Sistemas Cooperativos Geo-distribuídos para Monitoramento de Redes Sem-fio

Prof. Miguel Elias Mitre Campista

Monitoramento de Redes Sem-fio

- Uso de farejadores de tráfego
  - Capturam todos os pacotes enviados na rede
- Problemas do meio sem-fio afetam o monitoramento
  - Nem todos os pacotes são capturados

1. Sammarco, M., Campista, M. E. M., and Amorim, M. D. - "*Trace Selection for Improved WLAN Monitoring*", in 5th ACM HotPlanet Workshop, pp. 9-14, Hong Kong, China, August 2013.

2. Campista, M. E. M., Sammarco, M., Amorim, M. D., and Razafindralambo, T. - "*Monitoramento Colaborativo de Redes Sem-fio: Acurácia do Sistema e Denúncia de Farejadores Maliciosos*", in XIV Workshop em Desempenho de Sistemas Computacionais e de Comunicação - WPerformance 2015

Trace Selection for Improved WLAN Monitoring

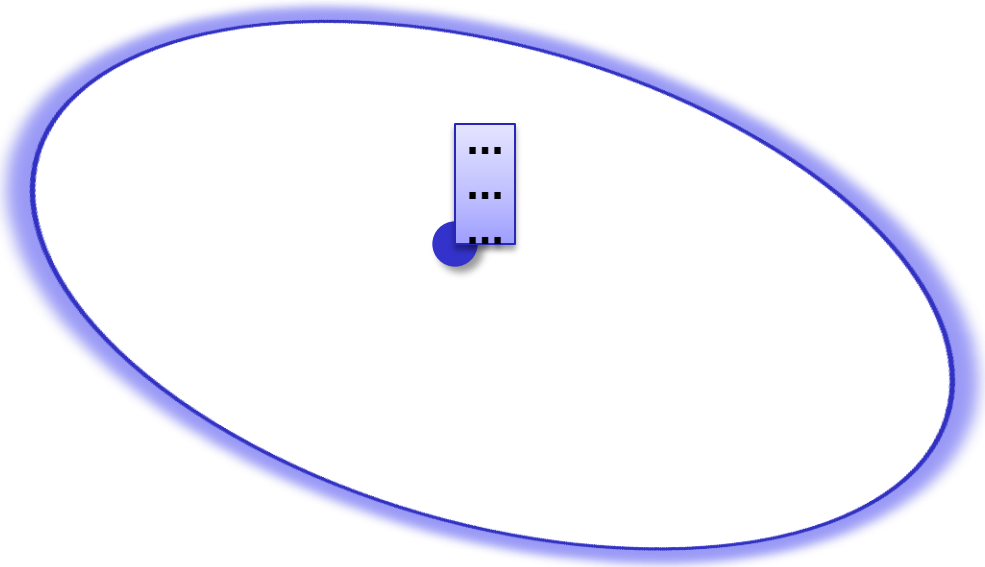
Matteo Sammarco[2], Miguel Elias M. Campista[1], and Marcelo D. de Amorim[2]

[1]GTA/PEE-COPPE/DEL-Poli – UFRJ – Brasil
[2]LIP6/CNRS – UPMC Sorbonne Universités – França

2nd WNetVirt'13, October 26, 2013, Angra dos Reis, Brazil

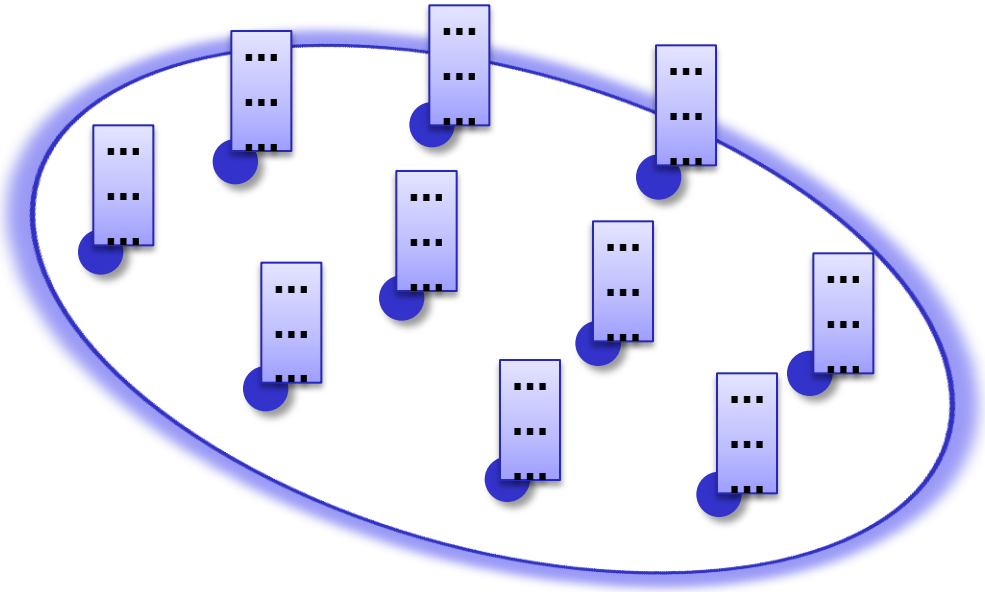
Supported by CAPES, CNPq, Faperj (Brazil), and ANR (France)

State of the Art



Target Area

State of the Art



Target Area

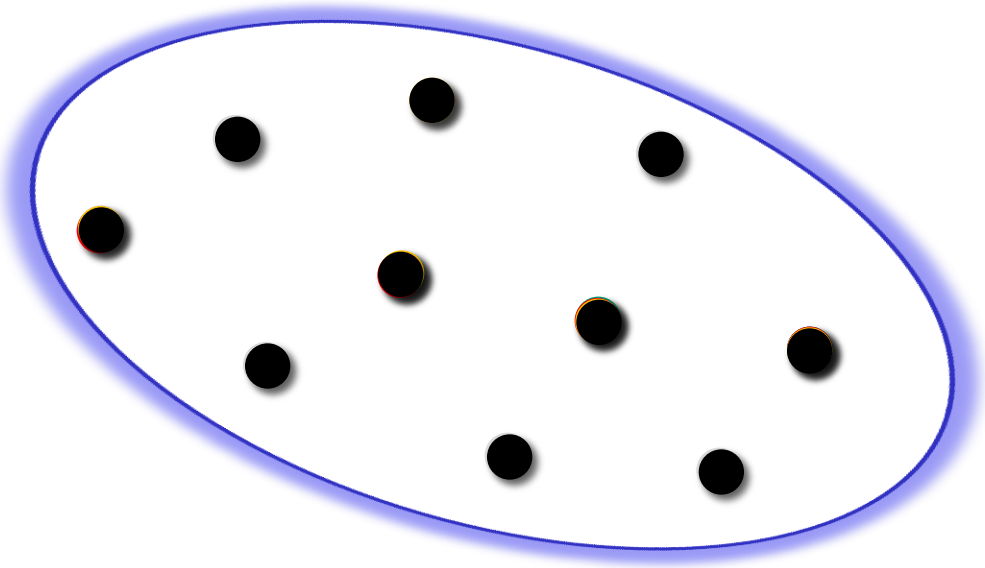
Central Unit

1. Synchronization

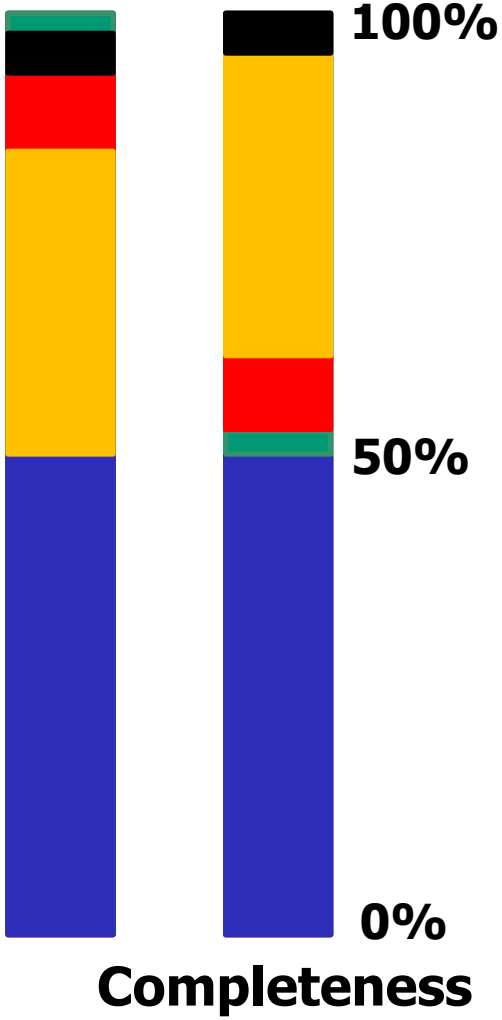
2. Merging

3. Presentation

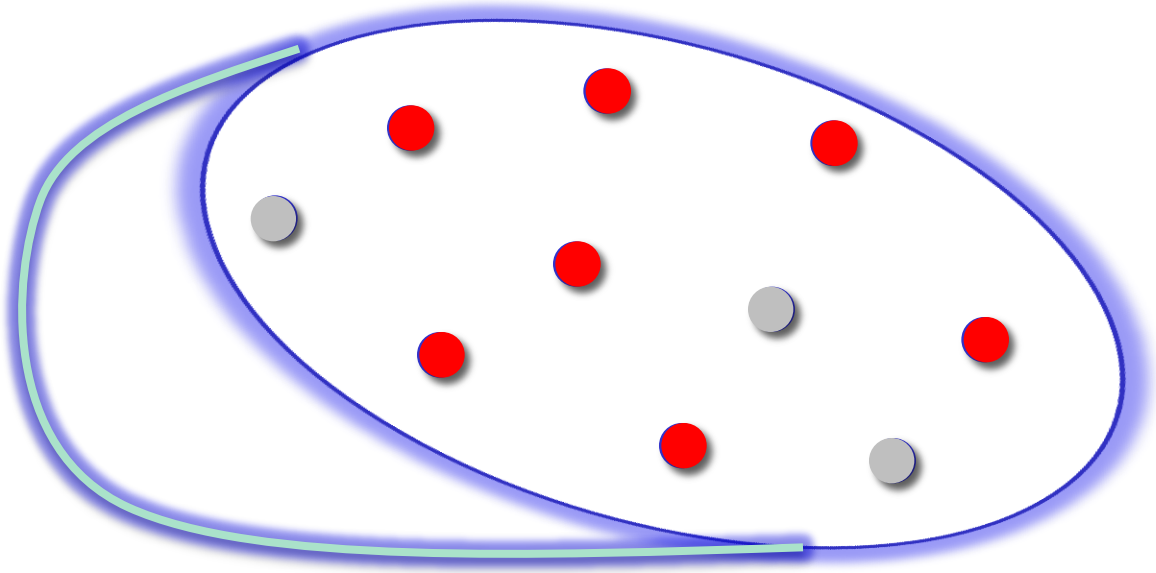
Merging Process

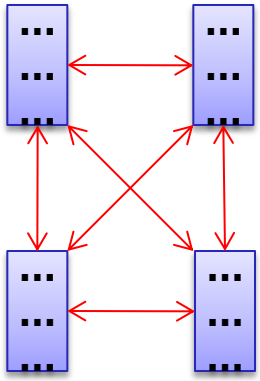


Target Area

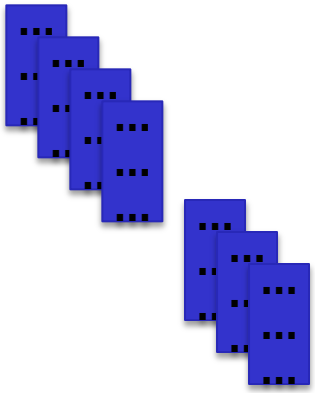


Our Approach

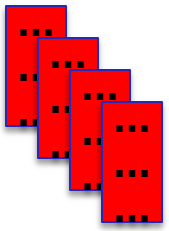




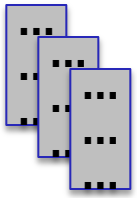
Similarity



Ranking



Merging



Moving

Trace Similarity

Intra-flow similarity:

$$\mathrm{J}(\mathrm{t}_i, t_j) = \frac{|t_i \cap t_j|}{|t_i \cup t_j|}$$

Inter-flow similarity:

$$\text{TF-IDF}(\mathrm{t}_i, l) = \frac{|f^l_{i \cup j}|}{|t_i|} \cdot \log \frac{|\mathcal{T}|}{|\{t_i \in \mathcal{T} | f^l_{i \cup j} \in t_i\}|}$$

$$\mathrm{IFS}(\mathrm{t}_i, t_j) = \frac{\sum_l \text{TF-IDF}_{(t_i,l)} \cdot \text{TF-IDF}_{(t_j,l)}}{\sqrt{\sum_l \text{TF-IDF}_{(t_i,l)^2}} \cdot \sqrt{\sum_l \text{TF-IDF}_{(t_j,l)^2}}}$$

