

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



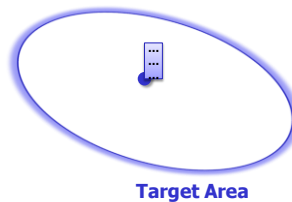
Trace Selection for Improved WLAN Monitoring

Matteo Sammarco², Miguel Elias M. Campista¹, and Marcelo D. de Amorim²

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

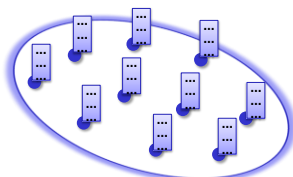
2nd WNetVirt'13, October 26, 2013, Angra dos Reis, Brazil
Supported by CAPES, CNPq, Faperj (Brazil), and ANR (France)

State of the Art



State of the Art

Central Unit



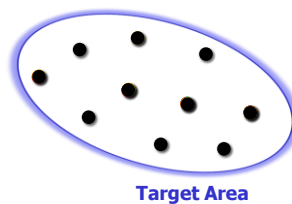
Target Area

1. Synchronization

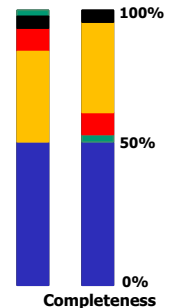
2. Merging

3. Presentation

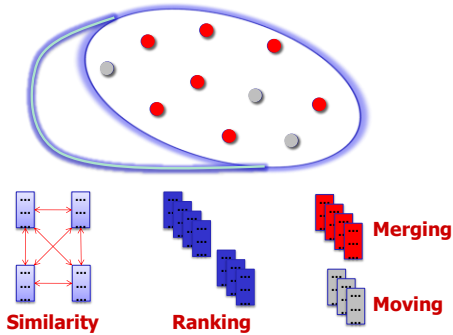
Merging Process



Target Area



Our Approach



Trace Similarity

Intra-flow similarity:

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

Inter-flow similarity:

$$\text{TF-IDF}(t_i, l) = \frac{|f_{i,l}|}{|t_i|} \cdot \log \frac{|\mathcal{T}|}{|\{t_i \in \mathcal{T} | f_{i,l} \in t_i\}|}$$

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

Trace Ranking

We consider a fully connected graph $G(V, E)$

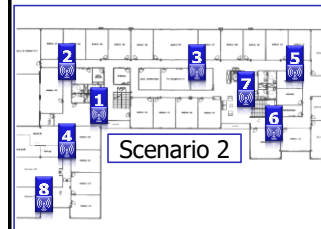
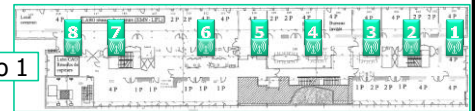
v_i : is the trace captured by the i -th monitor

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

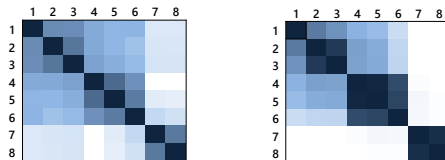
Experimental Setup

Scenario 1

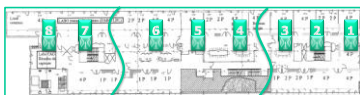


8 monitors
100 minutes

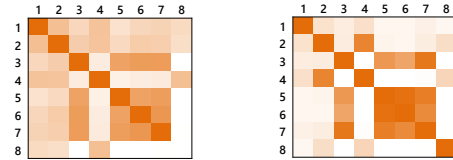
Similarity: Scenario I



similarity
low high

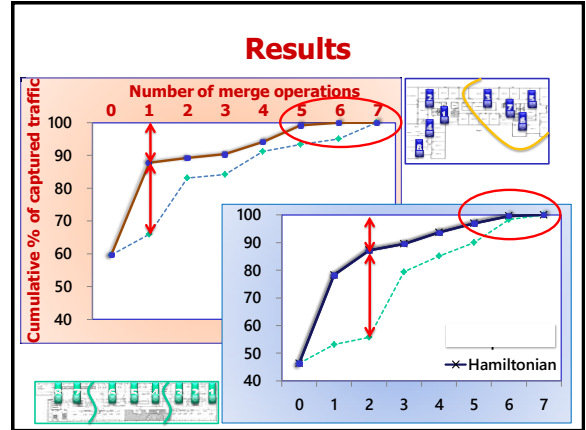
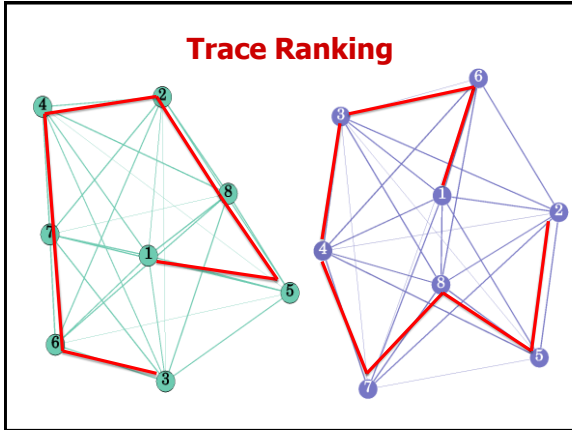


Similarity: Scenario II



similarity
low high





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. Campista¹, Matteo Sammarco²,
Marcelo D. de Amorim² e Tahiry Razafindralambo³

¹GTA/PEE-COPPE/DEL-Poli – UFRJ – Brasil
²LIP6/CNRS – UPMC Sorbonne Universités – França
³INRIA 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...

Número de smartphones no mundo (bilhões)

Nos próximos 5 anos, o número de smartphones será maior que o dobro atual!

2014 2019 Ano

Fonte: Cisco – VNI Forecast Highlights

O que fazer com essa disponibilidade de recursos?

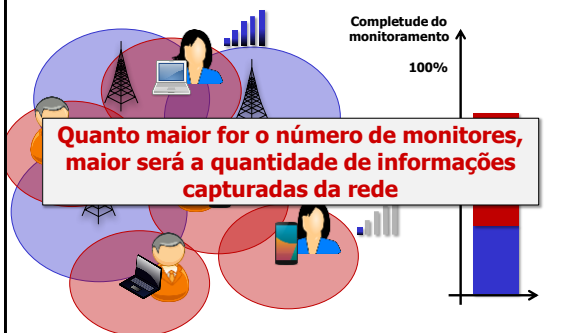
Monitoramento Colaborativo da Rede



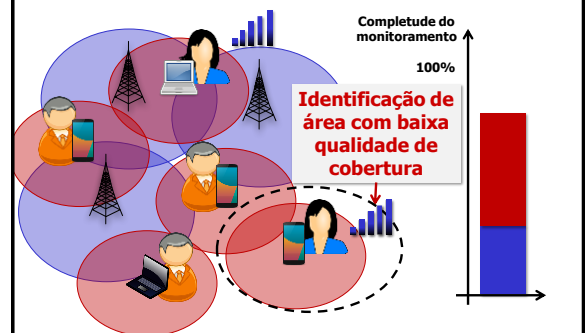
Monitoramento Colaborativo da Rede



Monitoramento Colaborativo da Rede



Possibilidade de Realizar Replanejamento da Rede



Problema da Colaboração: Presença de Usuários Maliciosos



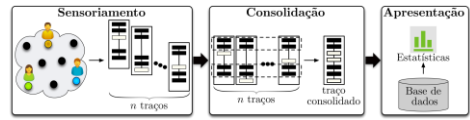
Problema da Colaboração: Presença de Usuários Maliciosos



Contribuições

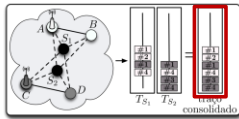
- **Proposta de um sistema de monitoramento colaborativo**
 - Participação dos usuários
- **Identificação de dois possíveis ataques**
 - Ataque de atração e ataque de repulsão
- **Proposta de uma metodologia para a detecção de possíveis nós maliciosos**
 - Metodologia baseada em grafos

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

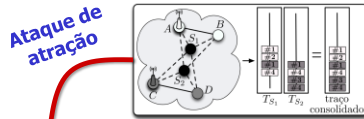
Problema da Colaboração: Consolidação dos Traços de Dados



**6/8 pacotes capturados:
75% de completude!**

Traço consolidado = merge dos traços individuais coletados
Merge aumenta a completude do traço final!

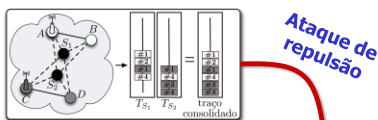
Problema da Colaboração: Consolidação dos Traços de Dados



Usuário malicioso cria fluxos de dados com quadros faltantes

**8/12 pacotes capturados:
66% de completude!**

Problema da Colaboração: Consolidação dos Traços de Dados



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 (α)**

$$\alpha = 1 - (m(t)/s(t))$$

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 α , enquanto um de repulsão aumenta α ...

Acurácia do Sistema

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

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

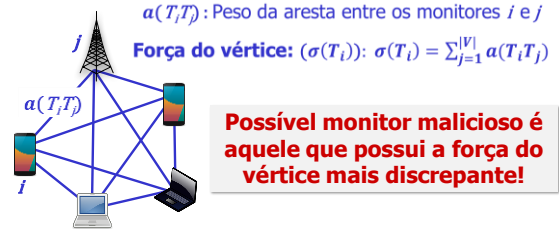
Quadros perdidos por todos os n Quadros enviados por todos os m

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

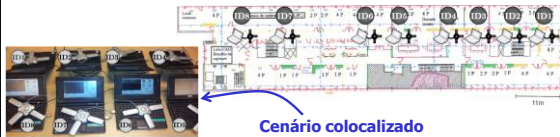
- Modelagem da rede de monitores como um grafo



