Monitoring of Multi-Domain Networks

Emna Salhi, Samer Lahoud, Bernard Cousin

INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTEMES ALÉATOIRES

UMR IRISA

Outline

- Network monitoring phases
- Monitoring costs
- Monitoring of multi-domain networks
- Per-domain monitoring
- Global monitoring
- Comparison metrics
- Comparison methodology
- Results
- Conclusion

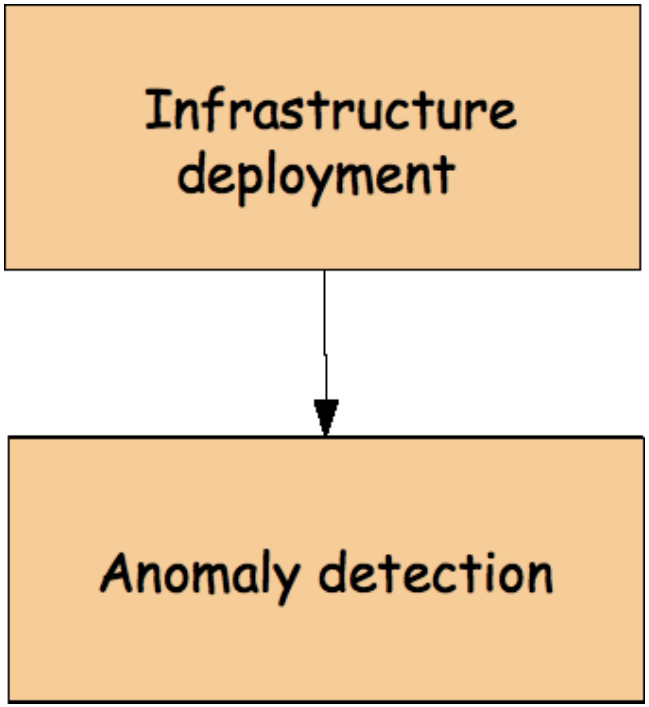
Network Monitoring Phases

Infrastructure deployment

- Select monitor locations
- Select monitoring paths

[E. Salhi & al. "Joint Optimization of Monitor Location and Network Anomaly Detection, LCN 2010].

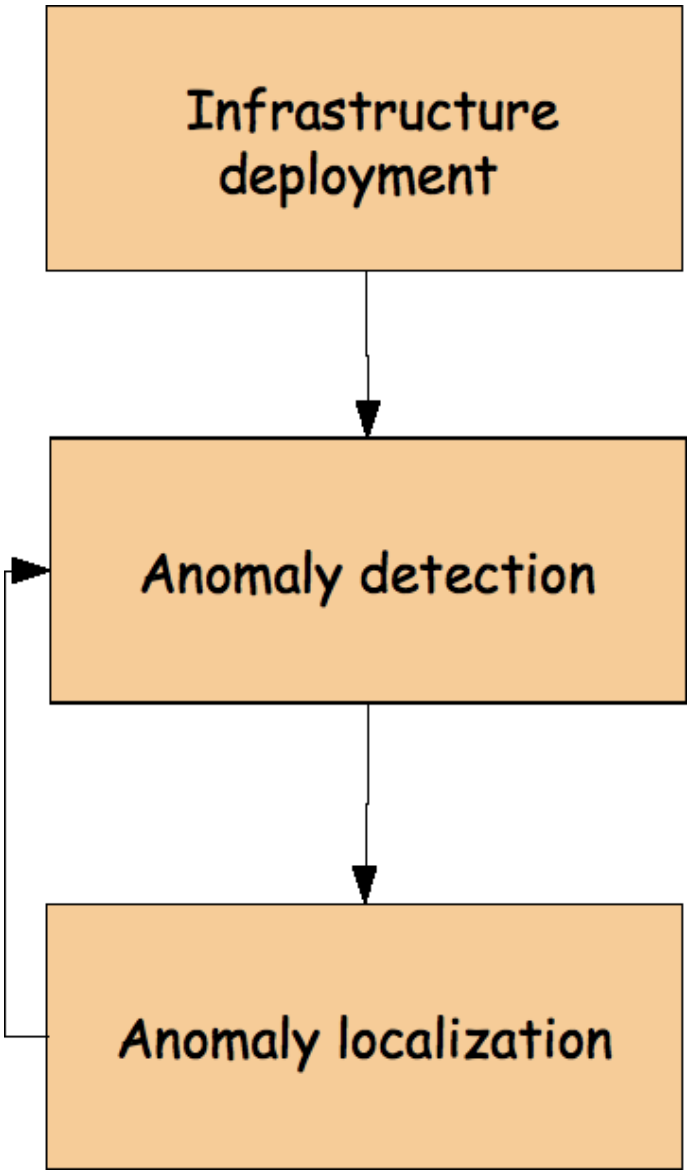
Network Monitoring Phases



- Select monitor locations
- Select monitoring paths

- Full coverage of network links

Network Monitoring Phases

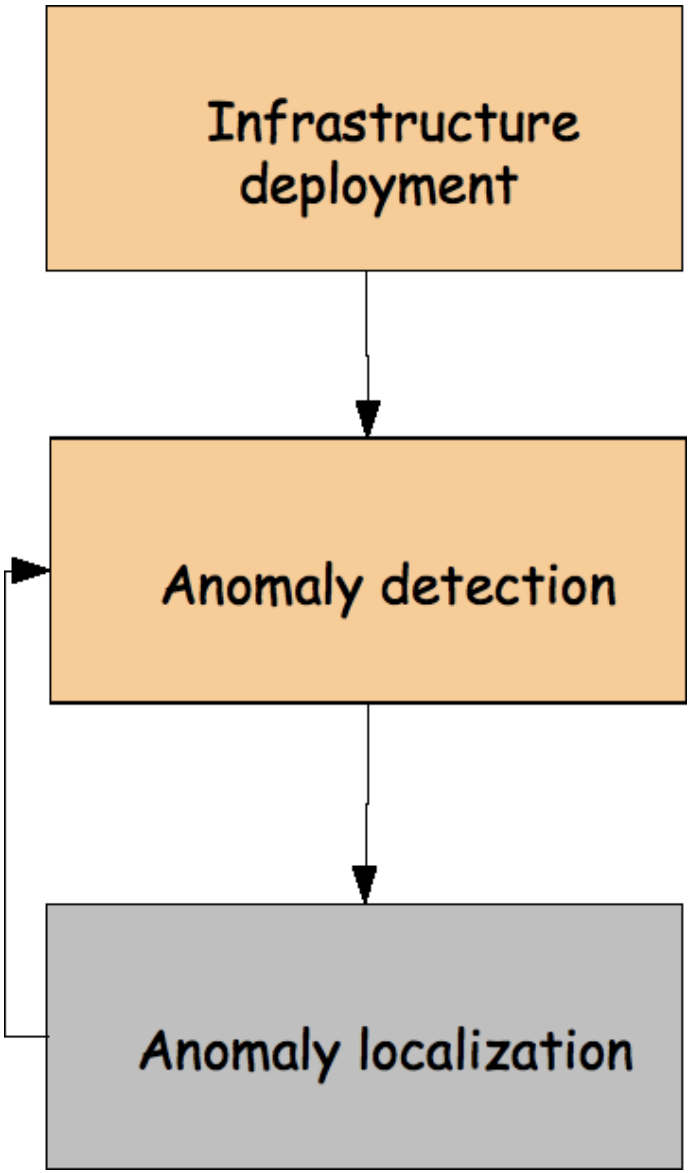


- Select monitor locations
- Select monitoring paths

- Full coverage of network links

- Pinpoint the anomalous link(s)

Network Monitoring Phases



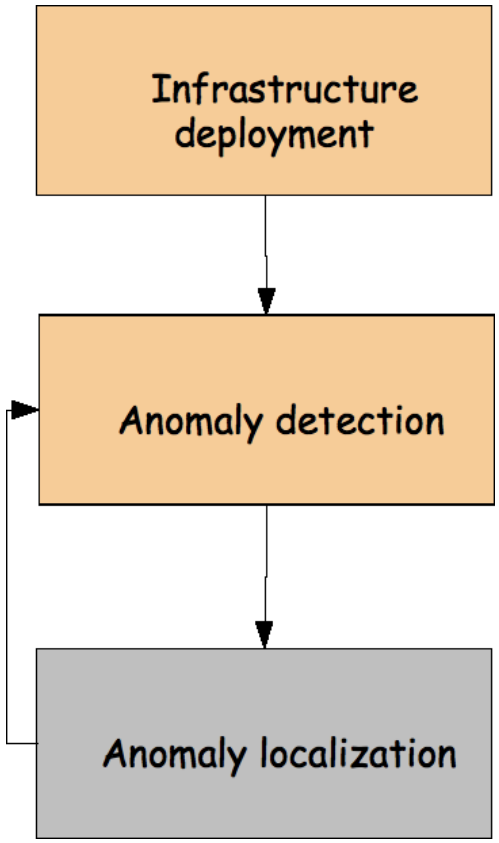
- Select monitor locations
- Select monitoring paths

- Full coverage of links

- **Pinpoint the anomalous link(s)**

[E. Salhi & al. Localization of Single Link-Level Network Anomalies. International Conference on Computer Communication Networks, 2012].

