LQG Reference Tracking with Safety and Reachability Guarantees under Unknown False Data Injection Attacks

Zhouchi Li, *Student Member, IEEE,* Luyao Niu, *Student Member, IEEE,* and Andrew Clark, *Member, IEEE*

Abstract—We investigate a linear quadratic Gaussian (LQG) tracking problem with safety and reachability constraints in the presence of an adversary who mounts an FDI attack on an unknown set of sensors. For each possible set of compromised sensors, we maintain a state estimator disregarding the sensors in that set, and calculate the optimal LQG control input at each time based on this estimate. We propose a control policy which constrains the control input to lie within a fixed distance of the optimal control input corresponding to each state estimate. The control input is obtained at each time step by solving a quadratically constrained quadratic program (QCQP). We prove that our policy can achieve a desired probability of safety and reachability using the barrier certificate method. Our control policy is evaluated via a numerical case study.

Index Terms—Barrier certificate, false data injection attack, LQG tracking, safety and reachability constraints.

I. INTRODUCTION

Safety [1], [2] and reachability [3] are critical properties of control systems. The safety constraint requires that the system state should remain in a safe region. The reachability constraint requires that the system should reach a set of goal states within a desired time interval. Safety and reachability are fundamental requirements for critical applications including healthcare, transportation, and power systems.

Control systems have been shown to be vulnerable to malicious attacks. Various attacks targeting at actuators and measurement channels have been reported [4], [5]. Particularly, false data injection (FDI) attacks, which compromise the sensor measurements, need special concerns because they are easily mounted [6], stealthy if the adversary knows the full information of the system [7], [8], and can cause serious financial loss or even personal damage [9]. One example is GPS spoofing against unmanned aerial vehicles and autonomous cars, which results in deviation from the desired trajectory, as well as violations of safety and reachability [10], [11]. The threat of such attacks has led to significant research interest in modeling [12]–[14], mitigating [15], and detecting FDI [8], [16]. Resilient state estimation is also investigated in [17]–[19]. The authors of [20] aim at computing a safe operational windows to guarantee the safety property of a deterministic linear system with complete information. [15] assumes that the correct sensor measurements of system state are always

available to the controller even when the system is under attack. An emergency controller is assumed in [21] which can be invoked when an alert on attacks is raised. In [22], a single-input single-output system under false data injection attack targeting at actuator is studied.

At present, less attention has been paid to the design of closed-loop controllers with safety and reachability guarantees under FDI attacks. In the preliminary conference version of this work [23], we investigated the linear quadratic Gaussian (LQG) reference tracking problem, in which there was only one possible set of compromised sensors. In this paper, we generalize the problem so that multiple possible compromised sensor sets are given, each of which corresponds to a different attack scenario. The goal of our approach is to develop a control policy that ensures safety and reachability under each attack scenario while also minimizing the LQG tracking cost when no adversary is present.

Under our approach, for each attack pattern, the system maintains a state estimate that ignores the sensor measurements corresponding to that attack pattern. The control action chosen at each time step is then constrained to be within a fixed distance of the optimal control action corresponding to each state estimate. The key challenge is that, when there are multiple possible attack scenarios, the state estimates may be inconsistent from each other. To overcome this difficulty, we propose a scheme for detecting and resolving inconsistencies between state estimates. The selected state estimates are utilized to construct constraints that guarantee safety and reachability with desired probability.

The contribution of this paper is two-fold. First, a barrier certificate based policy is proposed to solve the LQG tracking problem with safety and reachability constraints under FDI attack that targets at an unknown set of sensors. We solve a quadratically constrained quadratic program (QCQP) to calculate the control policy at each time step. We develop a procedure to resolve the potential infeasibility of the QCQP. We prove that the controller obtained using our approach guarantees safety and reachability with desired probabilities. We show the feasibility and performance guarantees of the controller when the adversary is absent. Second, we derive a closed-form solution of the controller for a special case of the problem where there is a unique attack pattern. The derived controller not only guarantees safety and reachability, but also achieves better approximation with respect to the expected cost, compared with our preliminary work [23].

The note is organized as follows. Section II states the system

and adversary models and the problem formulation. Section III and IV propose the control policy for the multiple- and single-adversary scenarios, respectively. Section V contains simulation results. Section VI concludes the paper.

II. System Model and Problem Statement

In this section, we first present the system and adversary models. We then give the problem formulation.

