Fifty-Fifth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 3-6, 2017

The Securable Subspace of a Linear Stochastic System with Malicious Sensors and Actuators

Bharadwaj Satchidanandan and P. R. Kumar, *Fellow, IEEE*

***Abstract*— Analogous to the notions of controllable and unobservable subspaces, the recently introduced notions of securable and unsecurable subspaces for linear dynamical systems have important operational meaning in the context of secure control of deterministic linear dynamical systems. Specifically, given a multiple input, multiple output linear dynamical system, an arbitrary subset of whose sensors and actuators are malicious, the unsecurable subspace has the operational meaning as the set of states that the malicious actuators can steer the system to, without detection of the visit to such a state by the honest sensors in the system. In this paper, we examine these subspaces from the standpoint of a fully-observed stochastic linear dynamical system, and establish operational meanings for them in this context.**

I. Introduction

The study of linear dynamical systems in terms of certain distinguished subspaces of its state space, such as the controllable, unobservable, controlled invariant, and conditioned invariant subspaces, has proven to be beneficial in tackling many analysis and synthesis problems arising in control theory. Known as the geometric approach to control, or simply geometric control, it derives its efficacy, in part, from the fact that it facilitates an intuitive understanding of the problem at hand. The application of this approach in solving standard control problems such as regulation, tracking, servo, and noninteracting control are described in [1].

Currently, the problem of securing industrial control systems and societal-scale cyberphysical systems is of great interest. It is in this context that recently, the notions of securable and unsecurable subspaces of a linear dynamical system have been introduced [2]. Specifically, consider a multiple-input, multiple-output stochastic linear dynamical system, an arbitrary subset of whose sensors and actuators may be "malicious." A malicious sensor may not report the measurements that it observes truthfully, and a malicious actuator may not adhere to the specified control law. We use the term "node" to mean a sensor or an actuator. We assume that the honest nodes in the system do not know which other nodes in the system are honest or malicious, but the malicious nodes know the identity of all other malicious nodes in the system. In this setting, the unsecurable subspace of a linear dynamical system is defined as a certain controlled invariant subspace of the state space, and has been shown to have, in deterministic systems, the operational meaning as the set of states that the malicious nodes can steer the system to, without the honest nodes in the system ever being able to detect, based on their measurements, that the system had visited that state or that there was any malicious activity in the system. This interpretation, however, does not extend to systems that are stochastic in nature.

In this paper, we view the securable and unsecurable subspaces from the standpoint of stochastic linear dynamical systems, and establish important operational meanings for them in the stochastic context. Of the many potential applications that the results developed in this paper may have, perhaps the most significant is in synthesizing control systems that are provably secure by design.

The rest of the paper is organized as follows. Section II gives a brief account of the related work on this topic. Section III formulates the problem, and defines the notions of securable and unsecurable subspaces of a linear dynamical system. Some of the content in this section is also reported in [2]. Section IV is devoted to establishing certain key geometric properties of the securable subspace. These properties are exploited in Section V to establish an operational meaning for the securable and the unsecurable subspace in the context of fully-observed stochastic systems. Section VI concludes the paper.

Notation: Given a vector $\mathbf{x}$ and a subspace W, x_i denotes the i^{th} entry of $\mathbf{x}$ and $\mathbf{x}_W$ denotes the projection of $\mathbf{x}$ on the subspace W. Given a matrix A, $A_{i,\times}$ denotes the i^{th} row of A, and $A_{\times,i}$ denotes its i^{th} column. Given a vector $\mathbf{x}$, we denote by $\mathbf{x}^{TT}$ the expression $\mathbf{x}^T\mathbf{x}$, and by $\mathbf{x}_W^{TT}$, the expression $\mathbf{x}_W^T\mathbf{x}_W$.

II. Related Work

Security of control systems has been a topic of active research for over a decade now. Some of the early works focused on defining the problem of secure control. Specifically, [9] introduces the notion of survivability, defined as the ability of a cyber-physical system to provide graceful degradation of operational goals when under attack. The theory of secure control can benefit from having mathematical models for different kinds of attacks, and [10] presents such models for two specific attacks on a control system, viz., the Denial of Service (DoS) attack and the deception attack.

Many techniques have been proposed in the literature to defend a control system against adversarial nodes. A well-known attack on control systems is the replay attack, which was employed in Stuxnet [20]. In the replay attack, a subverted sensor records, for some duration during normal operating conditions, the measurements that it observes. It then replays

This material is based upon work partially supported by NSF under Contract Nos. CNS-1646449, CCF-1619085 and Science & Technology Center Grant CCF-0939370, the U.S. Army Research Office under Contract No. W911NF-15-1-0279, and NPRP grant NPRP 8-1531-2-651 from the Qatar National Research Fund, a member of Qatar Foundation.