FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

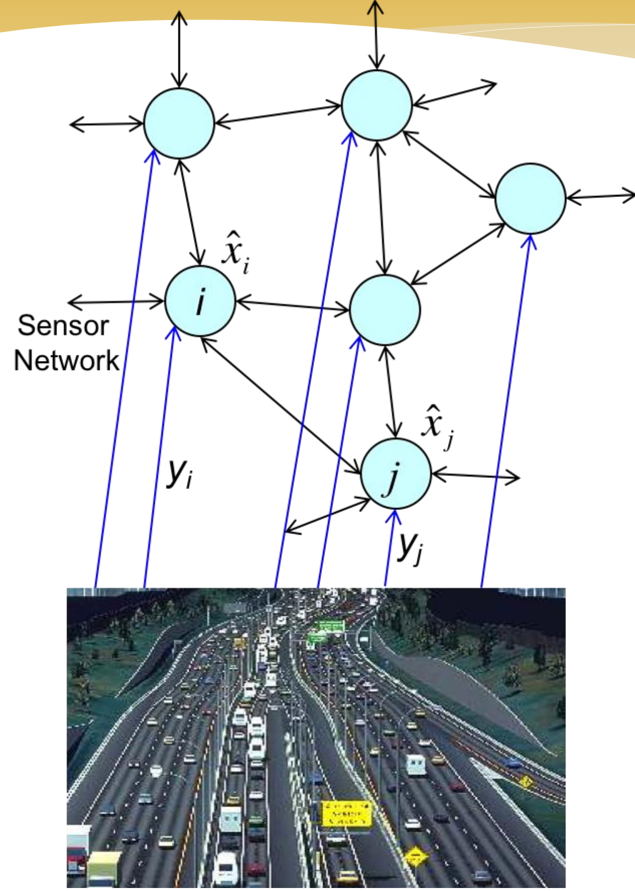
Resilience in Networked Dynamic Systems Using Trusted Nodes

Xenofon Koutsoukos

Waseem Abbas, Aron Laszka

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

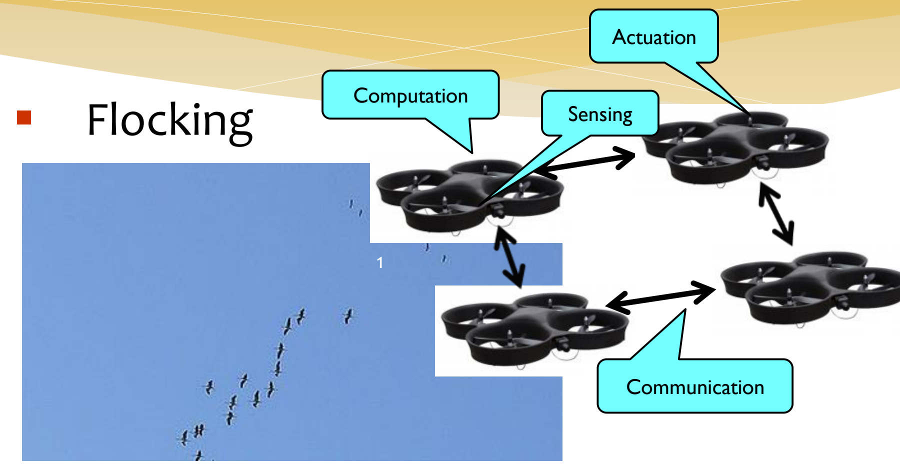
Motivation: Resilient Monitoring and Control of Distributed CPS using Consensus Algorithms

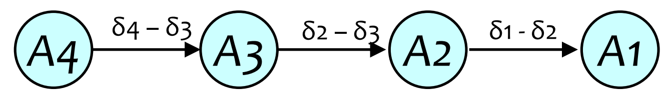


- Minimum variance estimate

$$\hat{\theta}_{MV} = \frac{\frac{1}{n}\sum_{i=1}^{n}\frac{1}{\sigma_i^2}y_i}{\frac{1}{n}\sum_{j=1}^{n}\frac{1}{\sigma_j^2}}$$

- Flocking





- Formation control

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

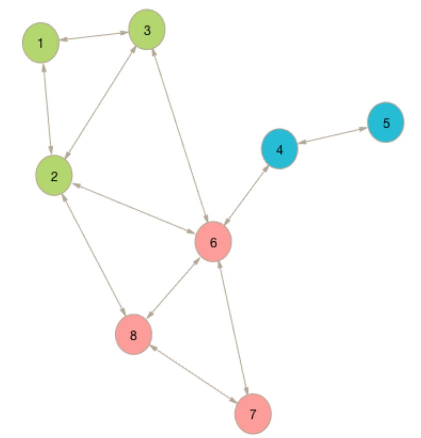
Learning by Networked Adaptive Agents

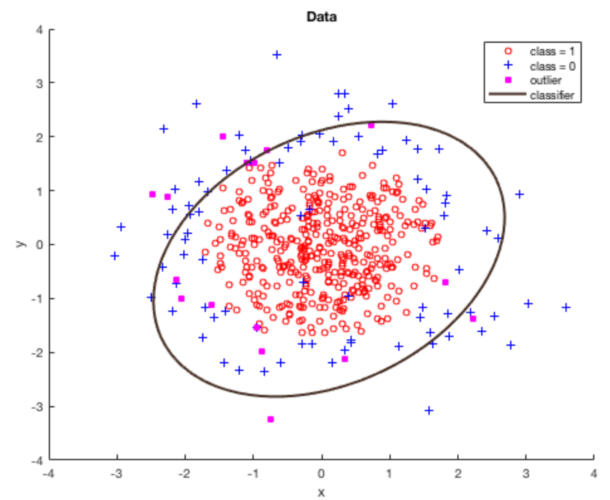
- Distributed collaborative classification
  - Each agent has access to some data and can share information with other agents
  - The objective is to classify the data using an elliptical curve
  - Each agent employs a logistic cost function

$$J_k(w) = \rho\|w\|^2 \; + \; \mathbb{E}\left\{\ln[1 + e^{-\gamma_k h_k^{T} w}]\right\}$$

  - The agents solve the optimization problem using a distributed collaborative consensus-algorithm

$$\begin{aligned} \psi_{k,i} &= w_{k,i-1} - \mu_k \, \widehat{\nabla_{w^{T}} J_k}(w_{k,i-1}) \\ w_{k,i} &= \sum_{\ell \in \mathcal{N}_k} a_{\ell k} \, \psi_{\ell,i} \end{aligned}$$



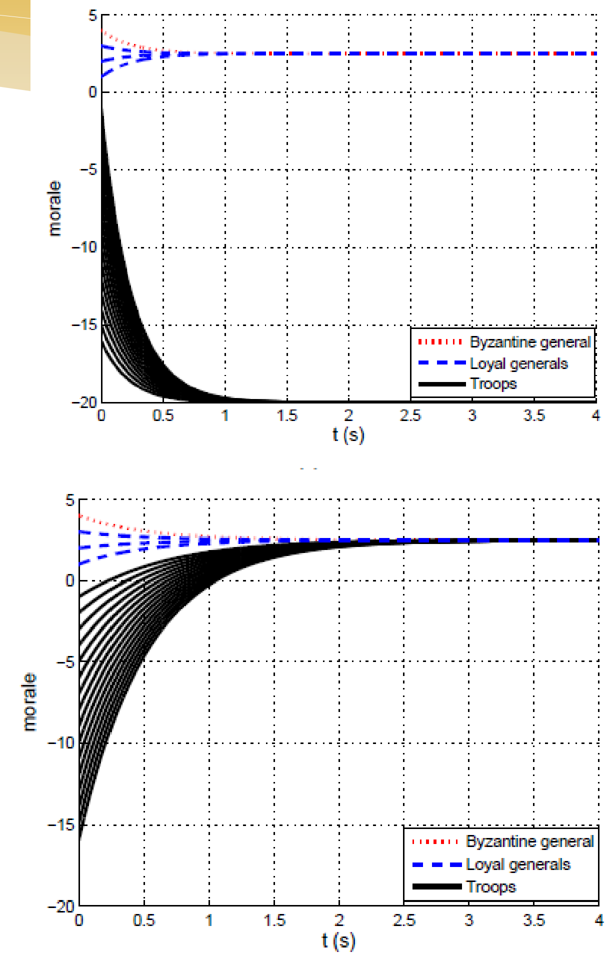


Outline

- Resilient distributed consensus in the presence of adversaries
- Resilient distributed consensus with trusted nodes
- Improving network connectivity by adding trusted nodes
- Conclusions and future directions

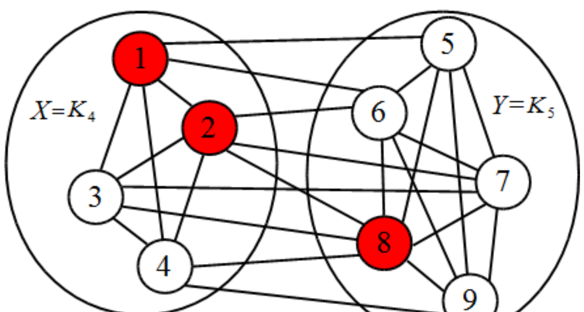
Resilient Distributed Consensus in the Presence of Adversaries

* Crash Adversary
* Malicious Adversary
  * Must convey the same information to all neighbors
    * Local broadcast model
* Byzantine Adversary
  * Can convey different information to different neighbors
* F-Total Model
  * At most F adversaries in the entire network
* F-Local Model
  * At most F adversaries in the neighborhood of any normal node
* f-Fraction Local Model
  * At most a fraction f of adversaries in the neighborhood of any normal node



(b) ARC-P.

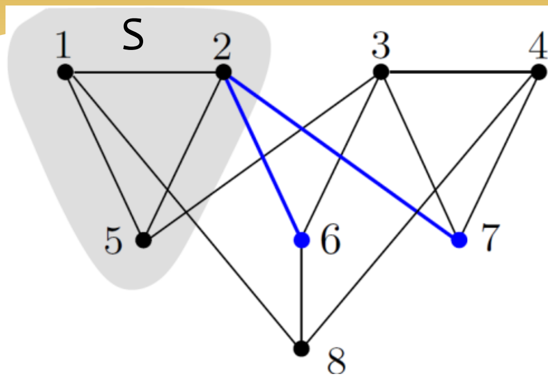
$$x_i(t+1) = w_{(i,i)}(t)x_i(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)} w_{(j,i)}(t)x_{(j,i)}(t)$$