A. System and Adversary Models

We consider a linear time invariant (LTI) system with state $\mathbf{x}(t) \in \mathbb{R}^n$, input $\mathbf{u}(t) \in \mathbb{R}^m$, and observations $\mathbf{y}(t) = [y_1(t), \ldots, y_p(t)]^T \in \mathbb{R}^p$. The system dynamics are

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t) + \mathbf{w}(t) \tag{1a}$$

$$\mathbf{y}(t) = C\mathbf{x}(t) + \mathbf{v}(t) + \mathbf{a}(t) \tag{1b}$$

In Equation (1), $\mathbf{w}(t)$ and $\mathbf{v}(t)$ are independent Gaussian processes with means identically zero and autocorrelation functions $R_{\mathbf{w}}(\tau) = \Sigma_{\mathbf{w}}\delta(\tau)$ and $R_{\mathbf{v}}(\tau) = \Sigma_{\mathbf{v}}\delta(\tau)$, respectively, where $\delta(\tau)$ denotes the Dirac delta function. We use $\Sigma_{\mathbf{w}}$ and $\Sigma_{\mathbf{v}}$ to denote the covariance matrices of $\mathbf{w}(t)$ and $\mathbf{v}(t)$ at each time t. We assume $(A, N_{\mathbf{w}})$ is stabilizable, where $N_{\mathbf{w}}N_{\mathbf{w}}^T = \Sigma_{\mathbf{w}}$. The initial state $\mathbf{x}(0)$ is equal to $\mathbf{x}_0$. Denote $\Im(t)$ as the information available to the controller at time t. We have $\Im(t) = \{y(t')|t' \leq t\} \cup \{u(t')|t' < t\}$ and $\Im(0) = y(0)$. The control policy of the system is defined as a function $\mu(\Im(t)) \in \mathbb{R}^m$.

In Equation (1b), $\mathbf{a}(t)$ is the attack signal injected by the adversary. There exists a collection of attack patterns $\{\mathcal{A}_i : i \in \{1, \ldots, q\}\}$. Here $\mathcal{A}_i \subseteq \{1, \ldots, p\}$ is a subset of sensors, in which it is possible that $\mathcal{A}_i \bigcap \mathcal{A}_j \neq \emptyset$. The adversary chooses one $\mathcal{A}^*$ from $\mathcal{A}_1, \ldots, \mathcal{A}_q$. The adversary then chooses $\mathbf{a}(t)$ with arbitrary values such that $support(\mathbf{a}(t)) \subseteq \mathcal{A}^*$ for all time $t \in [0, T]$. The controller knows the possible compromised sets $\mathcal{A}_1, \ldots, \mathcal{A}_q$, but does not know which set $\mathcal{A}^*$ has been chosen by the adversary. At each time t, the adversary knows the control policy $\mu(\Im(t))$, the system state $\mathbf{x}(t')$, the system output $\mathbf{y}(t')$, and the control input $\mathbf{u}(t')$ for all $t' \leq t$. Denote the adversary policy $\nu(t)$ as a function which maps $\{\mathbf{x}(t'), \mathbf{u}(t'), \mathbf{y}(t') : \forall t' \leq t\}$ to $\mathbf{a}(t)$.

Let G and U be the goal states and unsafe states defined as $G = \{\mathbf{x} \in \mathbb{R}^n : g_G(\mathbf{x}) \geq 0\}$, and $U = \{\mathbf{x} \in \mathbb{R}^n : g_U(\mathbf{x}) \geq 0\}$, respectively. Define the safety constraint as $\mathbf{x}(t) \notin U \ \forall t \in [0, T]$, which prevents the system state from reaching U for all time $t \in [0, T]$. We define the reachability constraint as $\mathbf{x}(T) \in G$, which requires the system state to be in G at final time T. A reference trajectory $\{\mathbf{r}(t) \in \mathbb{R}^n : t \in [0, T]\}$ is given, which satisfies $\mathbf{r}(t) \notin U$ and $\mathbf{r}(T) \in G$.

B. Problem Formulation

The problem studied in this work is

$$\min_{\mu} \mathbf{E}[(\mathbf{x}(T) - \mathbf{r}(T))^T F(\mathbf{x}(T) - \mathbf{r}(T)) + \int_0^T (\mathbf{u}(t)^T R\mathbf{u}(t)$$
$$+ (\mathbf{x}(t) - \mathbf{r}(t))^T Q(\mathbf{x}(t) - \mathbf{r}(t))) \, dt | \mu, \beta = 1] \tag{2}$$
$$\text{s.t. } \max_{\nu}\{Pr(\cup_{t \in [0,T]}\{\mathbf{x}(t) \in U\}|\mu, \nu)\} \leq \epsilon_s$$
$$\min_{\nu}\{Pr(\mathbf{x}(T) \in G|\mu, \nu)\} \geq 1 - \epsilon_r$$

The objective function implies that the goal of the system is to minimize the expected cost when there is no adversary ($\beta = 1$), while guaranteeing safety and reachability when the system is under attack ($\beta = 0$). The first constraint implies that the probability of violating the safety constraint in the worst case over all the adversary policies should be lower than the bound ϵ_s. The second constraint means that the probability of achieving the reachability constraint should be greater than the threshold $1 - \epsilon_r$ under any adversary's policy.

