Guarding Networks Through Heterogeneous Mobile Guards

Waseem Abbas and Xenofon Koutsoukos
Vanderbilt University

Motivation

* Mobile guards (such as UAVs) are being increasingly used for the surveillance and monitoring of critical infrastructure networks such as gas and oil pipelines.
* Advantages include
  * increased efficiency,
  * deployment in remote areas,
  * cost-effectiveness,
  * immediate response etc.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Motivation

British petroleum testing for use of UAVs in pipeline inspection at Prudhoe Bay, Alaska.
(Source: https://www.youtube.com/watch?v=UO0rgiS3wgw)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Outline

- Network monitoring through mobile guards
- A graph-theoretic problem formulation
  - Mobile guards deployment to detect and respond to a sequence of events
  - Eternal security in graphs
- Examples
- Further directions

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

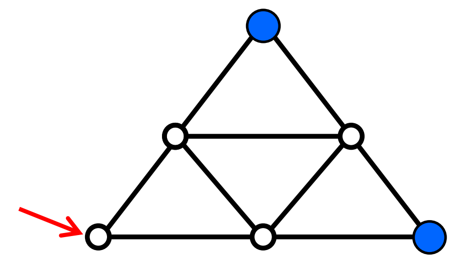
Monitoring through Mobile Guards

* Mobile guards can be equipped with sensors that can detect some event or measure some physical parameter within a certain *range*
* Mobile guards can perform remote attestation of cyber infrastructure devices by executing a query-response protocol
* Using mobile guards (possibly in conjunction with static sensors), how can we
* *efficiently* monitor networks for concerned events (intrusion detection, leak detection etc.)?
* **Challenges:** Using the capabilities of mobile guards (such as ranges) and considering the network structure
  * How many guards should be deployed?
  * At what critical points within the networks?
  * What could be the movement strategies of guards?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Monitoring through Mobile Guards

- We study the problem using a **graph-theoretic** set up.
- A network is modeled by a **graph**
- Mobile guards are located at nodes
- They can detect an event that occurs at some node within its **range** (k-hop), which depends on *physical aspects* of the network.

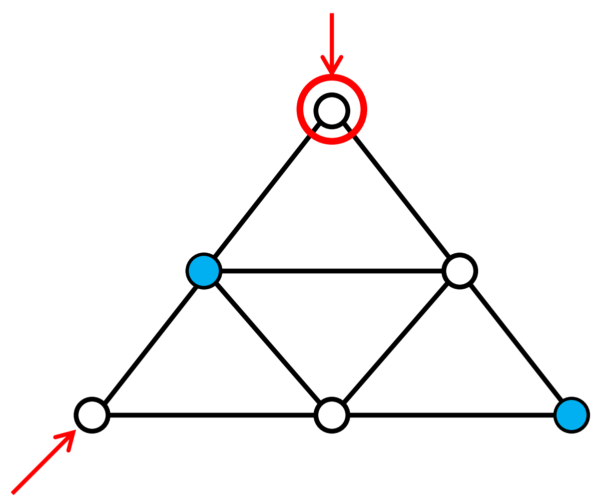


- Mobile guards respond by moving towards the affected node
- We want to achieve complete monitoring of the network at all times even when guards move within the network in response to a ***sequence*** of events

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Case: Single Event

- How to distribute guards such that each node is protected by at least one guard?
- Ans. **Dominating set :** $D \subseteq V, \quad \text{s.t.} \quad \bigcup_{v_i \in D} \mathcal{N}[v_i] = V$



● Guards

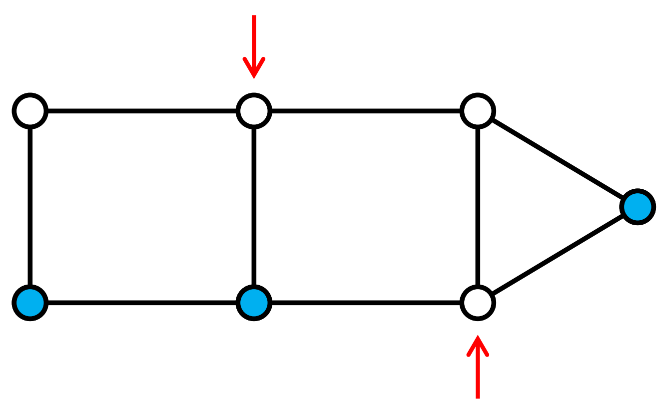
A single attack ✓

A seq. of attacks ✗

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Case: Sequence of Events

- Distribute guards that can defend against a **sequence** of single vertex attacks by a single guard shift along the edges.
- Ans. **Eternal security in graphs**

