Title of tutorial/workshop

Cyber Threats in Distributed Model Predictive Control and Distributed Estimation

Outline of the tutorial/workshop (topic and description)

Nowadays, advanced control and estimation techniques for large-scale systems consider the management of systems from the point of view of the improvement of key aspects such as modularity, computational burden, complexity, robustness, among others. The need for distributed model predictive control and distributed estimation comes from the coupling between the different entities that compose the overall system. The local controllers exchange information to coordinate their actions to avoid undesired effects derived from the mutual interaction. However, these schemes rely on assumptions that may not hold in real applications, which can cause a non-conforming behavior of the system and can be maliciously exploited, e.g., adequate information exchange, adequate implementation of local actions, and adequate sensing of local measurements.

Each violation of a controller or estimator to respect these assumptions leads to "non-conforming" behavior, hence representing a source of vulnerability for these schemes. Drivers for this behavior could be unintentional (e.g., due to disturbances/failures) or intentional (e.g., with a criminal or self-interest driver). In the former case, fault detection and fault-tolerant control come into play. These set of techniques provide control and estimation systems with the capability of continuing operating properly in the event of a failure in some of its components. In the latter case, the defense and protection of information systems from malicious attackers is provided by cyber security methods.

A novel generation of methods that take into account these concerns has to be developed and this workshop offers key insights regarding questions such as:

- What types of non-conform controllers/estimators can be defined?
- What is the impact on performance of different types of non-conform controllers within particular DMPC schemes?
- How could a non-conform control strategy be designed to maximize mal-intend for a particular DMPC scheme?
- How can DMPC schemes be designed in order to be able to handle certain types / levels of non-conformity?
- How can a non-conform controller/estimator be detected by other entities in the network?
- How can the above questions be addressed when considering multiple non-conform controllers/estimators?

Duration and sessions

14:00 – 14:30
Introduction: Cyber threats and Distributed MPC Commonalities
R. R. Negenborn
Transport Engineering & Logistics of Department Maritime & Transport Technology, Delft University of Technology
Abstract: The workshop starts with a talk introducing the basic concepts behind DMPC and the common elements that can be defined regarding the potential attacks that can be performed to exploit the vulnerabilities of these schemes.

14:30-15:15
Rationale for deception and defense mechanisms in distributed model predictive control
J. M. Maestre
Department of Systems and Automation Engineering
University of Seville
In this session, we present different games that allow the participants in the session to take the control of a subsystem of a larger system and experience themselves the incentives for deceiving other players. Game theoretical insights are also provided. Also, an analysis of the vulnerability of a distributed model predictive control (DMPC) scheme in the context of cyber-security is presented. Different types of the so-called insider attacks are considered. Then, two defense mechanisms to protect or, at least, relieve the consequences of the attack in a typical DMPC negotiation procedure are introduced. A realistic case study based on a local energy grid of households is provided to illustrate both the consequences of the attacks and the defense mechanisms.

15:15-15:45
Coffee Break

15:45-16:30
Safety issues in distributed predictive control: a fault tolerant control viewpoint
C. Ocampo-Martinez
Automatic Control Department
Technical University of Catalunya
This talk explores the most recent approaches proposed for treating topics such as faults and annoying behavioral modes in the dynamic evolution of closed-loop control of large-scale critical infrastructure systems. Related topics such as distributed fault diagnosis and isolation are also discussed and related to the considered distributed predictive control framework.

16:30-17:15
Cyber security and attack detections for power systems
Hideaki Ishii
Tokyo Institute of Technology

Abstract: Cyber security of control systems is of critical importance in view of the growing roles that communication networks play in such systems. In this talk, we provide an overview on security issues in power systems and motivate system theoretic approaches for detection of cyber attacks. The class of attacks considered is data manipulation in the measurement signals transmitted over networks. We first introduce the problem of static state estimation at the transmission grid level. In particular, we study the scenario of malicious and coordinated attacks on the data of grid topology and/or transmission line parameters. We approach this problem based on the robust estimation technique of least trimmed squares (LTS), which is capable of finding outliers in the data by performing least squares with a reduced number of measurement data.

17:15 – 17:30
Summary and discussion
J. M. Maestre
Department of Systems and Automation Engineering
University of Seville

Description of the intended audience and the expected learning outcomes

The intended audience of this workshop consists of researchers, (technically-oriented) control practitioners, MSc and PhD candidates.

Desired prerequisite knowledge of the audience

A basic knowledge of model predictive control is enough for following this workshop.

The tutorial speakers and their biographies

J. M. Maestre received his Ph.D. degree in automation and robotics in 2010 from the University of Seville, where he works as associate professor in the Department of Systems and Automation Engineering. His main research interests are the control of distributed systems and the integration of service robots in the smart home. He has authored and coauthored more than one hundred conference and journal papers regarding these topics. He is also editor of the books "Service robotics within the Digital Home: Applications and Future Prospects" (Springer, 2011), "Distributed Model Predictive Control Made Easy" (Springer, 2014), and "Domótica para Ingenieros" (Paraninfo, 2015). Finally, he is one of the founders of the technological firms Idener, Alacarta Tecnologías Integradas, and Eskesso.

Rudy Negenborn is associate professor in automatic control & coordination of transport technology at the Section Transport Engineering & Logistics of Department Maritime & Transport Technology, Delft University of Technology. He obtained the MSc degree in computer science / intelligent systems in 1998 at Utrecht University, and received the PhD degree in distributed control for networked systems from Delft University of Technology, the Netherlands, in 2007.

Dr. Negenborn's research interests include multi-agent systems, distributed control, model predictive control, simulation of large-scale transport systems, and applications in (waterborne) networked transport systems. Current research lines he is leading are developing control theoretical approaches for efficient and sustainable operation of future container terminals, inter terminal transport systems in port areas, and intermodal / synchromodal transport networks at national and European scale.
He has over 100 peer reviewed academic publications. He is on the editorial board of the series on "Intelligent Systems, Control and Automation: Science and Engingeering", and is on the international programming council of the International Journal on Marine Navigation and Safety of Sea Transportation. Dr. Negenborn was general chair of the 6th International Conference on Computational Logistics, has acted as member of the organizing committee of several other international conferences (including IEEE control conferences and maritime systems & logistics conferences) and was guest editor of a special journal issue on control of water systems. In addition, he is editor of the books "Intelligent Infrastructures", "Distributed Model Predictive Control Made Easy", and "Transport of Water versus Transport over Water", and guest editor of the Transportation Research Part E special issue on "Coordination for Real-Time Transport Logistics".

C. Ocampo was born in Manizales (Colombia) on August 30, 1978. I received my Electronics Engineering degree and my MSc. degree in Industrial Automation from the National University of Colombia, Campus Manizales in 2001 and 2003, respectively. In 2007, I received the Ph.D. degree in Control Engineering from the Technical University of Catalonia - BarcelonaTech (Barcelona, Spain). In 2007-2008, he held a postdoctoral position at the ARC Centre of Complex Dynamic Systems and Control (University of Newcastle, Australia), and, afterwards at the Spanish National Research Council (CSIC), Institut de Robòtica i Informàtica Industrial, CSIC-UPC (Barcelona) as a Juan de la Cierva Research Fellow between 2008 and 2011. Since 2011, he is with the Technical University of Catalunya, Automatic Control Department (ESAII), currently as Associate Professor in automatic control and model predictive control. Since 2014, I am also Deputy Director of the Institut de Robòtica i Informàtica Industrial, CSIC-UPC, a Joint Research Center of UPC and CSIC. His main research interests include constrained model predictive control, large-scale systems management (partitioning and non-centralized control), and industrial applications (mainly related to the key scopes of water and energy).

H. Ishii received the B.Eng. degree in engineering systems from the University of Tsukuba, Tsukuba, Japan, in 1996, the M.Eng. degree in applied systems science from Kyoto University, Kyoto, Japan, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2002. Currently, he is an Associate Professor in the Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan. His research interests are in the general area of control theory with specific emphasis on large-scale networked control systems.