Finite-time Consensus in the Presence of Malicious Agents

Sachit Rao and Shrisha Rao

International Institute of Information Technology, Bangalore, India

Resilient consensus protocol (RCP) for a connected network of n agents:

- when some of the agents are malicious (MA)
- cooperative (CO) agents do not know the identities and number of the MA agents
- information exchange is local and agents have first-order continuous dynamics
- consensus amongst the CO agents in finite-time

Introduction

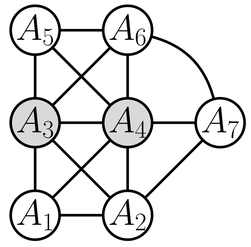
In a connected network of agents, where some are MA, in the consensus problem, MAs can drive the consensus value of the CO agents to an unsafe region. An RCP should satisfy the *agreement* condition—the states of any connected pair of CO agents should reach the same value; and the *validity* condition—the trajectories of the CO agents should lie within the interval defined by the agents' initial conditions (ICs) [1, 2].

Here, a sliding mode control (SMC)-based RCP is developed for agents with first-order dynamics $\dot{x}_i = u_i$. CO agents apply the same input form, while an MA need not do so. An MA can also transmit, as its state information, different values to different neighbors.

The input u_i is chosen to enforce sliding mode [3] on a manifold that leads to consensus amongst CO agents within a **finite-time** interval. The manifold for each agent is designed using states of its neighbours, thus making the RCP a local one. **Requirement to know the number and location of MAs is eliminated for MAs that send values that lie outside the convex hull formed by the agents' ICs, Conv$(x_i(t=0),\ 1 \leq i \leq n)$ - also, the safe region.** In Fault Identification and Detection literature, a faulty agent can be detected only if its input drives its state out of some known bounds [4], that is, the safe region is known.

The SMC-based RCP satisfies the validity and agreement conditions **if and only if the sub-graph induced by the removal of the MAs is connected**. Consensus occurs for any attack model; network topology, for instance, one with cycles and cliques; and for agents "becoming" MA at any time.

Main Results



Network of CO (in white) and MA (in gray) agents

The network topology is defined by an **undirected** graph G with n vertices. For G, the symmetric Laplacian matrix $\mathbf{L}(G) \in \Re^{n \times n}$ can be defined. $\mathbf{L}(G)$ is rank-deficient (by 1); hence, a vector $\mathbf{x}_r \in \Re^{n \times 1}$, with non-zero identical elements, can be found such that $\mathbf{L}(G)\mathbf{x}_r = \mathbf{0}$. It is this property of the Laplacian matrix that is used to provide consensus.

Theorem

For a network comprised of f MAs and $(n-f)$ CO agents, the SMC protocol

$$u_i = -M\,sign(s_i),\ s_i = \mathbf{L_i}(G_R)\mathbf{x}_{Ci},\ M > 0,$$

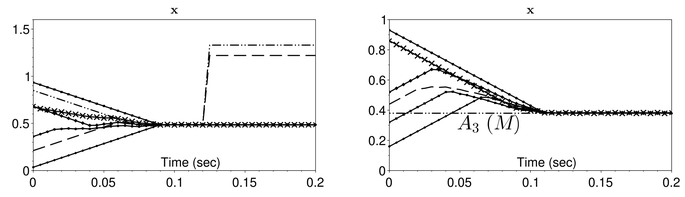
leads to consensus amongst the CO agents if and only if the graph G_R formed by the removal of the MAs is connected. $\mathbf{L_i}(G_R)$ is row i of the Laplacian matrix of the reduced graph G_R and $\mathbf{x}_{Ci}$ is the vector of the CO agents' states.

Proof.

When $0 < f < n$, a CO agent disregards the information sent by MAs connected to it. Now, if graph G_R consisting of only CO agents is connected, then its Laplacian matrix $\mathbf{L}(G_R)$ is also rank deficient $(n-f-1)$. Now, proof that the SMC-based RCP (**??**) guarantees consensus within a finite-time interval is similar to [5]. □

- The consensus value is the average of the minimum and maximum ICs of the CO agents
- consensus time can be tuned using the control gain M
- consensus occurs also if MAs transmit the same state to all their neighbors, but within the safe region

Simulation Results



Consensus when: (a) 2 agents become MA after initial consensus; (b) a single MA transmits a valid state

Agents A_3 and A_4 are MAs; the graph of CO agents is connected. *Left figure*: CO agents remain in consensus when $A_{3,4}$ become malicious. *Right figure*: the CO agents reach a consensus at the valid state of the single MA. The agreement and validity conditions are both satisfied.

Conclusion

The SMC-based RCP leads to finite-time consensus in the presence of a class of MAs, independent of their locations and network topology. The protocol is simple to implement and can be extended to other types of MAs.

References

[1] Seyed Mehran Dibaji, Hideaki Ishii, and Roberto Tempo. Resilient randomized quantized consensus. 63(8):2508–2522, 2018.

[2] Heath J. LeBlanc, Haotian Zhang, Xenofon Koutsoukos, and Shreyas Sundaram. Resilient asymptotic consensus in robust networks. 31(4):766–781, April 2013.

[3] Vadim I. Utkin. *Sliding modes in control and optimization*. Springer-Verlag, 1992.

[4] Daniel Silvestre, Paulo Rosa, Jo ao P. Hespanha, and Carlos Silvestre. Finite-time average consensus in a byzantine environment using set-valued observers. In *2014 American Control Conference*, pages 3023–3028, 2014.

[5] Sachit Rao and Debasish Ghose. Sliding mode control-based algorithms for consensus in connected swarms. *International Journal of Control*, 84(9):1477–1490, 2011.

Email: sachit@iiitb.ac.in; shrao@ieee.org

International Institute of Information Technology Bangalore

AAMAS2021 ONLINE, MAY 3–7