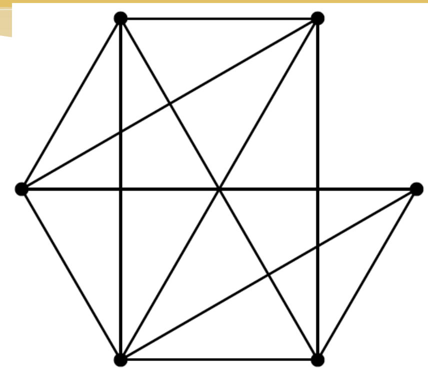
3-total, 3=local, (3/5)-fraction local

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

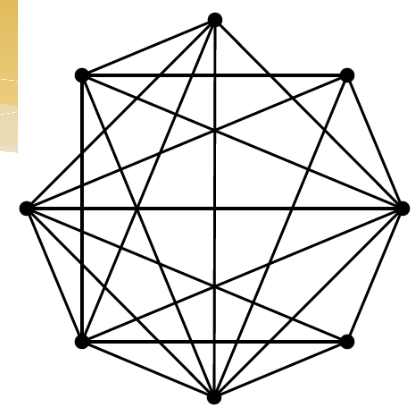
Robust Network Topologies



2-robust graph: Node 2 has two neighbors outside of S



(2,2)-robust



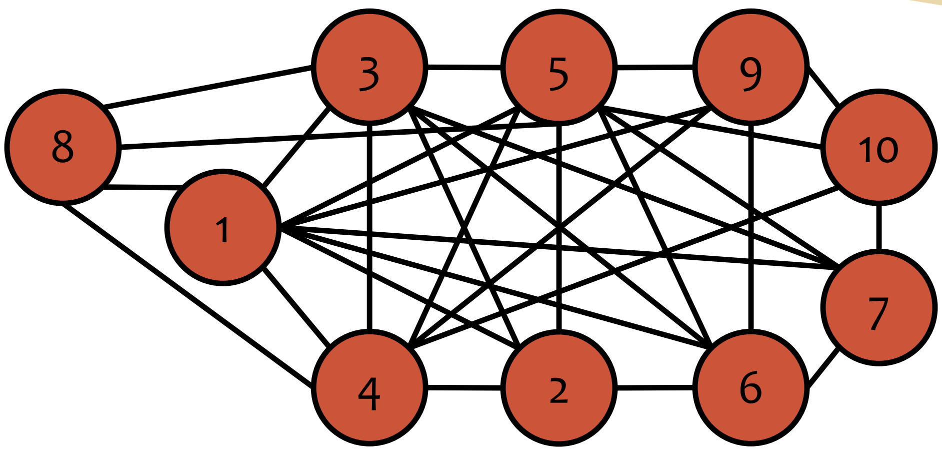
(3,3)-robust

- Graph robustness: New graph theoretic property to capture local redundancy
- Characterize a minimum number of nodes that are sufficiently influenced from outside their set
- r-robustness: For every pair of nonempty disjoint sets, at least one set has a node that has at least r neighbors outside the set
- (r,s)-robustness: For every pair of nonempty disjoint sets, there are at least s nodes with at least r neighbors outside their respective sets

Threat	Scope	Necessary	Sufficient
Crash & Malicious	F-Total	$(F+1,F+1)$-robust	$(F+1,F+1)$-robust
Crash & Malicious	F-Local	$(F+1,F+1)$-robust	$(2F+1)$-robust
Crash & Malicious	f-Fraction local	f-fraction robust	p-fraction robust, where $2f < p \leq 1$
Byzantine	F-Total & F-Local	Normal Network is $(F+1)$-robust	Normal Network is $(F+1)$-robust
Byzantine	f-Fraction local	Normal Network is f-robust	Normal Network is p-robust where $p > f$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Construction of Robust Networks

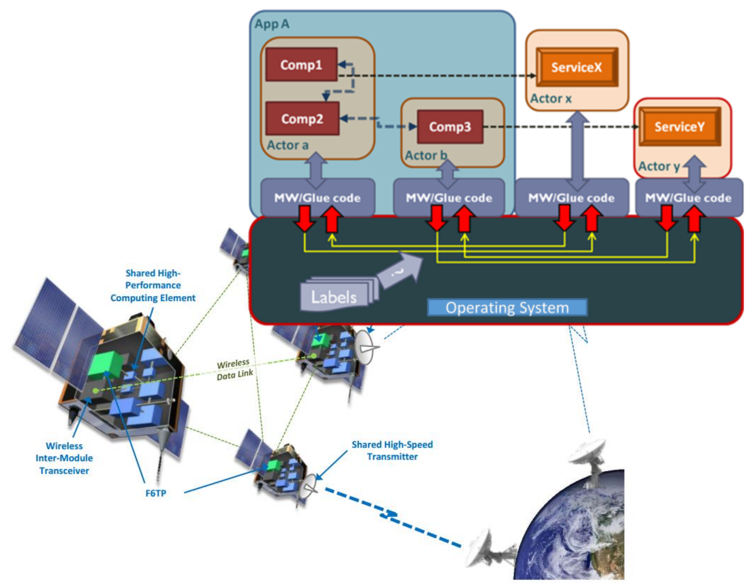


- Resilience requires high degree of redundancy (high connectivity)
- Redundancy increases the attack surface
- How can improve resilience without adding redundancy?

Preferential-attachment model

- Initial graph: K_5
- K_5 is (3,2)-robust
- Num edges / round: 4
- End up with (3,2)-robust graph
- Achieve resilient consensus in the presence of 1 adversary

Trusted Nodes

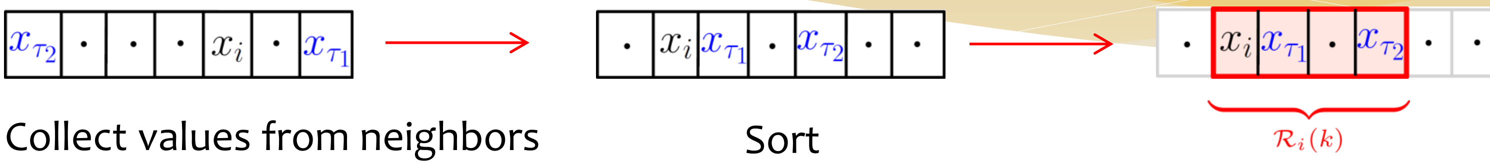


Karsai et al., DARPA F6 program

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Consensus Protocol with Trusted Nodes (RCP-T)

- If node *i* is connected to at least one trusted node



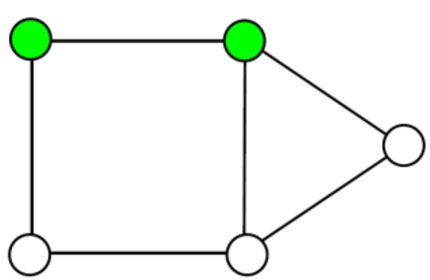
Collect values from neighbors

Sort

($x_{\mathcal{T}1}$, $x_{\mathcal{T}2}$ are trusted nodes' values)