Network Monitoring Phases



- Select monitor locations
- Select monitoring paths

- Full coverage of links

- Distinguish between suspect links

Our goal : Deploying a monitoring infrastructure for anomaly detection in multi-domain networks

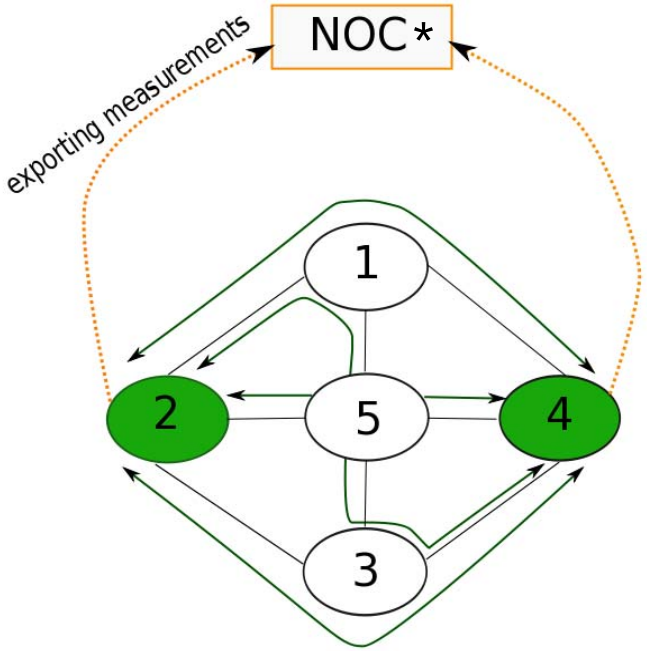
Monitoring Cost

- Infrastructure cost: proportional to the number of deployed monitoring devices

Monitoring Cost

- Infrastructure cost: proportional to the number of deployed monitoring devices

- Communication cost: function of the number and the locations of monitoring devices



* NOC denotes the Network Operation Center

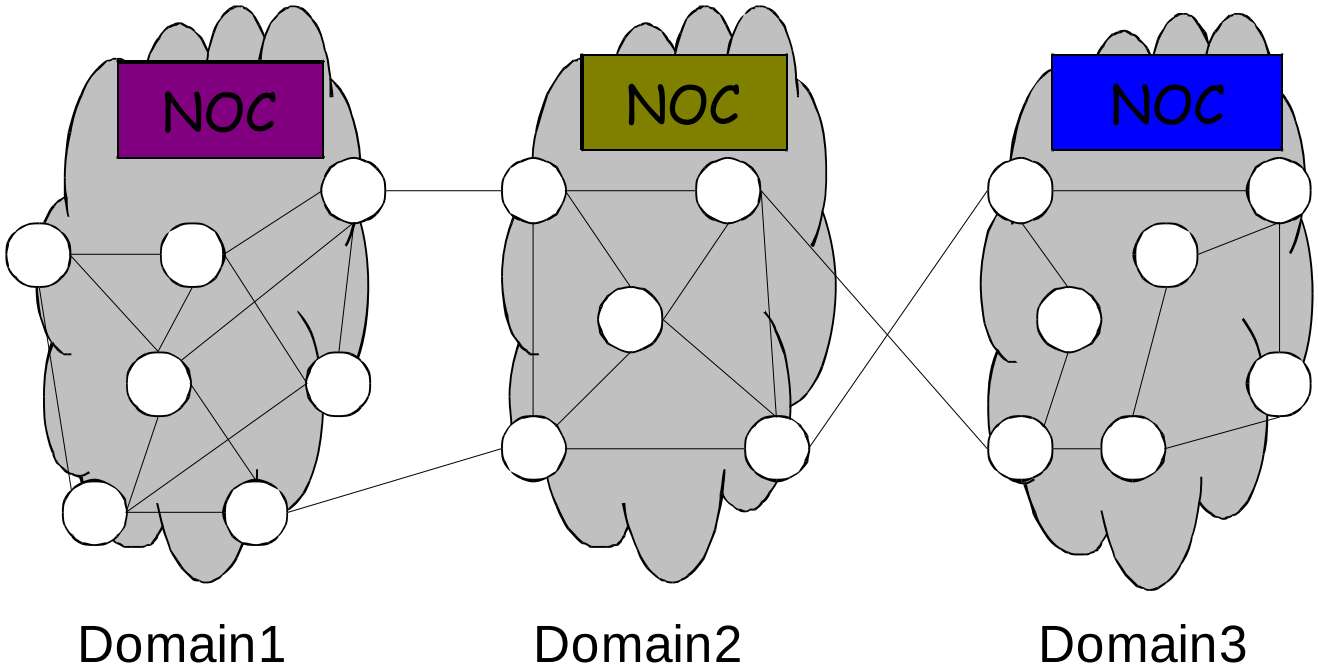
Monitoring Cost

- Infrastructure cost: proportional to the number of deployed monitoring devices

- Communication cost: function of the number and the locations of monitoring devices

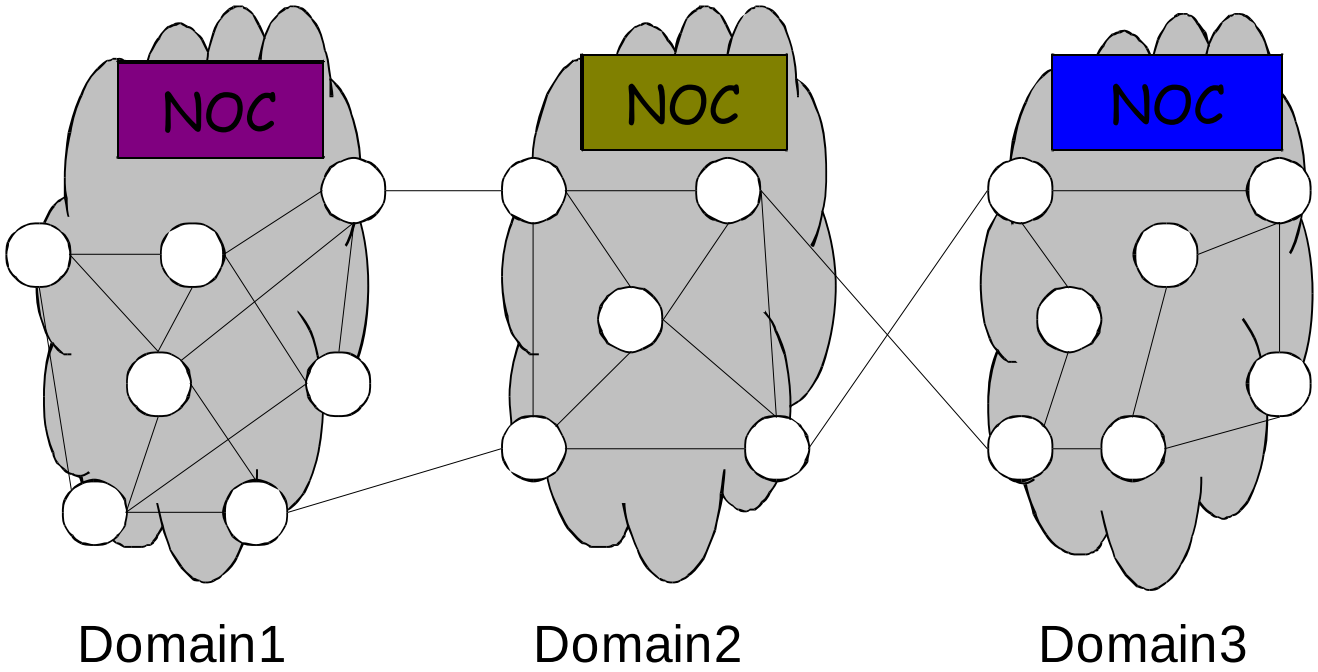
- Detection overhead: redundant monitoring of links

