Automatica 71 (2016) 1–9

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Resilient stabilization of Multi-Hop Control Networks subject to malicious attacks[☆]

Alessandro D'Innocenzo, Francesco Smarra, Maria Domenica Di Benedetto

The Center of Excellence DEWS, Department of Information Engineering, Computer Science and Mathematics, University of L'Aquila, Italy

ARTICLE INFO

Article history:
Received 27 May 2015
Received in revised form
1 February 2016
Accepted 1 April 2016
Available online 31 May 2016

Keywords:
Networked control systems
Cyber-Physical systems
Security
Fault-tolerant control
Fault detection and isolation

ABSTRACT

A Multi-hop Control Network (MCN) consists of a dynamical system where the communication between sensors, actuators and computational units is supported by a (wireless) multi-hop communication network and data flow is performed using scheduling and routing of sensing and actuation data. Secure stabilization of an MCN is a challenging open problem tightly related to Cyber-Physical Systems security. In this paper we address the co-design problem of controller and communication protocol of an MCN where the plant is a MIMO LTI system and the communication nodes are subject to failures and malicious attacks. We first characterize by means of necessary and sufficient conditions the set of network configurations that invalidate controllability and observability of the plant. Then, we investigate the problem of detecting and isolating failures and malicious attacks to communication nodes. We provide necessary and sufficient conditions for the solvability of this problem.

1. Introduction

Networked control systems (NCS) are distributed control systems where the communication between sensors, actuators, and computational units is supported by a possibly wireless communication network. The use of wireless NCS in industrial automation results in flexible architectures and generally reduces installation, debugging, diagnostic and maintenance costs with respect to wired networks (see e.g. Akyildiz & Kasimoglu, 2004; Han, Nixon, Chen, Mok, & Muston, 2016 and references therein). However modeling, analysis and design of secure wireless NCS are challenging open research problems since they require to take into account the joint dynamics of physical systems, communication protocols and network infrastructures. Recently, a huge effort has been made in scientific research on control of NCSs, see e.g. Aström and Wittenmark (1997), Gupta, Dana, Hespanha, Murray, and Hassibi (2009), Heemels, Teel, van de Wouw, and Nešić (2010), Hespanha, Naghshtabrizi, and Xu (2007), Pajic, Mangharam, Pappas, and Sundaram (2013) and Tabbara, Nešić, and Teel (2007), and on secure and fault tolerant control of Cyber-Physical Systems, see e.g. Anon (2015) and Gupta and Chow (2010) and the references therein. In general, the literature on NCSs addresses non-idealities (such as quantization errors, packets dropouts, variable sampling and delay and communication constraints) as aggregated network performance variables or disturbances, neglecting the dynamics introduced by the communication protocols. To the best of our knowledge the first formal model of a NCS that models the joint dynamics of a dynamical control system and of the MAC (scheduling) and Network (routing) layers of a time-triggered communication protocol over a shared multi-hop wireless network has been presented in Alur, D'Innocenzo, Johansson, Pappas, and Weiss (2011). This framework also models wireless industrial control protocols such as WirelessHART and ISA-100: note that many on-market engineering products are based on these protocols, see e.g. the Siemens SITRANS AW200, SITRANS AW210 and IE/WSN-PA Link.

As illustrated in Fig. 1 we define a Multi-hop Control Network (MCN) $\mathcal{M}$ as a continuous-time MIMO LTI plant $\mathcal{P}$ interconnected to a controller C via two multi-hop communication networks $\mathcal{R}$ (the controllability network) and $\mathcal{O}$ (the observability network) that implement a time-triggered communication protocol. $\mathcal{R}$ and $\mathcal{O}$ consist of communication nodes whose radio connectivity is modeled respectively by a controllability and an observability radio connectivity graph. We model failures and malicious attacks

[☆] The research leading to these results has received funding from the Italian Government under Cipe resolution n.135 (Dec. 21, 2012), project *INnovating City Planning through Information and Communication Technologies* (INCIPICT). The material in this paper was partially presented at the 3rd IFAC Workshop on Estimation and Control of Networked Systems (NecSys'12), September 14–15, 2012, Santa Barbara, CA, USA and at the 14th European Control Conference, July 15–17, 2015, Linz, Austria. This paper was recommended for publication in revised form by Associate Editor Hideaki Ishii under the direction of Editor Christos G. Cassandras.

E-mail addresses: alessandro.dinnocenzo@univaq.it, adinnoce@hotmail.com (A. D'Innocenzo), francesco.smarra@univaq.it (F. Smarra), mariadomenica.dibenedetto@univaq.it (M.D. Di Benedetto).

http://dx.doi.org/10.1016/j.automatica.2016.04.016
0005-1098/© 2016 Elsevier Ltd. All rights reserved.

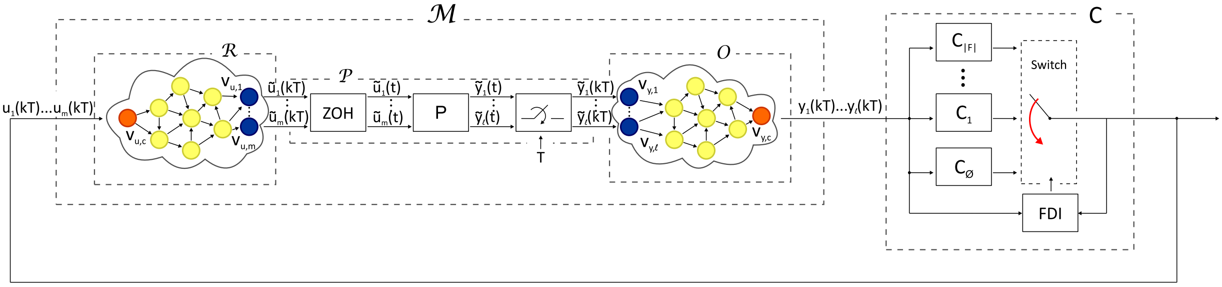

Fig. 1. Control scheme of an MCN subject to node failures and malicious attacks.

by means of arbitrary signals injected in a set of communication nodes, and we will call such set of nodes *malicious cluster*: this general framework allows modeling node failures (a node stops sending data or sends random data) as well as malicious attacks (an arbitrary signal is injected that overrides/sums to the original data due to e.g. stealth, false-data injection and replay attacks). We denote by F the set of all possible malicious clusters, i.e. the set of all subsets of nodes. We propose here a control architecture resilient to failures and malicious attacks. More precisely, we address and solve the problem of designing a set of controllers and the communication protocol parameters so that it is possible, only using sensing and actuation data (i.e. without adding further data communication among nodes for fault detection), to detect and isolate run-time (i.e. as the process is executing) the malicious cluster of the controllability and observability networks (we recall that *detecting* means perceiving that there is at least one faulty/attacked node, while *isolating* means distinguishing which are the faulty/attacked nodes): this allows segregating the malicious cluster by reconfiguring the scheduling of only its neighbors (which requires much less communication cost and time w.r.t. reconfiguring all nodes) and to switch the controller in order to stabilize the re-configured system. We propose a solution to the above problem by solving the following two sub-problems.

Problem 1. Assume that the malicious cluster $f \in F$ is *known*, and let $\mathcal{M}_f$ be the corresponding MCN dynamics due to a scheduling re-configuration that segregates the faulty/attacked nodes: design scheduling and routing so that, for any malicious cluster $f \in F$, the MCN $\mathcal{M}_f$ is controllable and observable.

If Problem 1 can be solved, then the computation of a stabilizing controller C_f can be guaranteed for any malicious cluster using standard techniques.

Problem 2. Assume that the malicious cluster is *unknown*: use the MCN input and output signals to detect and isolate the malicious cluster and find conditions under which this is possible.

Although Fig. 1 shows a switching structure in the controller, the above problem separation deliberately neglects the switching dynamics of the closed loop system since it is based on the assumption that failures and malicious attacks occur with a time scale much greater than the sampling time. Namely we do not consider *transient* failures (e.g. packet losses) (Weiss, D'Innocenzo, Alur, Johansson, & Pappas, 2010): indeed we believe that it makes sense to separately address the case when failures/attacks are just long-term (this paper) and the case when packet losses occur (see some preliminary results in Smarra, D'Innocenzo, and Di Benedetto (2012) and Smarra, D'Innocenzo, and Di Benedetto (2015)). The final goal of our research is to jointly take into account failures/attacks and packet losses, and the results in this paper directly translate to necessary conditions for probabilistic controllability/observability/fault detection and isolation (FDI) with packet losses. The results of this paper can be used in practice since there exist many real engineering applications (e.g. building automation (Di Benedetto, D'Innocenzo, & Smarra, 2014) and mining industry (D'Innocenzo et al., 2009)) where the plant dynamics are quite slow, so that packet losses are practically irrelevant, and the variables that most affect the performance and/or stabilizability are indeed related to long-term failures and to the dynamics of the higher levels of the ISO/OSI protocol stack, for example scheduling and routing, which are the aspects we specifically take into account in this paper.

Paper contribution: In D'Innocenzo, Di Benedetto, and Serra (2013) we introduced MCNs for SISO plants: such modeling framework, however, does not allow the representation of multiple plants and controllers sharing actuation and sensing data over one or more networks. For this reason, in Section 2 we extend the MCN modeling framework to take into account the presence of multiple components of the input and output vector of the plant. Solving Problems 1 and 2 in the MIMO setting requires solving substantially different technical results as well as taking into account new computational complexity issues due to the number of input and output signals. In particular, in Section 3 we provide necessary and sufficient conditions such that Problem 1 is solvable. Such conditions can be verified with combinatorial complexity with respect to the number of input and output signals, therefore we exploit the particular mathematical structure of our model to provide an algorithm solving Problem 1 characterized by linear complexity. In Section 4 we solve Problem 2. In D'Innocenzo et al. (2013) necessary and sufficient conditions on the network configuration for solving Problem 2 in the SISO case turned out to be true only for trivial network topologies. We derive here necessary and sufficient conditions for the MIMO case: the interesting outcome of such extension is that in the MIMO setting, thanks to the redundancy provided by multiple inputs and outputs, the restrictions on the network topology are much weaker, making such conditions useful in practice.

Stabilization and intrusion detection were addressed in Pajic, Sundaram, Pappas, and Mangharam (2011a) and Pajic, Sundaram, Pappas, and Mangharam (2011b), but for a different model of an MCN. To the best of our knowledge, our work is pioneering in addressing resilient *co-design* of controller and network configuration for a MIMO MCN that implements time-triggered communication protocols and is subject to node failures and malicious attacks. In particular we state stabilizability and FDI conditions for both *the plant dynamics* and *the communication protocol*, and we provide a methodology to explicitly design the network topology, scheduling and routing in order to satisfy such conditions.

Notation: We will denote by $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{R}_0^+$ respectively the sets of natural, real, positive real and non-negative real numbers. Given $n \in \mathbb{N}$, we denote by $\mathbf{n}$ the set $\mathbf{n} \doteq \{1, 2, \ldots, n\}$. Given a finite set F and a subset $H \subseteq F$, we define $|H|$ and $|F|$ as their cardinalities, $F \setminus H$ as the difference set and 2^F as the power set. Given a matrix A, we denote by $|A|$ its determinant. We denote