Azwirman Gusrialdi*

Resilient Cooperative Control of Cyber-Physical Systems Under Cyber-Attacks

Keywords: Resilient control, cooperative control, cyber-attacks, distributed algorithm, safety-critical systems

***Corresponding Author: Azwirman Gusrialdi:** Faculty of Engineering and Natural Sciences, Tampere University, E-mail: azwirman.gusrialdi@tuni.fi

1 Background

Cyber-physical systems (CPS) are the backbone of modern society, powering transformative applications such as smart grids, intelligent transportation systems, robotic networks, smart manufacturing, and smart buildings. These systems tightly integrate physical processes with cyber (e.g., computing, communication and networking) technologies, creating a vast network of interconnected devices. Cooperative control plays a crucial role in ensuring stability and optimizing performance of CPS. Specifically, the individual system collaboratively computes its control input to achieve a common/global goal through local communication and without centralized entity, thus enabling scalability, low latency, and robustness. However, the same network connectivity that facilitates these advantages also expands the attack surface, exposing vulnerabilities to cyber threats. These attacks compromise the confidentiality, integrity, and availability of data exchange, disrupting cooperative control mechanism and may result in physical damage as evidenced by the 2015 Ukraine power grid incident causing a 6-hour blackout. This calls for resilient cooperative control to ensure safe and optimal operation of CPS in presence of cyber-attacks. However, the design of resilient cooperative control against cyber-attacks is highly challenging due to the unpredictability of attack parameters, including their number, timing, duration, and location.

2 Aims

We present a resilient cooperative control algorithm that has been developed in our research group for the past ten years [1–3]. Specifically, the cooperative control algorithm ensures resilient operation of CPS against false data injection attacks, a prevalent form of deception attacks, which inject malicious signals into the communication links to alter exchanged data. The proposed method allows unlimited communication links/channel to be attacked while assuming a bounded attack magnitude, a reasonable precaution for intelligent attackers to avoid detection. The proposed cooperative control is independent of the networking technologies and also enables real-time attack detection and identification.

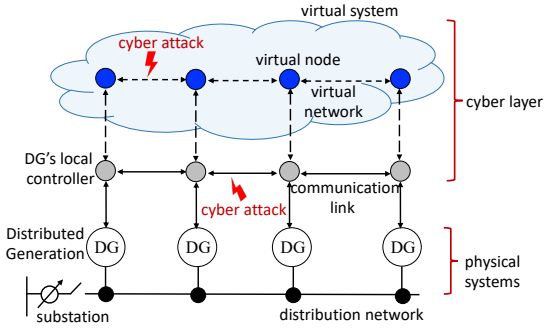
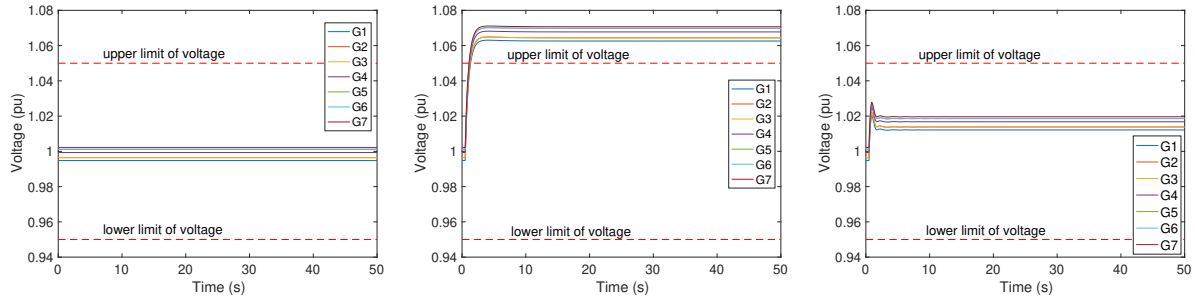


Fig. 1. Competitive interaction design featuring a virtual system interconnected with a local controller in a power system use case.

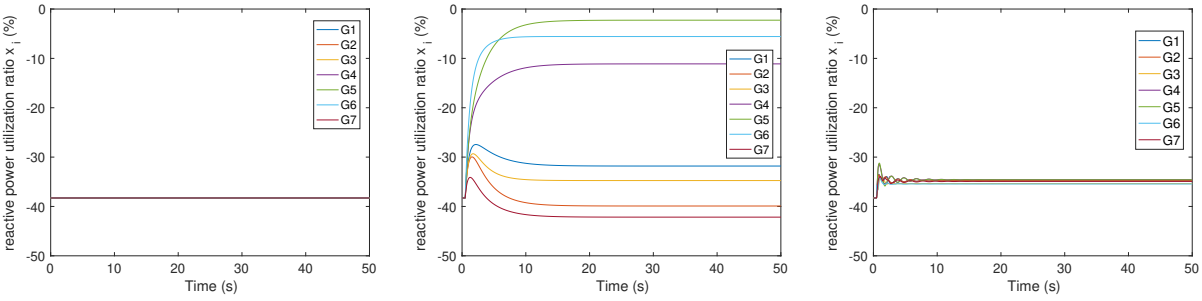
3 Materials and Methods

The resilient cooperative control algorithm is designed based on the competitive interaction design method proposed in the author's work [1–3]. This method introduces a virtual system consisting of virtual nodes, each maintaining a non-physically meaningful state variable (referred to as a virtual state), as illustrated in Fig. 1. These virtual nodes communicate through a virtual network, also susceptible to attacks, and interact with the local controllers of individual systems via an internal signal. This setup forms a competitive interaction. The virtual network can be implemented using cloud infrastructure or multiple communication channels, with the virtual states functioning as auxiliary states of the local dynamic controller. The dynamics of the virtual system is designed for ensuring convergence to a neighbourhood of normal operating point of the CPS, detecting attacks, and in the absence of attacks maintaining convergence to the normal operating point.



(a) cooperative control without attacks **(b)** cooperative control under attacks **(c)** resilient cooperative control

Fig. 2. Voltage profiles of PVs in a distribution network under three considered scenarios



(a) cooperative control without attacks **(b)** cooperative control under attacks **(c)** resilient cooperative control

Fig. 3. Utilization ratios of DGs in a distribution network under three considered scenarios

4 Results

We demonstrate the resilient cooperative control on voltage control for a distribution network consisting of distributed generations such as photovoltaics (PVs). High penetration of PVs will cause several technical issues such as the over-voltage problem in the network which occurs mainly when PV generation reaches its peak while the load demand is relatively low. One possible strategy to mitigate the over-voltage issue is to implement a cooperative control algorithm at each PV to control and coordinate their reactive power in the network during this time. Decisions at the local level are made by each PV exchanging information via a communication network. The goal is to control the reactive power of the PVs such that the voltage deviation of all PV buses are well regulated within the ANSI standard limits (5%) in order to ensure power quality. An additional control design goal is to have reactive power load sharing where all the PVs contribute equally to the voltage control. Applying cooperative control algorithm designed in [4] ensure that the voltage of the PVs are within the safe operating limit and achieving equal reactive power utilization ratios as shown in Figs. 2a, 3a. Next, we introduce false data injection attacks on the communication network. As shown in Figs. 2b, 3b, the attacks render overvoltage for all the PVs in the group and that their utilization ratios fail to reach a consensus. Finally, we implement the resilient cooperative voltage control developed in [4]. It can be observed from Fig. 2c that, due to the virtual network, the voltages of all the PVs are regulated and maintained within the operational limits even though some of the communication links are compromised. Furthermore, utilization ratios of all the PVs are also made to approach a consensus as evidenced from Fig. 3c.

References

[1] Gusrialdi A, Qu Z, Simaan M. Robust design of cooperative systems against attacks. In: *Proceedings of American Control Conference*. 2014; pp. 1456–1462.

[2] Gusrialdi A, Qu Z, Simaan MA. Competitive interaction design of cooperative systems against attacks. *IEEE Transactions on Automatic Control*. 2018;63(9):3159–3166.

[3] Iqbal M, Qu Z, Gusrialdi A. Distributed resilient consensus on general digraphs under cyber-attacks. *European Journal of Control*. 2022;p. 100681.

[4] Gusrialdi A, Xu Y, Qu Z, Simaan MA. Resilient cooperative voltage control for distribution network with high penetration distributed energy resources. In: *Proc. of European Control Conference*. 2020; pp. 1533–1539.