Monitoring Multi-domain Networks



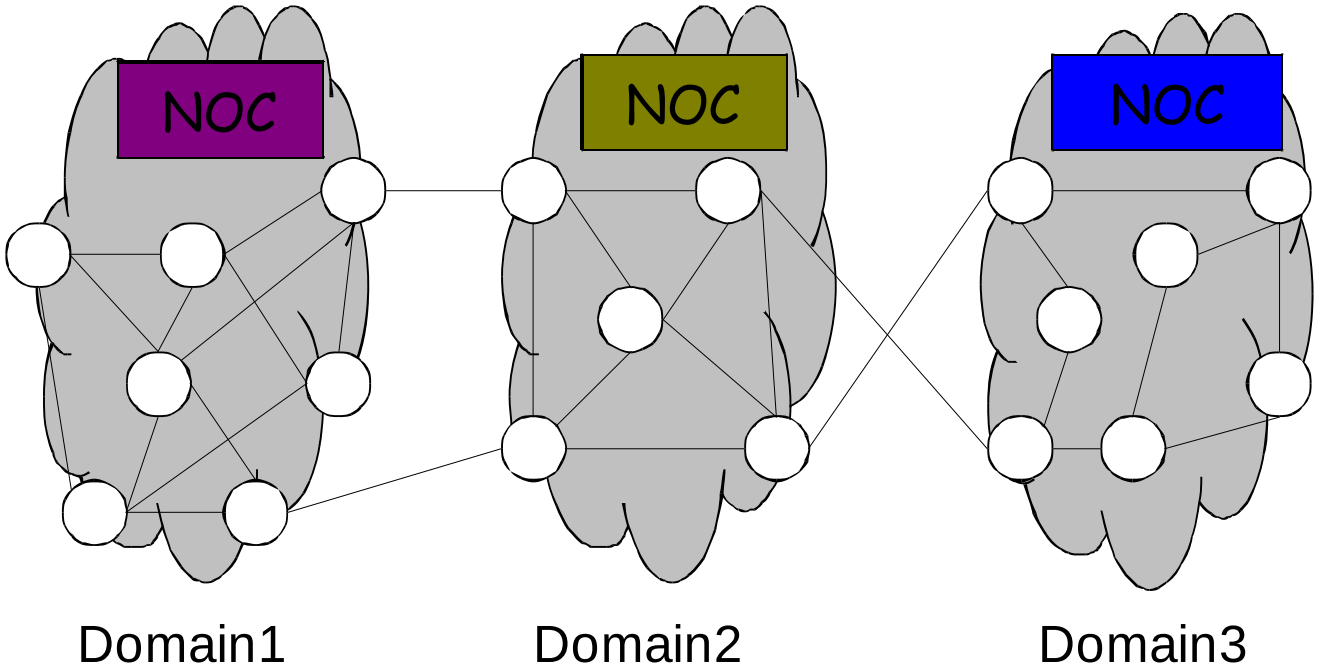
Monitoring Multi-domain Networks

- Dense intra-domain networks



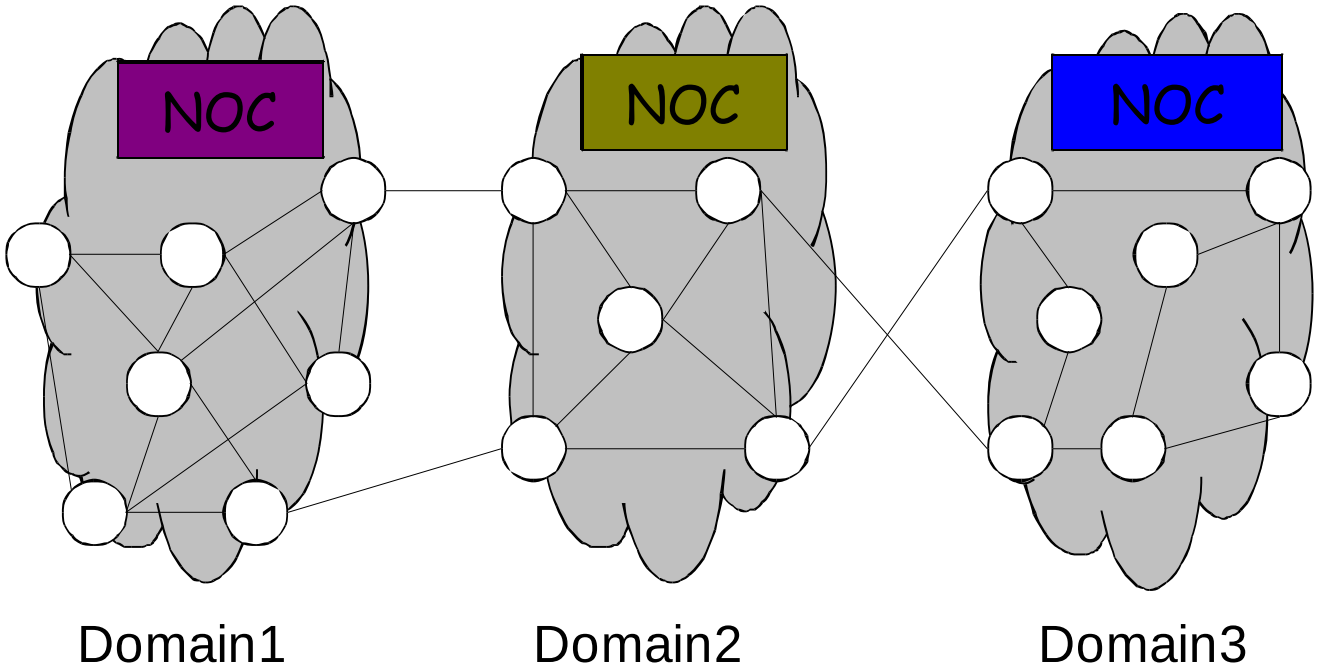
Monitoring Multi-domain Networks

- Dense intra-domain networks
- Few inter-domain connections



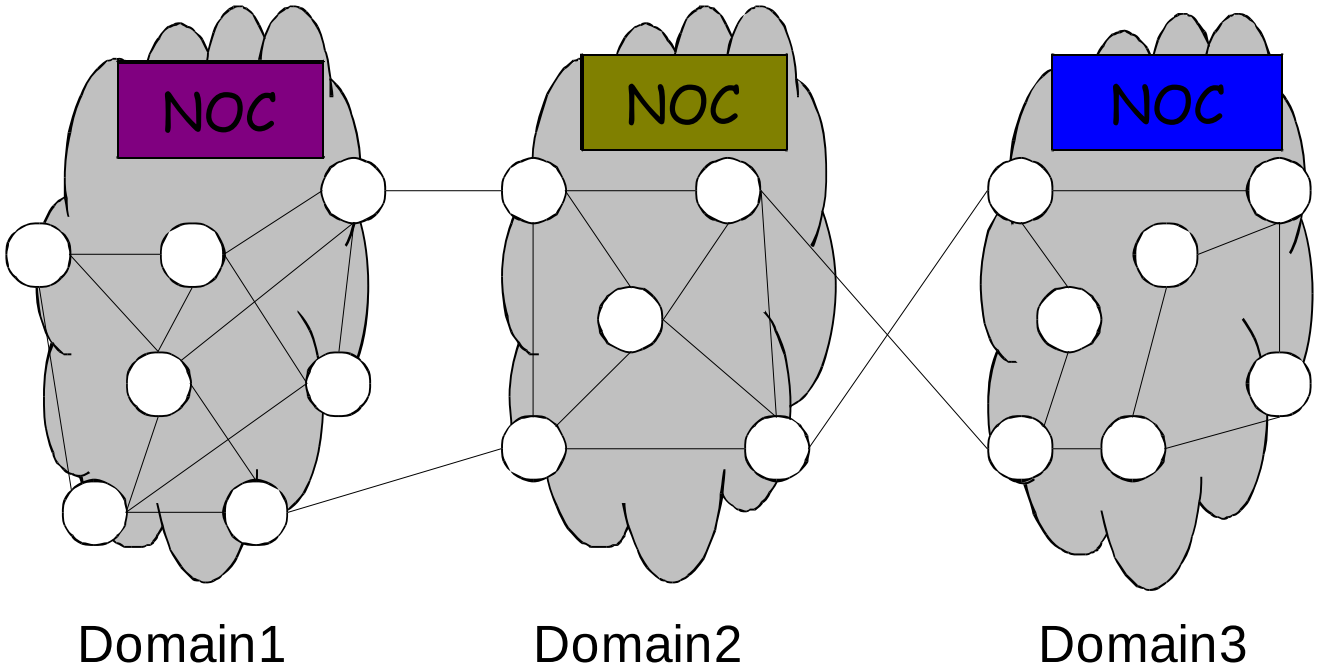
Monitoring Multi-domain Networks

- Dense intra-domain networks
- Few inter-domain connections
- Different domain authorities
  - Adaptation to local policy
  - Fairness



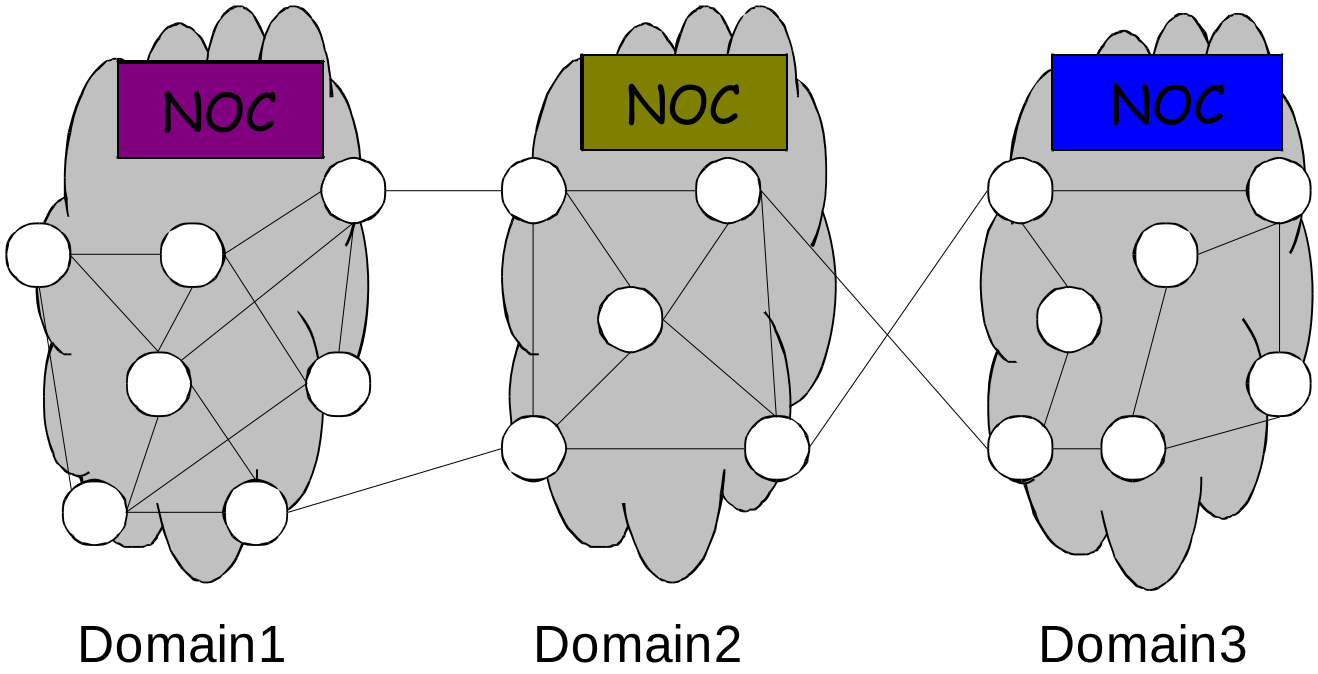
Monitoring Multi-domain Networks

- Dense intra-domain networks
- Few inter-domain connections
- Different domain authorities:
  - Adaptation to local policy
  - Fairness
- Confidentiality constraint

