Gossip Average Consensus in a Byzantine Environment Using Stochastic Set-Valued Observers

D. Silvestre, P. Rosa, R. Cunha, J. Hespanha and C. Silvestre

52nd IEEE Conference on Decision and Control, CDC 2013
Florence, Italy.

12th December 2013

Outline

Motivation

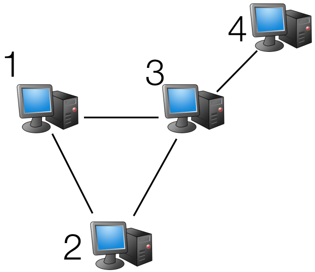
- Average Consensus Problem - m nodes wish to agree on the average of their initial values.
- Robot Coordination - Fleet of robots wishes to agree on direction/speed or rendezvous point.
- Sensor Network - Compute the mean of a noise corrupted set of sensor measurements.

Gossip Consensus

- Pairs of nodes exchange their states at random times.
- Nodes transmit only to adjacent nodes in the connectivity graph.
- Both nodes average their states.
- See S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," IEEE Transactions on Information Theory, vol.52, no.6, pp.2508 - 2530, June 2006.

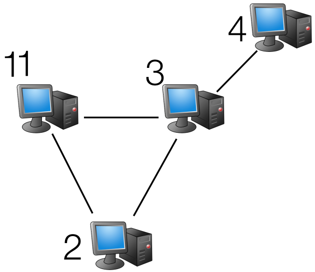
Motivating Example

- Take the network given by the following graph and state at time instant k, $x(k) = [1, 2, 3, 4]^\intercal$
- The consensus algorithm will asymptotically converge to all the nodes having $x_{\text{av}} = 2.5$
- If an attacker controlling one node in one time instant resets the state to $\tilde{x}_1(k) = x_1(k) + m(c - x_{\text{av}})$
- In this example $c = 5$, but the attacker can force the network to converge to any constant c!



Motivating Example

- Take the network given by the following graph and state at time instant k, $x(k) = [1, 2, 3, 4]^\intercal$
- The consensus algorithm will asymptotically converge to all the nodes having $x_{\text{av}} = 2.5$
- If an attacker controlling one node in one time instant resets the state to $\tilde{x}_1(k) = x_1(k) + m(c - x_{\text{av}})$
- In this example $c = 5$, but the attacker can force the network to converge to any constant c!



Problem Outline

- Take m agents running a consensus system of the form

$$\begin{cases} x(k+1) = U(k)x(k) + B(k)u(k) \\ y(k) = C(k)x(k) \end{cases}$$

- $u(k)$ is the attacker signal, $B(k)$ the matrix selecting which nodes are corrupted and $U(k)$ a matrix randomly selected.

Fault Detection Problem

Detect non-zero signals $u(k)$ using $y(k)$ without the knowledge of $B(k)$.

Proposed Solution

Worst-case Scenario

- The probabilistic information of each event is discarded;
- Assumption on bounded initial conditions;
- Use Set-Valued Observers (SVOs) to generate a set $\tilde{X}(k)$ where the state can take values.

Stochastic Scenario

- Includes the detection of faults which are possible but very unlikely;
- May generate false positives;
- Introduction of Stochastic Set-Valued Observers (SSVOs).

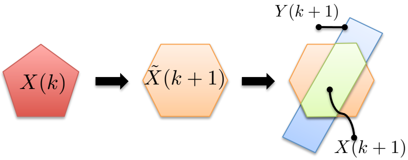
SVOs vs. SSVOs

- In both cases, we are addressing it as a Distinguishability problem between the measurements and a fault-free model;
- SSVOs are a generalization of SVOs and compute a α-confidence set where the state is guaranteed to be with probabilitiy $1-\alpha$;
- The generated set is a polytope containing points respecting the dynamics of the system and observations;
- In the SSVOs, the dynamics representing unlikely events are discarded.

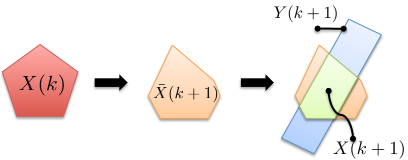
Algorithm

Given the previous set $X(k)$:

- Using SVOs, the algorithm predicts $\tilde{X}(k+1)$ using the dynamics;
- Then, the set is intersected with the measurement set $Y(k+1)$.



- Using SSVOs, the algorithm predicts $\bar{X}(k+1)$ using the dynamics of likely events;
- Then, the set is intersected with $Y(k+1)$ obtaining a smaller set.



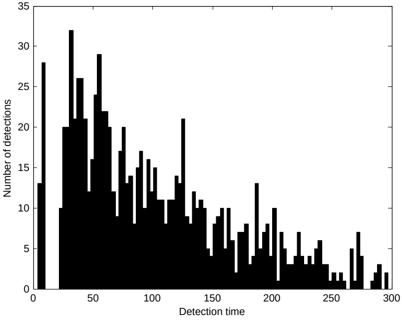
Properties

- The set $\tilde{X}(k)$ is bounded in terms of number of vertices and hyper-volume;
- The maximum magnitude of the attacker signal can be computed *a priori* using an optimization problem;
- The properties are generalized for the SSVOs case.

Simulation Results

Setup: 5 node network and initial states $x_i(0) = i - 1$ and a nominal bound $|x_i| \leq 5$ and a horizon $N = 1$.

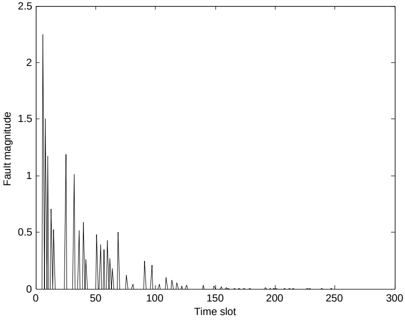
- For a stochastic fault, the same pair is forced to communicate for $10 < k < 20$.
- The likelihood of detection increases with time.
- An attacker injects the maximum undetectable signal at each time instant.
- The magnitude of the signal decays very rapidly in simulation.



Simulation Results

Setup: 5 node network and initial states $x_i(0) = i - 1$ and a nominal bound $|x_i| \leq 5$ and a horizon $N = 1$.

- For a stochastic fault, the same pair is forced to communicate for $10 < k < 20$.
- The likelihood of detection increases with time.
- An attacker injects the maximum undetectable signal at each time instant.
- The magnitude of the signal decays very rapidly in simulation.



Concluding Remarks

Contributions:

- Recast of the fault detection problem to that of Distinguishability of two systems;
- Upper bound on the magnitude of the attacker signal;
- The introduction of Stochastic Set-Valued Observers to deal with probabilistic faults.
  - Bounded number of vertices
  - Bounded Hyper-volume
- In Simulation is shown:
  - Worst attacker signal magnitude decays very fast;
  - Faults are more likely to be detected as time progresses.

The end

- Thank you for your time.

Gossip Average Consensus in a Byzantine Environment Using Stochastic Set-Valued Observers

D. Silvestre, P. Rosa, R. Cunha, J. Hespanha and C. Silvestre

52nd IEEE Conference on Decision and Control, CDC 2013
Florence, Italy.

12th December 2013