III. Control Strategy for Multiple-adversary Scenario

In this section, we present the solution approach for multi-adversary scenario. Our solution approach is based on the observation that the adversary can only bias the system state by injecting false measurements to the sensors to induce erroneous control inputs. Hence, if we can restrict the control inputs to stay within a particular neighborhood of each optimal control signal $\mathbf{u}_{\alpha,i}(t)$ that corresponds to the measurements from $\{1, \ldots, p\} \setminus \mathcal{A}_i$ for each attack pattern $\mathcal{A}_i$, then we can limit the impact from the adversary's attack signal.

A. Control Policy Construction

Let $\mathbf{y}_{\alpha,i}(t)$ be the measurements of sensors in $\{1, \ldots, p\} \setminus \mathcal{A}_i$. Denote $C_{\alpha,i}$ and $\mathbf{v}_{\alpha,i}(t)$ as C and $\mathbf{v}(t)$ with rows indexed by $\{1, \ldots, p\} \setminus \mathcal{A}_i$, so that $\mathbf{y}_{\alpha,i}(t) = C_{\alpha,i}\mathbf{x}(t) + \mathbf{v}_{\alpha,i}(t)$. We assume that all systems $(A, C_{\alpha,i}) \ \forall i \in \{1, \ldots, q\}$ are observable. Let $\Sigma_{\mathbf{v}_{\alpha,i}}$ denote the covariance matrix of $\mathbf{v}_{\alpha,i}$.

The Kalman Filter (KF) estimates $\hat{\mathbf{x}}_{\alpha,i}(t)$ are [24]

$$\dot{\hat{\mathbf{x}}}_{\alpha,i}(t) = A\hat{\mathbf{x}}_{\alpha,i}(t) + B\mathbf{u}_{\alpha,i}(t)$$
$$+ \Theta_{\alpha,i}(t)(\mathbf{y}_{\alpha,i}(t) - C_{\alpha,i}\hat{\mathbf{x}}_{\alpha,i}(t)) \tag{3}$$
$$\Theta_{\alpha,i}(t) = \Phi_{\alpha,i}(t)C_{\alpha,i}^T \Sigma_{\mathbf{v}_{\alpha,i}}^{-1} \tag{4}$$
$$\dot{\Phi}_{\alpha,i}(t) = A\Phi_{\alpha,i}(t) + \Phi_{\alpha,i}(t)A^T + \Sigma_{\mathbf{w}}$$
$$- \Phi_{\alpha,i}(t)C_{\alpha,i}^T \Sigma_{\mathbf{v}_{\alpha,i}}^{-1} C_{\alpha,i}\Phi_{\alpha,i}(t)^T \tag{5}$$

where $\Phi_{\alpha,i}(0)$ and $\hat{\mathbf{x}}_{\alpha,i}(0)$ are given.

From [24], the optimal LQG control based on $\hat{\mathbf{x}}_{\alpha,i}(t)$ is

$$\mathbf{u}_{\alpha,i}(t) = \frac{1}{2}K(t)\hat{\mathbf{x}}_{\alpha,i}(t) - \frac{1}{2}R^{-1}B^T\mathbf{s}(t)$$
$$K(t) = -R^{-1}B^T P(t)$$
$$-\dot{P}(t) = A^T P(t) + P(t)A - \frac{1}{2}P(t)BR^{-1}B^T P(t) + 2Q$$
$$\dot{\mathbf{s}}(t) = (-A^T + \frac{1}{2}P(t)BR^{-1}B^T)\mathbf{s}(t) + 2Q\mathbf{r}(t)$$

where $\mathbf{s}(t)$ and $P(t)$ have boundary conditions $\mathbf{s}(T) = -2F\mathbf{r}(T)$ and $P(T) = 2F$.

Denote $\hat{\mathbf{x}}_{\alpha}^*(t)$ as the KF estimate of $\mathbf{x}(t)$ based on $\mathbf{y}_{\alpha}^*(t)$ of sensors in $\{1, \ldots, p\} \setminus \mathcal{A}^*$. Dynamics of $\hat{\mathbf{x}}_{\alpha}^*(t)$ is analogous to Equations (3)-(5). Similarly, we define $\mathbf{u}_{\alpha}^*(t)$ as the LQG tracking optimal control input based on $\{\mathbf{y}_{\alpha}^*(t') \ t' \leq t\}$.