Trace Ranking

We consider a fully connected graph $\mathrm{G(V,E)}$

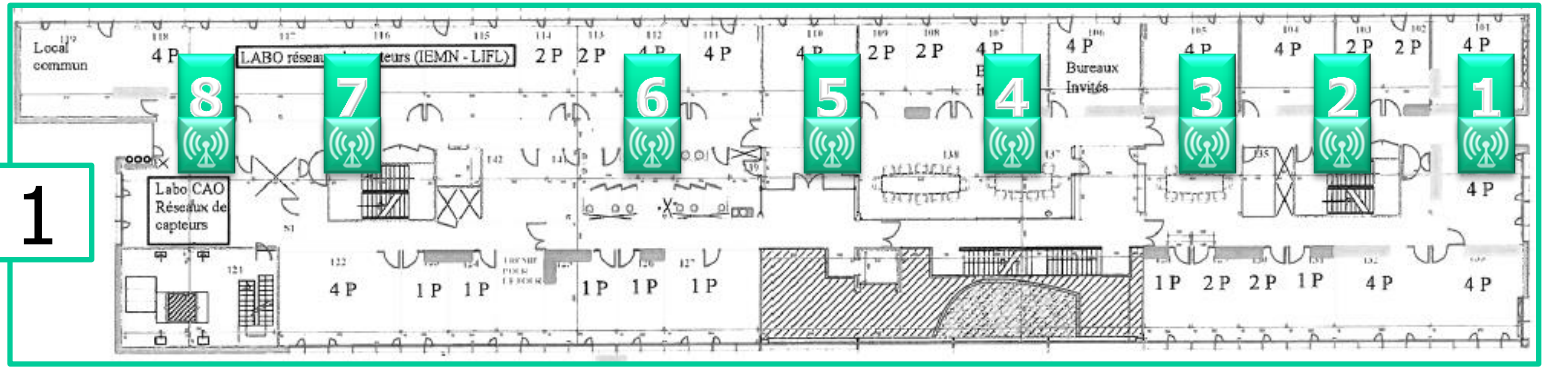
v_i : is the trace captured by the i-th monitor

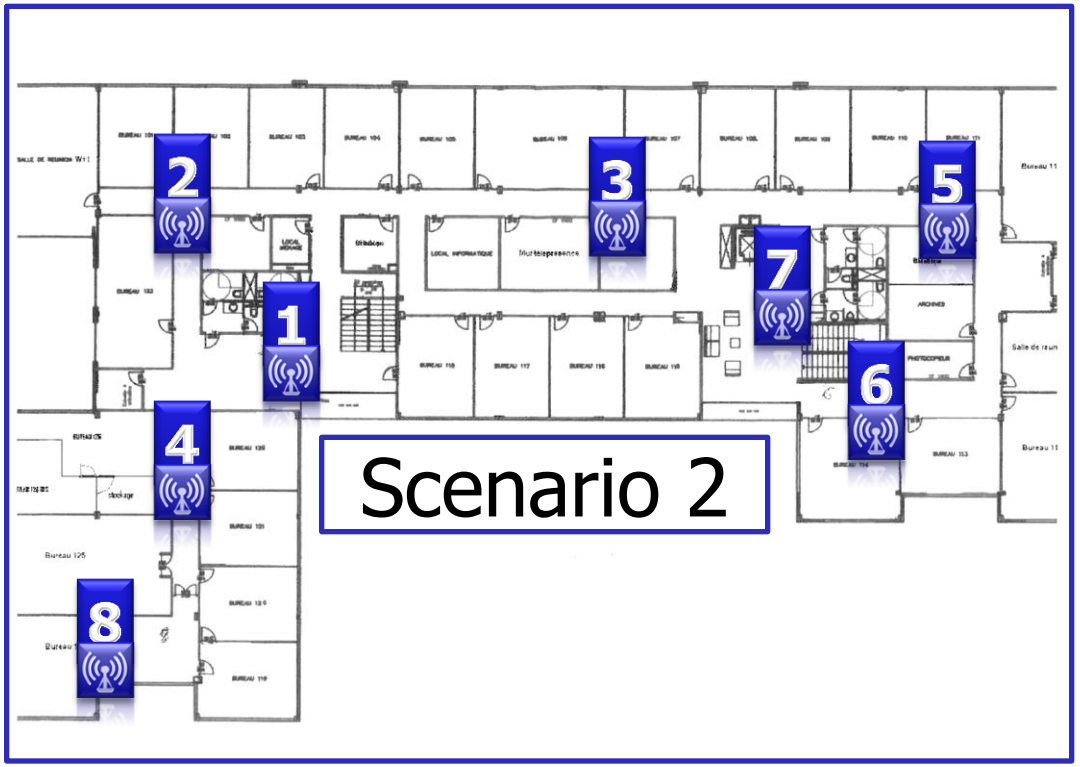
e_{ij} : has a weight linearly proportional to the similarity between the i-th and the j-th trace

Ranking all the nodes in according to the minimum Hamiltonian path is a good way to iteratively select traces to merge