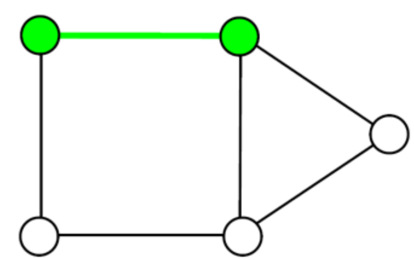
- Under RCP-T, consensus is always achieved in the presence of *arbitrary number of adversaries* if and only if there exists a set of trusted nodes that form a **connected dominating set**

Dominating Set



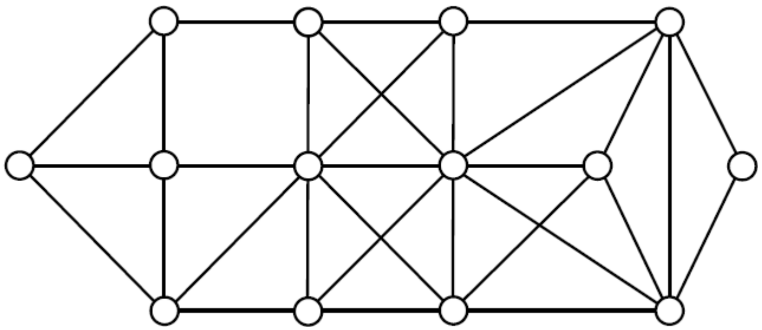
Connected Dominating Set

Nodes in the dominating set induce a connected subgraph



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Trusted Nodes and Network Robustness



(2,2)-robust ⟷ Resilient against a single attack (with no trusted nodes)

d = 4 ⟷ Resilient against any no. of attacks (with 4 trusted nodes)

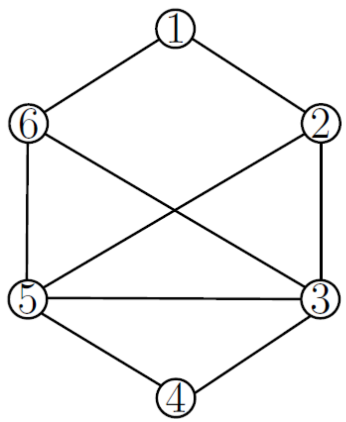
Can we improve resilience if the number of trusted nodes < d?

* The **connected domination number** d is the number of vertices in the minimum connected dominating set
* If the number of trusted nodes is at least d, the network can be made resilient against any number of adversaries

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

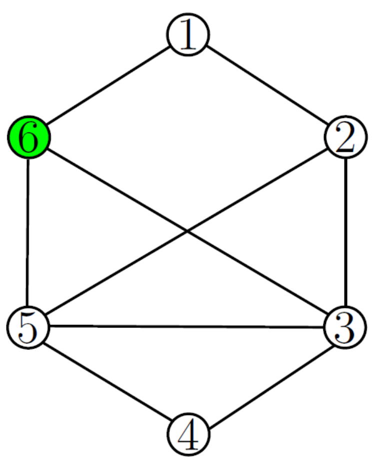
(r,s)-Robustness with Trusted Nodes

(r,s)-robustness with trusted nodes: For every pair of nonempty disjoint sets, there are at least s nodes with at least r neighbors or have trusted neighbors outside their respective sets



- The graph is **not (2,2)-robust.**
- For instance, consider

  $S_1 = \{1,2\}$; $S_2 = \{3,4,5,6\}$
- Node 1 has only neighbor outside S_1



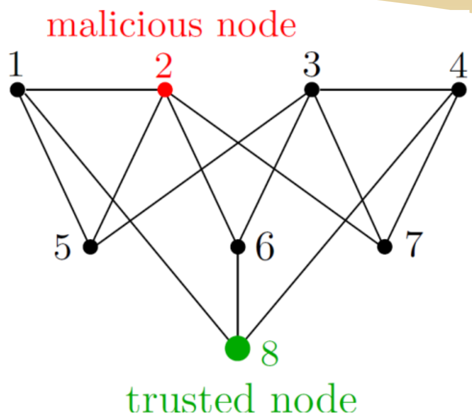
- The graph **is (2,2)-robust with 6 as a trusted node.**
- For instance, consider

  $S_1 = \{1,2\}$; $S_2 = \{3,4,5,6\}$
- Node 1 has a trusted neighbor outside S_1

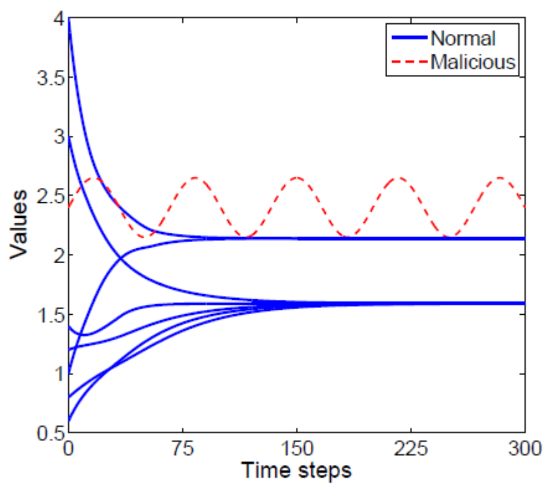
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Consensus with Trusted Nodes: Example

F-total model

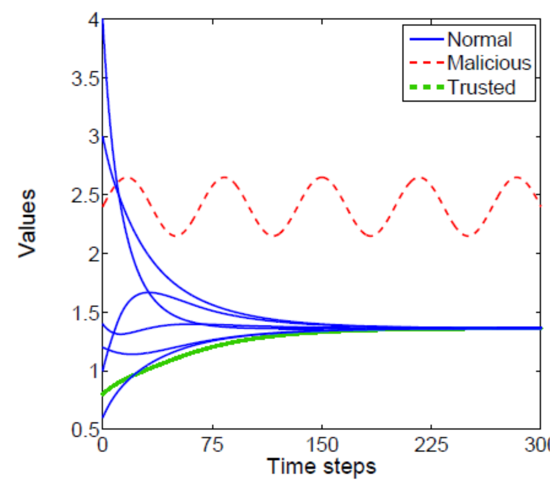


- G is (2,2)-robust with T = {8}.



