

SOS: Sensoriamento Overlay Seguro em Redes de Sensores Sem Fio Hierárquicas

Leonardo B. Oliveira, A.A.F. Loureiro,

Ricardo Dahab, Hao Chi Wong

UNICAMP, UFMG, PARC

Agenda

- Introdução
- Solução
- Simulação
- Resultados
- Conclusão

Roteamento

- Protocolos de roteamento projetados p/ eficiência e escalabilidade
 - Inviabilizou o uso de algoritmos sofisticados
 - Na prática, a maioria das técnicas
 - Emprego de **métricas fixas e simples** p/ seleção de rotas
 - Rotas alternativas **ignoradas**

Rede Overlay

- Rede lógica sobre uma rede física subjacente
- Função: **migrar** parte da **complexidade** de roteamento **p/** a camada de **aplicação**
- Monitoram a rede e fornecem caminhos alternativos aos usuários

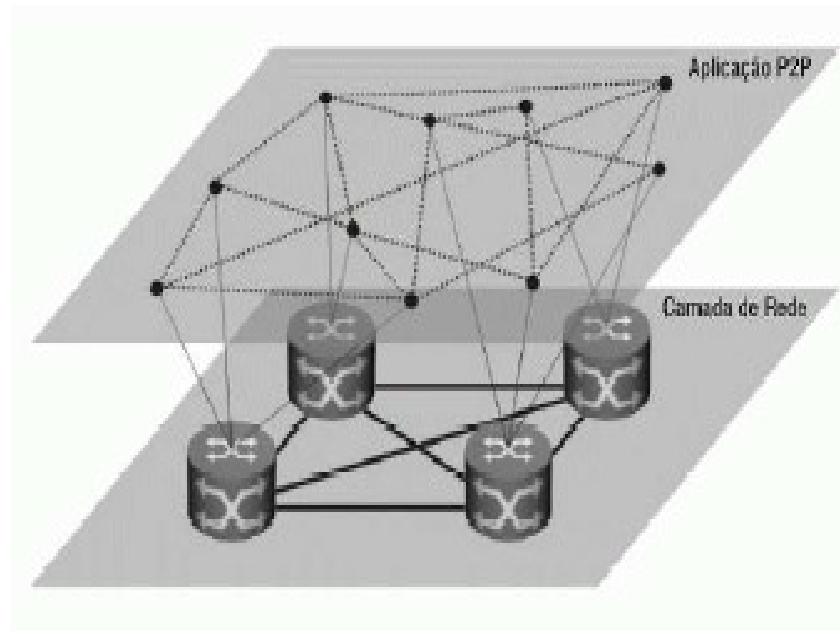
Rede Overlay

- Rede lógica sobre uma rede física subjacente
- Função: migrar parte da complexidade de roteamento p/ a camada de aplicação
- Monitoram a rede a fornecem caminhos alternativos aos usuários - **Como?**

Rede Overlay

- Rede lógica sobre a rede física subjacente
- Função: migrar parte da complexidade de roteamento p/ a camada de aplicação
- Monitoram a rede a fornecem caminhos alternativos aos usuários - **Como?**
 - Nós estabelecem enlaces alternativos para efetuar a comunicação
- Ex. redes P2P, CDNs e MBones

