Stochastic and Deterministic Fault Detection for Randomized Gossip Algorithms

Daniel Silvestre, Paulo Rosa, João Hespanha and Carlos Silvestre

澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

Objectives

•Compute the average of the initial states in finite-time

•Guarantee fault detection and bounds on the maximum possible deviation from an attack

•Incorporate the transmissions stochastic information in the fault detection mechanism.

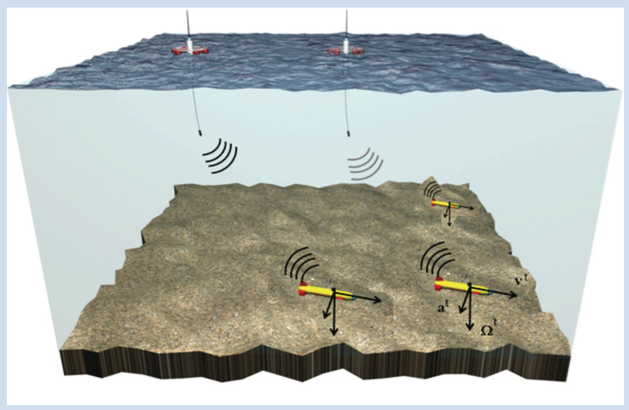
① Motivation

Nodes need to distributedly agree on a common value:

•Smart Grids when deciding the needed power

•Robot swarms to find rendezvous points

•Social Networks making a pool about a subject.



In all these examples a single node can drift the entire network to any desired value!

② Problem Statement

The objective is to compute the average of some quantity of interest. If faulty, any node must detect the fault using only local information communicated from their neighbors.

$G = (V, E) \qquad E \subseteq V \times V$

$$S^i : \begin{cases} x(k+1) = \left(A_0 + \sum_{\ell=1}^{n_\Delta} \Delta_\ell(k) A_\ell\right) x(k) + B(k)u(k) \\ y^i(k) = C^i(k)x(k) \end{cases}$$

n_Δ number of uncertainties

Each S^i is a Linear Parameter-Varying (LPV) system

$\Delta_\ell(k)$ are scalar uncertainties

Byzantine Consensus Problem:

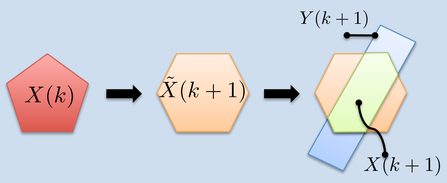
Either detect non-zero signals $u(k)$ using $y(k)$ without the knowledge of $B(k)$ or compute the final consensus value.

③ Proposed Solution

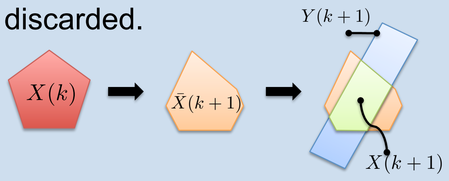
Each node runs a Stochastic Set-Valued Observer (SSVO). The estimates are intersected as to produce less conservative polytopes.

1) Compute the next set-valued estimates

Example of a SVO update for horizon 1.



Example of a SSVO update where low probability events are discarded.



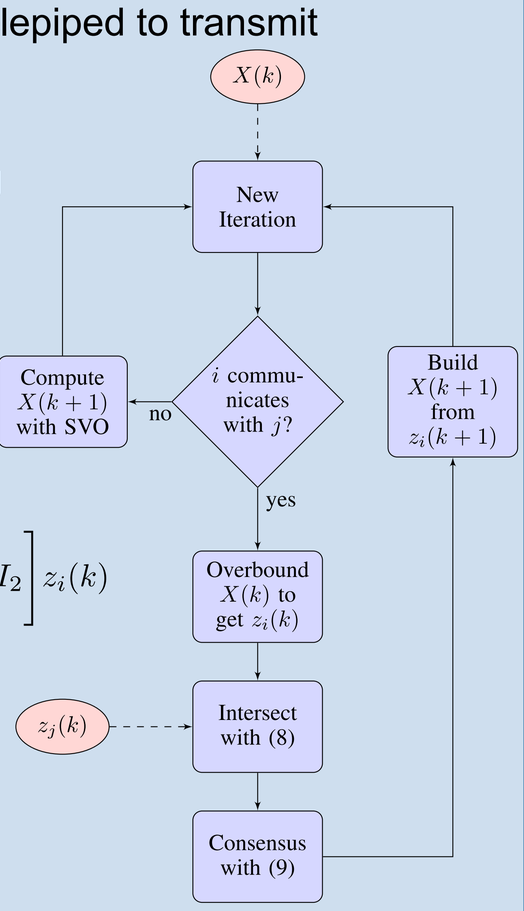
2) Overbound using a hyper-parallelepiped to transmit estimates to neighbors

3) Intersect estimates by performing

$$z_i(k) = z_j(k) = \max(z_i(k), z_j(k))$$

4) Perform a consensus update on the estimates interval

$$z_i(k+1) = \left[\left(\frac{1}{2}(e_i - e_j)(e_j - e_i)^\intercal + I_{n_x}\right) \otimes I_2\right] z_i(k)$$



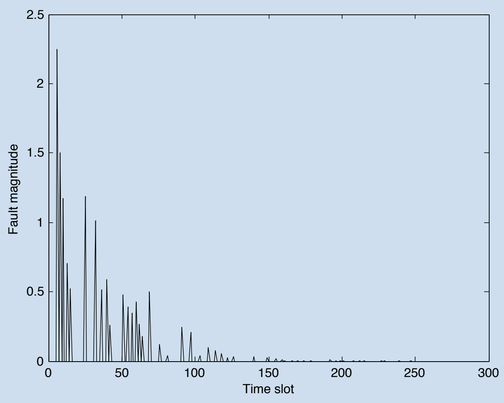
Flowchart of the proposed algorithm

Remark:

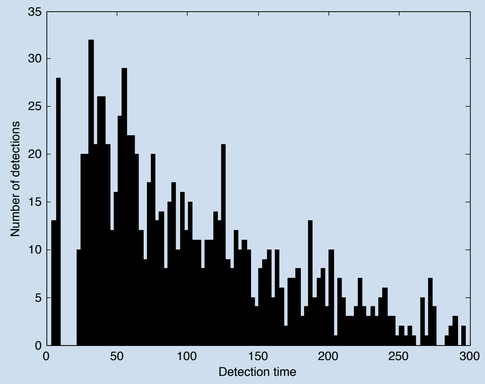
Fault detection consists in checking if the result of the intersection in step 3) is the empty set.

④ Results

• The magnitude of an attacker fault signal is bounded.



• Faults are more likely to be detected as time increases.



• Finite-time consensus is achieved.

• Less conservative set-valued estimates.

Main result:

The algorithm can either detect and intruder or compute the average consensus in finite-time.

Daniel Silvestre, Paulo Rosa, João Hespanha and Carlos Silvestre, Stochastic and Deterministic Fault Detection for Randomized Gossip Algorithms, **Automatica**, Volume 78, Pages 46-60, 2017.