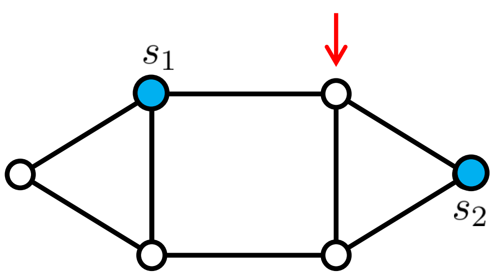


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Major Issues

Eternal Security

- No. of guards
- Deployment of guards
- Guards' movements in case of activity

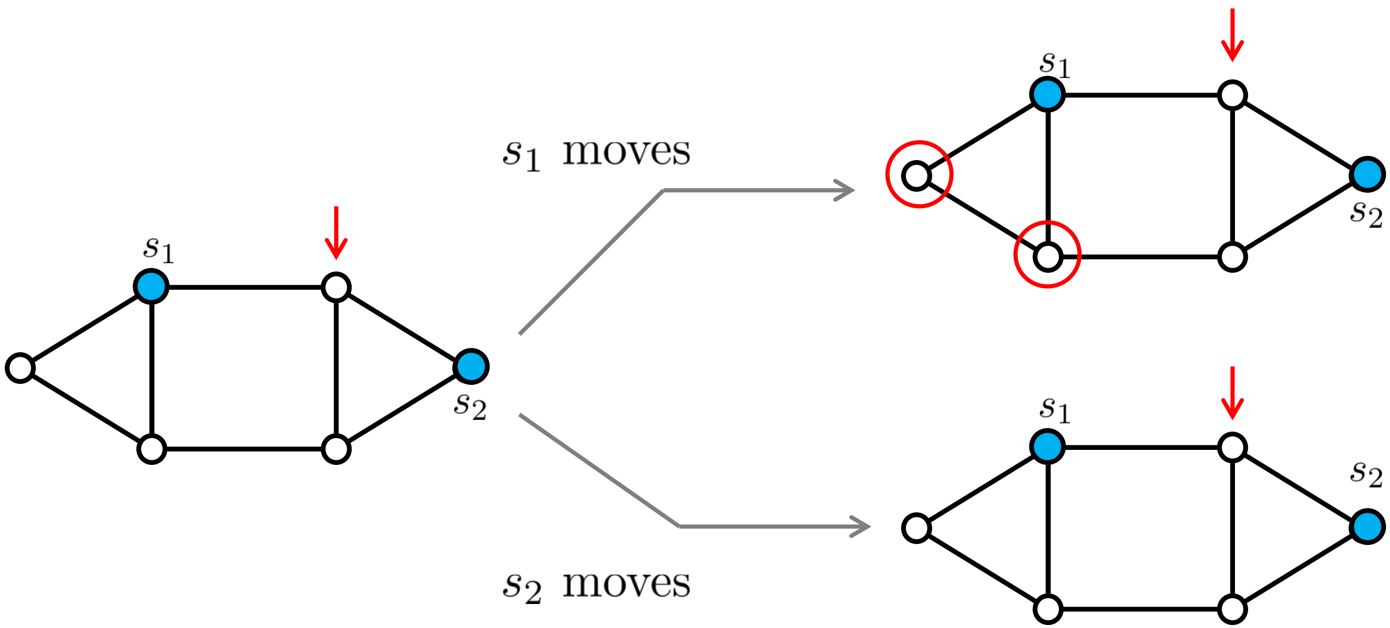


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Major Issues

Eternal Security

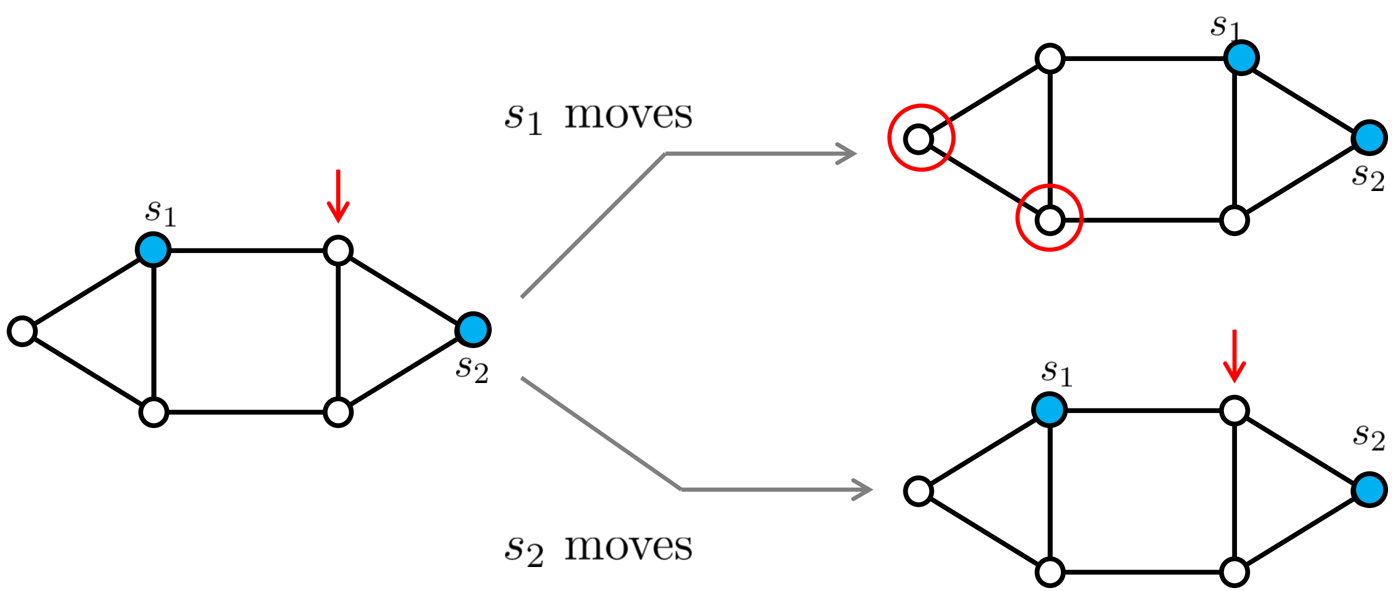
- No. of guards
- Deployment of guards
- Guards' movements in case of activity



Major Issues

Eternal Security

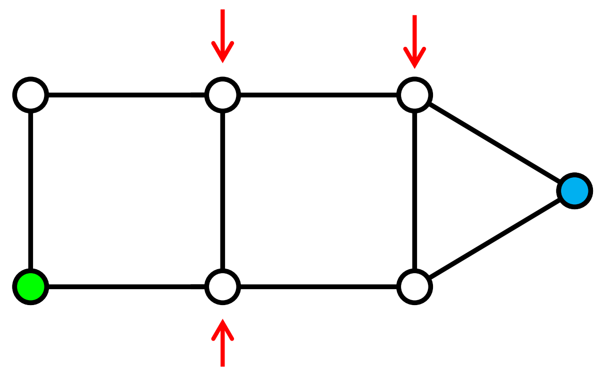
- No. of guards
- Deployment of guards
- Guards' movements in case of activity



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Heterogeneous Guards

- **Heterogeneity:** Guards may have different ranges from each other.



- Range = 1
- Range = 2

Problem Formulation

* Set of guards: $\mathcal{S} = \{s_1, \cdots, s_\sigma\}$;   Ranges: $\mathcal{R} = [r_1, \cdots, r_\sigma]$
* Vertex at which s_i is located at time k = $f_k(s_i)$
* $$f : (\mathcal{S}, k) \to V$$
* Vertices at which guards are located at k = $f_k(\mathcal{S}) = \{f_k(s_i) : s_i \in \mathcal{S}\}$
* A **vertex v is secured** whenever $\exists s_i : d(f_k(s_i), v)_G \leq r_i$
* $f_k(\mathcal{S})$ is a **secure configuration** whenever all vertices are secured.
* **Eternal Security :**

$f_k(\mathcal{S})$ Secure configuration —leads to→ $f_{k+1}(\mathcal{S})$ Secure configuration ; $\forall k$

where, $|f_{k+1}(\mathcal{S}) - f_k(\mathcal{S})| \leq 1$

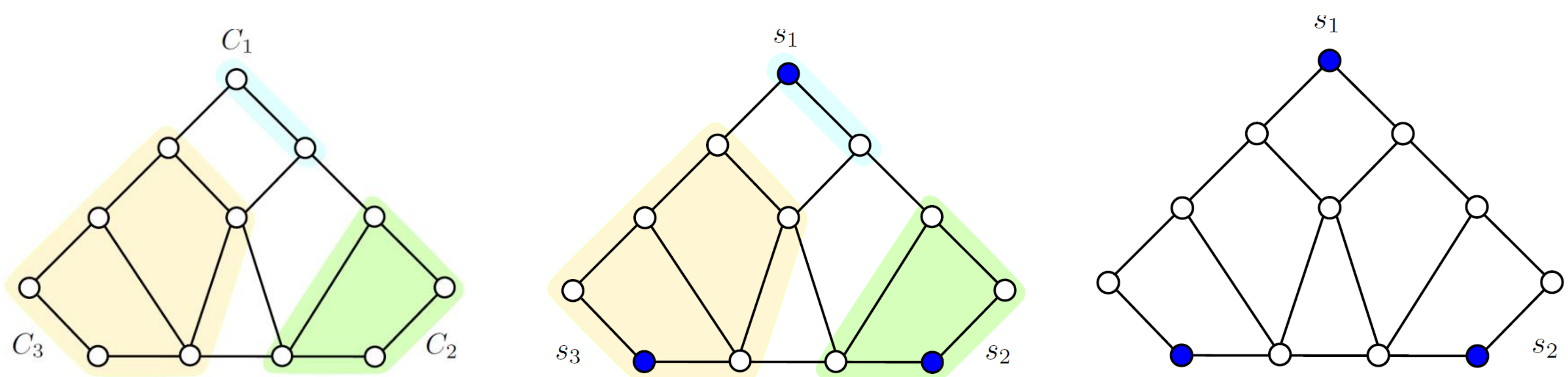
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

A Solution (Clustering)

Partition a graph G into clusters C_i, s.t.
$$d(u,v)_G \leq r_i$$
$$u,v \in C_i$$

→ **Assign** a **single** guard s_i with a range r_i to a cluster C_i.

→ A guard s_i eternally secures the vertices in **cluster** C_i **only**



$$\mathcal{S} = \{s_1, s_2, s_3\}$$
$$\mathcal{R} = [1, 2, 3]$$

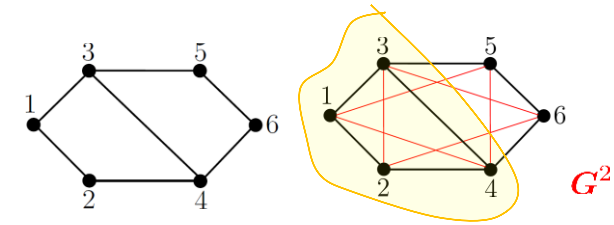
Clustering based approach

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Clustering Algorithm

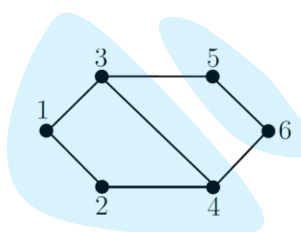
Inputs:	G ; Network; $\boldsymbol{\alpha} = [\alpha_1, \cdots, \alpha_\sigma]$; Guards' ranges; $\boldsymbol{\beta} = [\beta_1, \cdots, \beta_\sigma]$ Guards' numbers
Graph powers:	G^{α_1} G^{α_2} $\cdots$ G^{α_σ}
Maximal cliques:	M_1 M_2 $\cdots$ M_σ $\mathcal{M} = [\ M_1 \quad M_2 \quad \cdots \quad M_\sigma\ ]$
Greedy step:	Pick the column, $m \in M_j$, with the max. no. of uncovered nodes
Condition:	If guards with range α_j used are less than β_j
Cluster:	Make a cluster consisting of nodes in m
Update $\mathcal{M}$ and repeat the greedy steps	

$\boldsymbol{\alpha} = [\ 1 \quad 2\ ]; \qquad \boldsymbol{\beta} = [\ 1 \quad 1\ ];$



$$M_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad M_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\mathcal{M} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Clustering Algorithm

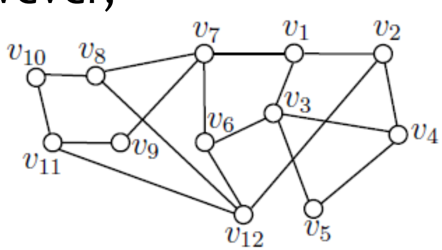
Proposition:

- Clustering is NP-hard.
- For a given set of guards along with their ranges, if ***Op*** is the maximum number of vertices that can be included in some cluster, then the algorithm includes at least ***(1 – 1/e).Op*** number of vertices in some cluster.

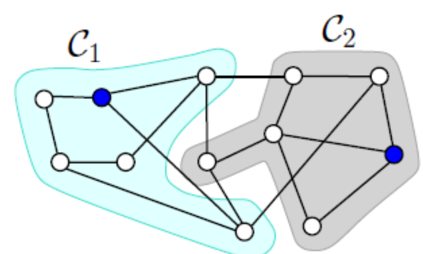
- If there are ℓ clusters, and each node is equally likely to be attacked, then the *average distance* moved by a guard is

$$\frac{1}{n}\left[\sum_{i=1}^{\ell} \frac{1}{(n_i-1)} \sum_{u,v\in C_i} d_G(u,v)\right]$$

- The clustering here is related to the low diameter decomposition of a graph. However,



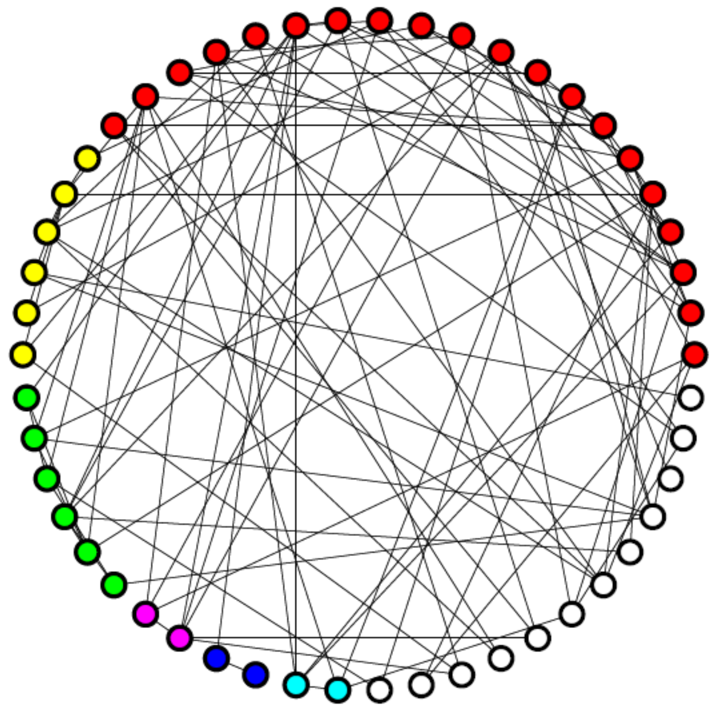
We cannot obtain two induced subgraphs, each having a diameter 2



It is possible to eternally secure a graph with two guards each having a range 2

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

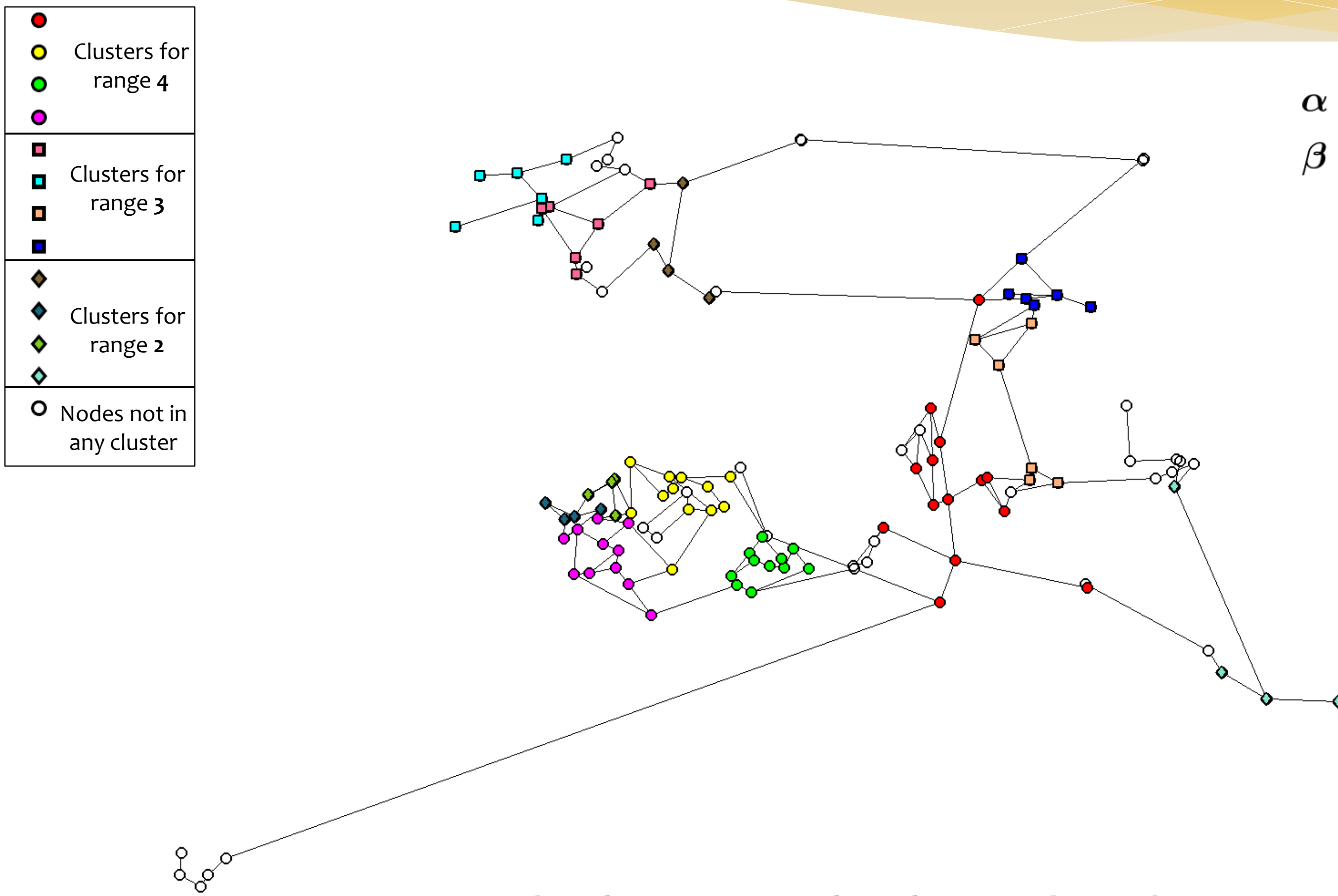
Example



$$\boldsymbol{\alpha} = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$$
$$\boldsymbol{\beta} = \begin{bmatrix} 3 & 2 & 1 \end{bmatrix}$$

A random (ER) graph with 50 nodes and p=0.08 (average degree = 4)

Example



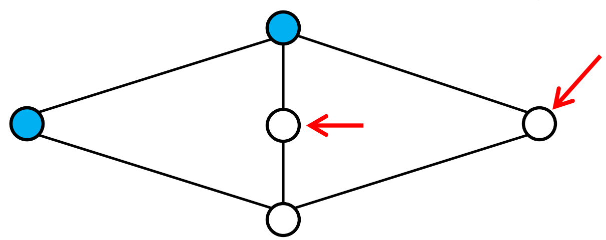
$$\boldsymbol{\alpha} = [\ 2 \quad 3 \quad 4\ ]$$
$$\boldsymbol{\beta} = [\ 4 \quad 4 \quad 4\ ]$$

A water distribution network with 126 nodes and 168 pipes

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Further Directions

- **Communication between guards:** What are the implications if moving guards with heterogeneous ranges also communicate with each other? How the solution will change?
  - e.g., If multiple guards move in response to an activity on a node, the number of guards required for eternal security might be lesser.



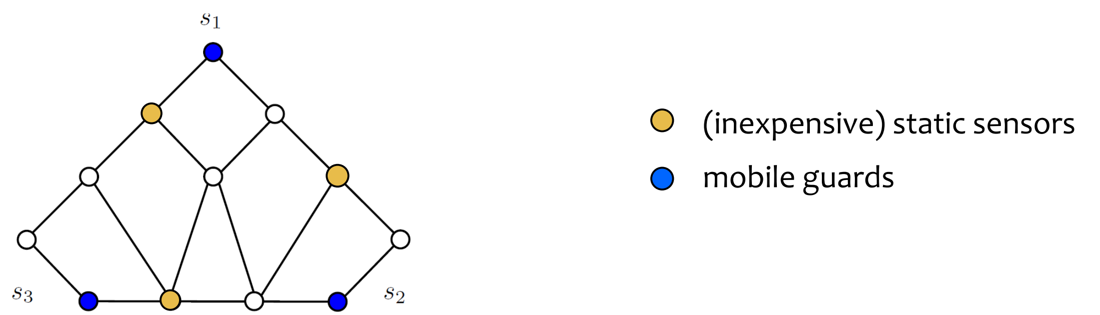
- **Comparing solutions**: The pairs (α_1, β_1) and (α_2, β_2) are both solutions. How can we associate a cost with a solution?

- **Dynamic graphs**: How can we solve eternal security problem for changing network topology?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Further Directions

- **Static and Mobile guards:** How can we combine (inexpensive) static sensors and sophisticated mobile guards to obtain more efficient monitoring in CPS?
  - e.g., Fault detection and localization in flow networks

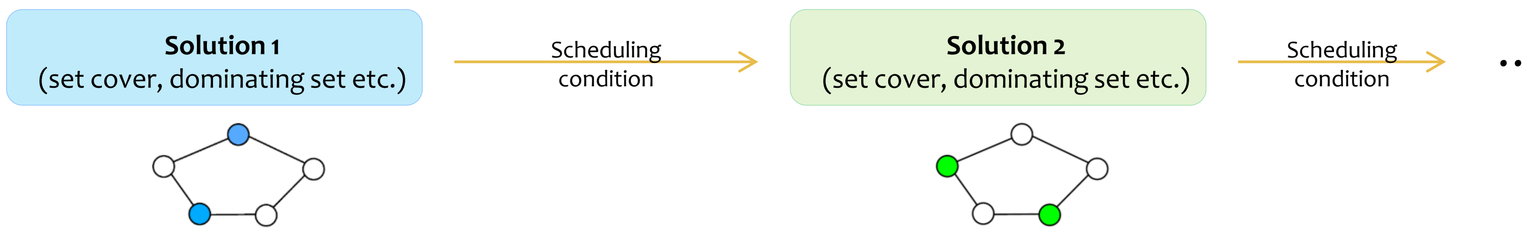


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Thank You

Remark

* Eternal security is an example of ‘*rotating between solutions*’ concept.
  * Example: Consider a typical sensor scheduling problem



* In the case of eternal security, a solution remains a solution whenever one of the guards moves towards its ‘neighbors’ in response to an activity on the neighbor node
  * Scheduling condition: An event on one of the nodes (discrete event dynamic system)
  * New solution: Previous solution except a change in the position of one of the guards