WMSR - algorithm

If there is no trusted node, consensus cannot be achieved.



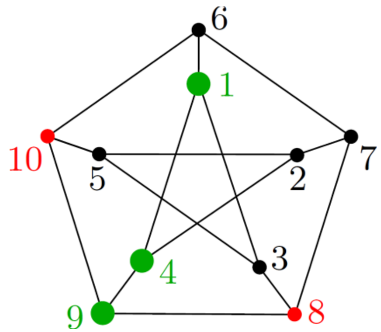
RCP-T - algorithm

Consensus is achieved with one trusted node.

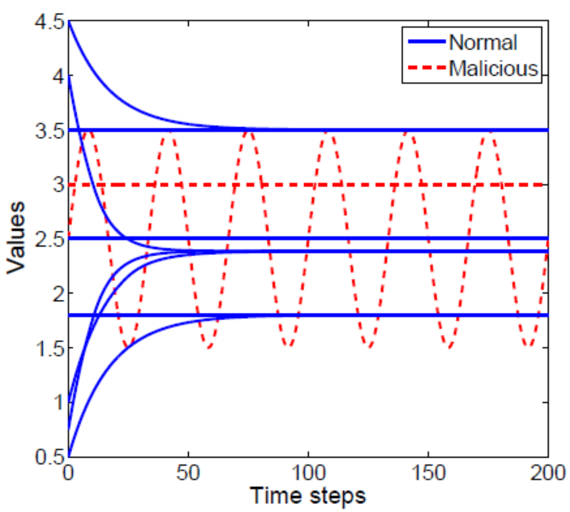
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Consensus with Trusted Nodes: Example

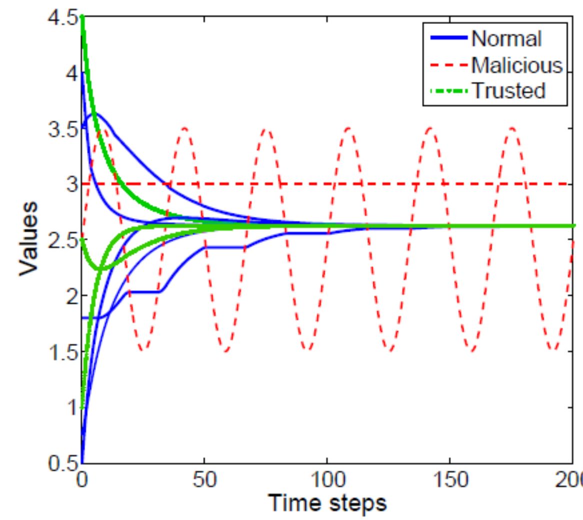
F-local model



- G is 3-robust with T = {1,4,9}.



WMSR - algorithm
If there is no trusted node, consensus cannot be achieved.



RCP-T - algorithm
Consensus is achieved with three trusted nodes.

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Consensus with Trusted Nodes

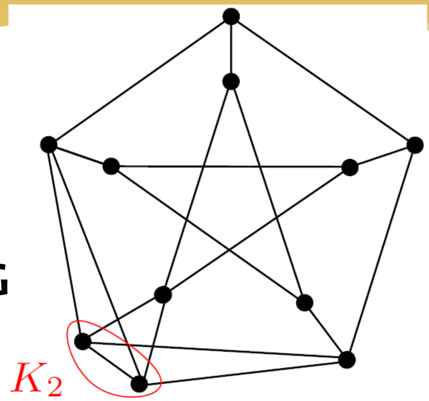
- The conditions for resilient consensus based on (r,s)-robustness can reformulated using the notion of **(r,s)-robustness with trusted nodes**
- For instance

Theorem :
Under the F-total malicious model, resilient asymptotic consensus is achieved using RCP-T algorithm if and only if the network topology is **(F+1,F+1)-robust with trusted nodes.**

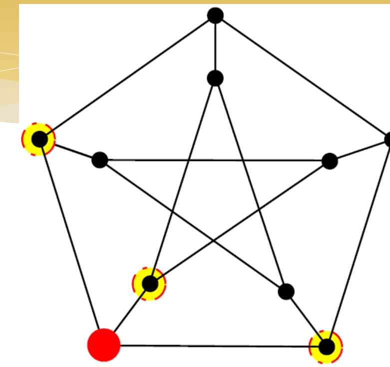
- A graph that is (F+1,F+1)-robust with trusted nodes could be much sparser than the one that is (F+1,F+1)-robust without trusted nodes

Construction of Robust Graphs with Trusted Nodes

G

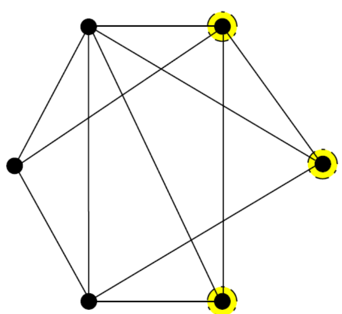


- G is 2-robust
- Clique K_2 is replaced by a trusted node
- H is still 2-robust

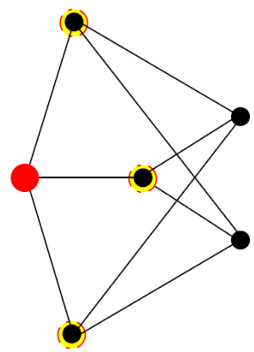


H

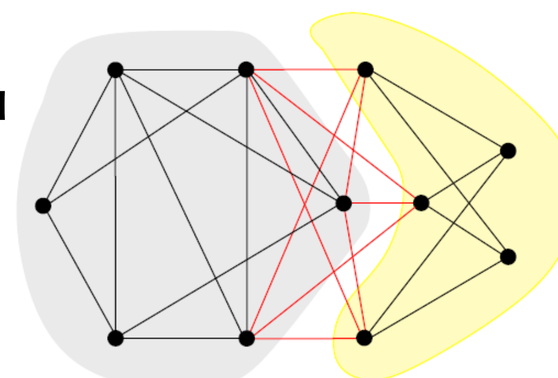
G'