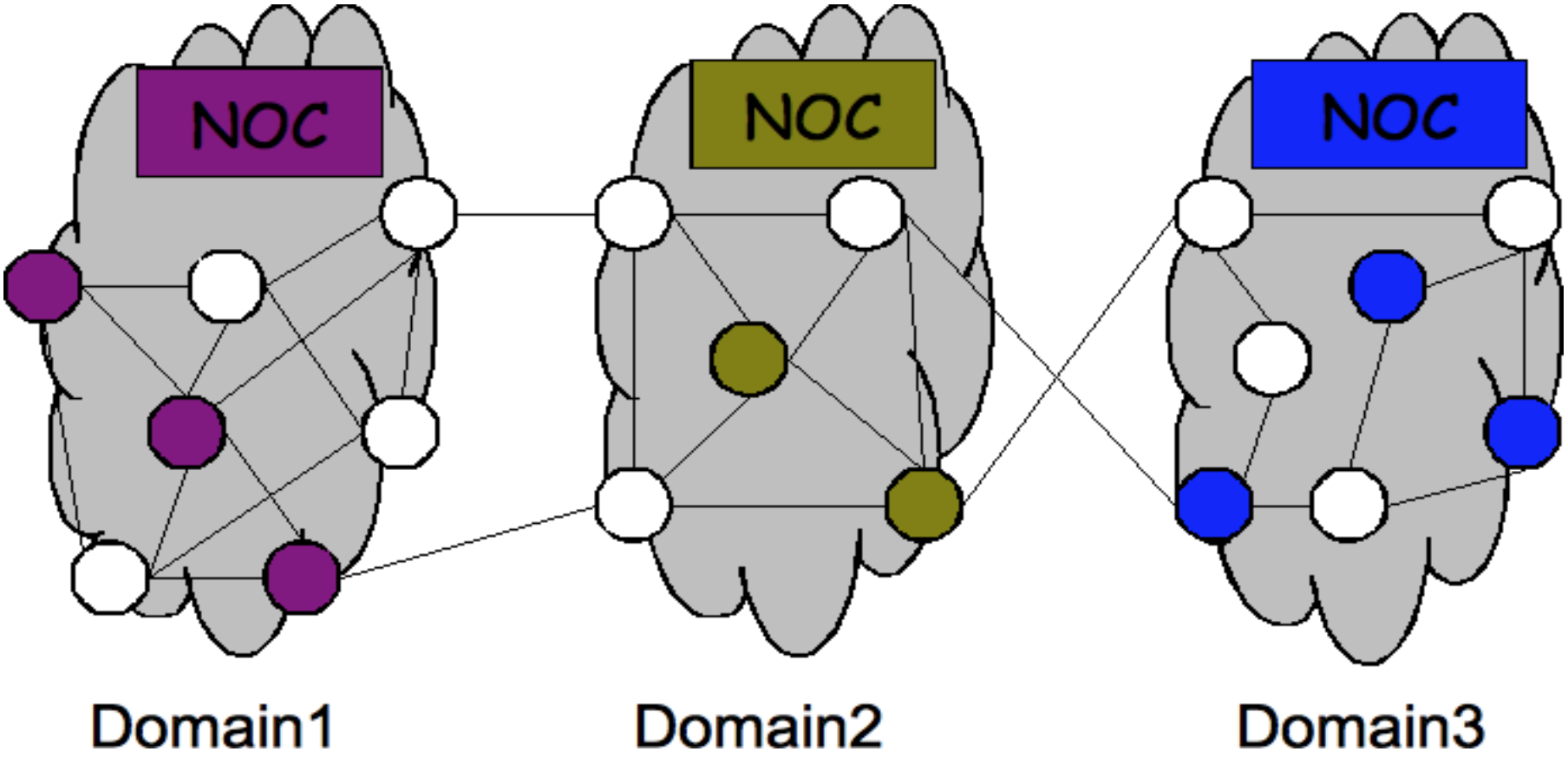


Monitoring Multi-domain Networks

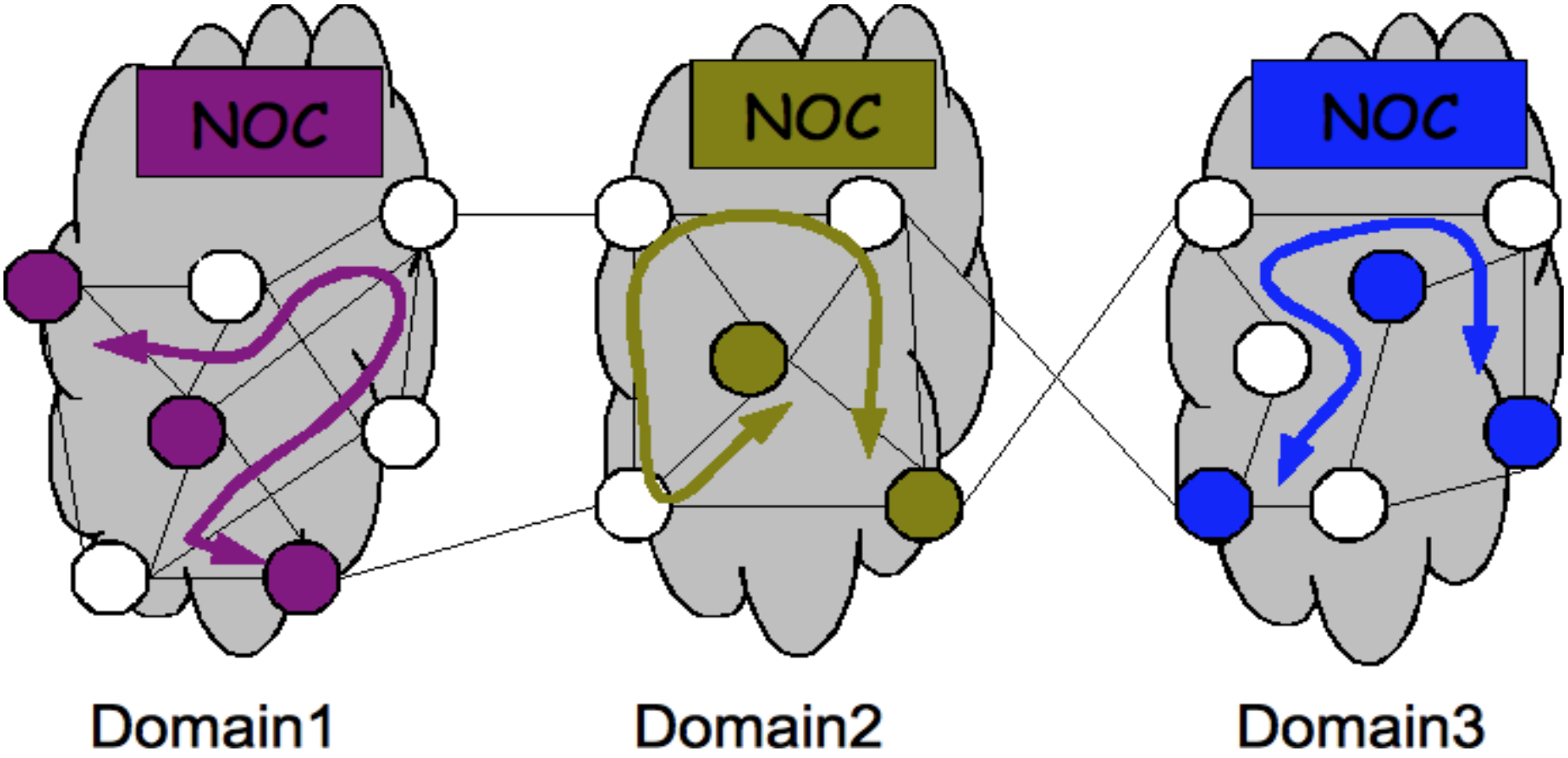
- Dense intra-domain networks
- Few inter-domain connections
- Different domain authorities:
  - Adaptation to local policy
  - Fairness
- Confidentiality constraint
- Short detection delay