Redes Overlay

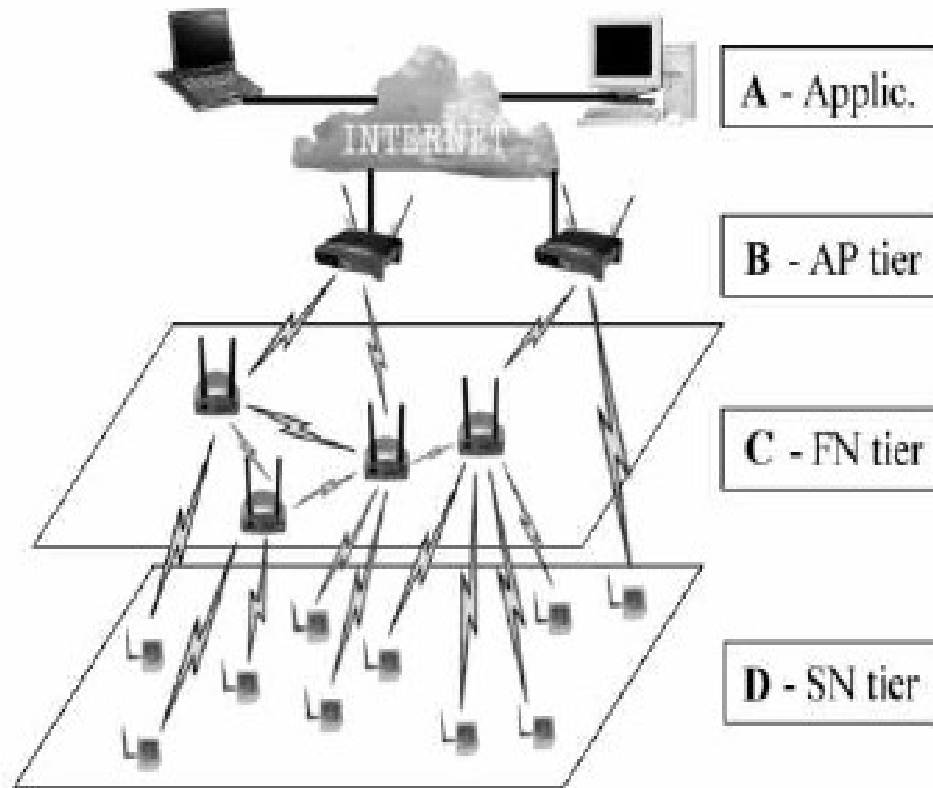


RO: ilustração

Redes de Sensores Sem Fio

- Redes de Sensores Sem Fio (RSSFs)
 - São uma classe de redes *ad hoc*
 - Formadas por nós sensores de recursos extremamente limitados
 - Ex. Mica motes: 4 KB RAM, 7.8 MHz CPU
 - Empregadas em uma grande gama de aplicações:
 - Ex. operações de resgate em desastres e detecção de exploração ilegal de recursos

RSSFs Hierárquicas



Objetivos

- Avaliar o uso de ROs p/ transmissão segura de dados em RSSFs Hierárquicas
 - Mitigar os efeitos de ataques DoS
 - buraco negro (*blackhole*)
 - repasse seletivo (*selective forwarding*)
 - Aumentar a taxa de entrega de mensagens que carregam informações sensíveis
- (até onde sabemos) 1ª solução baseada em ROs p/ RSSFs

Trabalhos Correlatos

- D. Andersen, *Resilient Overlay Networks* (2001)
- Ganesan et alli, *Highly-resilient, energy-efficient multipath routing in wireless sensor networks* (2001)
- Deng et alli, *A performance evaluation of intrusion-tolerant routing in wireless sensor networks* (2003)
- Oliveira et alli, *LHA-SP: Secure Protocols for Hierarchical WSNs* (2005)

Agenda

- Introdução
- Solução: SOS (nossa proposta)
- Simulação
- Resultados
- Conclusão

