Secure Distributed State Estimation for Large-Scale Systems
Aritra Mitra and Shreyas Sundaram

1. MOTIVATION

- To control complex systems (e.g., power grids, gas turbines, transportation systems), we need to monitor their state dynamics.
- Consider an LTI dynamical system whose state $x(k)$ is monitored by a network $g = (V, E)$ of N sensor nodes.
- Each node $i$ has measurement $y_i(k) = C_i x(k)$.

Objective: Each node must estimate the state $x(k)$ (asymptotically).

Key Question: What if some sensors are compromised by adversaries?
- Can have catastrophic effects in safety critical systems.
- Must develop secure distributed state estimation algorithms.

2. ADVERSARY MODEL

- We consider worst-case adversarial behavior (Byzantine adversaries).
- Adversaries have complete knowledge of system dynamics and network.
- Adversaries can deviate arbitrarily from any prescribed algorithm.
- In contrast, regular (non-adversarial) nodes possess only local information.
- At most $f$ adversaries in the neighborhood of any regular node ($f$-local model).

3. OUR CONTRIBUTION

- We develop a secure distributed state estimation algorithm with provable guarantees.
- Algorithm is lightweight, fully distributed and runs on a single-time-scale.
- We characterize feasible network topologies that guarantee success of our algorithm.

4. ESTIMATION STRATEGY

- Each node estimates a portion of the state using local measurements.
- For estimating the rest of the state, it communicates with neighbors.
- Key is to identify "leaders" or "source nodes" for certain portions of the state.
- Disseminate information from source nodes to the rest of the network via "sufficient number of redundant" paths.

5. LOCAL LUENBERGER OBSERVERS

- For identifying source nodes, diagonalize the system: $x(k) = V^{-1} k(\hat{k})$.
- Each node $i$ constructs a local Luenberger observer contains eigenvalues node $i$ can detect $\mathcal{L}_i(k) = \mathcal{L}_i(k) + L_i(y_i(k) - C_i z_i(k))$.

Portion of state node $i$ can estimate independently: $\mathcal{L}_i(k+1)$ locally designed gain matrix

Local observer guarantees that $\Delta_i(k+1)$ converges to true value.

The tricky part: Node $i$ has to communicate with neighbors (can be adversarial) to estimate the rest of the state. Dependent on certain "source nodes" for this purpose.

6. SECURE CONSENSUS SCHEME

Question: How to transmit info from source nodes to the rest of the network securely?
Solution: Construct Mode Estimation Directed Acyclic Graphs (MEDAGs).
MEDAGs provide sufficient number of redundant paths for information transmission.
In particular, each non-source node has $(2f+1)$ parents in a MEDAG.

MEDAG construction algorithms are fully distributed and resilient to adversarial attacks.

7. LOCAL FILTERING DYNAMICS

- Suppose node $i$ cannot estimate the state $z_i(k)$.
- Let $s_i$ denote the set of source nodes that can estimate $z_i(k)$.
- Construct MEDAG to transmit info from $s_i$ to node $i$.
- At each time-step $k$, node $i$ collects estimates from its parents in the MEDAG.
- It throws away the highest and lowest $f$ estimates, and takes a convex combination of the rest of the estimates as follows:

$$
\hat{z}_i(k+1) = \sum_{j \in \text{parents}(i)} w_j \hat{z}_j(k)
$$

Unstable eigenvalue that node $i$ cannot detect
Convex weights
Parents after removing extreme values

KEY IDEA: Ignore extreme values in neighborhood, take weighted average of the rest.

8. FEASIBLE NETWORK TOPOLOGIES

- Feasible networks allow success of our algorithm.
- They are characterized by a graph property known as "robustness".
- Robustness is defined in terms of $r$-reachable sets.
- A set $s$ of nodes is $r$-reachable if it contains at least one node that has $r$ neighbors outside the set.

MAIN RESULT: If the network is "strongly $(3f+1)$-robust" w.r.t. every set of source nodes, then all regular nodes can asymptotically estimate the state using the proposed secure distributed state estimation technique, despite the actions of any $f$-local set of adversaries.

9. OVERALL TECHNIQUE

- Identify source nodes.
- Construct MEDAGs to transmit info from source nodes to rest of the network.

DESIGN PHASE

- Each node uses local Luenberger observer to estimate portion of state.
- For the rest of the state, it listens to its parents in the MEDAG and applies the local filtering scheme.

ESTIMATION PHASE

- Real-time control of complex systems requires precise state estimation of distributed systems via sensor measurements.
- Investigated the problem where certain sensors are compromised by adversaries.
- Developed a lightweight, fully distributed secure state estimation algorithm with provable guarantees against worst-case attacks.
- Characterized communication networks that facilitate our method.

10. TAKE-AWAY POINTS

- Real-time control of complex systems requires precise state estimation of distributed systems via sensor measurements.
- Investigated the problem where certain sensors are compromised by adversaries.
- Developed a lightweight, fully distributed secure state estimation algorithm with provable guarantees against worst-case attacks.
- Characterized communication networks that facilitate our method.

11. REFERENCE


Contact: (mitra14,sundara2)@purdue.edu