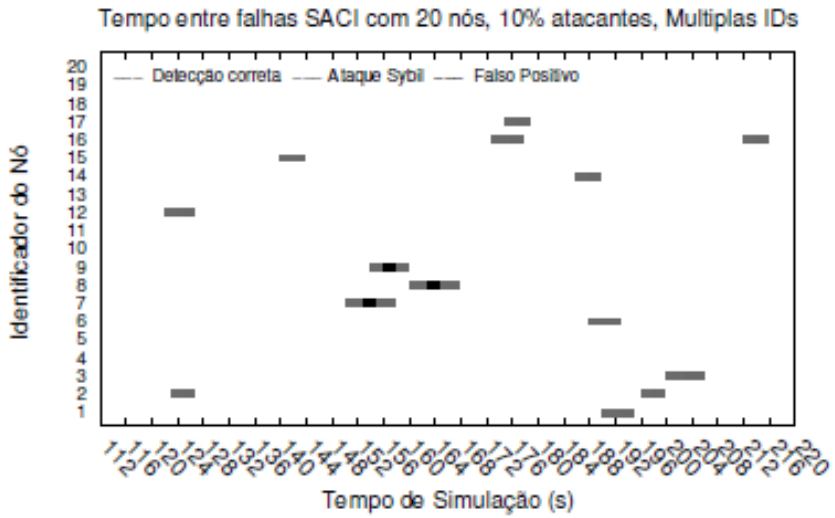
Parâmetro	Valores
Área	$25m$x$25m$
Qtd. de nós	20,40,60
Raio de alcance	$10m$ (KDC) e $100m$ (MOV)
Mod. de mobilidade	Random Waypoint
Vel. dos nós	0,2m/s a 2m/s
Tempo de simulação	600 s

Tabela 2. Parâmetros da Rede e do Ataque

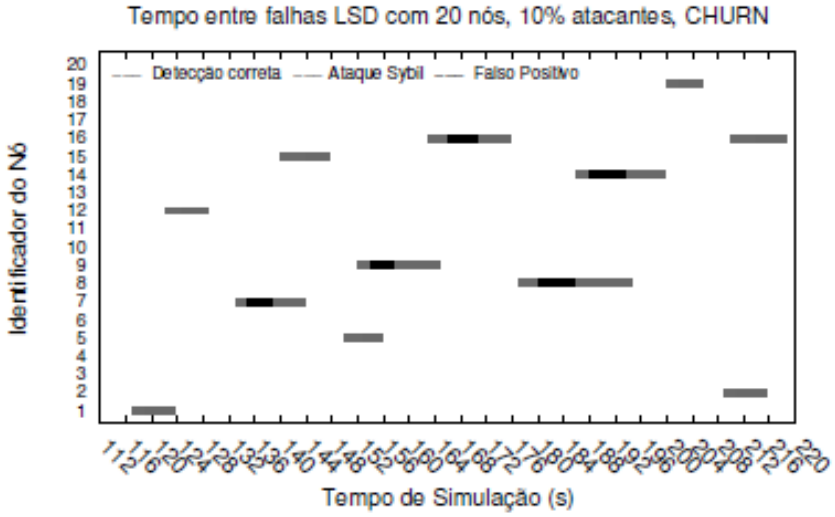
Parâmetro	Valores
Tipo do pacote	UDP
Protoc. de roteamento	RPL
Período transiente	40s
Protoc. de enlace	IEEE 802.15.4
Nós Sybil	10%
Quant. Múltiplas IDs	1 a 5



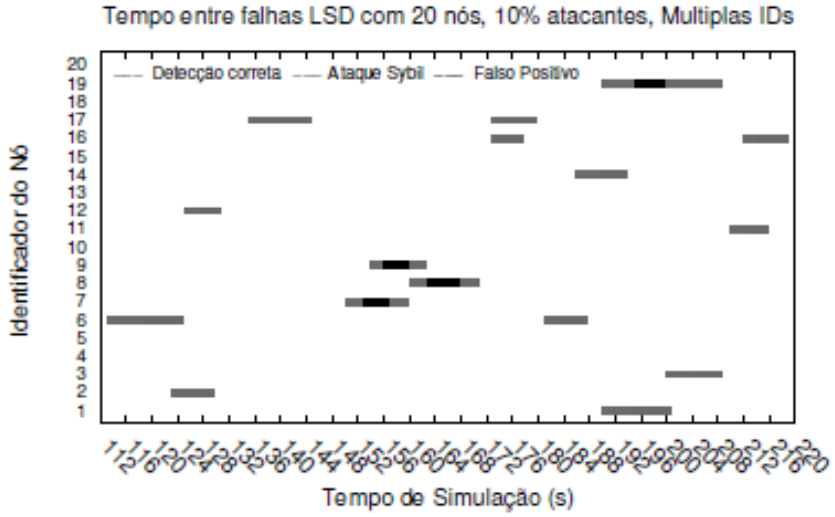
(a) Fabricada



(b) *Roubada*



(c) Fabricada



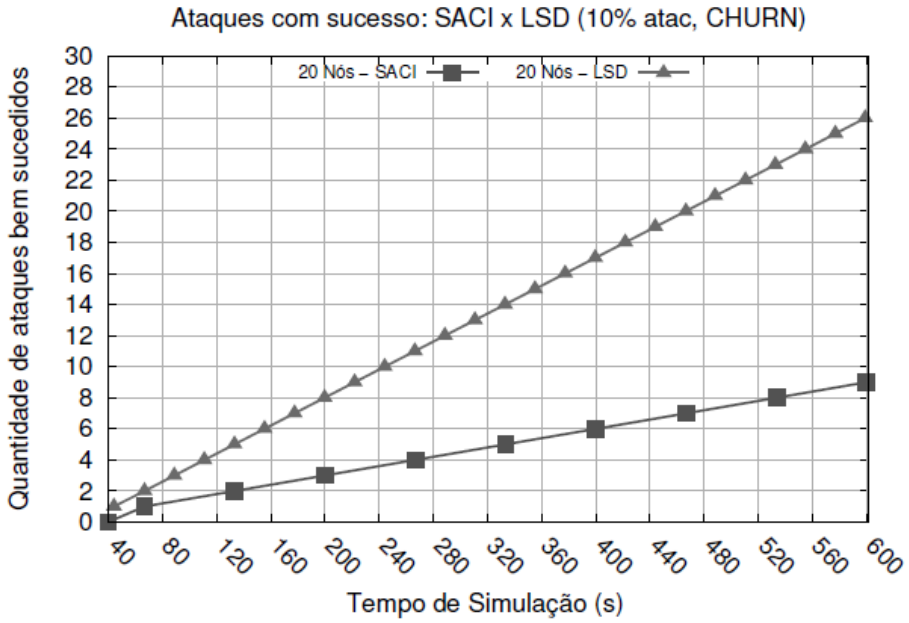
(d) *Roubada*

Tabela 3. Tempo entre falhas e recuperação do SA^2CI e LSD

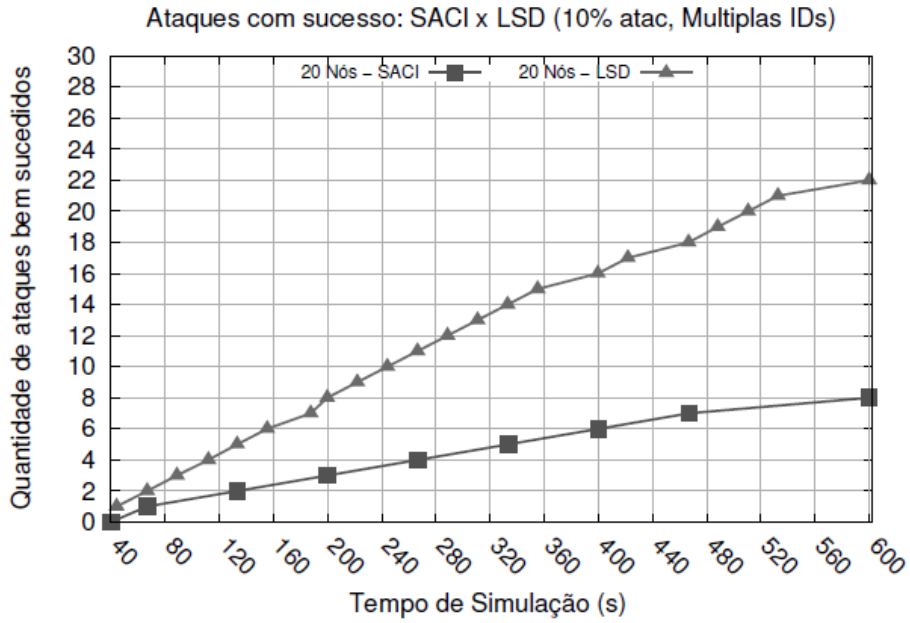
Qtd. Nós	MTBF – SA^2CI	MTTR – SA^2CI	MTBF – LSD	MTTR – LSD
20	66.7 s	2.3 s	22.2 s	5.566 s
40	69.3 s	2.5 s	23.4 s	5.89 s
60	70.1 s	2.5 s	24.2 s	5.93 s

4 Avaliação

- SA²CI 9 ataques com sucesso.
- LSD. 29 ataques com sucesso.

