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

SUJEET KUMAR

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI

JANUARY 2025

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

by

SUJEET KUMAR

Submitted
in fulfilment of the requirements of the degree of Doctor of Philosophy

to the
Department of Electrical Engineering

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JANUARY 2025

CERTIFICATE

This is to certify that the thesis entitled **RESILIENT COOPERATIVE CONTROL OF MULTI-AGENT SYSTEMS AGAINST A CLASS OF CYBER ATTACKS** submitted by **SUJEET KUMAR** to the Indian Institute of Technology Delhi, for the award of the Degree of **Doctor of Philosophy**, is a record of the bona fide research work carried out by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other University or Institute for the award of any degree or diploma to the best of my knowledge.

Prof. Indra Narayan Kar
Department of Electrical Engineering,
Indian Institute of Technology Delhi.
(Supervisor)

ACKNOWLEDGEMENTS

I want to start by expressing my gratitude to Prof. Indra Narayan Kar, who oversaw my thesis, for all of his help, counsel, encouragement, support, tolerance, and enthusiasm throughout my Ph.D. studies at IIT Delhi. Additionally, I would like to express my gratitude to my SRC members, Profs. S. Janardhanan, Shubhendu Bhasin, and Sudipto Mukherjee, for their invaluable assistance and remarks.

Obtaining a Ph.D. entails more than just writing a thesis; it also entails expanding one's knowledge base and learning new topics. I would especially want to thank Abhilash, Kishore, Neetish and Bhabani for our regular discussions on a variety of subjects in this regard. To Bhabani in particular, I am very grateful for his help throughout all the important phases of my doctoral path. Nevertheless, this journey would not have been pleasant without the warm reception of all my lab mates and staff members of the Control and Automation group of IIT Delhi.

On a personal note, I would like to thank my Parents for their constant support and encouragement throughout my roller-coaster career. I want to express my gratitude to my wife for tolerating all my frustrations and being the backbone of my life. Finally, I thank the almighty for the blessings which have made this thesis possible.

SUJEET KUMAR

ABSTRACT

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 summarized as follows:

- 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 agent's state converges to a small neighborhood 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 convergence of the interaction gain to a finite value have been demonstrated.
- A resilient consensus protocol with fixed 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, a fully distributed adaptive law has been proposed to update the heterogeneous interaction gain that relies solely on local information.
- 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.

Keywords: Multi-agent systems, Cooperative Control, False Data Injection Attack, Competitive Interaction, Resilient Control, Synchronization.

सार

बहु-एजेंट प्रणालियाँ, जैसे विद्युत ग्रिड, परिवहन नेटवर्क, जल प्रबंधन प्रणाली, और रोबोटिक समूह, जटिल प्रणालियों की एक व्यापक श्रेणी का प्रतिनिधित्व करती हैं। ये प्रणालियाँ भौतिक प्रक्रियाओं और संचालन एवं नियंत्रण के लिए संचार तंत्र के संयोजन पर आधारित होती हैं। हालांकि, इन प्रणालियों में संचार तंत्र के माध्यम से जानकारी का आदान-प्रदान इन्हें साइबर हमलों के प्रति संवेदनशील बना सकता है। ऐसी स्थिति में, साइबर हमलों के दौरान इन प्रणालियों की कार्यक्षमता बनाए रखना अत्यंत महत्वपूर्ण हो जाता है।

इस शोध प्रबंध में, बहु-एजेंट प्रणालियों के लिए लचीले सहयोगात्मक नियंत्रण की रणनीतियों का अध्ययन किया गया है। इसमें रेखीय और गैर-रेखीय युग्मन से संबंधित प्रणालियाँ शामिल हैं। साथ ही, प्रतिस्पर्धात्मक पारस्परिक क्रिया पर आधारित एक लचीला नियंत्रण ढाँचा प्रस्तुत किया गया है, जिसे आभासी नेटवर्क की संरचना के माध्यम से इन प्रणालियों के साथ जोड़ा गया है। इस शोध में झूठे डेटा सम्मिलन (एफडीआई) हमलों के प्रभाव और उनके समाधान का गहन अध्ययन किया गया। एकल समाकलन एजेंटों पर आधारित प्रणालियों में यह पाया गया कि मूल नोड पर हमला प्रणाली की सहमति प्रक्रिया को अस्थिर कर सकता है, जबकि अन्य नोड पर हमला स्थिति को नाममात्र सहमति से विचलित करता है। इन हमलों का समाधान करने के लिए आत्म-प्रतिक्रिया आधारित सहमति विधि विकसित की गई।

प्रतिस्पर्धात्मक पारस्परिक क्रिया आधारित सहमति विधि में समरूप अनुकूलन योग्य पारस्परिक लाभ का उपयोग किया गया, जो सामान्य परिस्थितियों में सहमति सुनिश्चित करने के साथ-साथ हमले के दौरान प्रणाली की स्थिति को सहमति के करीब बनाए रखने में सक्षम है। हालांकि, उच्च पारस्परिक लाभ के असीमित बढ़ने की समस्या को हल करने के लिए एक मजबूत अनुकूलन विधि विकसित की गई। इसके अतिरिक्त, एक स्थिर विषम पारस्परिक लाभ आधारित सहमति विधि भी प्रस्तुत की गई, जो झूठे डेटा सम्मिलन हमलों के विरुद्ध लचीलापन प्रदान करती है। यह विधि पूरी तरह से वितरित प्रणाली पर आधारित है और केवल स्थानीय जानकारी का उपयोग करती है।

प्रतिस्पर्धात्मक पारस्परिक क्रिया के सिद्धांत को रेखीय बहु-एजेंट प्रणालियों में भी विस्तारित किया गया है। इसमें संचार तंत्र और एजेंट की गतिकी का उपयोग करते हुए झूठे डेटा सम्मिलन हमलों के प्रभाव का विश्लेषण किया गया। लायापुनोव स्थिरता सिद्धांत के माध्यम से इन प्रणालियों की स्थिरता सुनिश्चित की गई और इन हमलों से निपटने के लिए प्रभावी समाधान प्रस्तुत किए गए।

गैर-रेखीय बहु-एजेंट प्रणालियों, जैसे एकल समाकलन और कुरामोटो नेटवर्क, के लिए सहमति और समकालिकता की समस्याओं का भी अध्ययन किया गया। इस अध्ययन में आभासी नेटवर्क आधारित लचीला प्रोटोकॉल विकसित किया गया, जो सीमित समय में सहमति सुनिश्चित करता है। सीमित हमलों की स्थिति में, इस प्रोटोकॉल ने यह गारंटी दी कि त्रुटियाँ सीमित सीमा तक सिमट जाएँगी। कुरामोटो नेटवर्क के संदर्भ में, प्रतिस्पर्धात्मक पारस्परिक क्रिया आधारित समकालिकता विधि ने स्थिरता और लचीलापन सुनिश्चित किया।

यह शोध प्रबंध बहु-एजेंट प्रणालियों पर साइबर हमलों के प्रभाव को कम करने और लचीली सहयोगात्मक नियंत्रण रणनीतियों के विकास के लिए एक प्रभावी दृष्टिकोण प्रस्तुत करता है।

Contents

List of Figures

List of Symbols

s	scalar s
$\mathcal{D}$	set $\mathbb{D}$
$\mathbb{R}$	Set of real numbers
$\mathbb{R}^n$	n-dimensional Euclidean space
$\mathbb{R}^{m \times n}$	space of $m \times n$ real matrices
$\exists$	there exists
$\forall$	for all
$\otimes$	kronecker product
$\lambda_{\min}(L)$	minimum eigenvalue of the matrix L
$\lambda_{\max}(L)$	maximum eigenvalue of the matrix L
$\parallel \mathbf{s} \parallel$	Euclidean norm of the vector $\mathbf{s}$
$\parallel \mathbf{s} \parallel_p$	p - norm of the vector $\mathbf{s}$
$\mathbf{I}$	Identity matrix with dimension $N \times N$

List of Abbreviations

MAS	Multi-agent System
FDI	False Data Injection
ARE	Algebraic Riccati Equation
CPS	Cyber-physical Systems
LSS	Large Scale Systems
UUB	Uniformly Ultimately Bounded