Define the set of feasible control inputs at time t with respect to attack pattern $\mathcal{A}_i$ as $\mathcal{U}_{\gamma_i}(t) \triangleq \{\mathbf{u}(t) : (\mathbf{u}(t) - \mathbf{u}_{\alpha,i}(t))^T (\mathbf{u}(t) - \mathbf{u}_{\alpha,i}(t)) \leq \gamma_i^2\}$, where $\gamma_i \geq 0$ is a parameter that will be discussed in Section III-B. Define $\mathcal{U}_{\gamma}^*(t) \triangleq \{\mathbf{u}(t) : \|\mathbf{u}(t) - \mathbf{u}_{\alpha}^*(t)\|_2 \leq \gamma^*\}$ and $\mathcal{U}(t) \triangleq$

$\bigcap_{i=1}^{q} \mathcal{U}_{\gamma_i}(t)$. Using this constraint instead of the constraint in (2), the problem becomes

$$\min_{\mathbf{u}(t)} \mathbf{E}[\int_0^T ((\mathbf{x}(t) - \mathbf{r}(t))^T Q(\mathbf{x}(t) - \mathbf{r}(t)) + \mathbf{u}(t)^T R\mathbf{u}(t))dt$$
$$+ (\mathbf{x}(T) - \mathbf{r}(T))^T F(\mathbf{x}(T) - \mathbf{r}(T))] \quad (6a)$$
$$\text{s.t. } \mathbf{u}(t) \in \mathcal{U}(t), \forall t \in [0, T]. \quad (6b)$$

The solution of (6) can be computed by solving a stochastic Hamilton-Jacobi-Bellman (HJB) equation [25]

$$0 = \min_{\mathbf{u}(t) \in \mathcal{U}(t)} \{ (\mathbf{x}(t) - \mathbf{r}(t))^T Q(\mathbf{x}(t) - \mathbf{r}(t))$$
$$+ V_{\mathbf{x}}(t, \mathbf{x})(A\mathbf{x}(t) + B\mathbf{u}(t)) + \frac{1}{2}\mathbf{tr}(V_{\mathbf{xx}}(t, \mathbf{x})\Sigma_{\mathbf{w}}) \quad (7)$$
$$+ \mathbf{u}(t)^T R\mathbf{u}(t) + V_t(t, \mathbf{x}) \},$$

where the optimal $\mathbf{u}(t)$ with respect to Equation (7) is equal to the minimizer of Equation (7) for all $t \in [0, T]$.

Solving the constrained partial differential equation (PDE) (7) is challenging, so we relax the constraint of problem (7), and approximate the value function of (7) by relaxing the constraint (6b). We observe that, while we relax (6b) when approximating the value function, the input will still satisfy $\mathbf{u}(t) \in \mathcal{U}(t)$. The value function is equal to [24]

$$V(t, \mathbf{x}) = \frac{1}{2}\mathbf{x}(t)^T P(t)\mathbf{x}(t) + \beta(t) + \mathbf{s}(t)^T \mathbf{x}(t) + s_0(t), \quad (8)$$

where $\dot{s}_0(t) = \frac{1}{4}\mathbf{s}(t)^T BR^{-1}B^T\mathbf{s}(t) - \mathbf{r}(t)^T Q\mathbf{r}(t)$ and $-\dot{\beta}(t) = \frac{1}{2}\mathbf{tr}(P(t)\Sigma_{\mathbf{w}})$.

Substituting Equation (8) into Equation (7), we have

$$0 = \min_{\mathbf{u}(t) \in \mathcal{U}(t)} \Big\{ (\mathbf{x}(t) - \mathbf{r}(t))^T Q(\mathbf{x}(t) - \mathbf{r}(t)) + \dot{s}_0(t) + \dot{\beta}(t)$$
$$+ \mathbf{u}(t)^T R\mathbf{u}(t) + \mathbf{x}(t)^T P(t)(A\mathbf{x}(t) + B\mathbf{u}(t)) + \mathbf{x}(t)^T \dot{\mathbf{s}}(t)$$
$$+ \frac{1}{2}\mathbf{x}(t)^T \dot{P}(t)\mathbf{x}(t) + \mathbf{s}(t)^T(A\mathbf{x}(t) + B\mathbf{u}(t)) \Big\} \quad (9)$$

We approximate the optimal $\mathbf{u}(t)$ with respect to Equation (7) by the minimizer of Equation (9). Computing the minimizer of Equation (9) is equivalent to solving a QCQP

$$\min_{\mathbf{u}(t)} \mathbf{u}(t)^T R\mathbf{u}(t) + \hat{\mathbf{x}}(t)^T P(t)B\mathbf{u}(t) + \mathbf{s}(t)^T B\mathbf{u}(t)$$
$$\text{s.t. } \mathbf{u}(t) \in \mathcal{U}(t), \forall t \in [0, T]. \quad (10)$$

at each time t. QCQPs in the form of Equation (10) can be solved efficiently using existing solvers [26] [27].

