18th International Conference on Innovative Computing, Information and Control (ICICIC2024)
Onsite (Qinhuangdao, China) and Online, September 10-13, 2024

PS-29: ICICIC2024-SS17-02

Leader-Follower Consensus of Multiple Euler-Lagrange Systems with Sensor and Actuator Attacks

Rui Gao[1,*], Jiangshuai Huang[2], Yao Wen[3], Hong Cheng[4] and Zeqiang Li[5]

[1]College of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China
[2]College of Automation, Chongqing University, Chongqing 400044, P. R. China
[3]College of Automation, Chongqing University of Post and Telecommunication, Chongqing 400065, P. R. China
[4]College of Electrical Engineering, Sichuan University, Chengdu 610065, P. R. China
[5]College of Faculty of Science and Technology, University of Macau, Macau SAR, P. R. China
*Corresponding author: gaorui@cqupt.edu.cn

Introduction

This paper investigates the leader-follower consensus control of multiple uncertain Euler-Lagrange systems under sensor and actuator attacks. To handle the adverse effects from the attacks due to vulnerability of the communication network, a fully distributed adaptive leader-follower consensus control strategy is proposed to tackle the time-varying uncertainties of the cyber attacks. The main difficulty lies in the negative interaction, which results from time-varying gains of the attackers and the Laplacian graph of multi-agent systems and has been successfully solved.

Research Questions

The existing control protocols are hard to generalize due to its specificity and could not be used in consensus control of multiple nonlinear systems such as Euler-Lagrange systems when there exist sensors and actuator attacks. Hence, it is more tricky and worthy to be deeper investigated to solve the problem of the vicious attacks and the uncertainties synchronously for Euler-Lagrange systems.

Methodologies

The leader-follower consensus issue of multiple uncertain Euler-Lagrange systems subjected to cyber attacks is considered. In fact, we assume that the signals from controller to actuator and sensor to controller transmission channel would be both attacked. Therefore, the transmitted control signal of each agent containing its own signals and the signals derived from the neighbors, are perturbed through cyber-attacks, which results in adverse impact on the closed-loop system stability of each entity and consensus of the multiple Euler-Lagrange systems.

Conclusion

In this paper, the proposed control algorithm is capable of dealing with the leader-follower consensus problem for multiple uncertain Euler-Lagrange systems when there exist venomous attacks in sensor and actuator. The developed fully distributed consensus control protocol ensures that all the closed-loop signals are uniformly ultimately bounded against the damage to system performance from adversaries attacks. The theoretical proof and numerical simulation are both performed to verify the proposed control strategy. Our future work will include but not limited to designing new control strategy to tackle different attacks with more universal models.

Mathematical Formulas

$$\begin{cases}\dot{\tilde{x}}_{i,1}=\tilde{x}_{i,2}\\ \dot{\tilde{x}}_{i,2}=F_i\left(\tilde{x}_i,p_i,t\right)+G_i\left(\tilde{x}_{i,1},p_i\right)\left[u_i+W_I^T\left(t\right)\xi_i\left(\tilde{x}_i\right)\right]\end{cases}\tag{1}$$

$$y_r\left(t\right)=\sum_{i=1}^{v}f_{r,l}^T w_{r,l}+c_r=f_r^T w_r+c_r=\overline{f}_r^T\overline{w}_r \tag{2}$$

$$0\le\left|z\right|-z\cdot sg\left(z\right)\le\sigma \tag{3}$$

$$\dot{V}_2\le-\rho_v V_2+C_v+\left[\lambda N_i\left(\chi_i\right)-1\right]\dot{\chi}_i \tag{4}$$

Figure

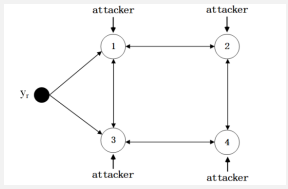

Figure 1. Communication graphs subject to attacks

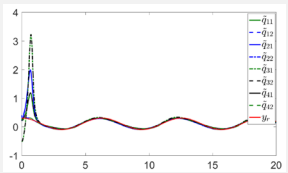

Figure 2. Positions of all agents

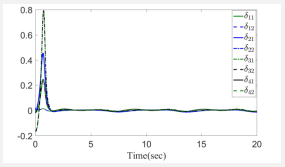

Figure 3. Tracking errors of all the agents

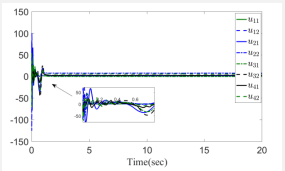

Figure 4. Input signals of the agents

In the communication topology, the leader and the four followers subjected to attacks are shown in Figure 1. Figure 2 shows the positions of the four manipulators. Figure 3 illustrates the tracking errors. Figure 4 shows the control input signals of the agents. It can also be observed that all of the signals for multiagent systems are bounded and output of the *i*th agent can track the given reference with an arbitrarily small error even though there exist cyber attacks.