Experimental Setup

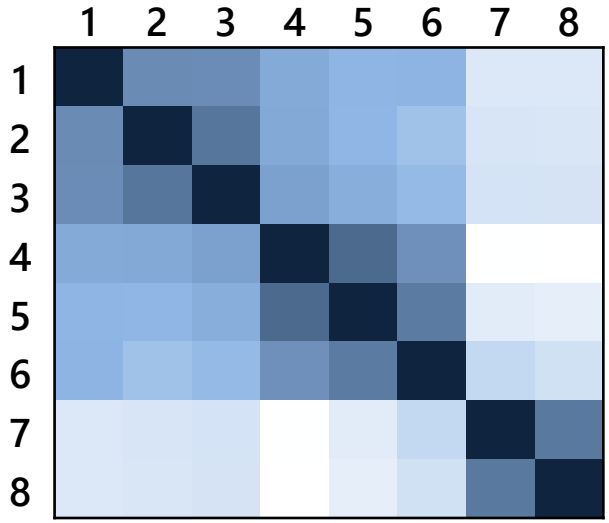
Scenario 1

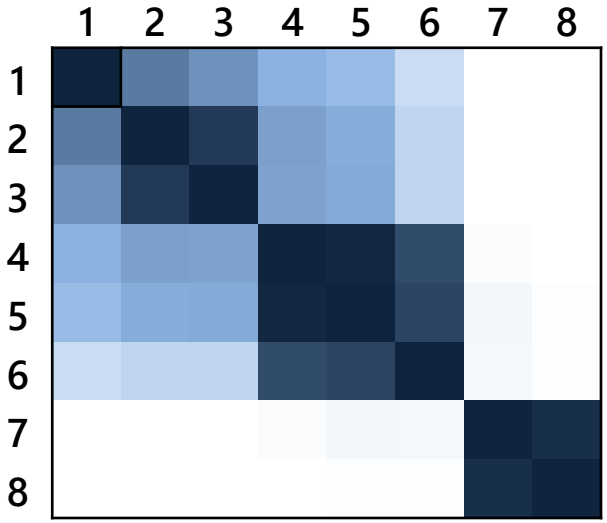


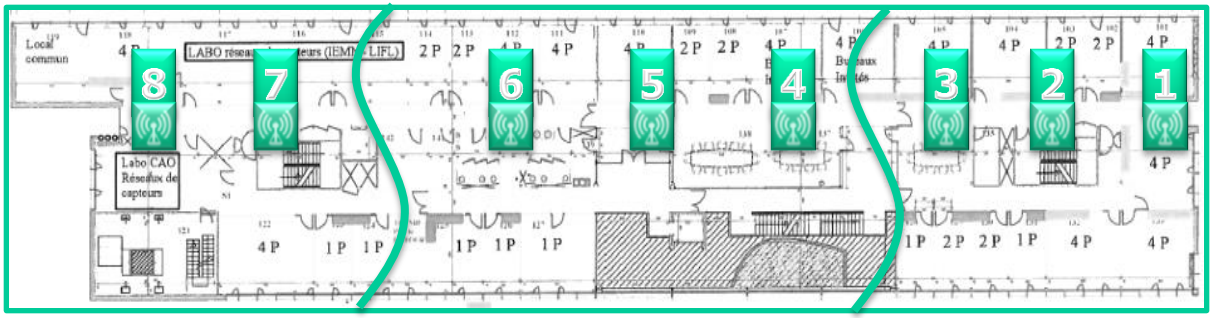


8 monitors
100 minutes

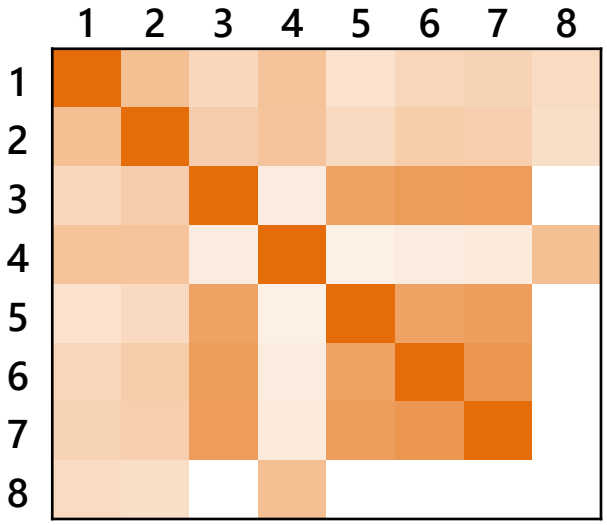
Similarity: Scenario I

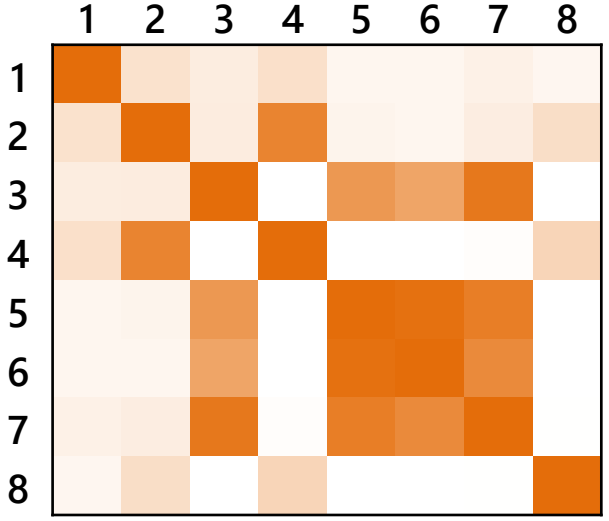


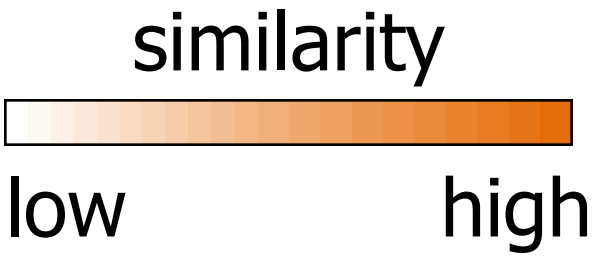


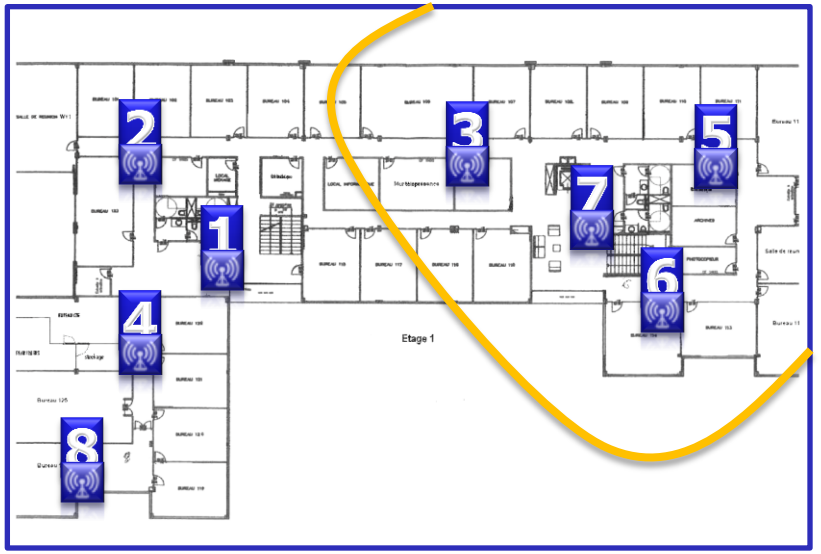


Similarity: Scenario II

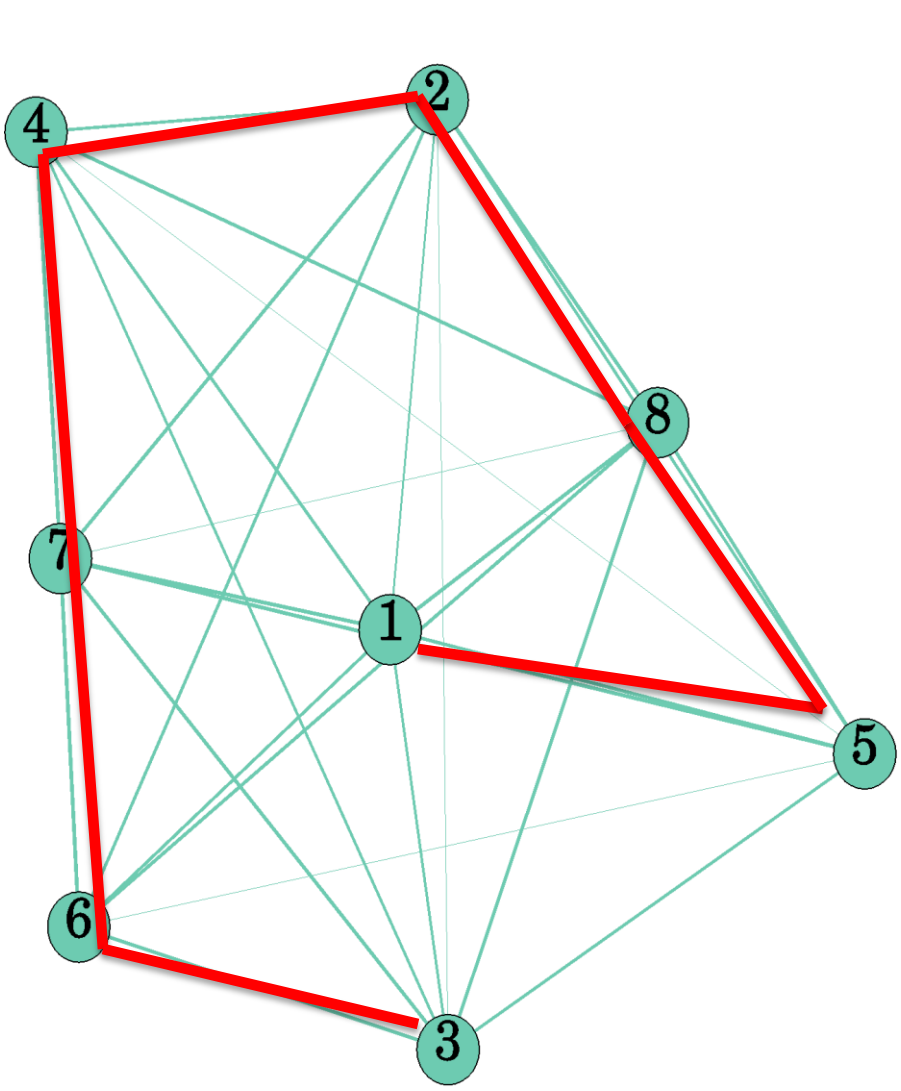


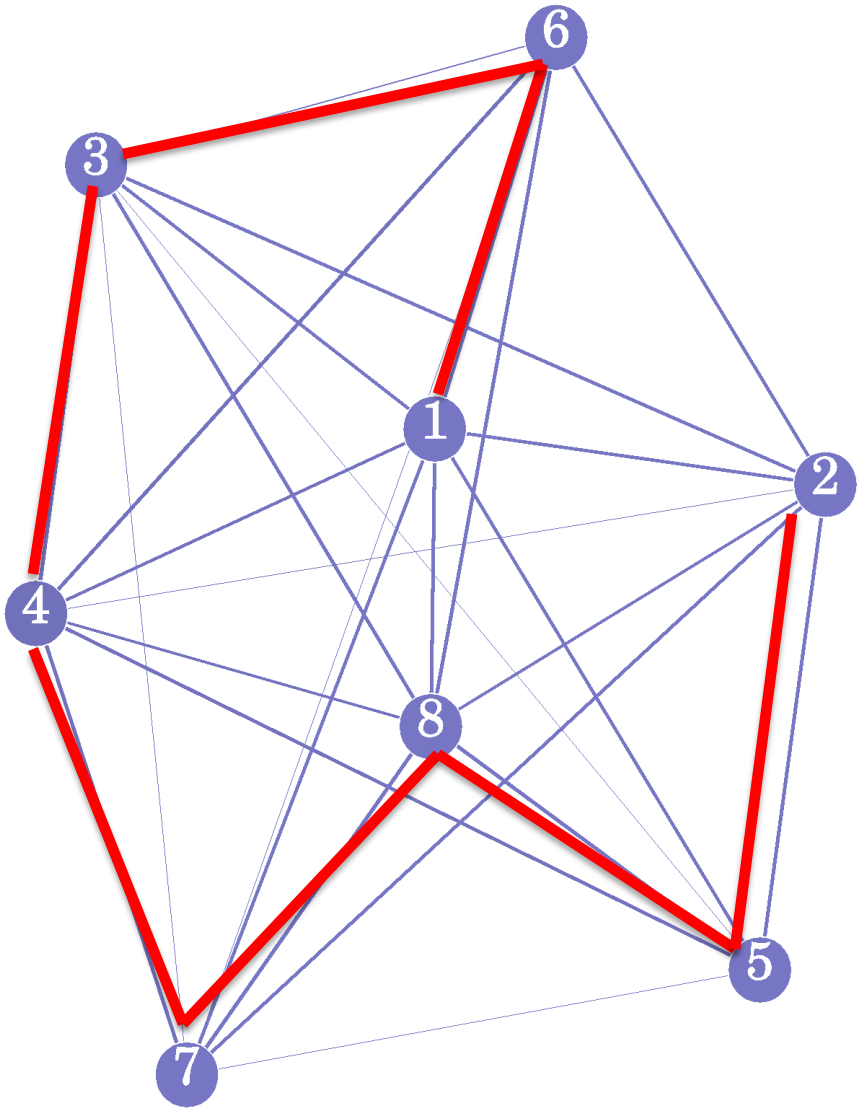




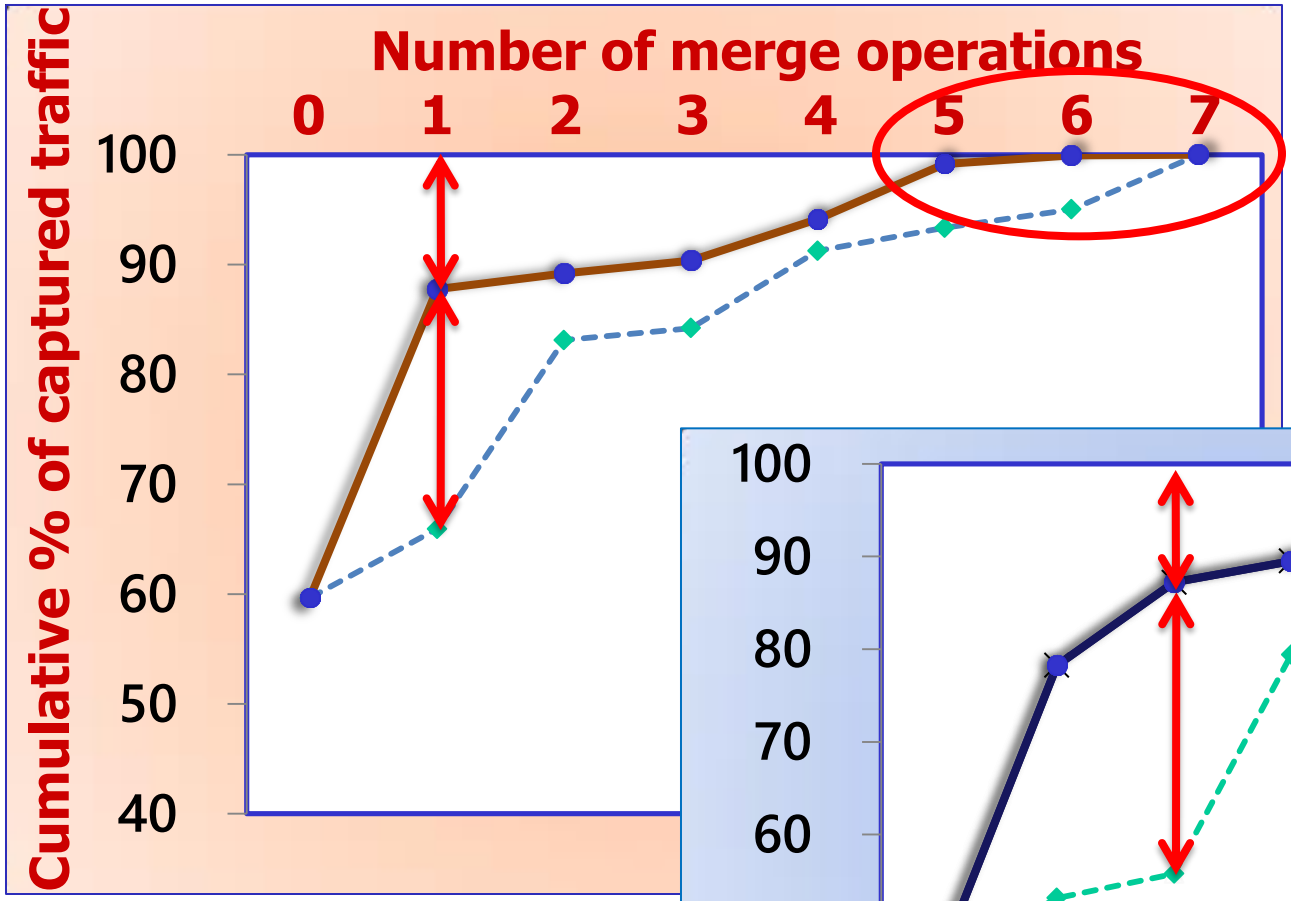


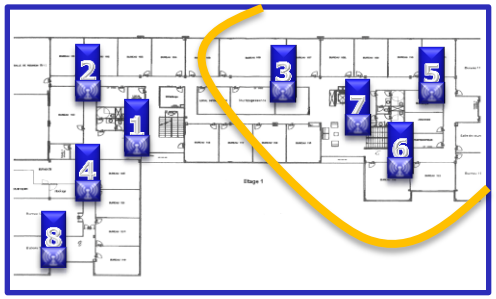
Trace Ranking

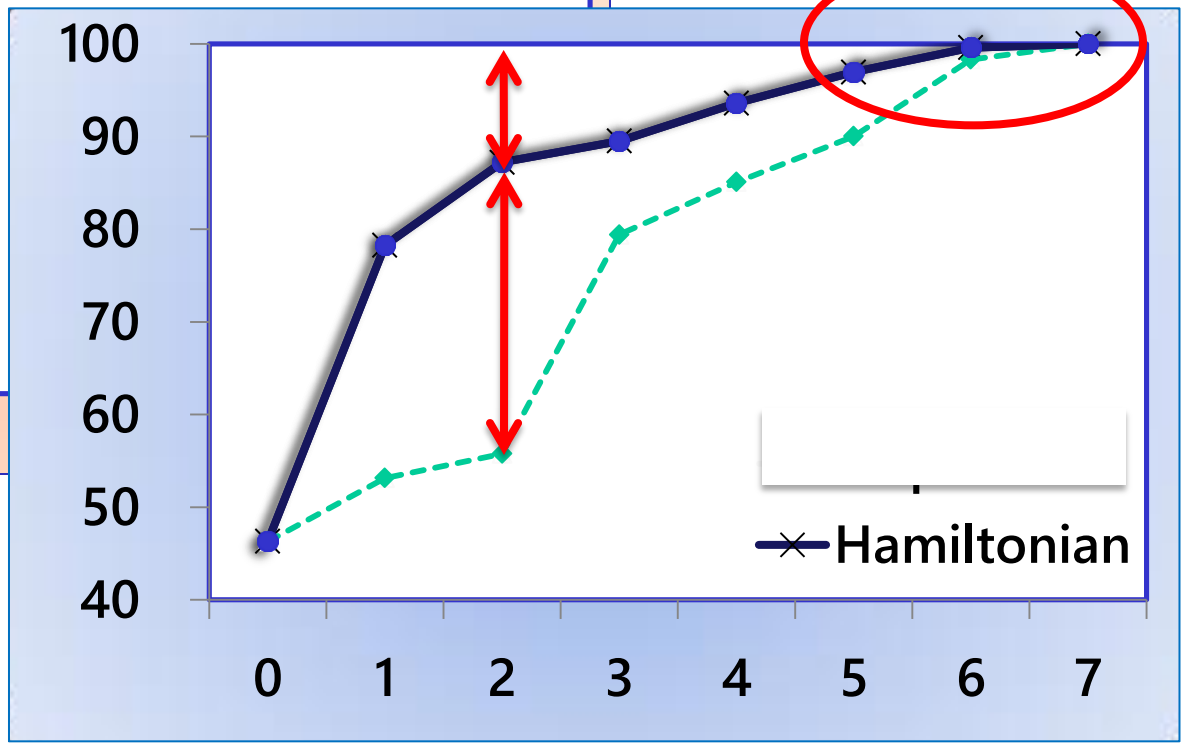


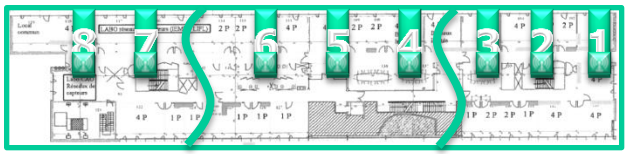


Results


Number of merge operations
0 1 2 3 4 5 6 7
Cumulative % of captured traffic
100
90
80
70
60
50
40


1
2
3
4
5
6
7
8


100
90
80
70
60
50
40
0 1 2 3 4 5 6 7
Hamiltonian


8 7 6 5 4 3 2 1

Summary

Scalability Merging is limited to a subset of traces

Effectiveness Traces merged at the beginning give the higher contribution

Extension Last ranked monitors can be moved to enlarge the target area

Future Work

Similarity More similarity metrics

Ranking Use community detection algorithms to find the exact number of traces to merge

Monitoramento Colaborativo de Redes Sem-fio: Acurácia do Sistema e Denúncia de Farejadores Maliciosos

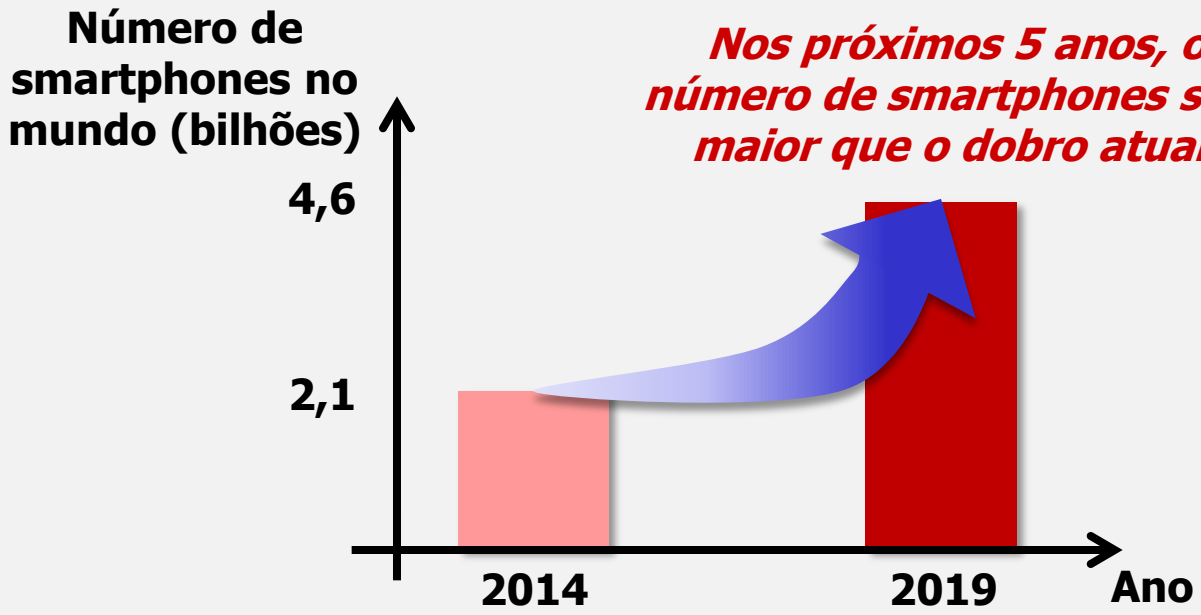