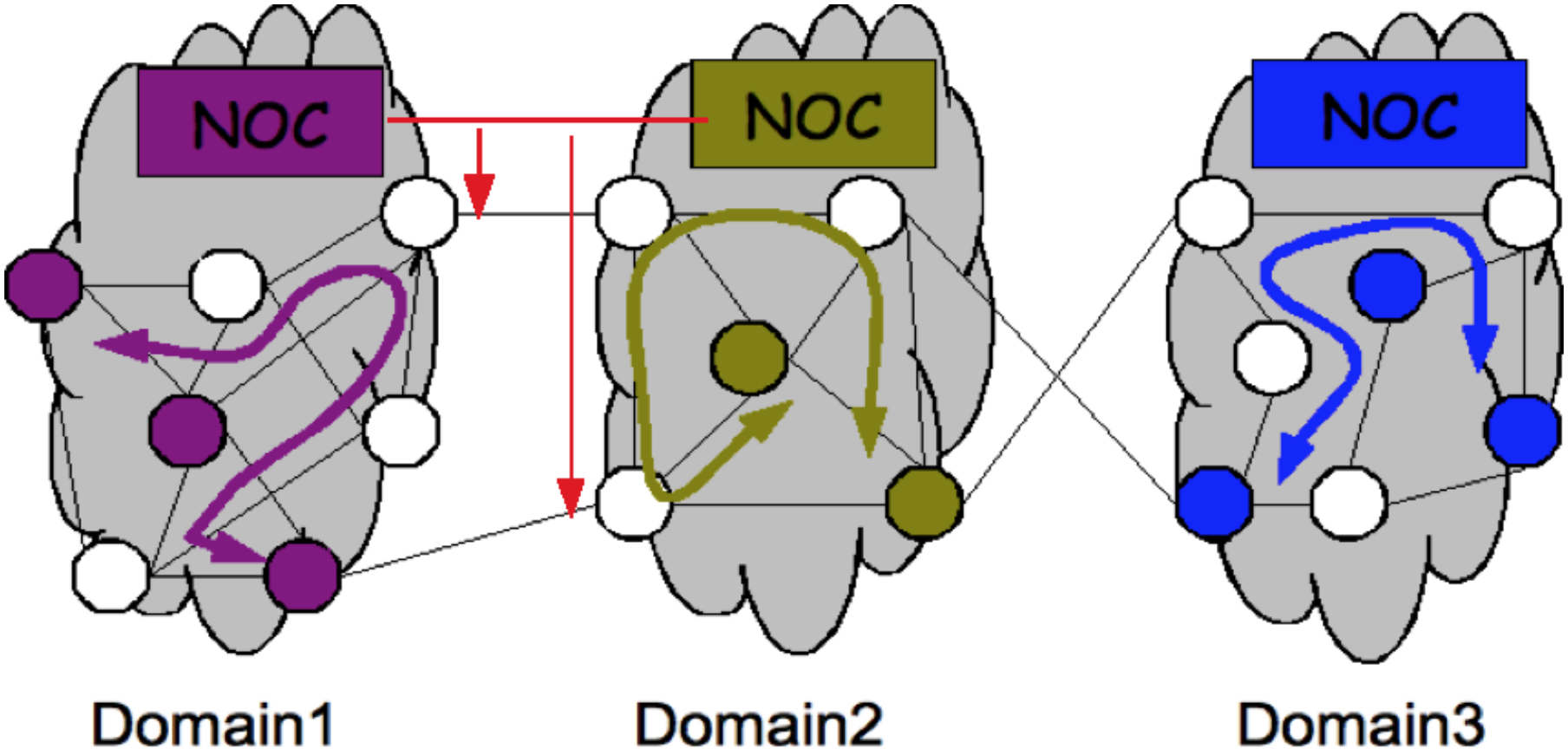
Per-Domain Monitoring



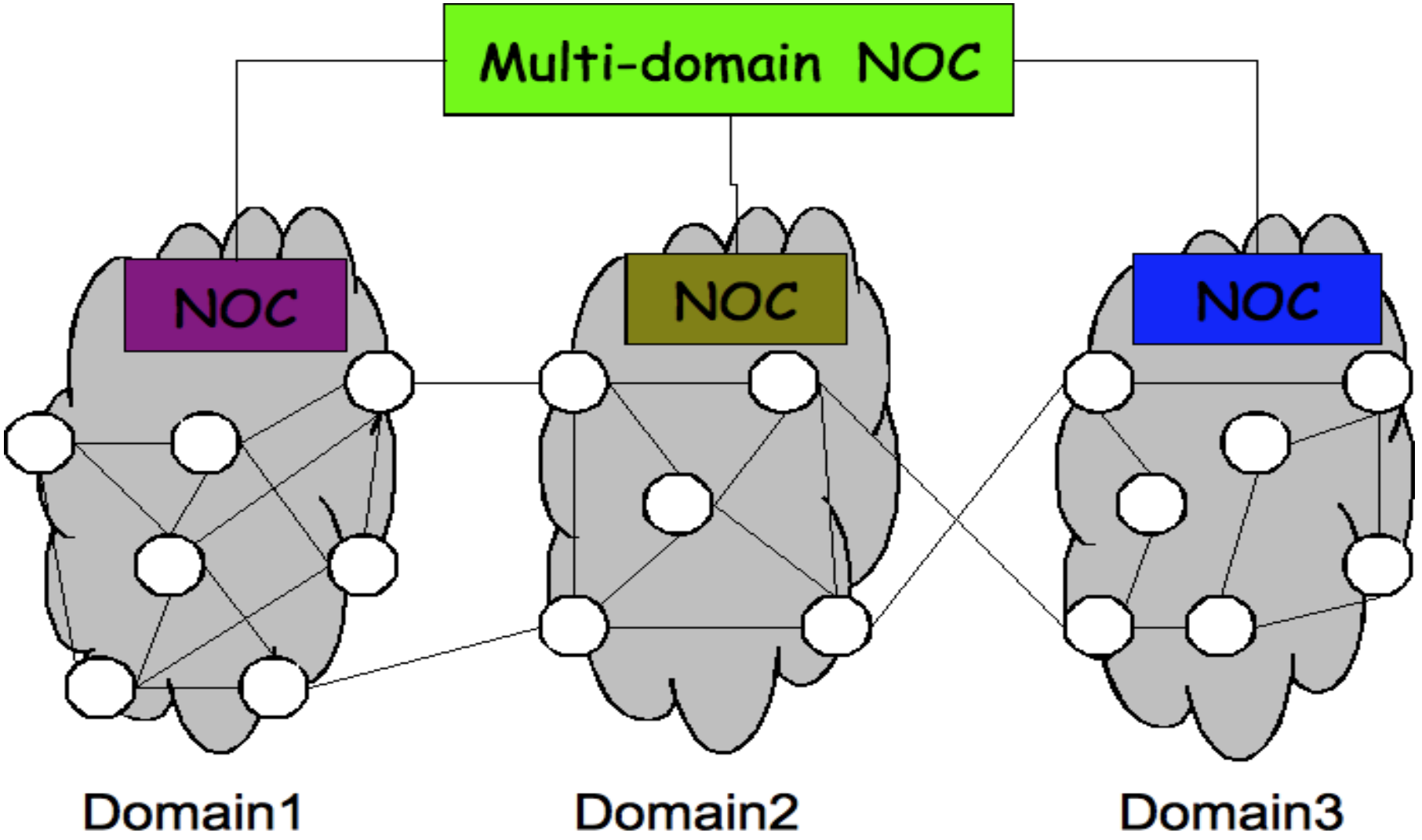
Per-Domain Monitoring



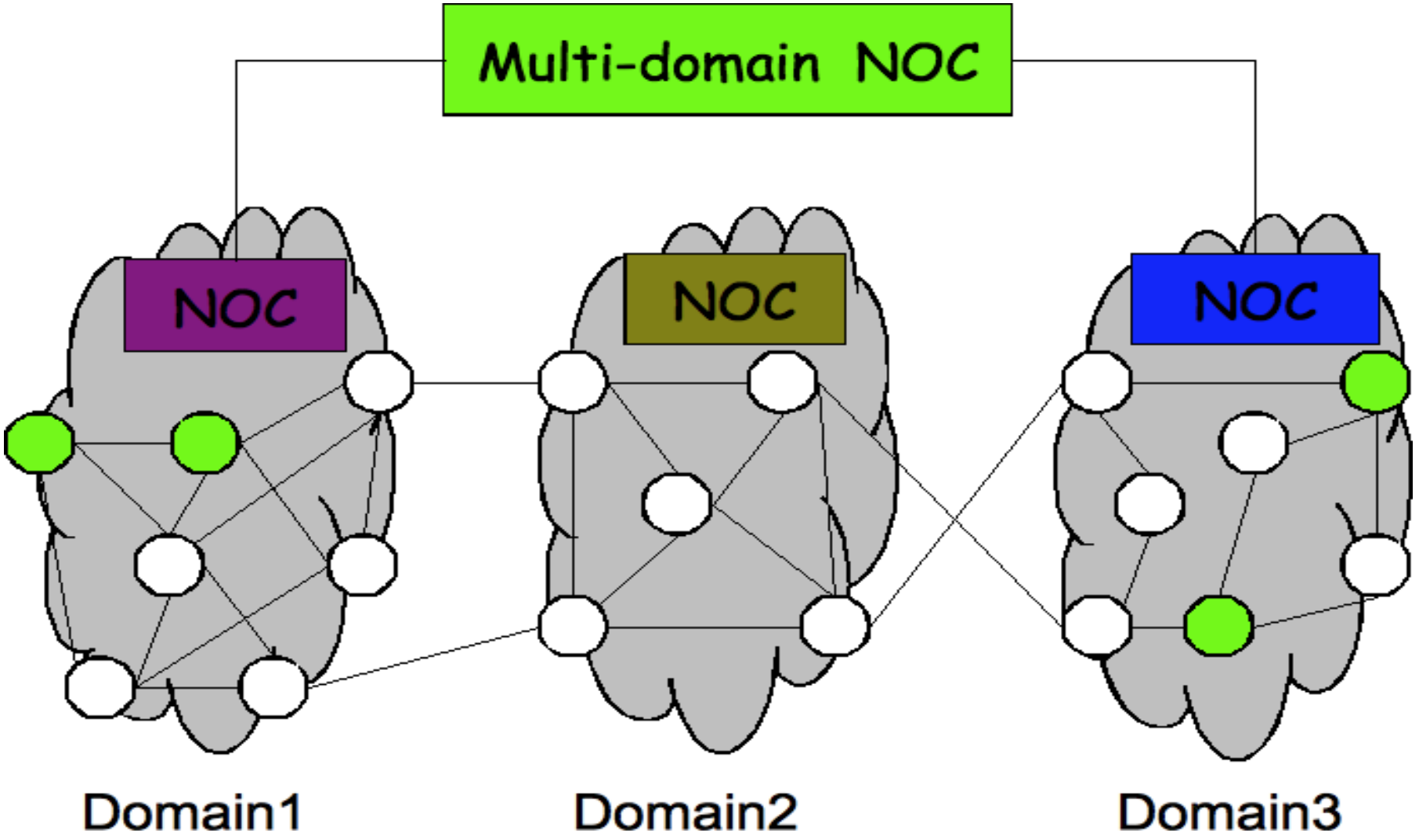
Per-Domain Monitoring



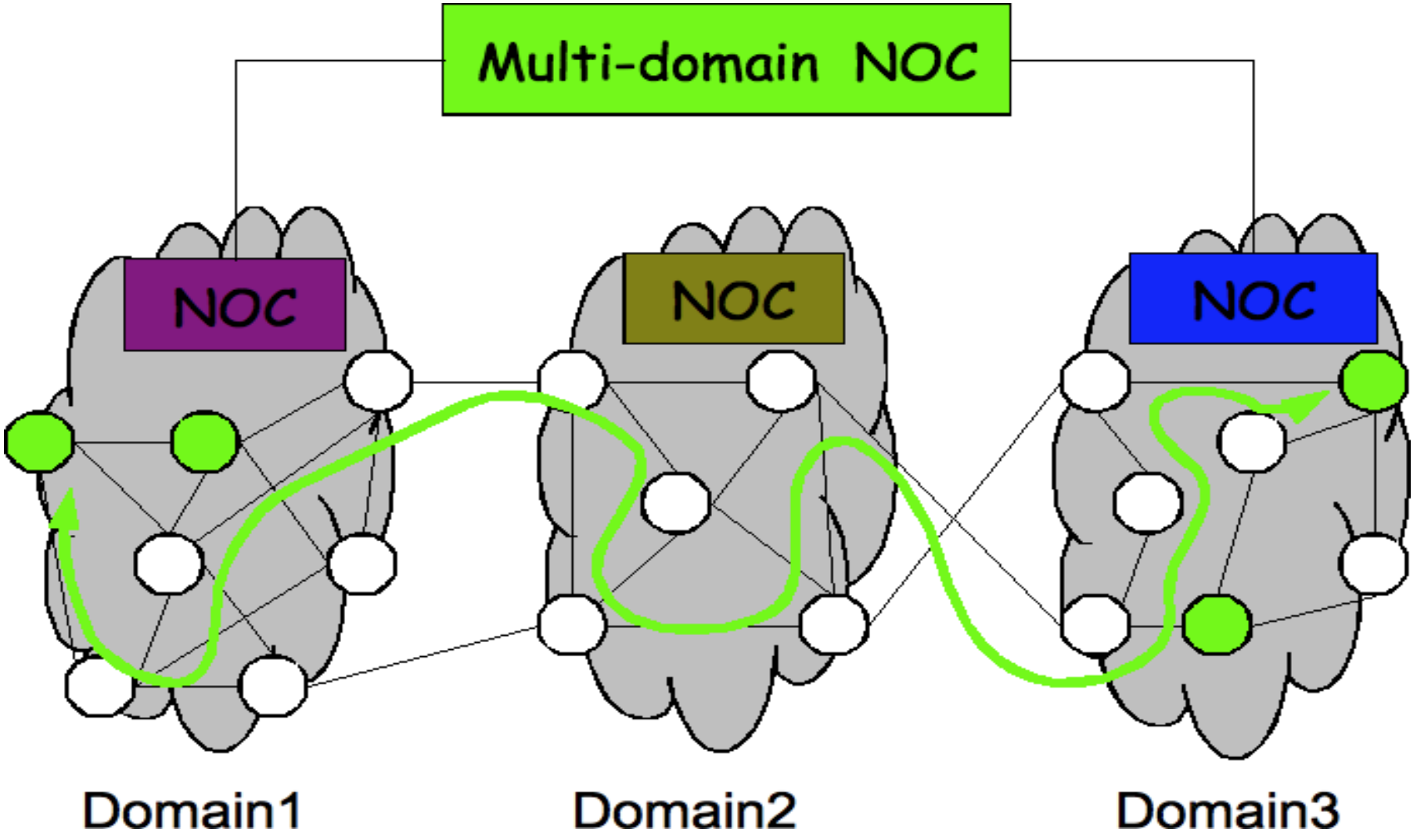
Global Monitoring



Global Monitoring



Global Monitoring



Comparison Metrics

- Cost: infrastructure cost + communication cost + detection overhead

Comparison Metrics

- Cost: infrastructure cost + communication cost + detection overhead

- Fairness: fair distribution of the monitoring load among domains

Comparison Metrics

- Cost: infrastructure cost + communication cost + overhead

- Fairness: fair distribution of the monitoring load among domains

- Quality of the detection solution: detection delays are proportional to the length of the monitoring paths

Evaluation Methodology

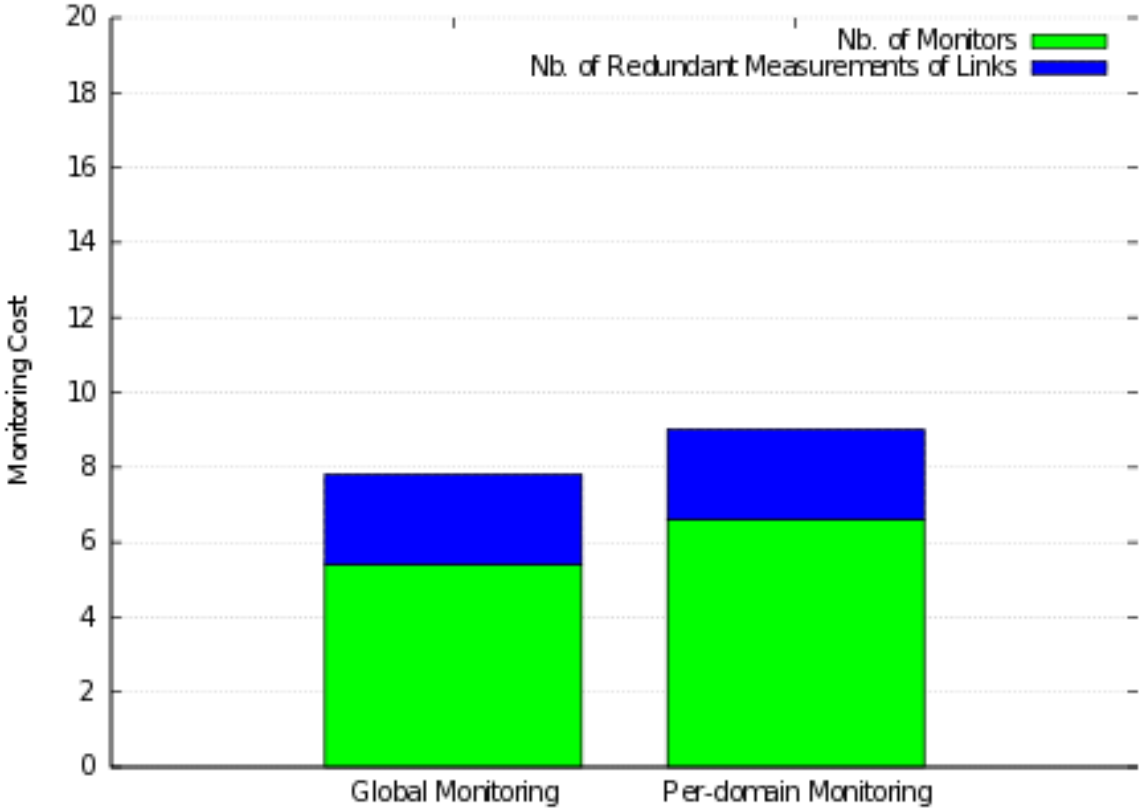
- A multi-domain network of 3 domains
- Random topology generator: Brite

	Nodes	Intra-domain Links	Inter-domain Links
Domain 1	10	31	4-6
Domain 2	15	59	4-6
Domain 3	10	31	4-6

- Anomaly detection heuristic:
  - Joint optimization of the 3 detection costs (*)

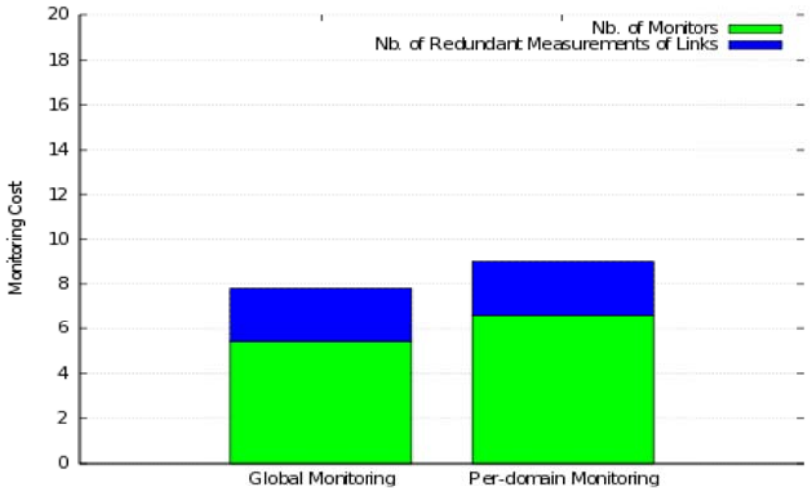
(*) : [E. Salhi & al. "Joint Optimization of Monitor Location and Network Anomaly Detection, IEEE Local Computer Network, 2010].
and [E. Salhi & al. "Heuristics for Joint Optimization of Monitor Location and Network Anomaly Detection". IEEE International Conference on Communications, 2011]

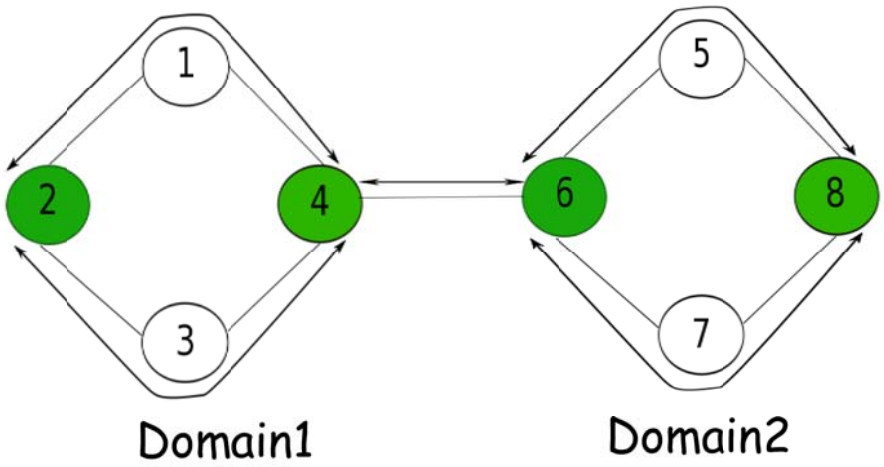
Results: Cost



[E. Salhi & al. "Global Versus Per-Domain Monitoring of Multi-Domain Networks". 36th Annual IEEE Conference on Local Computer Networks, 2011]

