RESILIENT COOPERATIVE CONTROL OF MULTI-AGENT SYSTEMS AGAINST A CLASS OF CYBER ATTACKS

Multi-agent Systems (MAS) represent a large class of systems such as power networks, transportation systems, water networks, robotic swarms etc. These systems are characterized by the combination of physical processes and a communication network for operation and control. However, information exchange on the communication network exposes MAS to the cyber-attacks. Therefore, it is important to ensure acceptable performance of the MAS in the event of a cyber-attack. In this thesis, resilient cooperative control for various classes of MAS are investigated which include MAS described by linear and nonlinear coupling. Then, a resilient cooperative control framework is developed that utilizes the concept of competitive interaction and realized by the introduction of a virtual network to be interconnected with the MAS. The main contributions of this thesis are briefly summarised below:

- A class of false data injection (FDI) attacks has been investigated for MAS described by the single integrator agents on a directed graph. It has been shown that the attack on a root node destabilizes the consensus dynamics. However, the state of MAS deviates from the nominal consensus when the attacker targets a non-root node. Self-feedback-based resilient consensus protocol has been proposed to counter the effect of attack.
- Competitive interaction-based resilient consensus protocols with homogeneous adaptive interaction gain have been proposed. The adaptive law for interaction gain alleviates the need to select a high, potentially conservative interaction gain. It is demonstrated that in the absence of an attack, the nominal consensus is preserved. In the presence of an attack, the agents' state converges to a small neighbourhood of the consensus state. However, in the event of an attack, the value of the interaction gain grows unbounded. In order to solve this problem, a robust adaptive law is proposed to update the interaction gain. Using Lyapunov methods, the resilience to FDI attacks and the interaction gain's convergence to a finite value has been demonstrated.
- A resilient consensus protocol with heterogeneous interaction gain has been proposed that guarantees nominal consensus in the absence of an attack and ensures resilience against FDI attacks on the communication channel. Furthermore, for the interaction gain, a fully distributed adaptive update law that solely relies on the agent's local knowledge is proposed.
- Competitive interaction-based framework has been extended for the resilient cooperative control problem for linear MAS. The impact of an FDI attack on the sensor of the agent and the communication channel has been investigated. It is demonstrated that by using knowledge of the communication graph and agent dynamics, an attacker can cause agents to diverge from the nominal consensus state. The stability of the MAS interconnected with the virtual network has been established using Lyapunov stability theory.
- The synchronization and resilient consensus issues for two classes of nonlinear MAS have been investigated in the competitive interaction framework. A network of single integrators on an undirected network is considered. This system with a nonlinear consensus protocol converges to the average of initial states in finite time. An investigation is conducted into its susceptibility to FDI attacks, and a virtual network-based resilient consensus protocol is proposed. This protocol guarantees finite-time convergence to the consensus state in the absence of attack. Using the Lyapunov stability theorem, it is shown that the consensus error converges to a bounded set in finite time in case of a bounded attack. Moreover, a distributed synchronization protocol based on competitive interaction is also proposed for the Kuramoto network. The resilience against a constant FDI attack is illustrated with the help of a numerical simulation.