Miguel Elias M. Campista[1], Matteo Sammarco[2], Marcelo D. de Amorim[2] e Tahiry Razafindralambo[3]

[1]GTA/PEE-COPPE/DEL-Poli – UFRJ – Brasil
[2]LIP6/CNRS – UPMC Sorbonne Universités – França
[3]INRIA Lille Nord Europe – França

WPerformance 2015

Financiado pela CAPES, CNPq e Faperj (Brasil) e ANR (França)

O número de smartphones (dispositivos móveis) vem crescendo aceleradamente ao longo dos anos...



Fonte: Cisco – VNI Forecast Highlights

O que fazer com essa disponibilidade de recursos?

Monitoramento Colaborativo da Rede

Como saber que há um usuário com baixa qualidade de cobertura se o monitoramento for parcial?

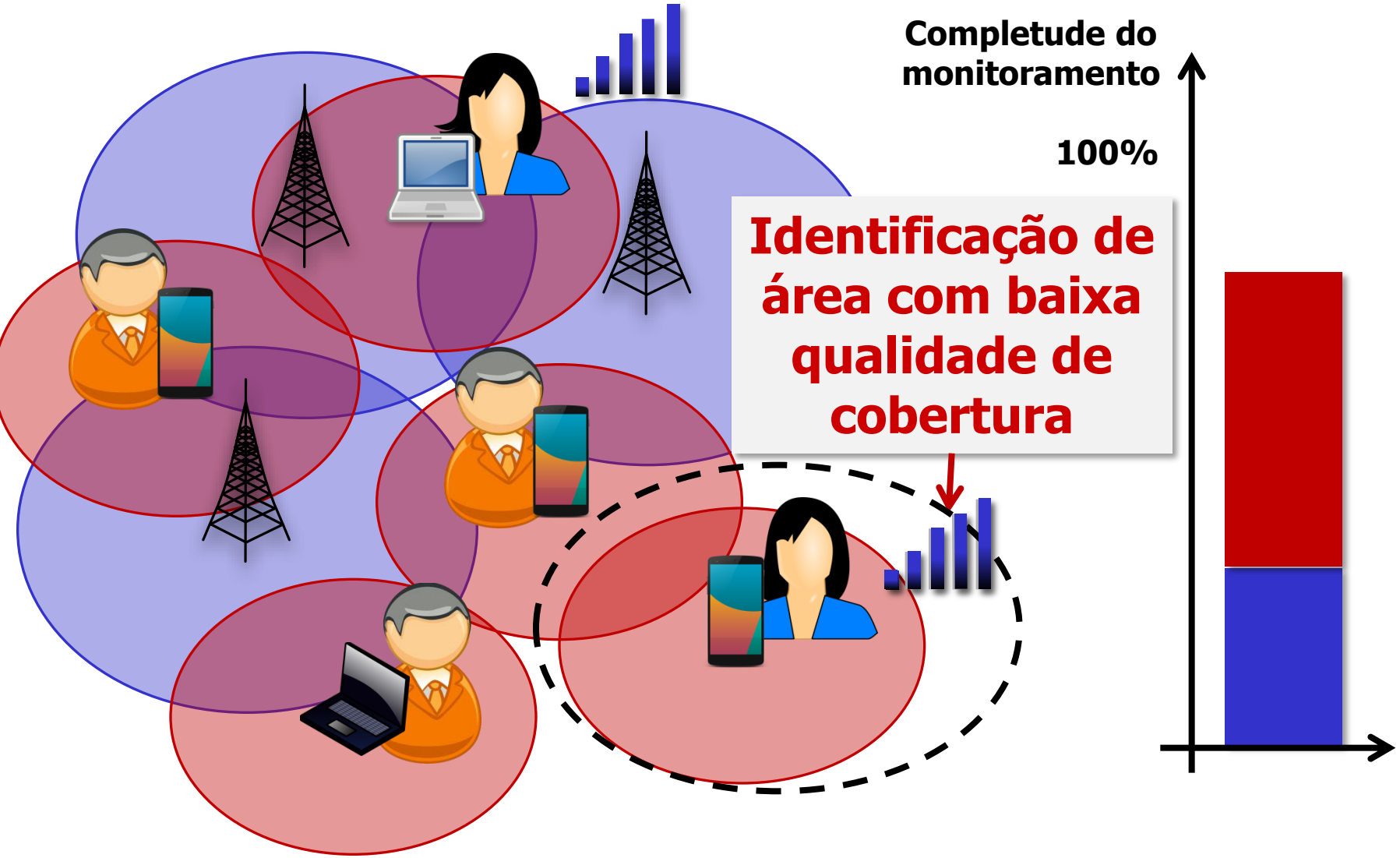
Monitoramento Colaborativo da Rede

Aumentando o número de nós monitores, aproveitando a disponibilidade de recursos dos próprios usuários!

Monitoramento Colaborativo da Rede

Quanto maior for o número de monitores, maior será a quantidade de informações capturadas da rede

Possibilidade de Realizar Replanejamento da Rede



Problema da Colaboração: Presença de Usuários Maliciosos

Mesmo possuindo uma boa cobertura, um usuário malicioso pode atrair recursos anunciando falsa informação de monitoramento...

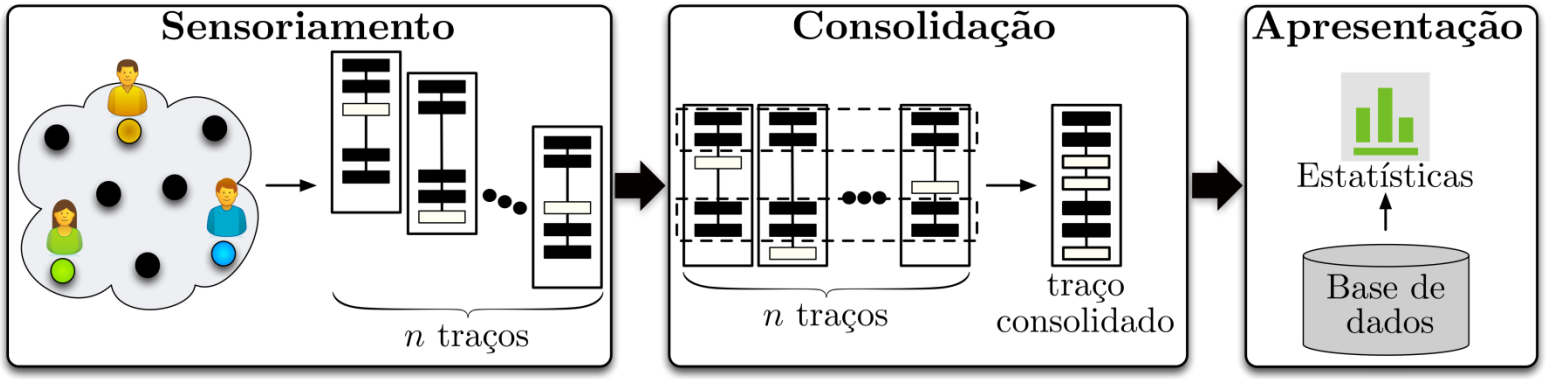
Problema da Colaboração: Presença de Usuários Maliciosos

Usuário legítimo perde qualidade de cobertura!

Contribuições

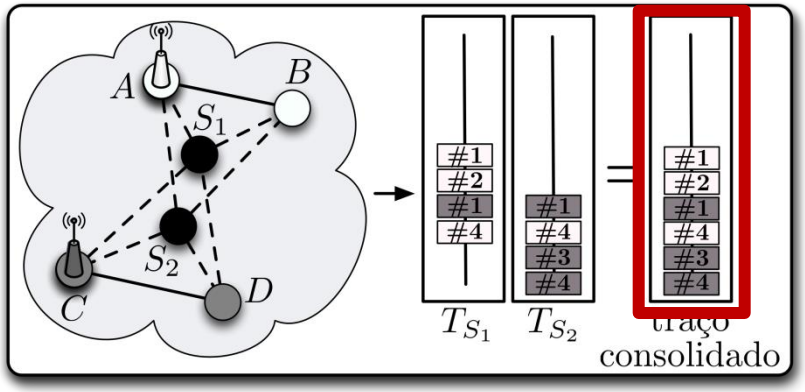
- **Proposta de um sistema de monitoramento colaborativo**
  - Participação dos usuários
- **Identificação de dois possíveis ataques**
  - Ataque de atração e ataque de repulsão
- **Proposta de uma metodologia para a detecção de possíveis nós maliciosos**
  - Metodologia baseada em grafos

Arquitetura



- **Módulo de sensoriamento:**
  - Produz traços de dados compostos por uma sequência de quadros em ordem cronológica de recepção
- **Módulo de consolidação:**
  - Constrói um traço final consolidado
- **Módulo de apresentação:**
  - Armazena e entrega estatísticas de uso da rede

Problema da Colaboração: Consolidação dos Traços de Dados



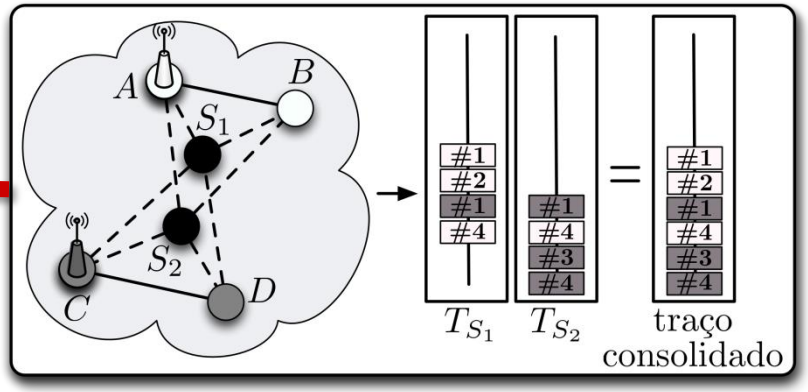
6/8 pacotes capturados:
75% de completude!

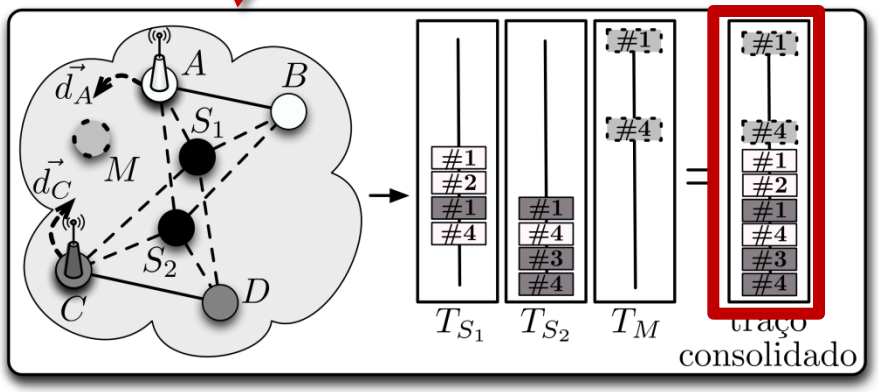
Traço consolidado = merge dos traços individuais coletados

Merge aumenta a completude do traço final!

Problema da Colaboração: Consolidação dos Traços de Dados

Ataque de atração

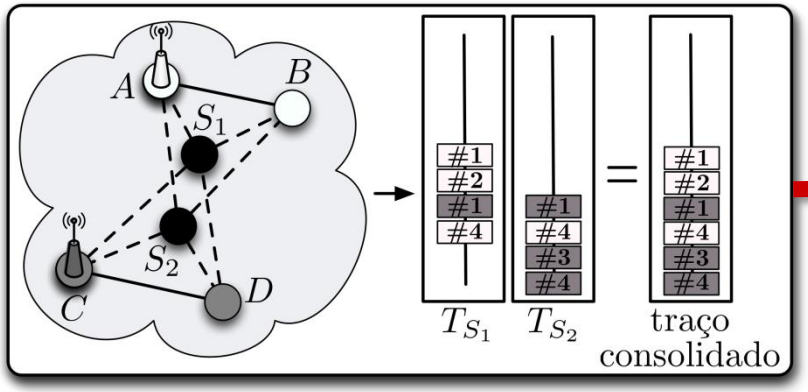




Usuário malicioso cria fluxos de dados com quadros faltantes

8/12 pacotes capturados:
66% de completude!

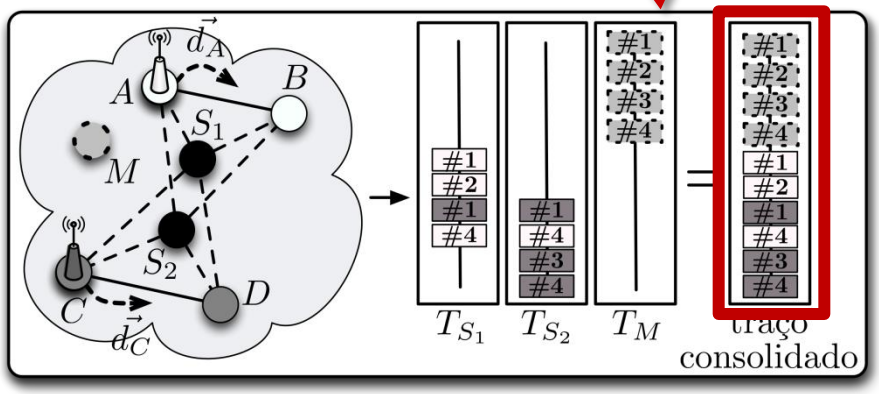
Problema da Colaboração: Consolidação dos Traços de Dados



Ataque de repulsão

Usuário malicioso cria fluxos de dados com todos os quadros

10/12 pacotes capturados:
83% de completude!



Acurácia do Sistema

- Taxa de completude ≡ **Acurácia do monitoramento (a)**

$$a = 1 - (m(t)/s(t)$$

Quadros perdidos por todos os monitores da rede em um instante t

Quadros enviados por todos os nós da rede em um instante t

Logo, um ataque de atração diminui a, enquanto um de repulsão aumenta a...

Acurácia do Sistema

- Taxa de completude ≡ **Acurácia do monitoramento (a)**

$$a = 1 - (m(t)/s(t)$$

Quadros perdidos por todos os n

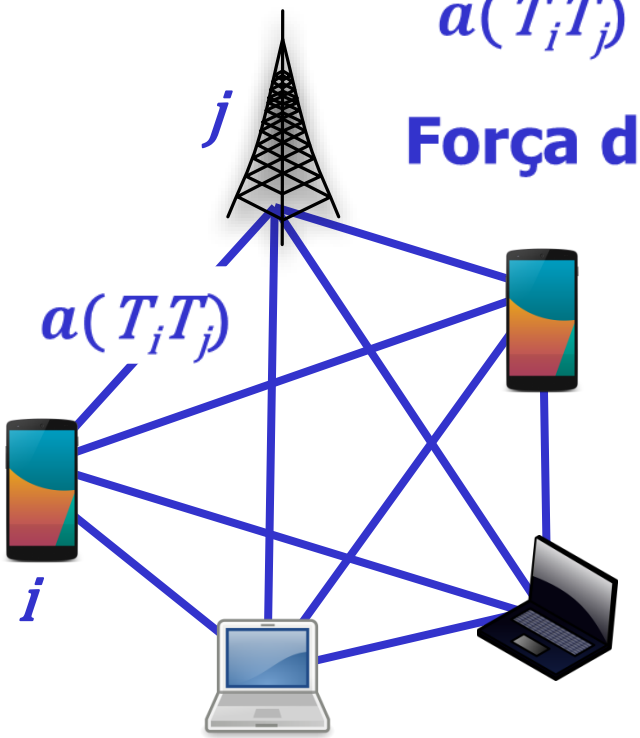
Quadros enviados por todos um

Independente do ataque, como é possível identificar um atacante?

Logo, um ataque de atração diminui a, enquanto um de repulsão aumenta a...

Sistema de Detecção

- Modelagem da rede de monitores como um grafo



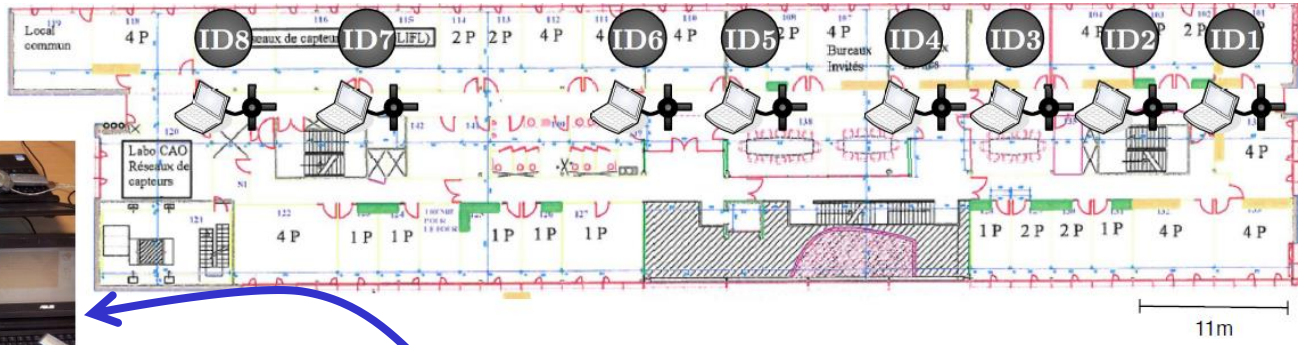
$a(T_iT_j)$: Peso da aresta entre os monitores i e j

Força do vértice: $(\sigma(T_i))$: $\sigma(T_i) = \sum_{j=1}^{|V|} a(T_iT_j)$

Possível monitor malicioso é aquele que possui a força do vértice mais discrepante!