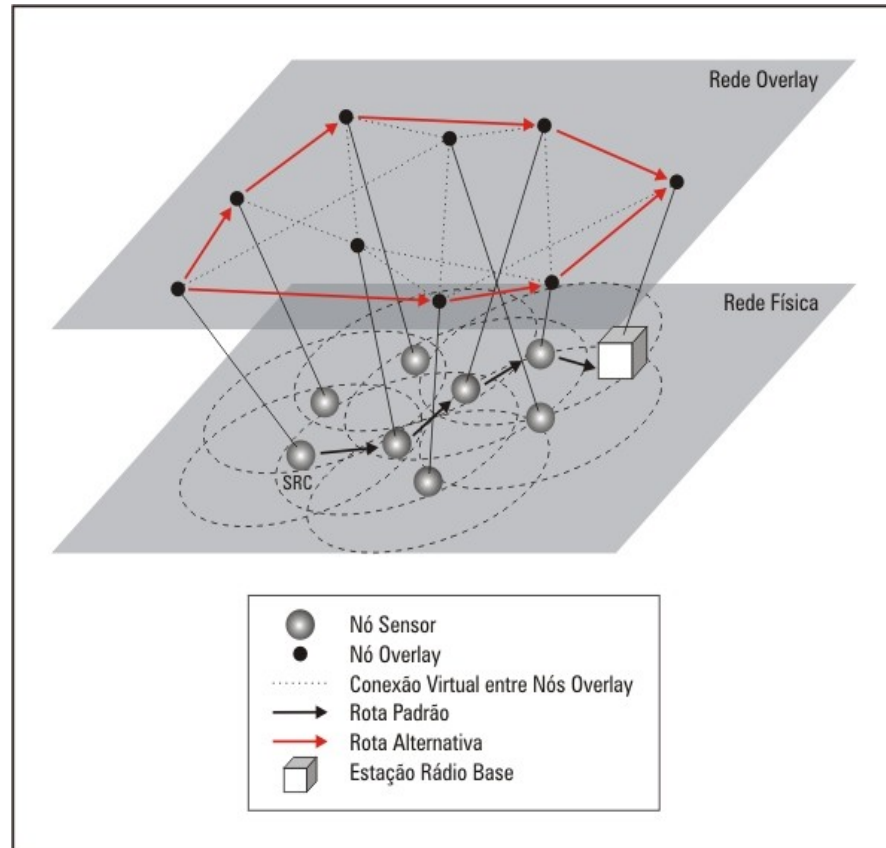
Modelo de Rede

- Redes hierárquicas e heterogêneas dirigidas a relógio
- Msgs de sensoriamento classificadas em prioritárias (MPs) e não prioritárias (MNs)
 - **MPs contêm informação sensível**
- Nós sensores comuns enviam dados p/ o CH via single-hop, que reencaminha à BS via um caminho *multi-hop*
- Estação Rádio Base (ERB) é confiável

Visão Geral

- SOS: Sensoriamento Overlay Seguro
 - Constrói uma RO sobre a RSSF subjacente
 - MNs possuem a dupla função de monitorar rotas e enviar dados
 - MPs trafegam por rotas (overlay) mais seguras
 - Taxa de entrega de MPs à ERB aumenta

SOS



Nó SRC conta c/ rotas overlay, além da rota padrão, p/ envio de dados

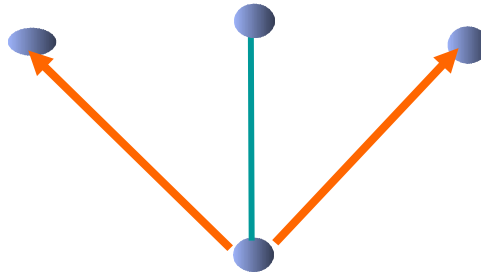
Solução

Construção da RO

- Alguns nós são escolhidos p/ compor a RO
- P/ cada um é atribuída uma lista de vizinhos lógicos (ex. dois)
- Tais vizinhos são usados como intermediários em rotas alternativas à rota padrão

Solução

Funcionamento



- Inicialmente, CHs alternam (round robin) o envio de MNs entre as 3 rotas possíveis
 - Rota padrão (usa vizinho estab. pelo rot.)
 - Overlay #1 (usa vizinho overlay #1)
 - Overlay #2 (usa vizinho overlay #2)
- MPs são enviadas através da rota padrão
- Tipos de msgs/rotas identificadas c/ *flags*

Solução

- A ERB identifica então as *melhores rotas*, usando
 - Granularidade do envio nós->BS (epoch)
 - Registro da taxa de entrega de MNs

nó sensor	taxa de entrega de rotas		
	padrão	overlay #1	overlay #2
1	76%	54%	65%
2	70%	78%	73%
3	31%		39%
4	55%	82%	97%
5	83%	89%	42%

Solução

- BS divulga aos CHs suas respectivas melhores rotas
 - CHs utilizam a rota as melhores rotas sempre que forem enviar MPs

Solução

- BS divulga aos CHs suas respectivas melhores rotas
 - CHs utilizam a rota as melhores rotas sempre que forem enviar MPs
- **SOS não replica msgs** p/ efetuar a monitoração
 - Tira proveito de msgs que não carregam informação sensível

SOS: resumo de políticas

classe da mensagem	Inicialmente		Após divulgação de melhor rota	
	envio	repasse	envio	repasse
prioritária	padrão	padrão	melhor rota	melhor rota
não prioritária	alternado	padrão	alternado	padrão

Nota

- Dois aspectos de segurança
 - Adversários podem
 - Usar a divulgação de melhores rotas p/ inferir por onde MPs trafegarão
 - Tirar proveito dos *flags* que identificam as msgs
- Solução
 - Empregar o SOS juntamente c/ soluções criptográficas que fornecem autenticação e sigilo a comunicação (ex. SecLEACH)

Agenda

- Introdução
- Solução
- Simulação
- Resultados
- Conclusão

Simulação

- Simulação
 - Comparação de uma rede c/ e sem o SOS
- Simulador
 - Network Simulator (ns-2)
- A arquitetura da rede
 - Rede hierárquica e heterogênea
 - *One-hop downlink, multi-hop uplink*
- Protocolo de roteamento
 - Similar ao TinyOS beaconing - árvore contruída a partir da BS c/ busca em largura

Simulação

- Tamanhos de msgs
 - 30 e 36 bytes p/ as redes c/ e sem o SOS, resp.
 - Delta entre um MAC e CRC (MAC-CRC)
- Duração
 - Duração 1000s c/ *epoch* de 10s
- Escolha de vizinhos overlay
 - +ou- aleatoriamente dentre os CHs vizinhos
 - Mecanismo p/ evitar *loops*

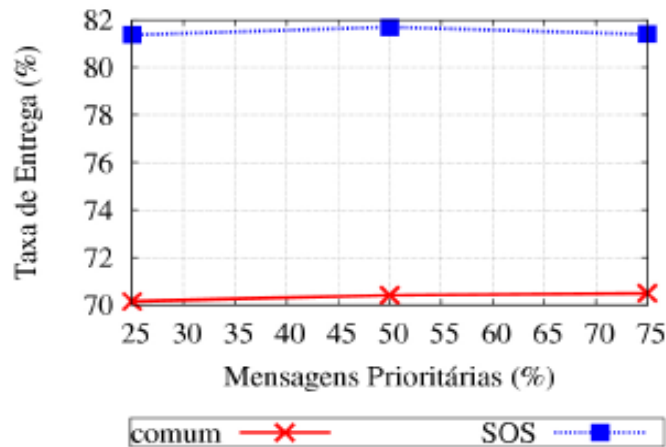
Simulação

- Modelo de Ataque
 - Aleatório dentre os nós CHs
- Parâmetros variados
 - % de msgs prioritárias (padrão: 25%)
 - % de CHs atacados (padrão: 25%)
 - Tamanho da rede (padrão: 1100)
- Métricas
 - Taxa de entrega (ganho)
 - Energia consumida (custo)
 - Energia/msg entregue (eficiência):

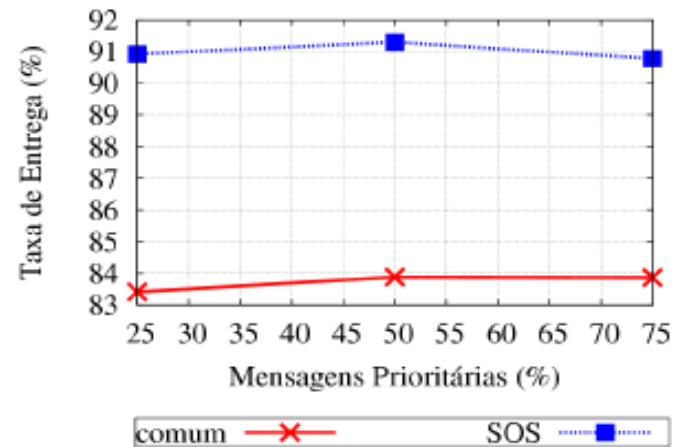
Agenda

- Introdução
- Solução
- Simulação
- Resultados
- Conclusão

% de msgs prioritárias



(a) buraco negro



(b) repasse seletivo

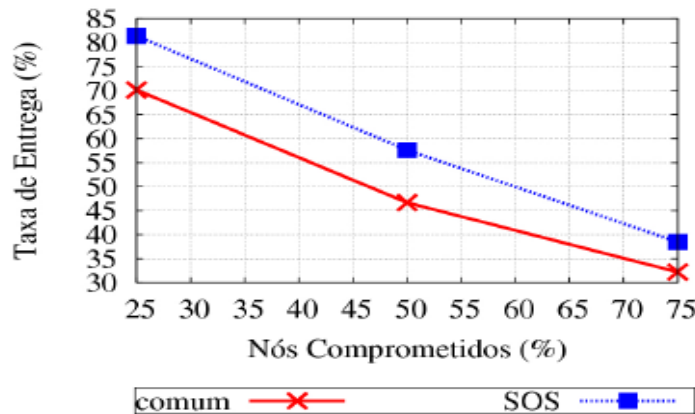
- Ganho mais ou menos estável
 - 11% p/ o ataque buraco negro
 - 7% p/ o ataque de repasse seletivo