G



H



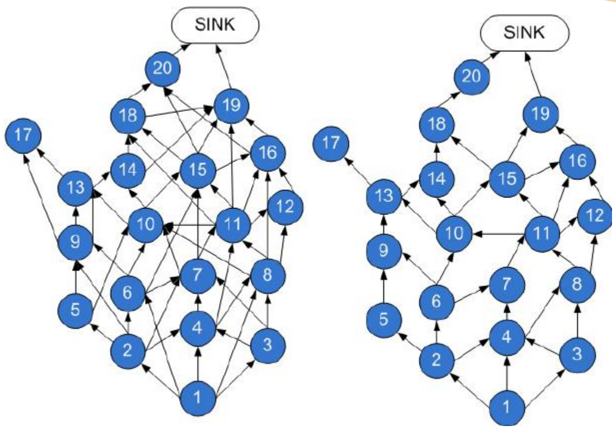
- G' is **3-robust.**
- Nodes in subset η are highlighted

- G is **3-robust** with red trusted node.
- Neighbors of trusted node are highlighted

- H is also is **3-robust.**
- New edges added are shown in red.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

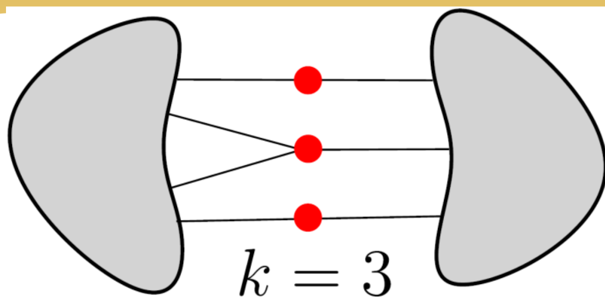
Improving Network Connectivity Using Trusted Nodes and Edges

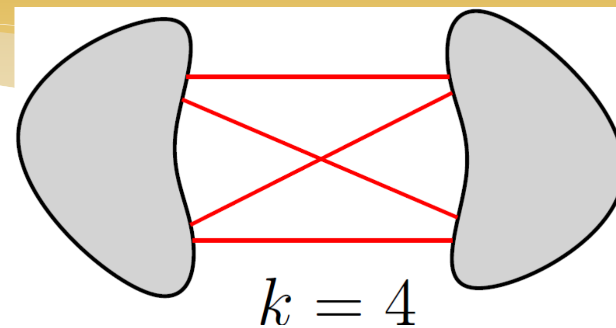


- Connectivity is primary attribute of every network
- Many important network properties depend on vertex (edge) connectivity
- How can we efficiently place trusted nodes in a network to increase vertex (edge) connectivity?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Improving Network Connectivity



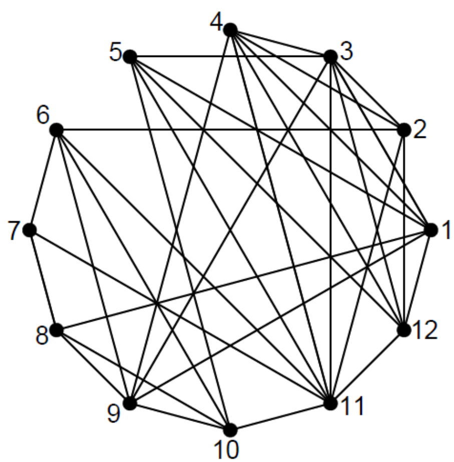


- k-vertex Connectivity: A graph remains connected even if any set of (k-1) vertices are removed
- k-edge Connectivity: A graph remains connected even if any set of (k-1) edges are removed
- **Connectivity augmentation:** Determine the *smallest set of edges* which must be added to a given graph to make it k-edge connected or k-vertex connected
- Connectivity augmentation may be difficult due to practical and economical reasons and increases the attack surface
- Improving network connectivity using trusted nodes: Deploy a small subset of trusted nodes

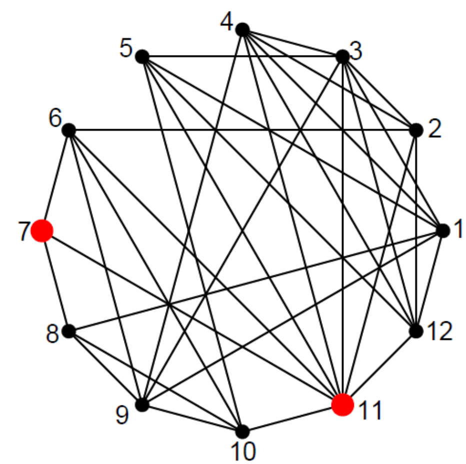
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network Connectivity with Trusted Nodes

Network connectivity can be measured by the number of *non-trusted nodes* that need to be removed to make the graph disconnected.



- The graph is 3-vertex connected.
- At least 3 nodes need to be removed to disconnect the graph.