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

Rede de Testes e Conjunto de Dados

Cenário esperso



Cenário colocalizado

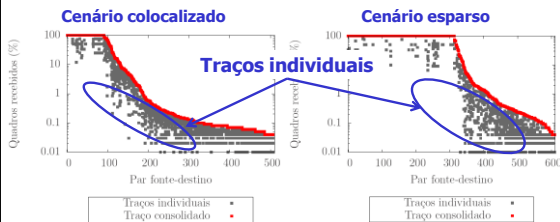
Acurácia de cada traço em comparação ao consolidado ($\times 10^{-3}$)

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

Experimentos

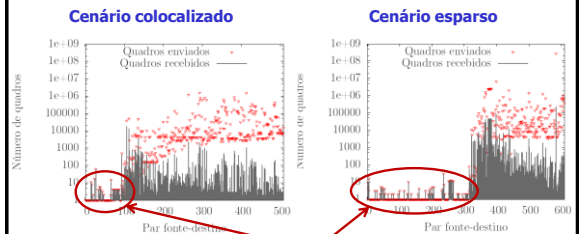
- Desempenho do monitoramento colaborativo em rede livre de atacantes
- Impacto dos ataques identificados e desempenho do sistema de detecção

Fração de Quadros Capturados pelos Diferente Traços



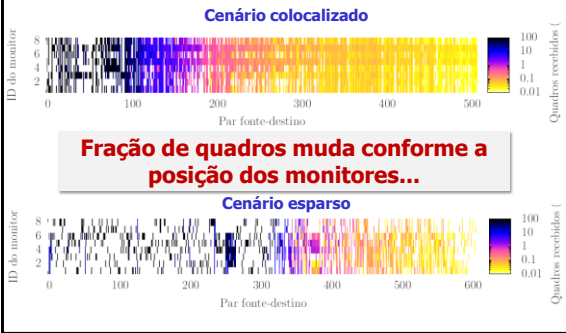
Grande diferença entre a acurácia dos traços individuais e do consolidado

Fração dos Quadros Capturados em Função do Tamanho dos Fluxos

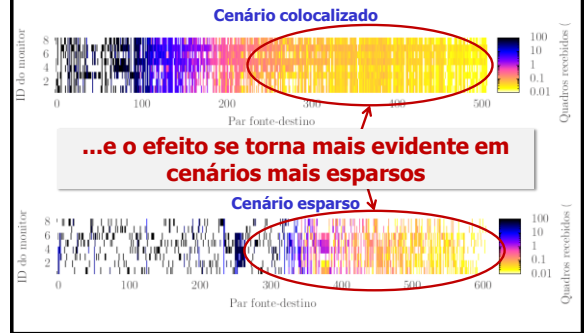


Fluxos com menos quadros têm menor perda...

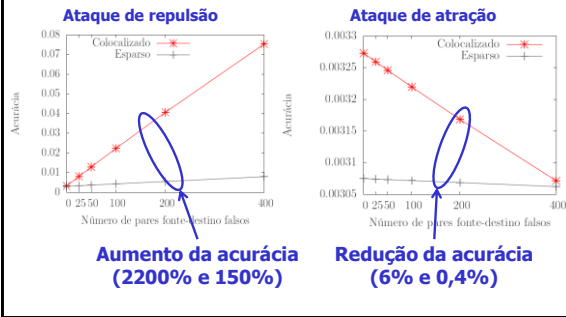
Fração de Quadros Capturados em Função da Posição dos Monitores



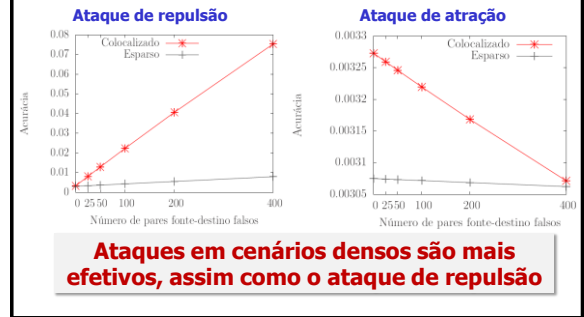
Fração de Quadros Capturados em Função da Posição dos Monitores



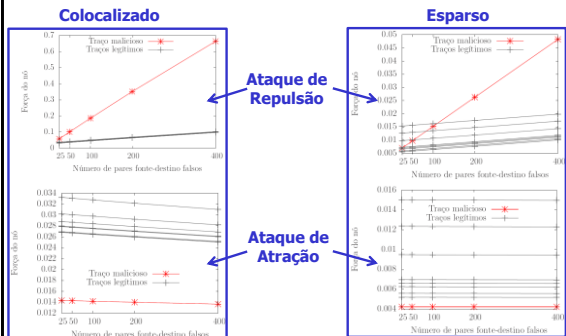
Impacto dos Ataques: Efeito da Participação de Usuários Maliciosos



Impacto dos Ataques: Efeito da Participação de Usuários Maliciosos



Detecção de Atacantes Potenciais: Variação da Força dos Monitores



Detecção de Atacantes Potenciais: Variação da Força dos Monitores



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

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



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. Campista¹, Matteo Sammarco²,
Marcelo D. de Amorim² e Tahiry Razafindralambo³

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

WPerformance 2015

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