Multi-Agent Systems – Issues, Design and Challenges

Abstract: Multi-Agent Systems (MAS) are characterized by communication, coordination, and collaboration among agents, enabling the collective achievement of complex and demanding objectives with greater effectiveness and efficiency. Although MAS offer significant advantages and have been widely applied across diverse domains, they continue to face critical challenges, particularly in resilient communication, safe cooperation, and adaptability to dynamic and uncertain environments. This talk explores real-world applications of MAS, with a focus on autonomous systems, and examines the key challenges arising in open and dynamic settings. It further presents the analysis and design of novel cooperative control strategies aimed at addressing these challenges. Experimental case studies are used to validate the proposed methodologies and to evaluate their practical performance. Finally, the talk discusses potential technological breakthroughs over the next five years, highlighting MAS as a foundational paradigm in the ongoing advancement of autonomous systems and robotics.

Cyber-Physical Systems: Issues, Design and Challenges

Abstract: Cyber-physical systems (CPS), including smart grids and intelligent transportation systems, are complex systems in which tightly integrated software and hardware components work together to accomplish well-defined tasks. While such integration enables high performance and efficiency, it also significantly increases system vulnerability by creating more opportunities for cyber-attacks, which may lead to serious economic, societal, and human consequences. Consequently, cybersecurity has emerged as a critical challenge in the design and operation of CPS.

This talk examines CPS security from an attacker's perspective. It begins with an overview of CPS fundamentals, key security issues, and representative research on cyber-attacks. The talk then presents our recent work on the design of stealthy hybrid attacks on CPS, demonstrating how coordinated cyber-attacks can be executed to maximize system performance degradation while reducing the likelihood of detection. By exposing these attack mechanisms, the work underscores the need for more effective, efficient, and resilient defense strategies capable of detecting intrusions and ensuring that CPS operate in a secure, reliable, and desired manner.