% de msgs prioritárias

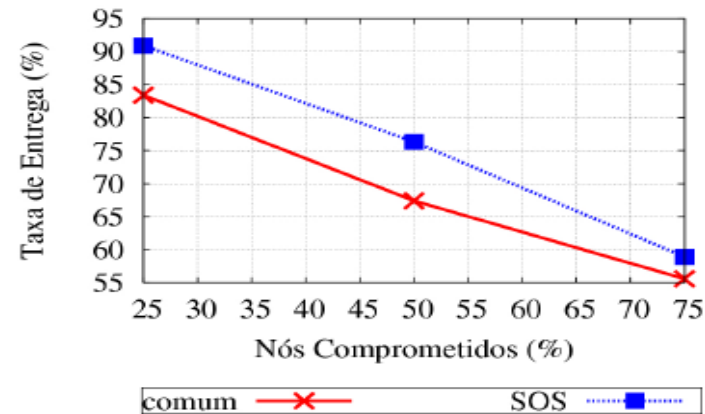
mensagens prioritárias	buraco negro			repasse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
25%	43%	24%	7%	50%	26%	16%
50%	44%	25%	7%	54%	27%	16%
75%	44%	25%	8%	55%	27%	17%

- Por CH: considerável
- Geral: aceitável
 - Overhead dos CHs é **amortizado** entre todos os nós
- Por msg: eficiente
 - 7% buraco negro
 - 16% repasse seletivo

% de CHs comprometidos



(a) buraco negro



(b) repasse seletivo

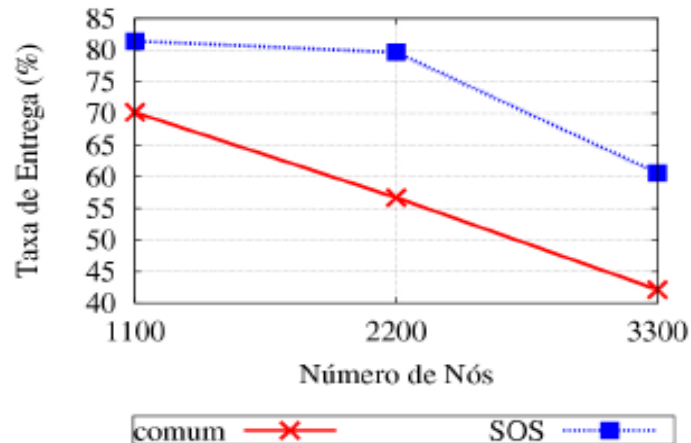
- Ganho cai c/ aumento de nós comprometidos
(**difículdade de se encontrar rotas não comprometidas**)
 - 7% e 11% de ganho no buraco negro
 - 7,5 e 9% de ganho no repasse seletivo

% de CHs comprometidos

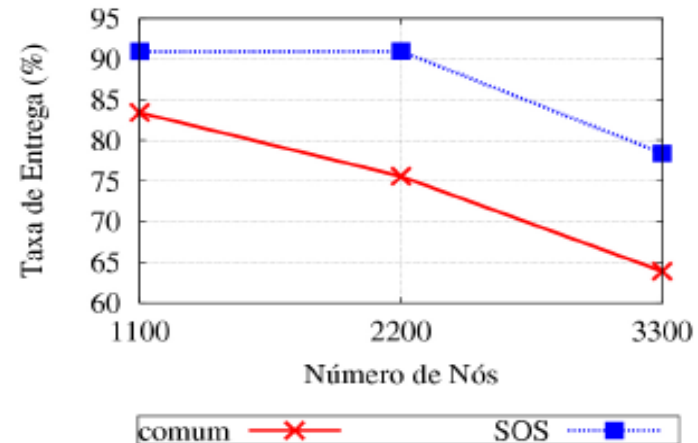
nós comprometidos	buraco negro			repassse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
25%	43%	24%	7%	50%	26%	16%
50%	32%	22%	-1%	45%	24%	9%
75%	26%	21%	1%	31%	21%	15%

- *Overhead* diminui c/ o aumento de nós comprometidos
 - < ganho do SOS, < o delta no tráfego de msgs
- Por CH: entre 26 e 50%
- Geral: entre 21 e 26%
- Por msg: chegou a ser negativo p/ o buraco negro

Tamanho da rede



(a) buraco negro



(b) repasse seletivo

- Queda na taxa de entrega c/ aumento da rede
 - Prob. de uma mgs ser descartada aumenta
- Ganho
 - 11 a 23% p/ o buraco negro
 - 7,5 a 15,5% p/ o repasse seletivo