- By making nodes 7 and 11 as *trusted*, we need to remove at least 6 of the remaining nodes to disconnect the graph.
- In other words, with nodes 7 and 11 as trusted, the graph behaves like a 6-vertex connected.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

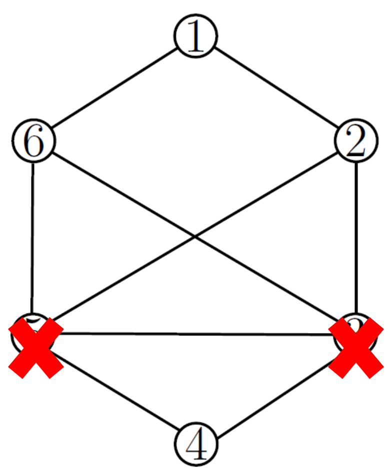
Menger's Theorem: Independent Paths

The minimum number of nodes whose removal disconnects two nodes, say *u* and *v*, is equal to the maximum number of pairwise node-independent paths from *u* to *v*.

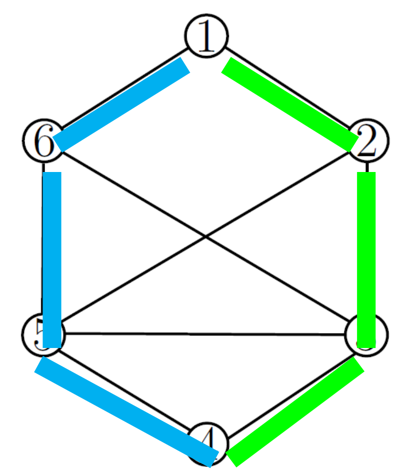
In other words,

Node connectivity ⟷ No. of node independent paths between any two nodes

- Removal of two nodes can disconnect the graph.
- In particular, nodes 1 and 4 can be disconnected by 2 node removals.



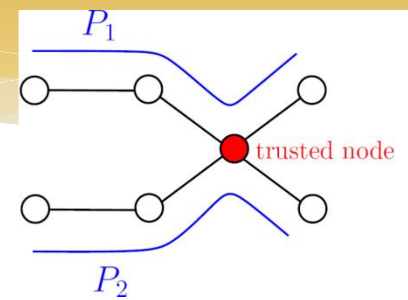
- There are two node-independent paths between any two nodes.
- The ones between nodes 1 and 4 are shown.



Independent Paths with Trusted Nodes

Definition (Node-independent paths with trusted nodes):

Two paths are node-independent with trusted nodes if common nodes between them are only the trusted nodes.



P_1 and P_2 are node-independent paths with trusted nodes.

Definition (Node trusted path):

A path with all trusted nodes is a node trusted path.

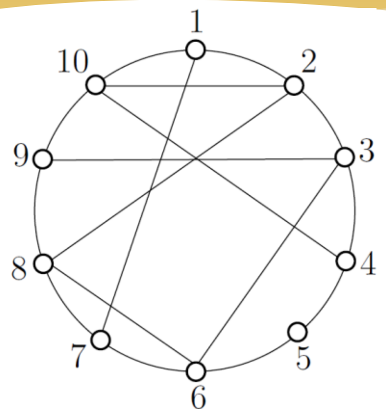
Theorem:

For a graph G(V,E) and a set of trusted nodes T_v , following statements are equivalent.

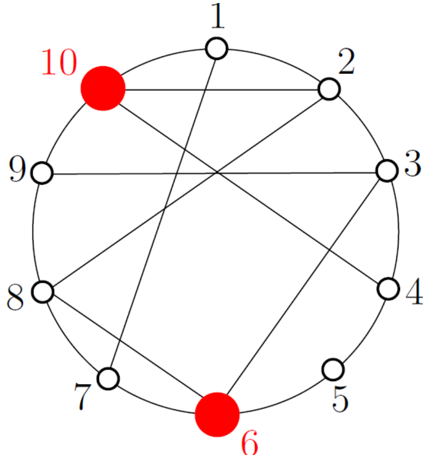
1. G is k-vertex connected with T_v.
2. For any two distinct, non-adjacent vertices u and v, either there exists a node-trusted path between u and v, or there exists at least k paths between u and v that are vertex-independent with T_v.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

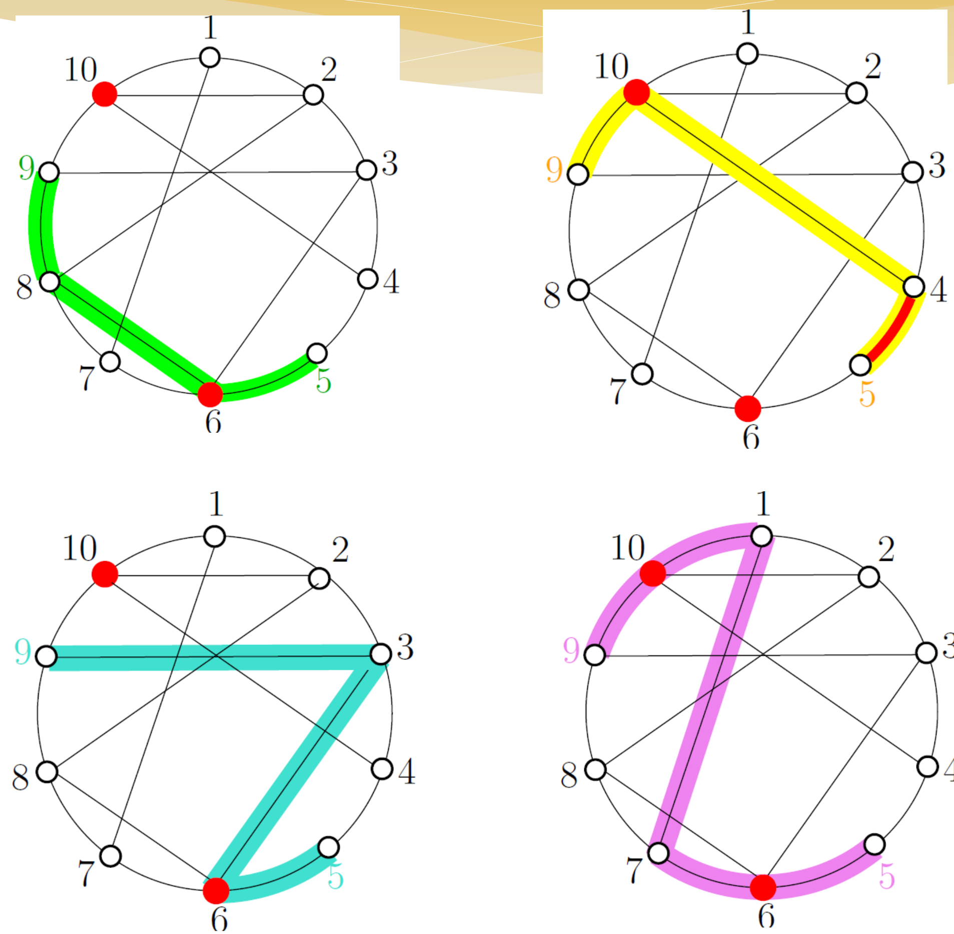
Vertex-Connectivity with Trusted Nodes: Example