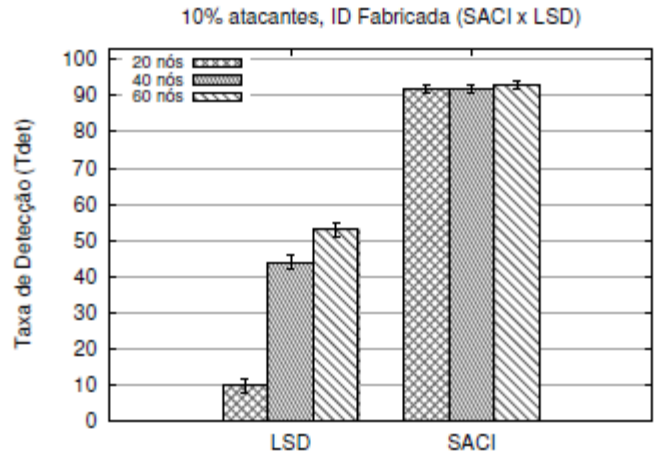


(a) *Churn*

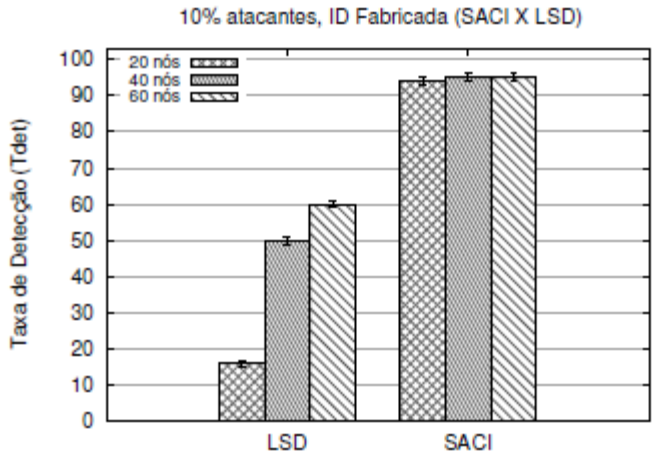


(b) Múltiplas Identidades

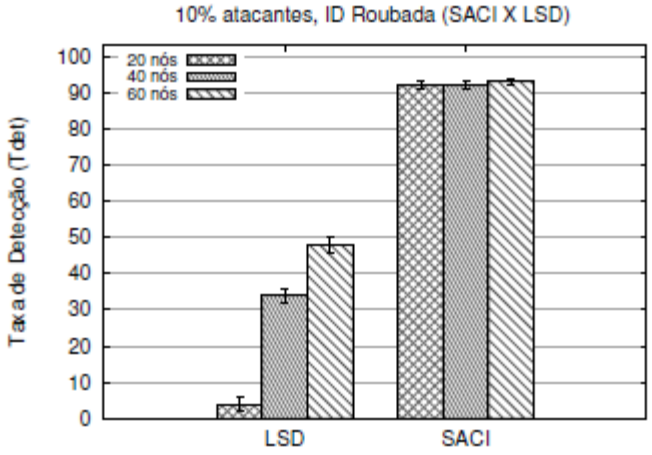
4 Avaliação



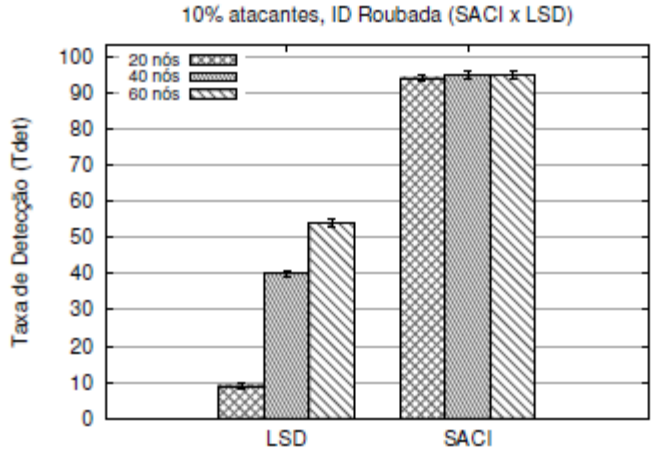
(a) Churn



(b) *Múltiplas Identidades*



(c) Churn



(d) *Múltiplas Identidades*

5 Conclusão

- O trabalho apresentou um mecanismo SA²CI para controle de associações resistente a ataques Sybil.
- Leva em conta a heterogeneidade computacional.
- Eficácia comprovada quando comparado ao LSD.
- Trabalhos futuros
  - Avaliação em domínios maiores.