Tamanho da rede

número de nós	buraco negro			repassse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
1100	43%	24%	7%	50%	26%	16%
2200	51%	27%	-10%	53%	28%	6%
3300	41%	25%	-13%	56%	29%	5%

- Por CH: entre 41 e 56%
- Geral: entre 24 e 29%
- Por msg: novamente chegou a ser negativo p/ o buraco negro

Agenda

- Introdução
- Solução
- Simulação
- Resultados
- Conclusão

Conclusão

- Estudo pioneiro na aplicação de ROs p/ oferecer segurança em RSSFs
- A solução possibilita ganho no número de msgs prioritárias
- Custo-benefício em termos de energia bom p/ a maioria das aplicações

Trabalhos Futuros

- Identificar o intervalo de monitoração ideal p/ um dado cenário
 - Uma MN a cada qtos segundos?
- Investigar número ideal de rotas overlay (alternativas) atribuídas por nó
 - Dois, três ou quatro rotas por nó?
- Avaliar a eficácia da solução para melhorar métricas de QoS da rede:
 - atraso e *jitter*

Perguntas

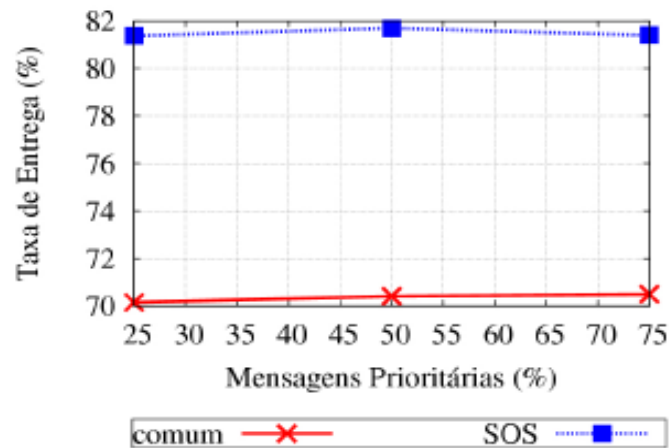
leob@ic.unicamp.br

Obrigado!

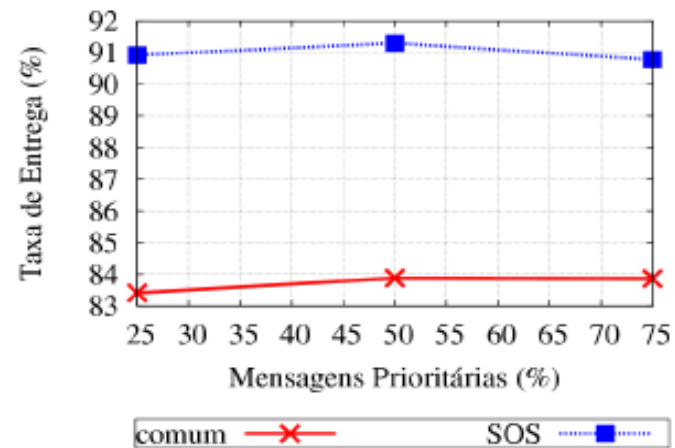
Overhead

- Nós comuns
 - Se deve principalmente à adição de MACs
- CHs (nós *overlay*)
 - Se deve
 - Aumento do tráfego de msgs
 - Aumento do número médio por *hops*
 - MACs
- Não existem msgs redundantes
 - Monitoração efetuada por msgs já existentes