Rede de Testes e Conjunto de Dados

Cenário esparso



Cenário colocalizado

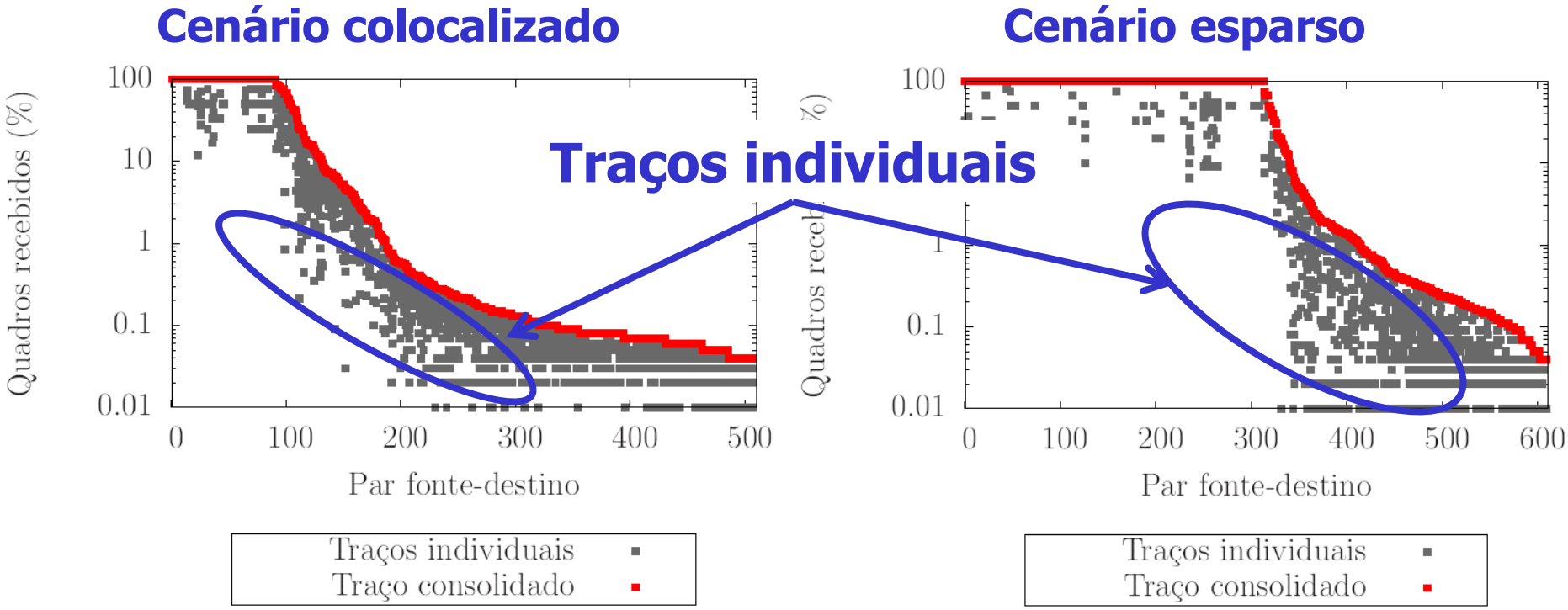
Acurácia de cada traço em comparação ao consolidado (x10^{-3})

Cenários	Traços								
	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	Consolidado
Colocalizado	1,57	1,58	1,70	1,57	1,99	1,82	2,37	1,71	**3,27**
Esparso	0,34	0,29	0,25	1,35	1,01	0,65	0,17	0,12	**3,07**

Experimentos

- Desempenho do monitoramento colaborativo em rede livre de atacantes
- Impacto dos ataques identificados e desempenho do sistema de detecção

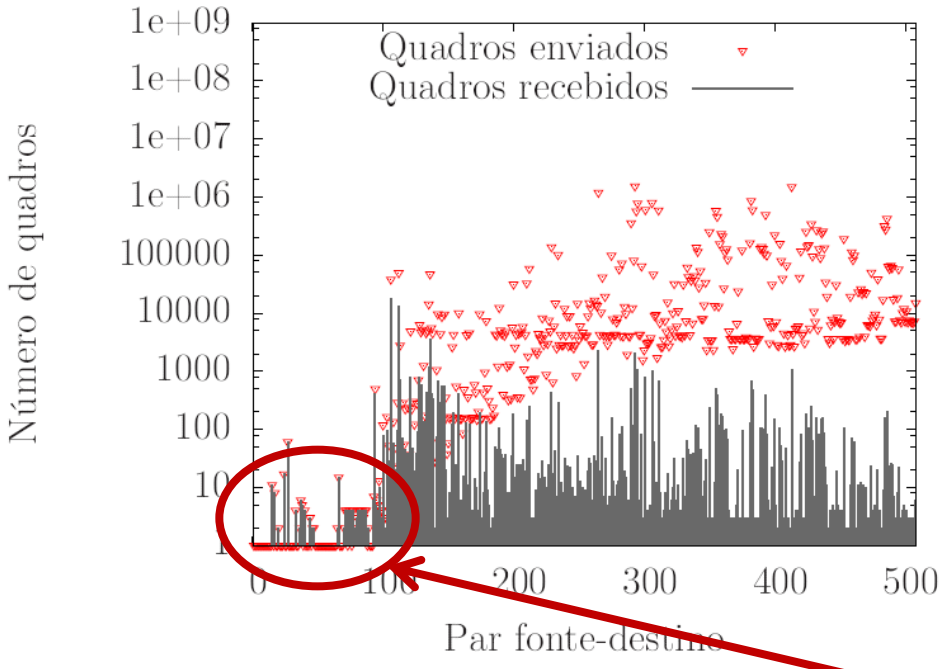
Fração de Quadros Capturados pelos Diferente Traços



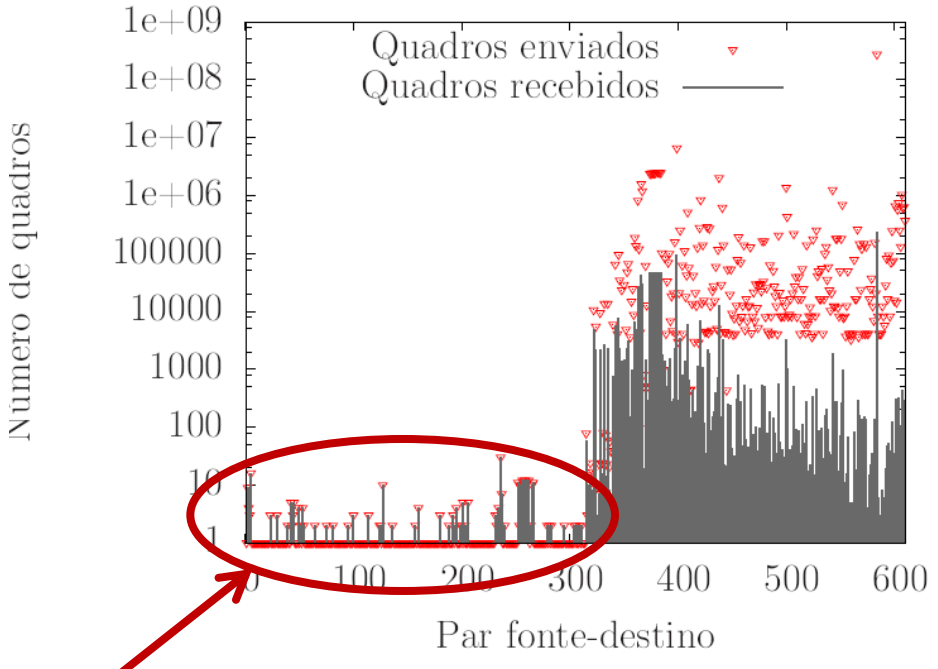
Grande diferença entre a acurácia dos traços individuais e do consolidado

Fração dos Quadros Capturados em Função do Tamanhos dos Fluxos

Cenário colocalizado



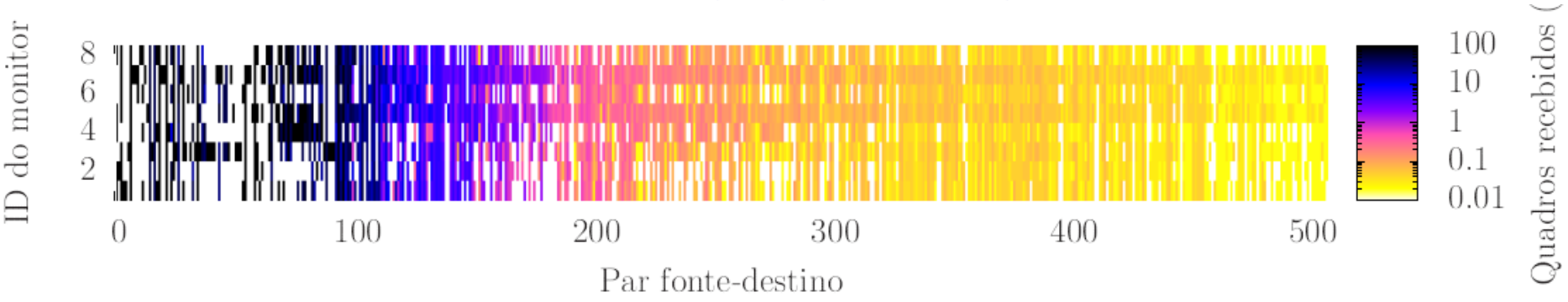
Cenário esparso



Fluxos com menos quadros têm menor perda...

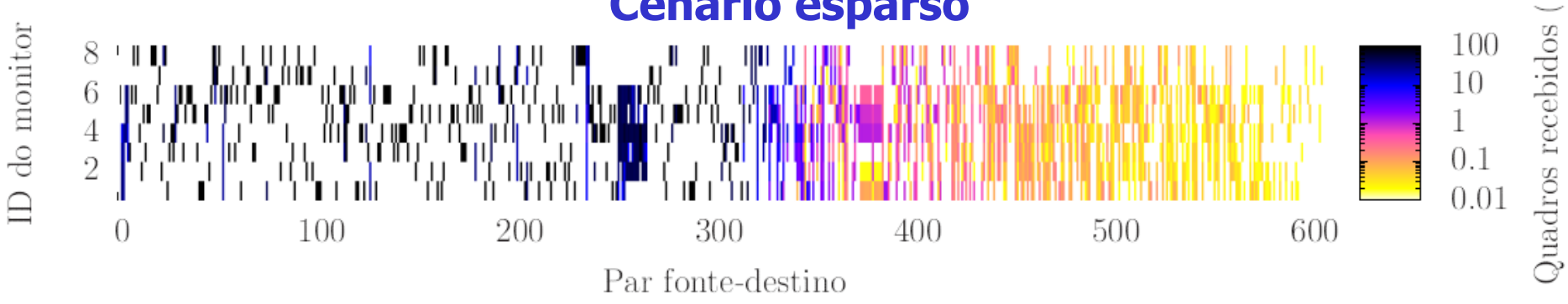
Fração de Quadros Capturados em Função da Posição dos Monitores

Cenário colocalizado



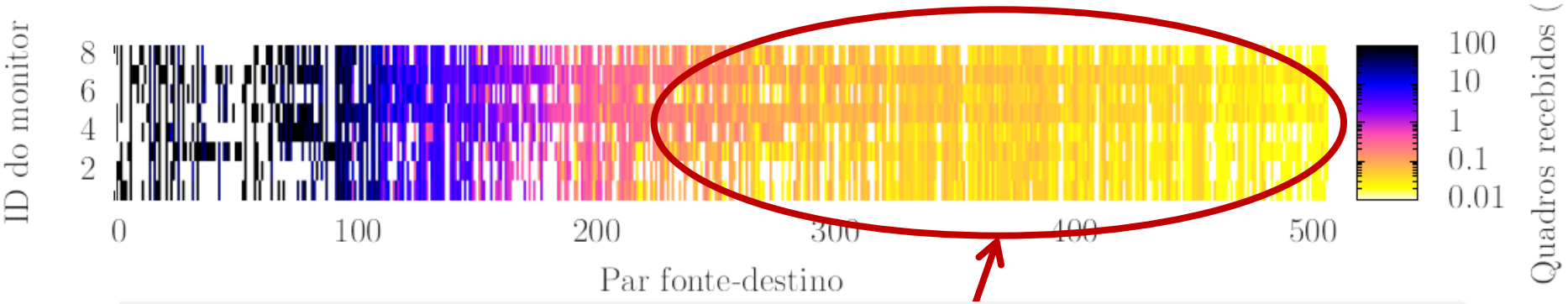
Fração de quadros muda conforme a posição dos monitores...

Cenário esparso



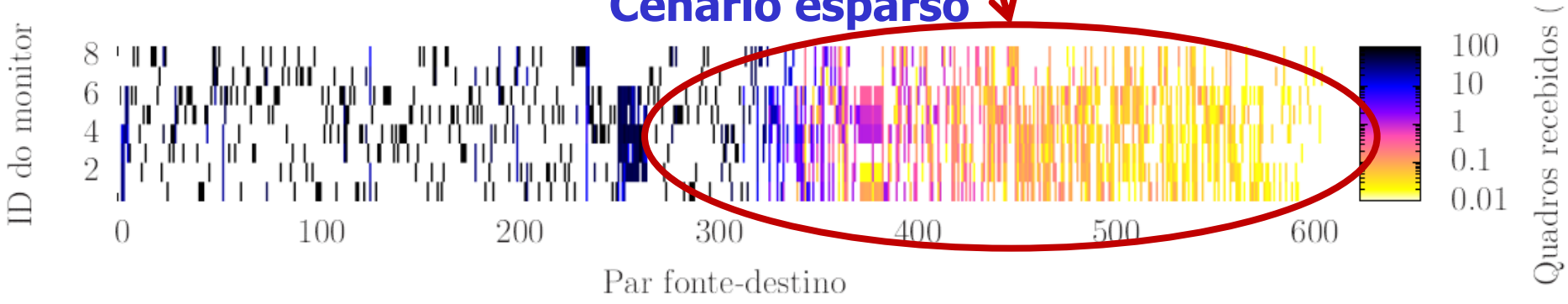
Fração de Quadros Capturados em Função da Posição dos Monitores

Cenário colocalizado



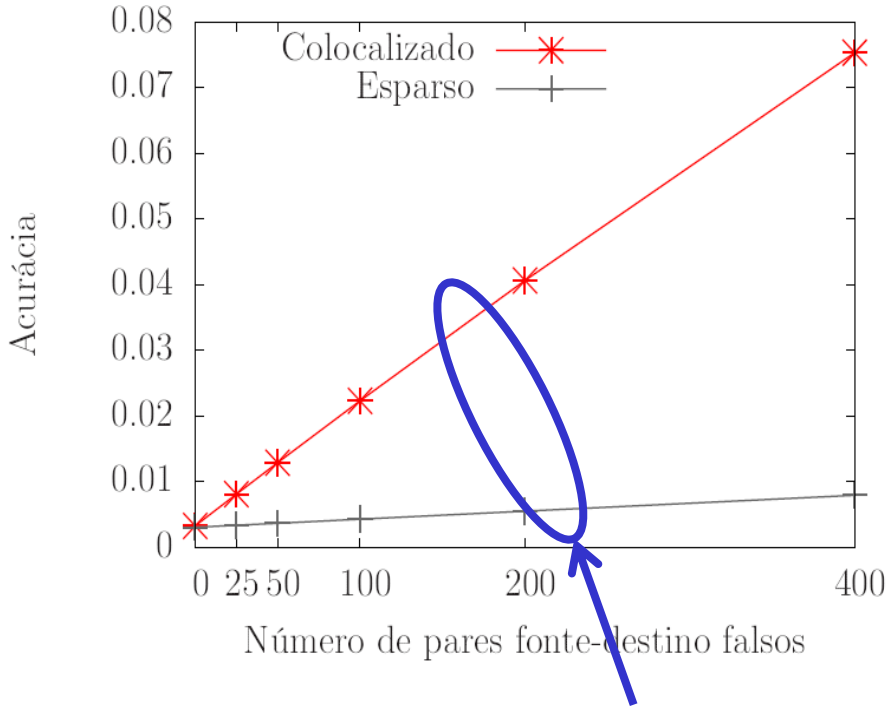
...e o efeito se torna mais evidente em cenários mais esparsos

Cenário esparso



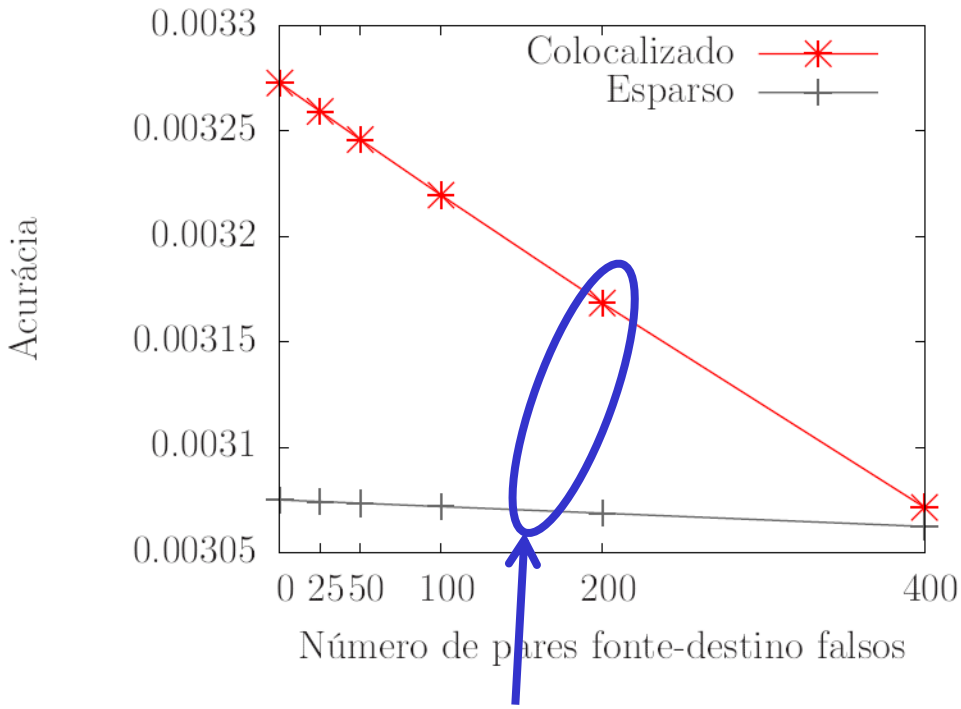
Impacto dos Ataques: Efeito da Participação de Usuários Maliciosos

Ataque de repulsão



Aumento da acurácia (2200% e 150%)

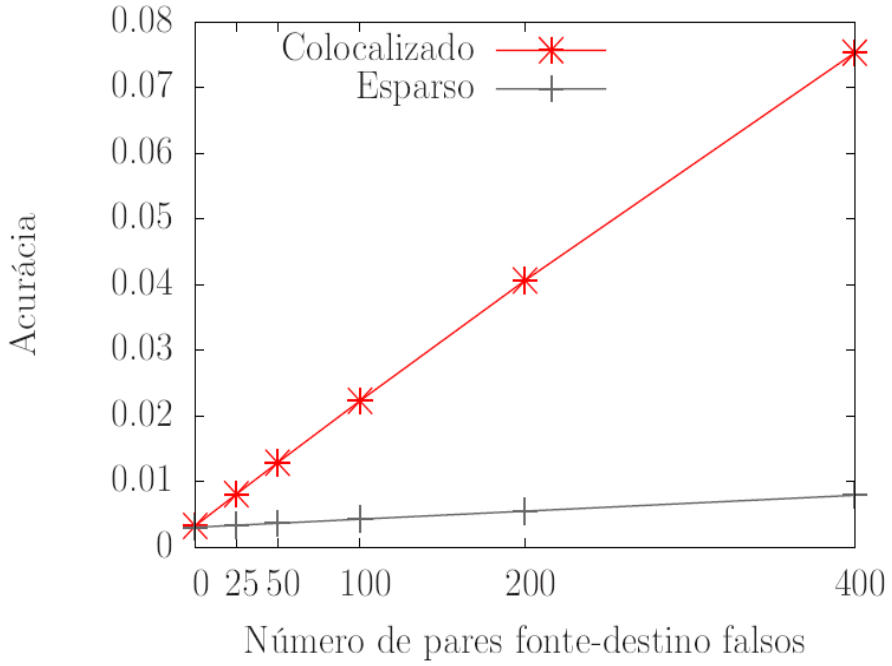
Ataque de atração



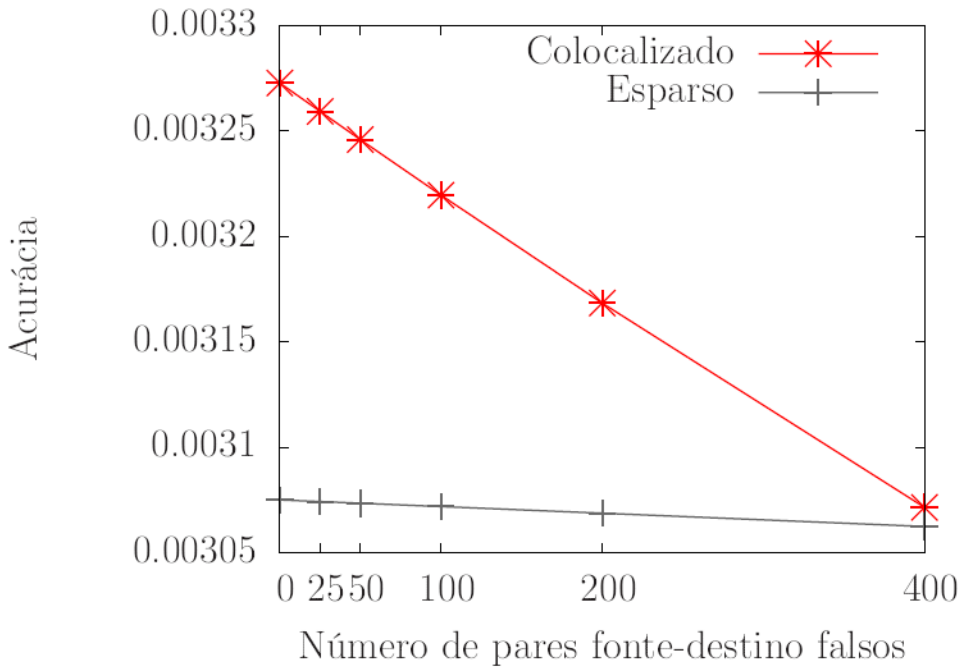
Redução da acurácia (6% e 0,4%)

Impacto dos Ataques: Efeito da Participação de Usuários Maliciosos

Ataque de repulsão



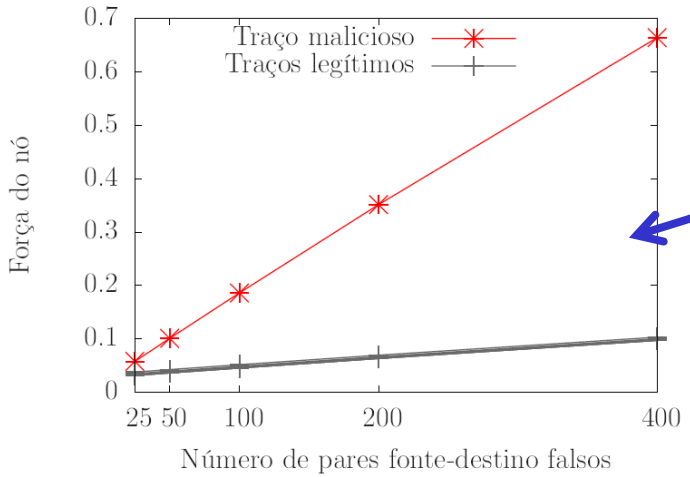
Ataque de atração

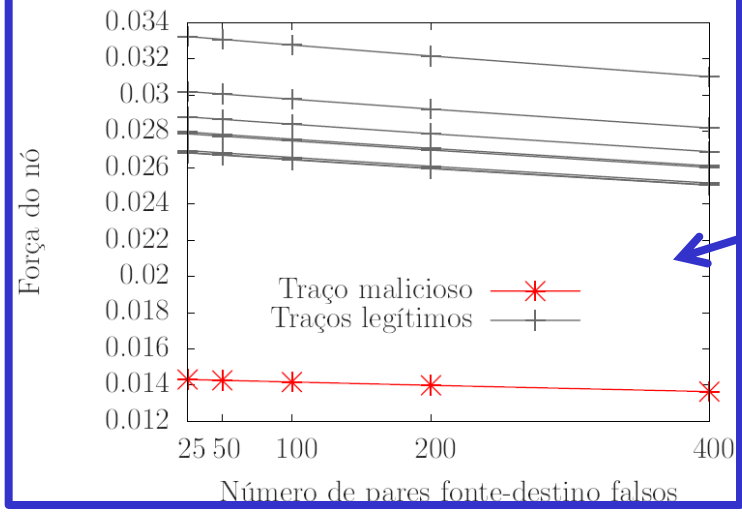


Ataques em cenários densos são mais efetivos, assim como o ataque de repulsão

Detecção de Atacantes Potenciais: Variação da Força dos Monitores

Colocalizado

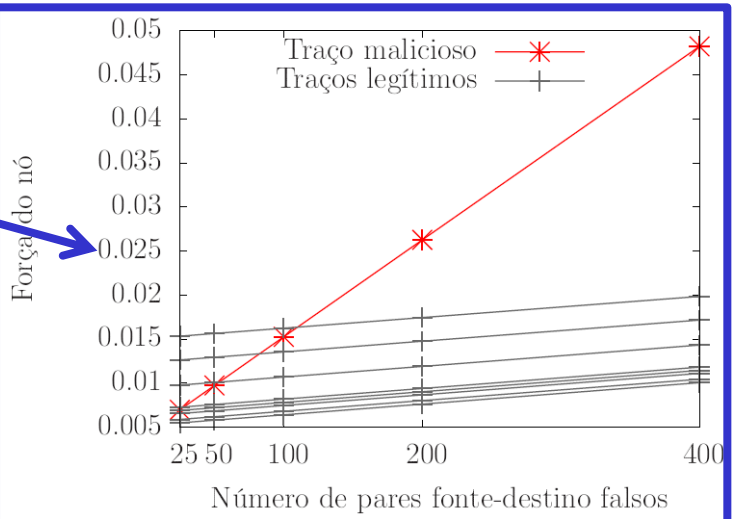


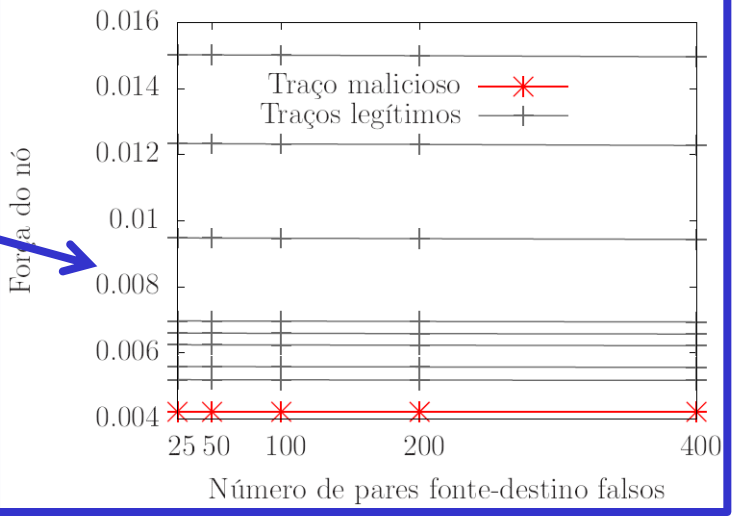


Ataque de Repulsão

Ataque de Atração

Esparso



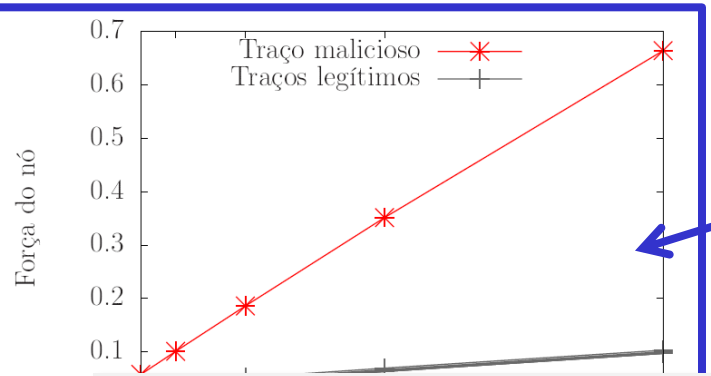


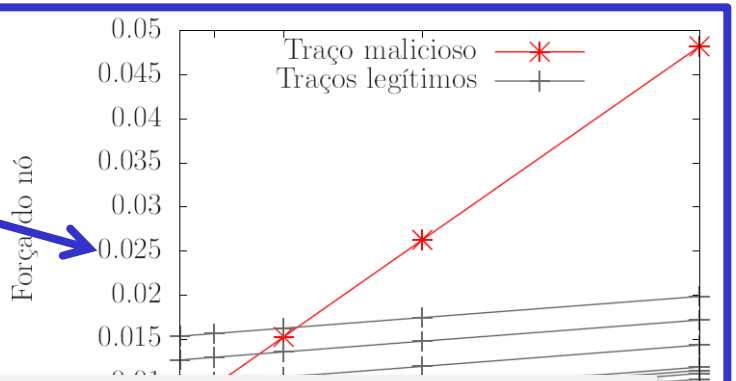
Detecção de Atacantes Potenciais: Variação da Força dos Monitores

Colocalizado

Esparso

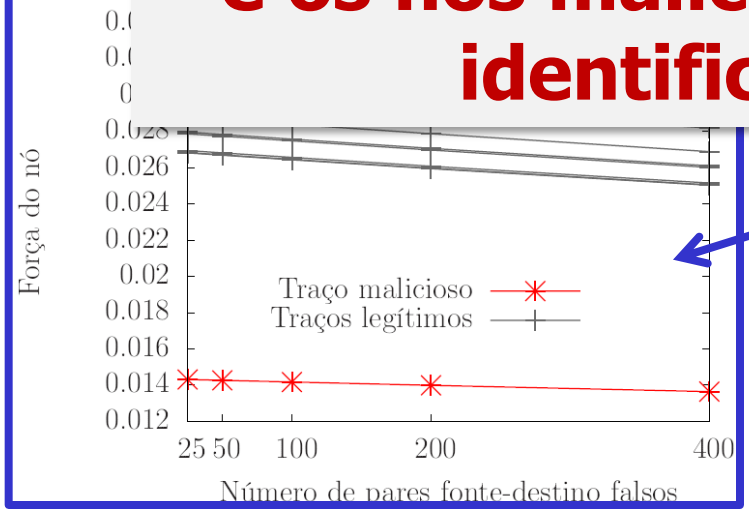
Ataque de Repulsão

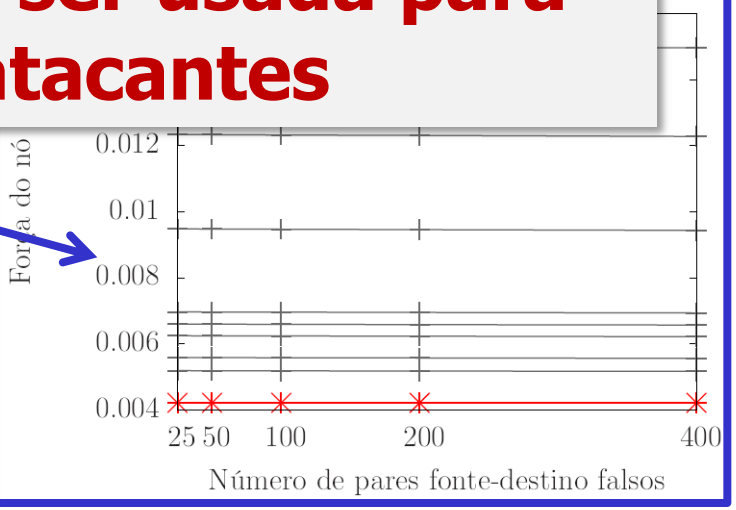




A diferença de força entre os nós legítimos e os nós maliciosos pode ser usada para identificação dos atacantes

Ataque de Atração

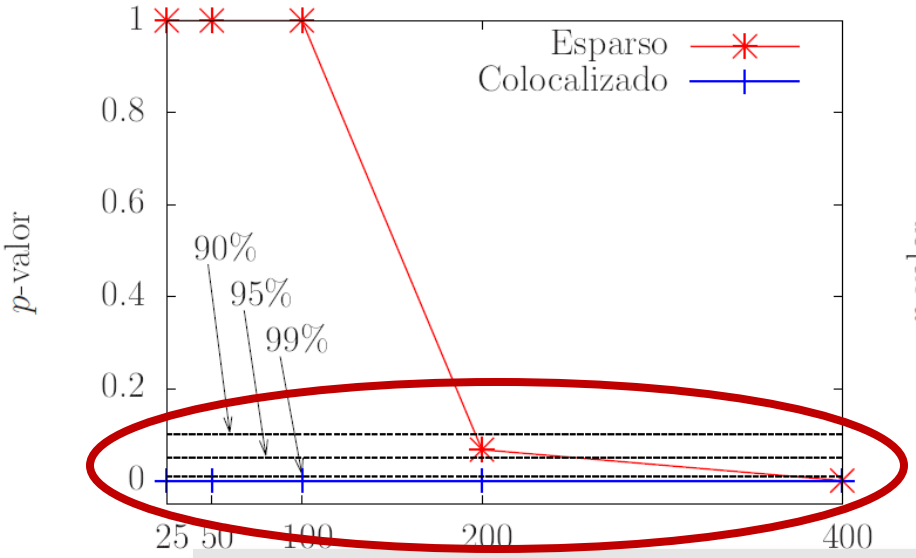




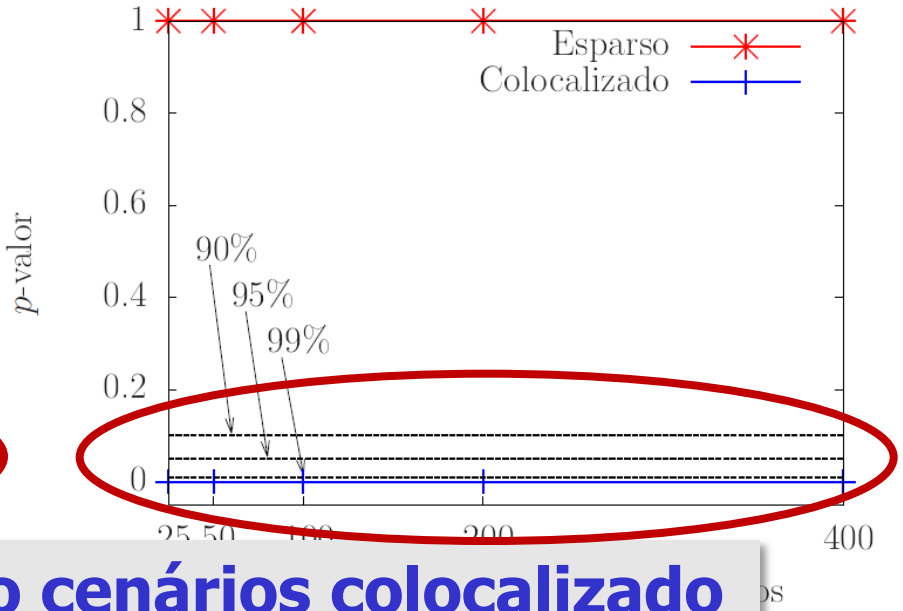
Detecção de Atacantes Potenciais: Teste de Detecção de *Outlier*

- Hipótese do traço malicioso *não ser* um *outlier*...

Ataque de repulsão



Ataque de atração



Hipótese rejeitada no cenários colocalizado e no cenário esparso para muitos nós

Conclusões e Trabalhos Futuros

- Trabalho demonstrou:
  - Acurácia aumenta com o número de traços
  - Participação de usuários pode levar a ataques
  - Ataques podem ser detectados em certas condições
- Trabalhos futuros
  - Realização de mais experimentos
  - Aprimoramento do sistema de detecção

Monitoramento Colaborativo de Redes Sem-fio: Acurácia do Sistema e Denúncia de Farejadores Maliciosos

Miguel Elias M. Campista[1], Matteo Sammarco[2], Marcelo D. de Amorim[2] e Tahiry Razafindralambo[3]

[1]GTA/PEE-COPPE/DEL-Poli – UFRJ – Brasil
[2]LIP6/CNRS – UPMC Sorbonne Universités – França
[3]INRIA Lille Nord Europe – França

WPerformance 2015

Financiado pela CAPES, CNPq e Faperj (Brasil) e ANR (França)