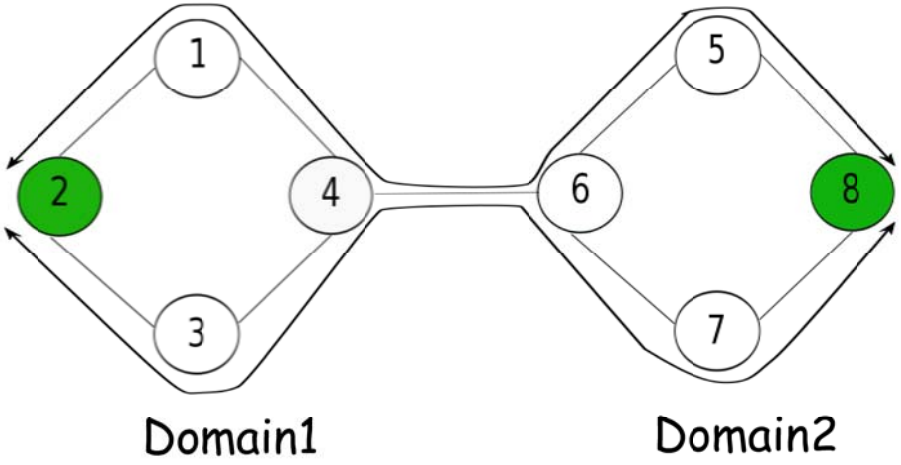
Performance Evaluation: Cost





Per-domain monitoring

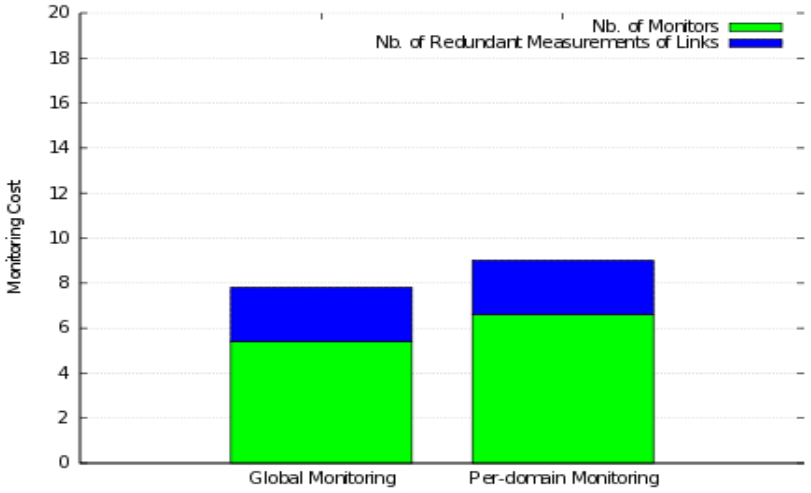
4 monitors, 0 redundant monitored link



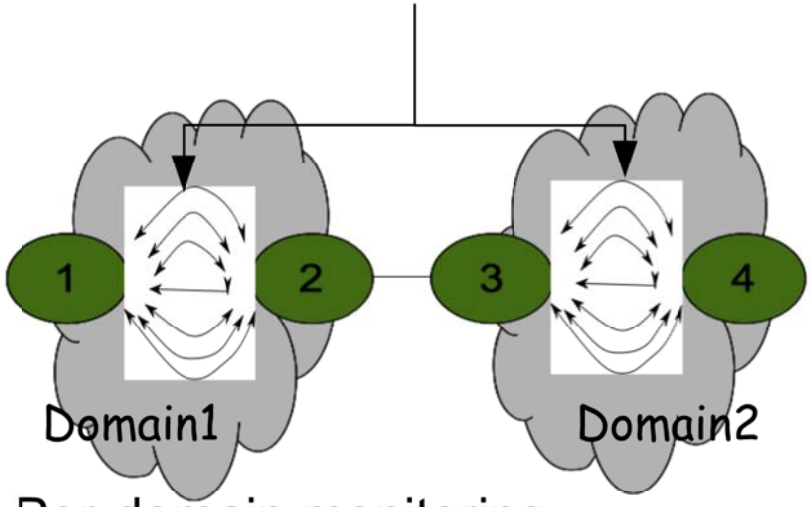
Global monitoring

2 monitors, 1 redundant monitored link

Performance Evaluation: Cost

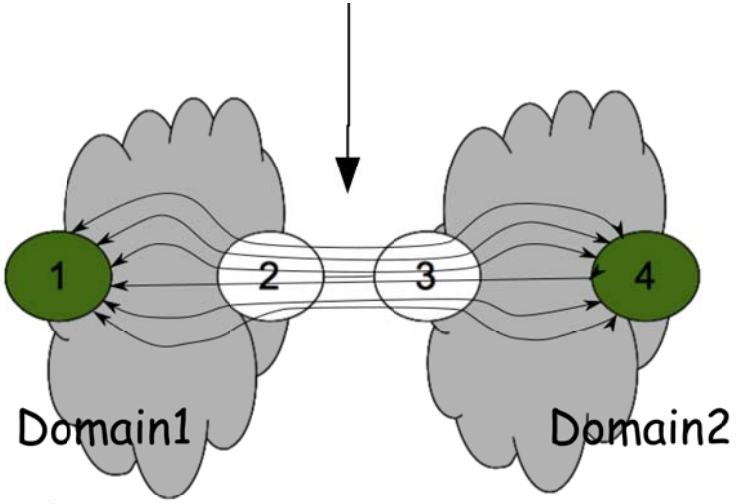


m1+m2 monitoring paths



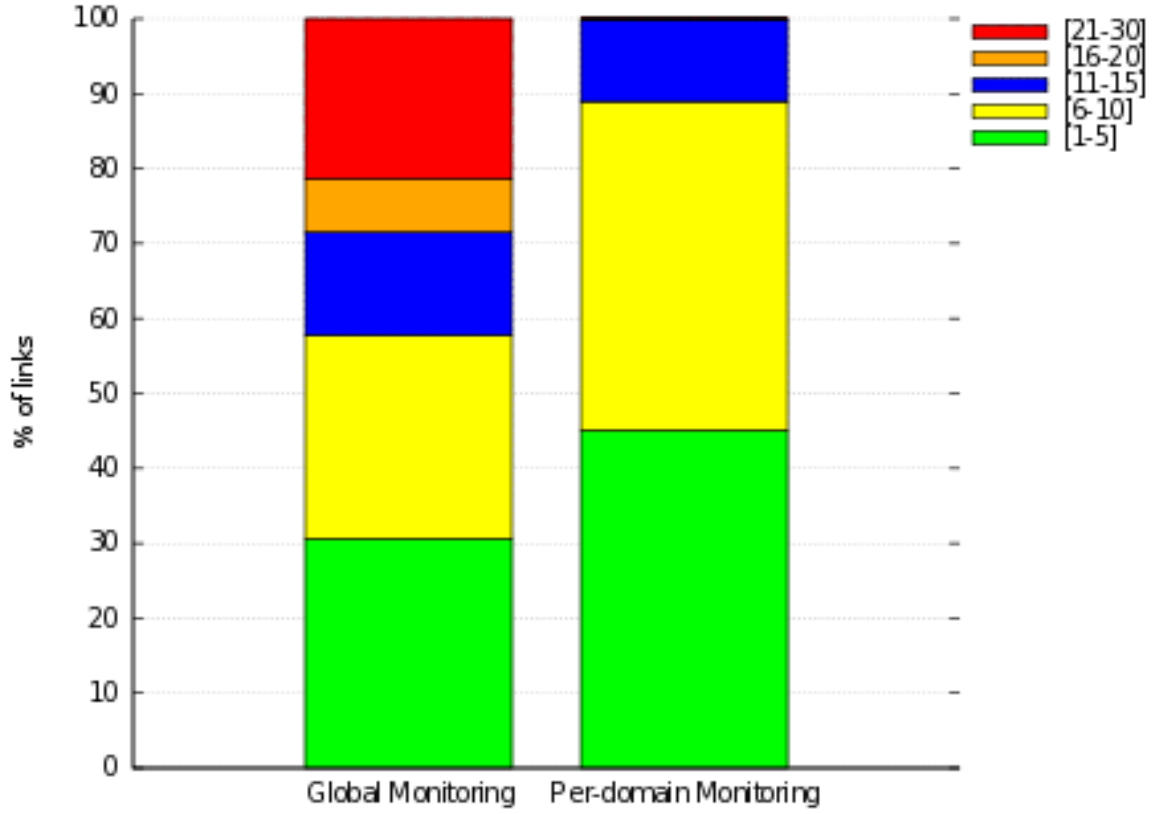
Per-domain monitoring

n-1 redundant monitored links



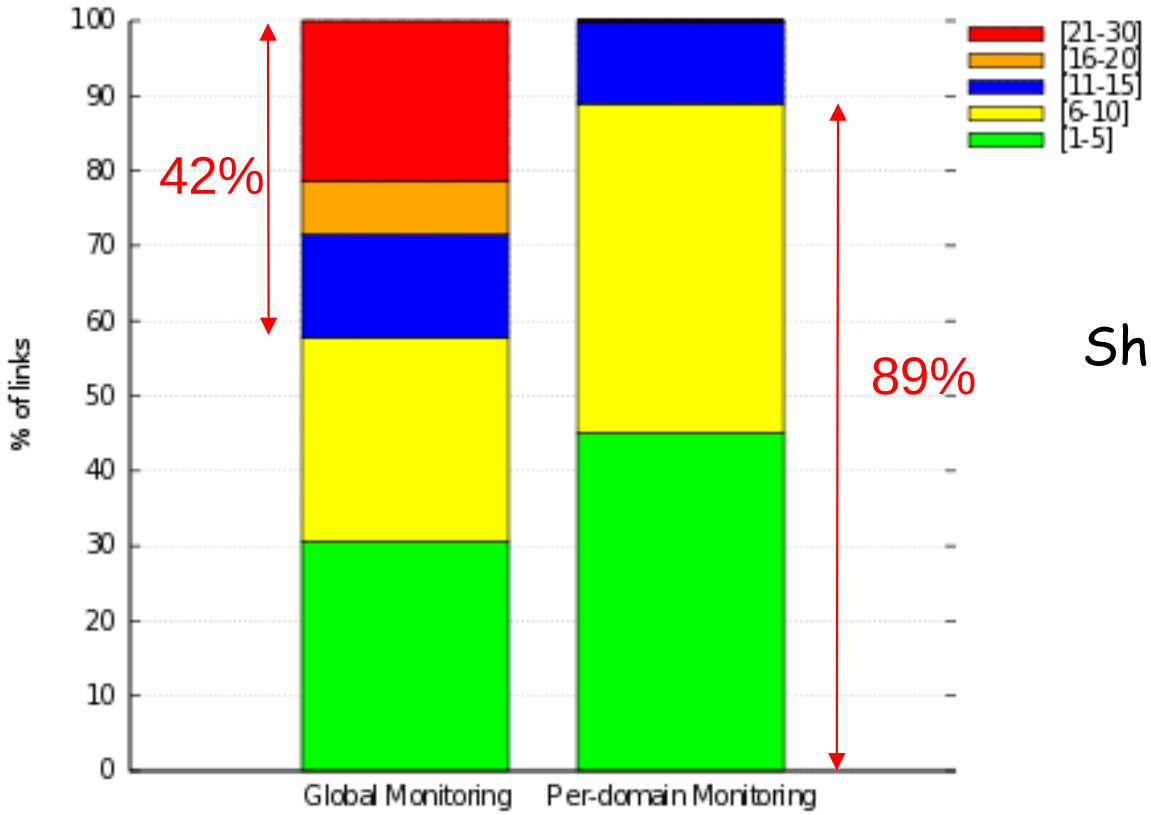
Global monitoring

Quality of the Solution



Distribution of links by path length

Quality of the Solution

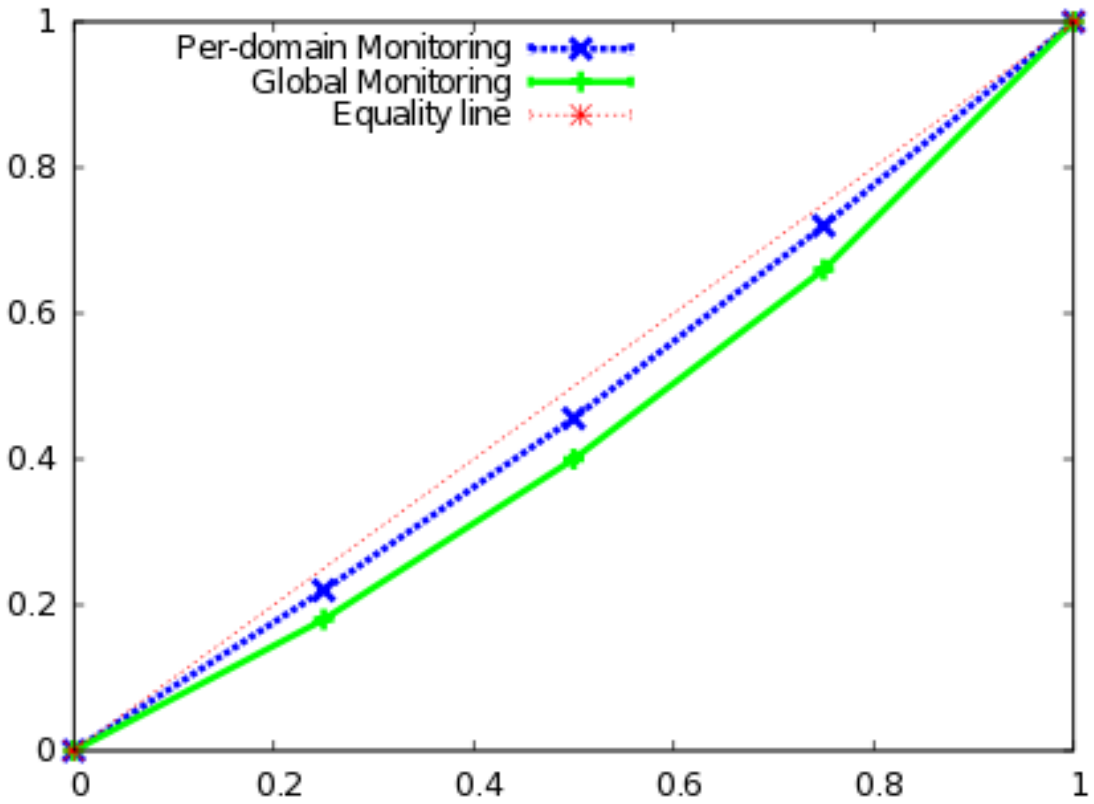


Distribution of links by path length

Shorter is better :

- Short path means small detection delay, because detection is done at the monitor (i.e. the end points of monitoring paths)

Performance Evaluation: Fairness



4 domains, each with 18 links and 8 nodes, symmetrically interconnected to 2 other domains.
Location of the redundant monitored links

Lorentz Curve (normalized cumulative distribution function)

Conclusion

- Global monitoring achieves :
  - Slight reduction of the monitoring cost
- But
  - Domain topologies are not confidential
    - It requires trust third party.
  - Fairness is not guaranteed.
  - It produces long monitoring paths:
    - Larger detection delays
- Go for per-domain monitoring !