% de msgs prioritárias



(a) buraco negro

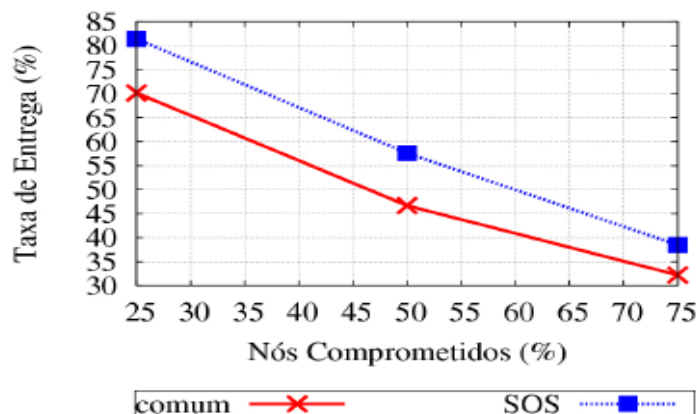


(b) repasse seletivo

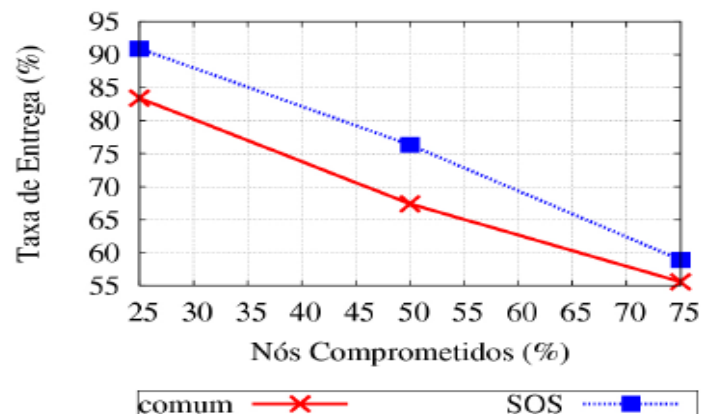
jljl

mensagens prioritárias	buraco negro			repasse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
25%	43%	24%	7%	50%	26%	16%
50%	44%	25%	7%	54%	27%	16%
75%	44%	25%	8%	55%	27%	17%

% de CHs comprometidos



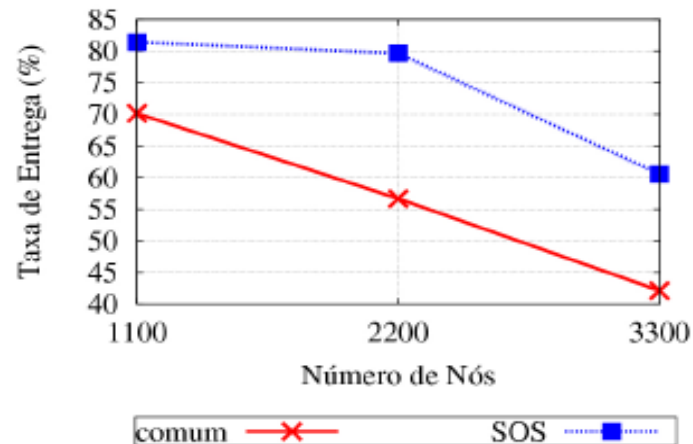
(a) buraco negro



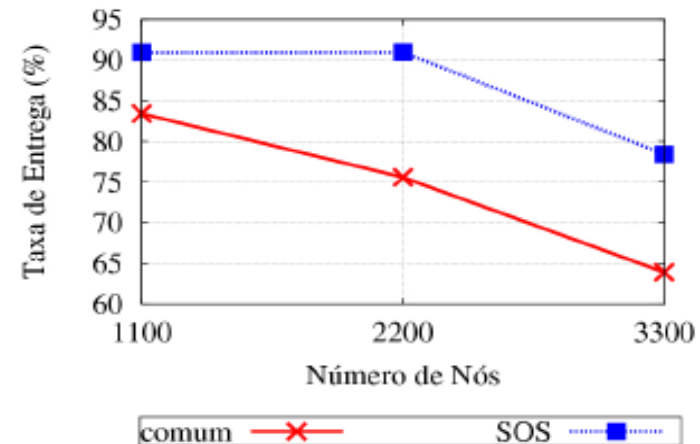
(b) repasse seletivo

nós comprometidos	buraco negro			repasse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
25%	43%	24%	7%	50%	26%	16%
50%	32%	22%	-1%	45%	24%	9%
75%	26%	21%	1%	31%	21%	15%

Tamanho da rede



(a) buraco negro



(b) repasse seletivo

número de nós	buraco negro			repassse seletivo		
	CH	geral	por mensagem	CH	geral	por mensagem
1100	43%	24%	7%	50%	26%	16%
2200	51%	27%	-10%	53%	28%	6%
3300	41%	25%	-13%	56%	29%	5%

Registro na ERB

nó sensor	taxa de entrega de rotas		
	padrão	overlay #1	overlay #2
1	76%	54%	65%
2	70%	78%	73%
3	31%		39%
4	55%	82%	97%
5	83%	89%	42%

Em destaque as “melhores rotas”, calculadas por meio de MNs