19th International Conference on Innovative Computing, Information and Control (ICICIC2025)
August 26-29, 2025, Kitakyushu, Japan

PS-1: ICICIC2025-SS14-01

Learning-Based Cooperative Control of Multi-Robot Systems under DoS Attacks

Rui Gao

School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China
gaorui@cqupt.edu.cn

Introduction

Distributed multi-robot systems are increasingly used in areas like environmental monitoring and warehouse automation, but their reliance on wireless ad hoc networks makes them vulnerable to cyber threats such as Denial-of-Service attacks. These attacks can disrupt communication, compromising system performance and stability. Traditional control methods often assume reliable communication and lack adaptability to such threats. To address this, we propose a resilient control framework that combines event-triggered consensus control with Proximal Policy Optimization reinforcement learning, enabling robots to adaptively manage control.

Research Questions

In the presence of DoS attacks, communication links between certain agents may become unavailable for periods of time. Under these conditions, the main research questions we address are

1) How can robots maintain stable and efficient cooperation when communication is intermittently disrupted by DoS attacks?
2) Can a reinforcement learning framework learn to adaptively adjust both control parameters and communication strategies based on the observed attack patterns?
3) What theoretical guarantees can be established regarding the stability and convergence of the system under bounded DoS attack models?

Methodologies

We propose a hybrid control framework that combines event-triggered consensus control with a deep reinforcement learning algorithm. The overall framework is designed as follows.

1) Each agent updates its control action only when certain state-dependent triggering conditions are met. This mechanism helps reduce unnecessary communication and improves resilience to disruptions.
2) An auxiliary module monitors the availability of communication links and estimates DoS attack patterns (e.g., frequency, and duration). This information is encoded into the agent's observation space.
3) To ensure that the proposed learning-based control framework is not only adaptive but also theoretically sound, we conduct a stability analysis under bounded DoS attack assumptions.

Mathematical Formulas

The dynamics of robot R_i is described by

$$\begin{aligned} \dot{x}_i &= v_i \cos\psi_i \\ \dot{y}_i &= v_i \sin\psi_i \\ \dot{\psi}_i &= w_i \\ M_i \dot{v}_i &= -C_i(w_i)v_i - D_i v_i + \tau_i \end{aligned} \tag{1}$$

$$\boldsymbol{M}_i = \frac{2}{r_i}\begin{bmatrix} m_{11i}+m_{12i} & 0 \\ 0 & b_i(m_{11i}-m_{12i}) \end{bmatrix}, \boldsymbol{v}_i = [v_i, w_i]^T,$$

$$\boldsymbol{C}_i = \frac{2}{r_i}\begin{bmatrix} 0 & -b_i c_i w_i \\ c_i w_i & 0 \end{bmatrix}, \boldsymbol{\tau}_i = [\tau_{vi}, \tau_{wi}]^T,$$

$$\boldsymbol{D}_i = \frac{1}{r_i}\begin{bmatrix} d_{11i}+d_{22i} & b_i(d_{11i}-d_{22i}) \\ d_{11i}-d_{22i} & b_i(d_{11i}+d_{22i}) \end{bmatrix}$$

Figure

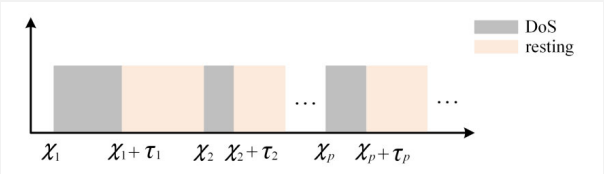

Figure 1. Denial-of-service attacks. Duration is the length of the interval over which communication is disabled. Resting time is length of the recovering interval between two consecutive attacks.

Denial-of-Service (DoS) attacks intend to block communication channels intermittently and prevent system (1) from being executed. In particular, both sensor-to-controller and controller-to-actuator channels are assumed to be blocked by DoS simultaneously.

Conclusion

We validate the proposed approach using a simulation environment based on Python and OpenAI Gym, with a custom multi-agent formation control scenario. Each agent controls its position in a 2D space and must maintain a predefined formation while experiencing random DoS attacks on its communication links. The baseline comparison includes conventional consensus control without attack mitigation, event-triggered control without learning and the proposed PPO-based adaptive control framework.