A graph is 2-vertex connected.



A graph is 4-vertex connected with the **red** nodes as the **trusted nodes**, i.e., between any two nodes there always exist four node-independent paths with trusted nodes.



Four node-independent paths with (red) trusted nodes between nodes **5** and **9**

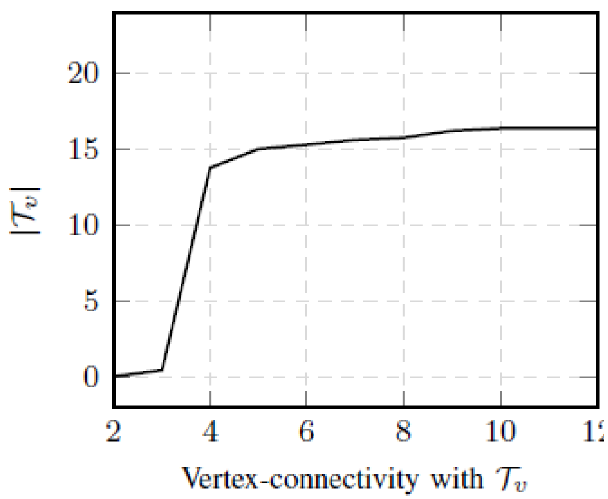
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Placement of Trusted Nodes

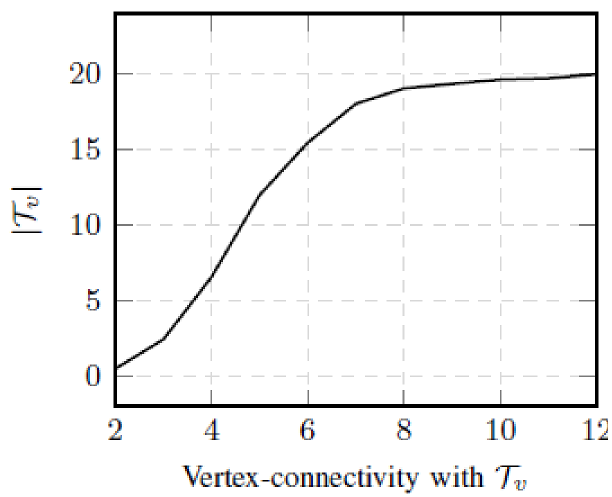
Theorem:
Given a graph G(V, E), a desired vertex connectivity k, and the number of trusted nodes T, determining if there exists a set of trusted nodes T_v of cardinality T such that G is k-vertex connected with T_v is NP-hard.

1. Heuristics based on Connected Dominating Set (CDS)
   * If trusted nodes form a CDS, then, between any two nodes, there is always a path consisting of only trusted nodes.
   * Start with a set of trusted nodes forming a CDS, and then successively reduce the set of trusted nodes as long as the desired connectivity is obtained.

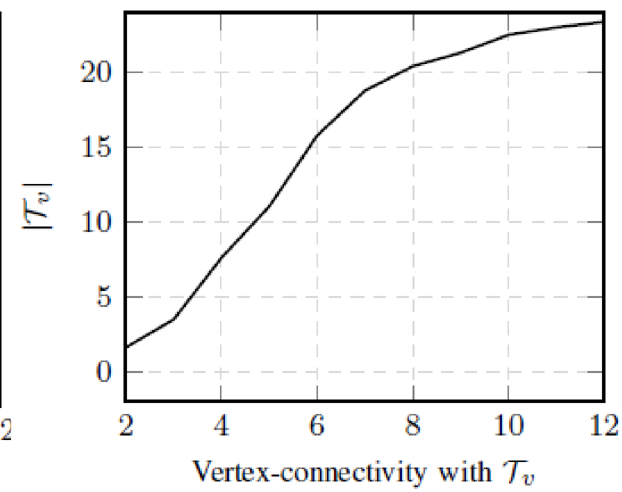
Number of Trusted Nodes T_v as a Function of the Vertex Connectivity



Preferential attachment networks



Erdos-Renyi random networks



Random geometric networks

(Each network has a total of 100 nodes. Details of the networks are in Abbas et al., 2017)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Conclusions and Future Directions

* Resilient Consensus Protocols in the Presence of Adversaries
  * Exploit local redundancy to ensure asymptotic consensus
  * Characterize robust network topologies
* Resilient Consensus Protocols with Trusted Nodes
  * Increase resilience by exploiting trust instead of redundancy
* Improving Network Connectivity with Trusted Nodes
  * Improve reliability, resilience, and other properties based on connectivity
* Can trusted nodes be used to improve resilience of other properties in networked CPS?
  * Participatory sensing
  * Learning by networked agents

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS