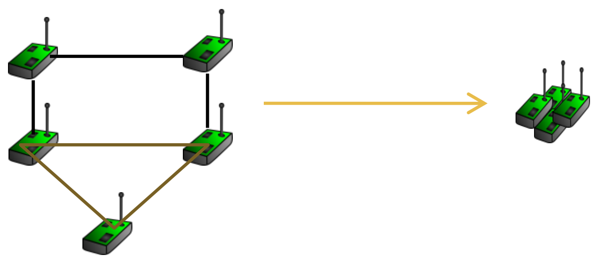
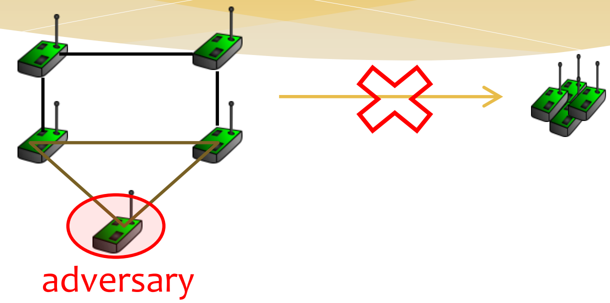
Resilient Consensus Through Trusted Nodes

Waseem Abbas, Yevgeniy Vorobeychik, and Xenofon Koutsoukos
Vanderbilt University

Motivation



Consensus: agents agree upon a common value
Applications: optimization, sensor networks, estimation, etc.



Resilient consensus: consensus in the presence of adversaries

Existing Resilient Consensus Protocols

- **Non-local information**
  e.g., node knows the overall network topology
- **High connectivity**
  e.g.,
  - ***(2F+1)*-connected**
  - **(r,s)-robust**
- **Conditions hard to verify**
  e.g., (r,s)-robustness
- **Dependence on parameter F (no. of possible attacks)**
  e.g., F-Total , F-local etc.

Can these issues be addressed?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Motivation

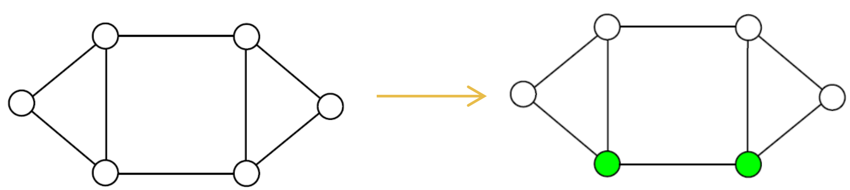
Resilient networks
(various approaches to resilience)

Connectivity of underlying graph

Nodes' capabilities **(security levels)**

some nodes are **more secured** against adversarial attacks

By **how much** can we improve the **resilience** of a network by adding **few trusted nodes**?



Trusted Nodes

- Highly secure.
- Cannot be compromised by attacks.

Resilient Consensus with Trusted Nodes

Design an update rule such that all normal nodes, a subset of which consists of **trusted nodes,** achieve consensus even in the presence of **any** number of adversaries.

i.e., design an update rule that achieves consensus.

Consensus:

- Agreement

$(\text{as } k \to \infty,\ x_i(k) \ = \ x_j(k))$

- Safety

$(\forall\ k,\ \ x_i(k) \in [x_{\min}(0) \qquad x_{\max}(0)])$

Trusted nodes:

For any no. of adversarial attacks, find ***necessary and sufficient*** conditions on the

- ❑ number
- ❑ location
- ❑ connectivity

of trusted nodes to achieve consensus.

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Consensus Protocol (RCP-T)

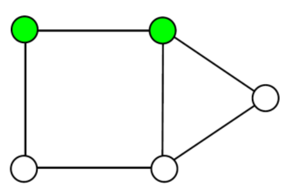
Under **RCP-T,** consensus is always achieved in the presence of ***arbitrary number of adversaries*** if and only if there exists a set of trusted nodes that form a **connected dominating set**.

Under RCP-T

- *Any* number of attacks can be handled
- *Sparse* networks can be made resilient

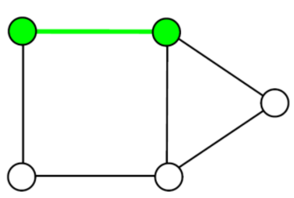
Dominating Set:

$$D \subseteq V, \quad \text{s.t.} \quad \bigcup_{v_i \in D} \mathcal{N}[v_i] = V$$



Connected Dominating Set:

Nodes in the dominating set induce a connected subgraph



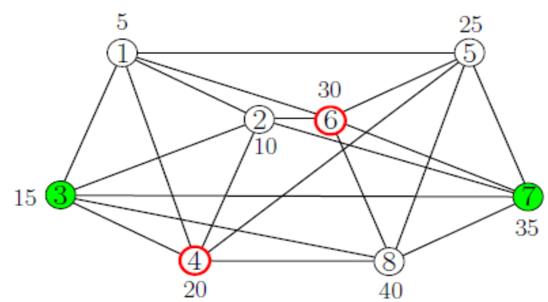
FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Example

Example:

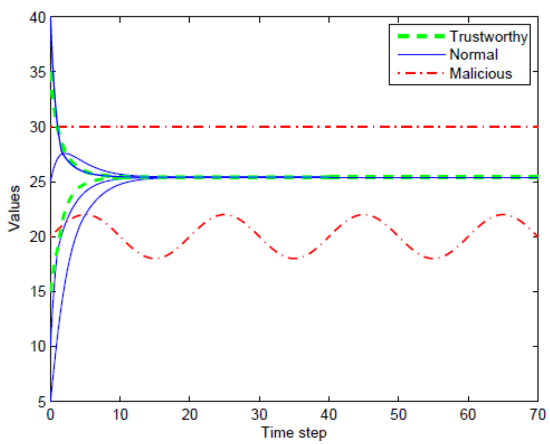
Attacked nodes $= \{4, 6\}$

Trusted nodes $= \{3, 7\}$

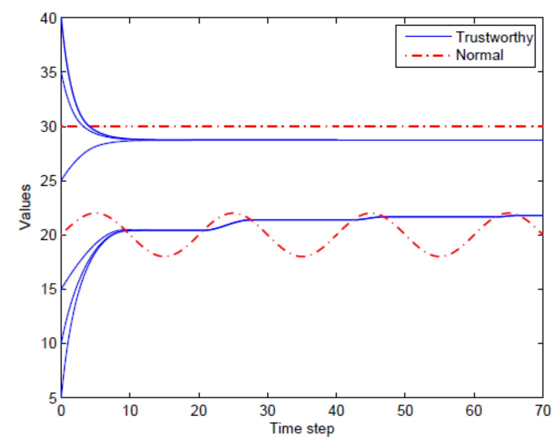


(2,2)-robust graph

RCP-T



W-MSR



- **RCP-T** achieves consensus even with two attacks
- **W-MSR** algorithm can handle a single attack, but not two adversaries

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Conclusions

Trusted nodes and Network Robustness

γ_c = Connected domination number

Resilience of networks if
$\text{No. of trusted nodes} < \gamma_c$

Sometimes adding as many as $(\gamma_c - 1)$ trusted nodes does not improve the resilience.

$\gamma_c \sim (r, s)-$ robust graphs

'Trusted nodes' ?

How can we generalize the notion of 'trusted nodes' for resilience in networks?

Graph domination

How can we utilize the concept of domination in graphs for resource distribution in networks.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS