Supporting Security with Advanced Multimodal Grid Data Analytics

Data Injection Attacks in Randomized Gossiping

Reinhard Gentz, Sissi Xiaoxiao Wu, Hoi-To Wai, Anna Scaglione, and Amir Leshem

MOTIVATION

- Gossiping algorithms are attractive:
  - No central point of failure.
  - Built-in fault tolerance to node failures.
    - Nodes can reorganize themselves.
  - Protected against outsider attacks with authentication and encryption.
  - Vulnerable against insider attacks.
    - Flat architecture => many attack vectors.
    - Network will still converge, but to the wrong value.

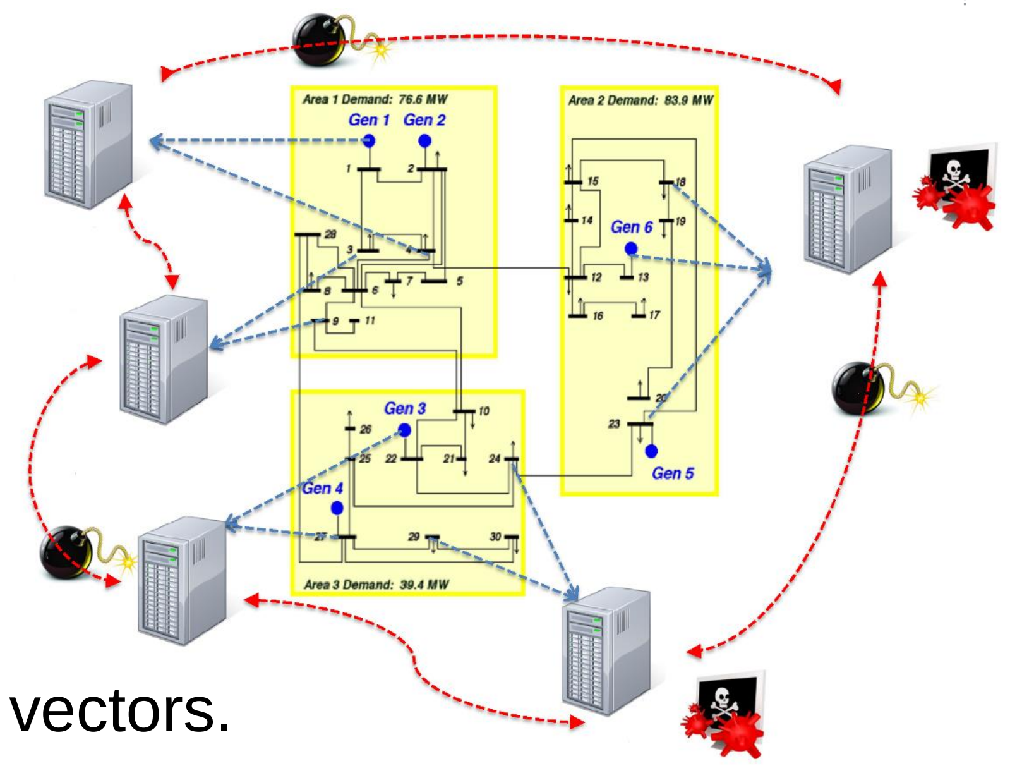


Fig. 1. Example application: state estimation in the grid.

- Our method provides:
  - Decentralized attack detection.
  - Decentralized attacker identification.
  - Self-Healing Network.
  - No communication overhead.

Works on the principle of expected protocol evolution

GOSSIPING ALGORITHM AND ATTACK MODEL

```
Algorithm 1: Randomized consensus protocol
  Input: the number of iterations $T$. %sufficiently large
  for $t = 1 : T$ do
      • Uniformly wake up a random node $i \in V$.
      • Node $i$ selects node $j$ from its neighborhood with
        the probability
            $P_{ij}$, where $j \in \mathcal{N}_i$ and $\mathcal{N}_i = \{j : (i,j) \in E\}$.
      • Nodes $i$ and $j$ update their states as follows
            $x_i^k(t+1) = x_j^k(t+1) = \frac{x_i^k(t) + x_j^k(t)}{2}$;        (1)
        Other nodes keep their original states, i.e.,
        $x_v^k(t+1) = x_v^k(t)$ for all $v \neq i, j$.
```

“good nodes”

Algorithm to find the system average of the nodes' state x_i^k.

- j ignores (1) and chooses its next state:
  $x_j^k(t) = \alpha^k + m_j^k(t),\ x_j^k(t+1) = \alpha^k + m_j^k(t+1)$
  - The attacker steers the network towards α^k, away from the true value (which is $x_{av}^k = \frac{1}{N}\sum_i x_i^k(0)$); $m^k(t)$ is a disguise term it uses to hide its malicious intent from normal nodes.
    - The disguise follows the expected convergence of the network.

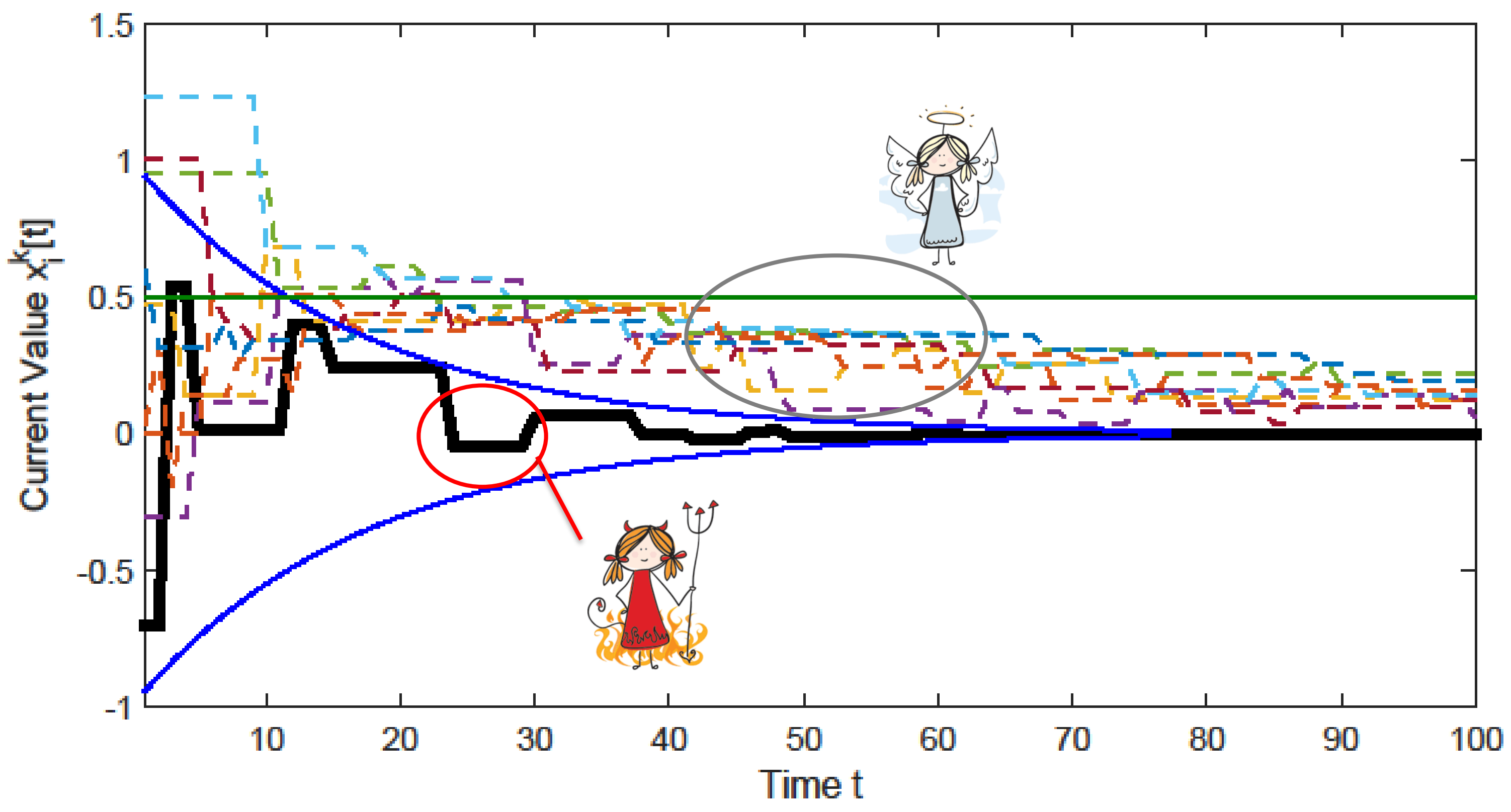
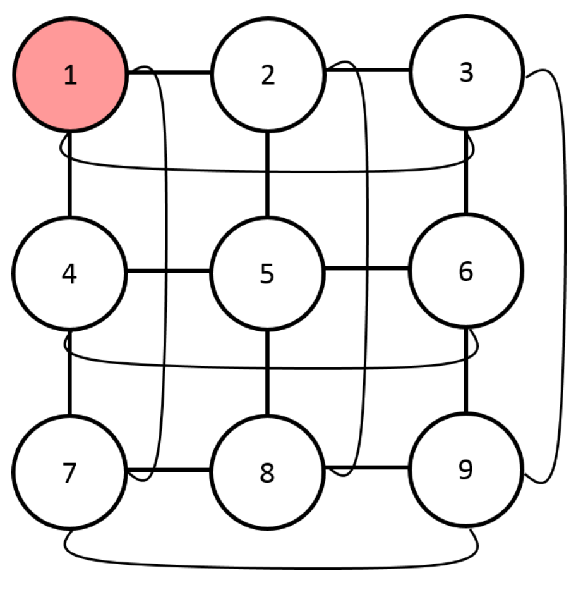


Fig. 2. Network convergence with one attacker present. Normal nodes (dashed) converge towards the value of the attacker (black) instead of the true mean (green). The attacker follows the expected convergence (blue).

SIMULATION PARAMETERS



Simulation parameters:

- Manhattan network with 9 nodes (see Fig. 3).
- Attacker target $\alpha^k \sim \mathcal{N}(0,1)$.
- Disguise $m_i^k(t) \sim \mathcal{U}[-\hat{\lambda}^t, \hat{\lambda}^t]$ (λ = expected convergence).
- Node 1 attacking.
- Normal nodes' initial state $\gamma_i^k \sim \mathcal{U}[-0.5,1.5]$.
- Stop gossiping with T = 500.
- Monte Carlo simulation of 10^3 trials.

Fig. 3. Simulation topology; node 1 is attacking.

DEFENSE STRATEGY: SPATIAL DIFFERENCE

- If both m and j are not attackers, then $\mathrm{E}[x_m^k(t) - x_j^k(t)] = 0$.
- If m or j is an attacker, then $\mathrm{E}[x_m^k(t) - x_j^k(t)] \neq 0$.

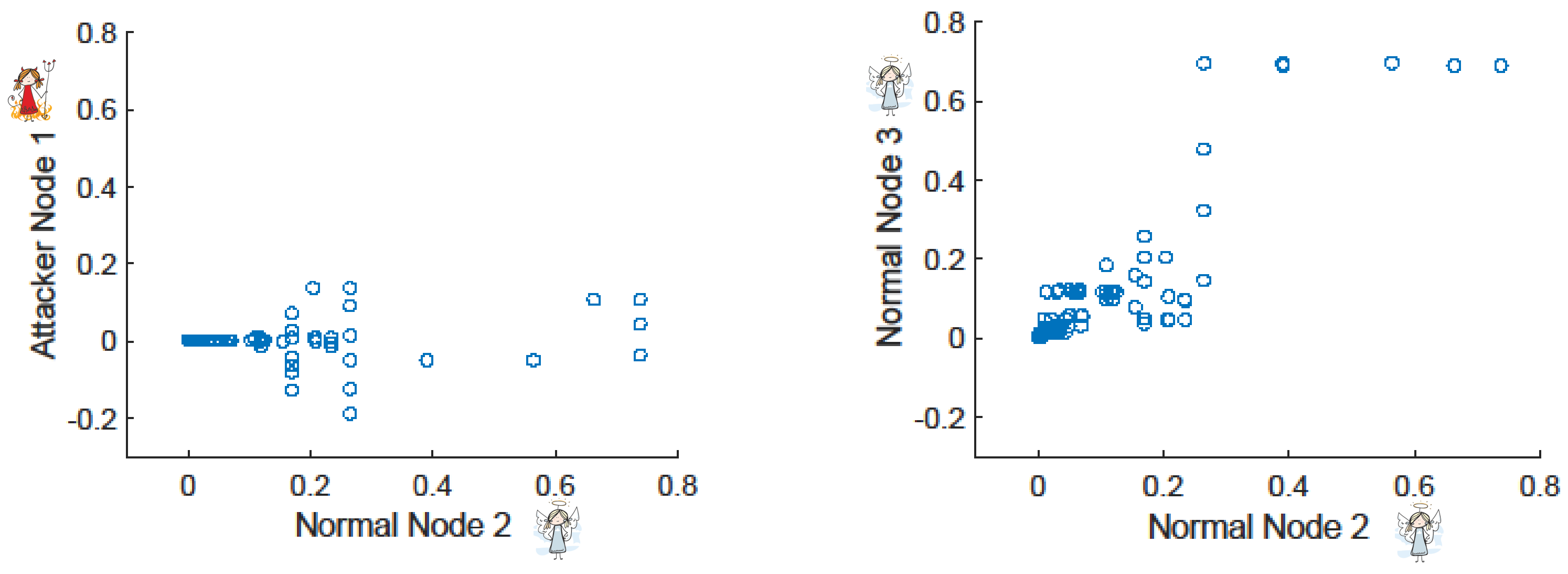


Fig. 4. Scatterplots of normal node vs. attacker, & two normal nodes. and not correlated, while and are correlated.

- We perform an anomaly test & detect whether an attacker is present and which node is malicious (see paper for details).

RESULTS

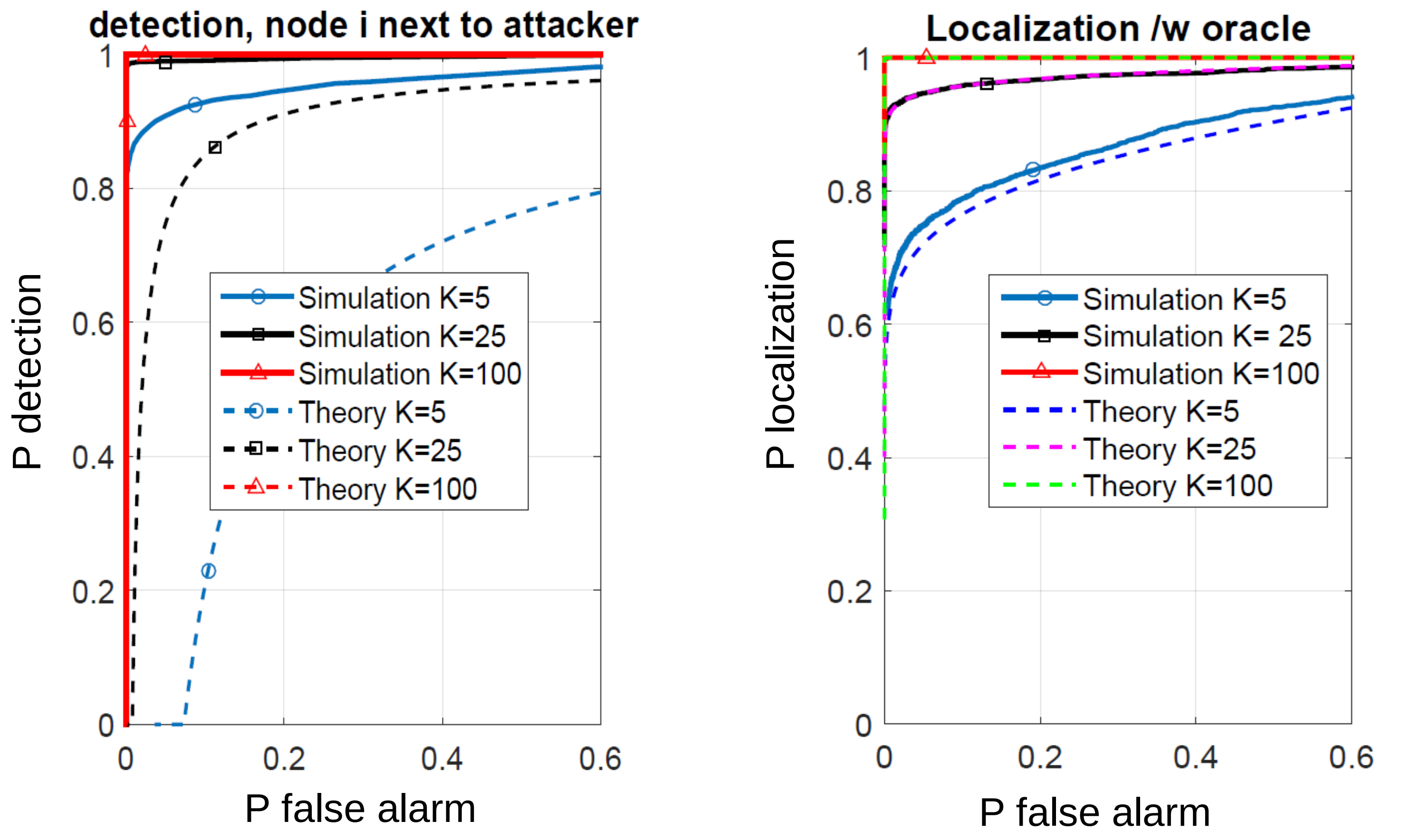


Fig. 5. Detection and localization of an attacker (solid lines = Monte Carlo simulation; dashed lines = theoretical bound)

Observations:

- The more we average over *K* instances, the better.
- Gaussian approximation is very good for localization, but only a bound for detection.
- Also works when the detecting node is not directly next to an attacker.
- Our method can also be applied to cases with more than one attacker.
  - Detection performance degrades as the number of attackers increases or if more attackers are surrounding a node.
  - As the number of attacking neighbors increases, localization performance degrades faster than detection.

ALTERNATIVE STRATEGY: TEMPORAL METHOD

- Node j converges towards the attacker's s state at time ∞.

$$\mathrm{E}[x_s^k(\infty)] = \bar{\alpha} = \mathrm{E}[x_j^k(\infty)]$$

- At the beginning of the algorithm, each node has a different state.

$$\mathrm{E}[x_s^k(0)] = \bar{\alpha} \neq \bar{\gamma} = \mathrm{E}[x_j^k(0)]$$

- Therefore, the quantity $\left|x_i^k(\infty) - x_i^k(0)\right|$ is (in expectation) close to zero if node i is an attacker; it is large if i is a normal node and an attacker is present.
- See paper for detailed description and results.

FUTURE EFFORTS

- Research more complicated topologies.
- Apply these results to our work in decentralized networks.
- Combine temporal and spatial method together for even better performance.

R. Gentz, S. X. Wu, H. T. Wai, A. Scaglione, and A. Leshem, “Data injection attacks in randomized gossiping,” submitted to *IEEE Transactions on Signal and Information Processing over Networks*, Feb. 2016.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY