2018 IEEE Conference on Decision and Control (CDC)
Miami Beach, FL, USA, Dec. 17-19, 2018

# On the Operational Significance of the Securable Subspace for Partially Observed Linear Stochastic Systems

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

***Abstract*—We address the problem of security for general partially observed linear stochastic systems, where some of the sensors and actuators may be malicious. We consider multiple-input-multiple-output linear stochastic systems that are under attack, where an arbitrary subset of its sensors and actuators are "malicious." A malicious sensor need not report its measurements truthfully, and a malicious actuator need not apply inputs in accordance with the prescribed control policy. For any such system, we show that there exists a decomposition of the state space into two orthogonal subspaces, called the securable and the unsecurable subspaces, and design a test that can be used by the honest sensors and actuators, such that if the malicious activity is to remain undetected by this test, then the covariance of the projection of the state estimation error of the honest nodes on the securable subspace remains at its designed value regardless of what attack strategy the malicious sensors and actuators choose to employ. This test therefore guarantees that the malicious nodes can degrade the state estimation performance only along the unsecurable subspace of the linear dynamical system.**

***Index Terms*—Cyber-Physical Systems, Secure Control, Securable subspace, Unsecurable subspace.**

## I. Introduction

The past decade has witnessed an immense surge in interest in the problem of security of cyber-physical systems (CPS). This is owing, at least in part, to the fact that there have been several instances of attacks on industrial control systems and cyber-physical systems in the recent past. Archetypal examples include the Stuxnet attack [1], the Maroochy-Shire incident [2], the attack on Davis-Besse nuclear power plant [3], and others such as a demonstration of remote hijacking of an automobile [4]. The increasing frequency of such attacks over the years has reinforced the concern of security of cyber-physical systems which has emerged as one of the primary challenges that needs to be addressed in order to enable their large-scale proliferation.

Cyber-physical systems, especially those arising in safety-critical applications, warrant deployments that are secure by design. This calls for the development of a suitable theory of security for control systems. The notions of controllable and unobservable subspaces introduced by Kalman [5], and the theory that has been developed subsequently, have taken center stage in the modern study of linear systems. However, this theory was developed in a "benign" age, where there were no adversarial nodes (sensors or actuators) in the system, and all disturbances affecting the system were stochastic in nature (with the exception of $H_\infty$ methods). However, as the recent attacks have shown, these assumptions may no longer be valid in a modern era where the sensors and actuators in a system may not be trustworthy, i.e., they may be "malicious." A malicious sensor need not report the measurements that it observes in a truthful fashion, and a malicious actuator may not apply inputs in accordance with the designated control policy. In such a setting, even though the overall system may be observable, the honest sensors and actuators in the system may not be able to accurately deduce the initial state of the system in the context of a deterministic linear dynamical system, and in the context of a stochastic system, may not be able to deduce the "optimal" state estimate at any given time - a quantity that that they could have deduced had all sensors and actuators in the system been honest. This is a result of the malicious actuators applying erroneous control inputs that are unknown to the honest nodes, and the malicious sensors reporting incorrect measurements.

It is against this backdrop that we introduced, analogous to the classical notions of controllable and unobservable subspaces, the notions of *securable* and *unsecurable* subspaces of a linear dynamical system [6], [7], which have important operational meanings in the context of secure control. Specifically, we showed in [6] that given an arbitrary combination of malicious sensors and actuators, the unsecurable subspace of a deterministic linear dynamical system has the operational meaning as the set of states that the system could actually be ever in (due to actions of the malicious actuators), without the honest sensors ever detecting that the system visited that state, or that there is any malicious activity in the system. These subspaces which were introduced in the context of deterministic systems also have important operational meanings in the context of stochastic systems. Specifically, we showed in [7] that in the context of a perfectly observed stochastic system, the securable subspace has the operational meaning as the subspace of the state space along which the projection of the state estimation error is guaranteed to be of zero power.

In this paper, we generalize the above results and establish the operational meaning of the securable subspace in the context of general multiple-input-multiple-output partially observed stochastic linear dynamical systems with both Gaussian process and observation noise, which class constitutes one of the most general models used in modern linear system theory. Specifically, we show that for these

This material is based upon work partially supported by NSF under Contract Nos. CNS-1646449, CCF-1619085 and Science & Technology Center Grant CCF-0939370, Office of Naval Research under Contract N00014-18-1-2048, the U.S. Army Research Office under Contract No. W911NF-15-1-0279, and NPRP grant NPRP 8-1531-2-651 from the Qatar