B. Safety and Reachability Verification

Parameters γ_i in $\mathcal{U}_{\gamma_i} = \{\mathbf{u}(t) : \|\mathbf{u}(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_i\}$ determines the size of the set of feasible control inputs at each time t. Larger γ_i provides a larger feasible region of $\mathbf{u}(t)$, which improves the performance of the system in the attack-free scenario. However, enlarging the feasible control input set also increases the probability that the system may be biased and leads to the unsafe states. Thus, there is a tradeoff between the performance and the risk of violating safety and reachability when selecting γ_i.

In [23], we developed a binary search algorithm to find the maximal feasible γ_i which satisfies the safety and reachability constraints in Equation (2). We used the barrier function method to determine whether safety and reachability are

guaranteed for each value of γ_i. The idea is to construct a barrier function $D_i(\mathbf{x})$ for each γ_i such that, for some $L < K$, $D_i(\mathbf{x_0}) \leq L$, $D_i(\mathbf{x}) > K$ for all $\mathbf{x}(t) \in U$, and $D_i(\mathbf{x})$ is decreasing over any feasible trajectories of $\mathbf{x}(t)$. Thus, if this $D_i(\mathbf{x})$ exists for each γ_i, $\mathbf{x}(t)$ will not enter the unsafe region.

Let $\gamma_i = \min\{\gamma_i^s, \gamma_i^r\}$. Satisfying $\mathcal{U}_{\gamma_i}(t)$ can guarantee safety and reachability if $\mathcal{A}^* = \mathcal{A}_i$. This result is formally stated using the following theorem based on [23].

Theorem 1. *If $\mathcal{A}^* = \mathcal{A}_i$, there exist γ_i^s and γ_i^r such that satisfying $\|\mathbf{u}(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_i^s$ and $\|\mathbf{u}(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_i^r$ guarantee safety and reachability with probabilities $1 - \epsilon_s$ and $1 - \epsilon_r$, respectively.*

Proof. Please see [23] for the detailed proof. $\square$

Since the controller does not know which $\mathcal{A}_i$ is $\mathcal{A}^*$, we let the control input $\mathbf{u}(t) \in \mathcal{U}(t) = \bigcap_{i=1}^{q} \mathcal{U}_{\gamma_i}(t)$ to guarantee safety and reachability for all attack patterns $\{\mathcal{A}_i\}$. However, it is possible that $\mathcal{U}(t) = \emptyset$. Thus, we need a mechanism to find out feasible solutions when $\mathcal{U}(t) = \emptyset$.

C. Selection of Constraints

In this subsection, we present a policy to provide feasible $\mathbf{u}(t)$ when $\mathcal{U}(t) = \emptyset$. Denote $\mathcal{I}(t)$ as the set of the indexes of the constraints $\mathcal{U}_{\gamma_i}(t)$. Define $\gamma_{min} = \min_i \gamma_i, i \in \{1, \ldots, q\}$. In order to identify those $\mathcal{U}_{\gamma_i}(t)$ which cause $\mathcal{U}(t) = \emptyset$, we first give a sufficient condition that $\mathcal{U}(t) \neq \emptyset$. We then express the sufficient condition in terms of the state estimates, and provide a method to select $\mathcal{I}(t)$ such that $\bigcap_{i \in \mathcal{I}(t)} \mathcal{U}_{\gamma_i}(t) \neq \emptyset$.

Proposition 1. *If there exists a ball of radius γ_{min} such that $\mathbf{u}_{\alpha,i}$ $i \in \{1, \ldots, q\}$ are contained in the ball, then $\mathcal{U}(t) \neq \emptyset$.*

Proof. Suppose there exists such a ball with center $\mathbf{u}_0$. We have $\|\mathbf{u}_0 - \mathbf{u}_{\alpha,i}\|_2 \leq \gamma_{min} \leq \gamma_i \forall i \in \{1, \ldots, q\}$. Hence, $\mathbf{u}_0 \in \mathcal{U}(t)$, and $\mathcal{U}(t) \neq \emptyset$. $\square$

In the following proposition we show the sufficient condition that the ball in Proposition 1 exists, and thus $\mathcal{U}(t) \neq \emptyset$.

Proposition 2. *For all $i, j \in \{1, \ldots, q\}$, denote $\{\hat{i}, \hat{j}\} = \arg\max_{i,j}\{d_{i,j}\}$, where $d_{i,j} = \|\mathbf{u}_{\alpha,i} - \mathbf{u}_{\alpha,j}\|_2$. If $d_{\hat{i},\hat{j}} > 2\gamma_{min}$, the ball which satisfies Proposition 1 does not exist. If $d_{\hat{i},\hat{j}} \leq 2\gamma_{min}$, and $\|\mathbf{u}_{\alpha,k} - (\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2\|_2 \leq \gamma_{min} \forall k \in \{1, \ldots, q\} \setminus \{\hat{i}, \hat{j}\}$ holds, then there exists a ball that satisfies Proposition 1.*

Proof. If $d_{\hat{i},\hat{j}} > 2\gamma_{min}$, then the distance between $\mathbf{u}_{\alpha,\hat{i}}$ and $\mathbf{u}_{\alpha,\hat{j}}$ is greater than the diameter of the ball in Proposition 1. Thus, there does not exist such ball that satisfies Proposition 1. If $d_{\hat{i},\hat{j}} \leq 2\gamma_{min}$, then $\|\mathbf{u}_{\alpha,\hat{i}} - (\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2\|_2 = \|\mathbf{u}_{\alpha,\hat{j}} - (\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2\|_2 = \frac{1}{2}\|\mathbf{u}_{\alpha,\hat{i}} - \mathbf{u}_{\alpha,\hat{j}}\|_2 = \frac{1}{2}d_{\hat{i},\hat{j}} \leq \gamma_{min}$. Since we also have $\|\mathbf{u}_{\alpha,k} - (\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2\|_2 \leq \gamma_{min} \forall k \in \{1, \ldots, q\} \setminus \{\hat{i}, \hat{j}\}$, we have that $\mathbf{u}_{\alpha,i}$ are in the ball with center $(\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2$ and radius γ_{min} for all $i \in \{1, \ldots, q\}$. $\square$

By definition of $\mathbf{u}_{\alpha,i}(t)$ and contraposition, if $\mathcal{U}(t) = \emptyset$, then

$$\|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))/4 + K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))/4\|_2$$
$$> \gamma_{min}. \quad (11)$$

where $K(t)$ is the KF gain. In the next lemma, we split (11) into two inequalities, with each containing only two estimates.

Lemma 1. *If* $\mathcal{U}(t) = \emptyset$, *then either* $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))\|_2 > \frac{1}{2}\gamma_{min}$ *or* $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))\|_2 > \frac{1}{2}\gamma_{min}$, *or both of them hold.*

Proof. Applying triangle inequality to the left hand side of inequality (11), we then have

$$\|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))/4\|_2 + \|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))/4\|_2$$
$$\geq \left\| \frac{K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))}{4} + \frac{K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))}{4} \right\|_2$$
$$> \gamma_{min}. \tag{12}$$

Inequality (12) is satisfied if at least one of $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))\|_2 > \frac{1}{2}\gamma_{min}$ and $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))\|_2 > \frac{1}{2}\gamma_{min}$ is satisfied. □

Motivated by Lemma 1, our approach to selecting $\mathcal{I}(t)$ such that $\bigcap_{i \in \mathcal{I}(t)} \mathcal{U}_{\gamma_i} \neq \emptyset$ is to compare between two state estimates. Next, we show this comparison.

Denote $C_{\alpha,i,j}$ as C with rows indexed by $\{1, \ldots, p\} \setminus (\mathcal{A}_i \bigcup \mathcal{A}_j)$. We assume that all systems $(A, C_{\alpha,i,j})$ $\forall i, j \in \{1, \ldots, q\}$ $i \neq j$ are observable. Introduce the KF state estimate $\hat{\mathbf{x}}_{\alpha,i,j}(t)$, which is obtained via $\mathbf{y}_{\alpha,i,j}(t)$, the output with the measurements indexed by $\{1, \ldots, p\} \setminus (\mathcal{A}_i \bigcup \mathcal{A}_j)$.

Lemma 2. *If* $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,j}(t)\|_2 > \frac{1}{2}\gamma_{min}$, *then at least one of* $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))\|_2 > \frac{1}{4}\gamma_{min}$ *and* $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,j}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))\|_2 > \frac{1}{4}\gamma_{min}$ *holds.*

Proof. Applying triangle inequality, we have

$$\gamma_{min}/2 < \|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,j}(t))/4\|_2$$
$$\leq \|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))/4\|_2$$
$$+ \|K(t)(\hat{\mathbf{x}}_{\alpha,j}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))/4\|_2 \tag{13}$$

In order for inequality (13) to hold, at least one of the following inequalities holds:

$$\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t)\|_2 > \frac{1}{4}\gamma_{min} \tag{14}$$

$$\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,j}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t)\|_2 > \frac{1}{4}\gamma_{min} \tag{15}$$

□

We use inequalities (14)-(15) later to identify the $\mathcal{U}_{\gamma_i}$ that leads to infeasibility of QCQP (16). Intuitively, for a certain pair of $\{i, j\} \in \{1, \ldots, q\}$, if the measurements are only affected by the noises, $\|\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,j}(t)\|_2$ should be smaller than some thresholds. If $\mathcal{A}_i = \mathcal{A}^*$ or $\mathcal{A}_j = \mathcal{A}^*$, $\hat{\mathbf{x}}_{\alpha,i,j}(t)$ should not be biased by $\mathbf{a}(t)$. Thus, when $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,j}(t)\|_2 > \frac{1}{2}\gamma_{min}$, $\hat{\mathbf{x}}_{\alpha,i,j}(t)$ can be utilized as a benchmark for checking whether $\hat{\mathbf{x}}_{\alpha,i}(t)$ and $\hat{\mathbf{x}}_{\alpha,j}(t)$ are affected by the attack and diverge from the unaffected values.

Since both the noise and attack may result in the divergence between state estimates, it is necessary to determine the worst case probability that the noise results in $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,j}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t)\|_2 > \frac{1}{4}\gamma_{min}$, which could result in measurements being excluded erroneously. We derive the following theorem to show the probability that $\|\frac{1}{4}K(t)(\hat{\mathbf{x}}_{\alpha,j}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t)\|_2 >$

$\frac{1}{4}\gamma_{min}$ $\forall i, j \in \{1, \ldots, q\}$ happens during $t \in [0, T]$ is upper-bounded when no adversary is present. We will utilize this theorem later to eliminate $\mathcal{U}_{\gamma_i}(t)$ which may render $\mathcal{U}(t) = \emptyset$.

Theorem 2. *Suppose* $\mathcal{A}^* = \mathcal{A}_i$. *There exists* $\eta^{i,j}$ *such that for each* $j \in \{1, \ldots, q\} \setminus \{i\}$

$$Pr(\sup_{t \in [0,T]} \|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))\|_2 > \gamma_{min}) \leq \eta^{i,j},$$

where $\eta^{i,j} = 4(\lambda_i^* \Gamma_i + \lambda_{i,j}^* \Gamma_{i,j})\overline{K}^2 / \gamma_{min}^2$, $\hat{\mathbf{x}}_{\alpha,i}(t)$ *and* $\hat{\mathbf{x}}_{\alpha,i,j}(t)$ *are estimates calculated using KF and measurements of sensors indexed by* $\{1, \ldots, p\} \setminus \mathcal{A}_i$ *and* $\{1, \ldots, p\} \setminus (\mathcal{A}_i \bigcup \mathcal{A}_j)$, *respectively,* $\overline{K} = \sup_{t \in [0,T]} \|K(t)\|_2$, $\lambda_i^* = \sup_{t \in [0,T]} \{\lambda_{max}(\Sigma_i(t))\}$, $\lambda_{i,j}^* = \sup_{t \in [0,T]} \{\lambda_{max}(\Sigma_{i,j}(t))\}$, $\Sigma_i(t)$ *and* $\Sigma_{i,j}(t)$ *are the covariance matrices of* $(\mathbf{x}(t) - \hat{\mathbf{x}}_{\alpha,i}(t))$ *and* $(\mathbf{x}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))$, *respectively,* $\lambda_{max}(\cdot)$ *denotes the maximum eigenvalue of a matrix,* $\Gamma_i = \mathbf{E}\left(\mathbf{e}_i(0)^T \Sigma_i(0)^{-1} \mathbf{e}_i(0)\right)$, $\Gamma_{i,j} = \mathbf{E}\left(\mathbf{e}_{ij}(0)^T \Sigma_{ij}(0)^{-1} \mathbf{e}_{ij}(0)\right)$, $\mathbf{e}_i(0) = \hat{\mathbf{x}}_{\alpha,i}(0) - \mathbf{x}_0$, *and* $\mathbf{e}_{ij}(0) = \hat{\mathbf{x}}_{\alpha,i,j}(0) - \mathbf{x}_0$.

Proof. The proof is analogous to the proof of Theorem 1 in [23] and we omit the proof due to space constraints. □

Define $\{\|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))\|_2 > \gamma_{min}\}$ as Ω_i^{ij}, $\{\|K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t))\|_2 \leq \gamma_{min}\}$ as $\overline{\Omega}_i^{ij}$. Theorem 2 implies that the probability that Ω_i^{ij} occurs during $t \in [0, T]$ is bounded above by $\eta^{i,j}$ $\forall i, j \in \{1, \ldots, p\}$ when $\mathcal{A}^* = \mathcal{A}_i$. In other words, we can eliminate $\hat{\mathbf{x}}_i(t)$ if Ω_i^{ij} occurs, and the probability that we improperly eliminate an uncompromised estimate $\hat{\mathbf{x}}_i(t)$ ($\mathcal{A}^* = \mathcal{A}_i$ but we eliminate $\mathcal{U}_{\gamma_i}$) is bounded above by $\eta^{i,j}$. Applying the results of Propositions 1 and 2 and Theorem 2, we propose the function $\mathcal{I}\_Selection$ in Algorithm 1 to select constraints that can provide feasible control inputs $\mathbf{u}(t)$ to guarantee safety and reachability requirements.

Algorithm 1 works as follows. It requires the number of attack patterns q, the LQG controller gain $K(t)$, the state estimates excluding each attack pattern $\hat{\mathbf{x}}_{\alpha,i}(t)$, the state estimates excluding each pair of attack patterns $\hat{\mathbf{x}}_{\alpha,i,j}(t)$, the minimum of radii for all constraints γ_{min}, the feasible control input set corresponding to each attack pattern $\mathcal{U}_{\gamma_i}$ as the inputs, and returns the set of indexes of selected constraints $\mathcal{I}(t)$ as the output. The algorithm selects constraints $\mathcal{U}_{\gamma_i}(t)$ that can provide feasible control inputs $\mathbf{u}(t)$ to guarantee safety and reachability properties with desired probability. The existence of the feasible control inputs $\mathbf{u}(t)$ is guaranteed by satisfying the sufficient conditions in Proposition 2. Specifically, the condition $d_{\hat{i},\hat{j}} \leq 2\gamma_{min}$ is guaranteed by line 5 - line 10. The condition $\|\mathbf{u}_{\alpha,k} - (\mathbf{u}_{\alpha,\hat{i}} + \mathbf{u}_{\alpha,\hat{j}})/2\|_2 \leq \gamma_{min}$ $\forall k \in \{1, \ldots, q\} \setminus \{\hat{i}, \hat{j}\}$ is verified via line 11 - 22. The judgment statements in line 12 and line 17 select the pairs of state estimates that may be affected by the adversary based on Lemma 1. The constraints that are likely to be affected are eliminated in line 13 - 16 and line 18 - 21 based on Lemma 2.

D. Control Strategy Design

Our proposed control design is summarized in Algorithm 2. In line 2 and 3, we initialize $\mathcal{I}(t)$ and $\mathcal{U}(t)$ as the indexes and

---

Algorithm 1 Algorithm for selecting constraints $\mathcal{U}_{\gamma_i}(t)$ that can guarantee safety and reachability properties with desired probability.

1: **procedure** $\mathcal{I}\_\text{SELECTION}(q,\ K(t),\ \hat{\mathbf{x}}_{\alpha,i}(t),\ \hat{\mathbf{x}}_{\alpha,i,j}(t),$
$\quad \gamma_{min}, \mathcal{U}_{\gamma_i}(t), i, j \in \{1, \ldots, q\}, i \neq j)$
2: $\quad \mathcal{I}(t) \leftarrow \{1, \ldots, q\}$
3: $\quad d_{i,j} \leftarrow \|\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,j}(t)\|_2,\ i, j \in \mathcal{I}(t),\ i \neq j$
4: $\quad \{\hat{i}, \hat{j}\} \leftarrow \arg\max_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
5: $\quad$ **while** $d_{\hat{i}, \hat{j}} > 2\gamma_{min}$ **do**
6: $\quad\quad$ **if** $\Omega_{\hat{i}}^{\hat{i}\hat{j}}$ **then**
7: $\quad\quad\quad \mathcal{I}(t) \leftarrow \{1, \ldots, q\} \setminus \{\hat{i}\}$
8: $\quad\quad$ **if** $\Omega_{\hat{j}}^{\hat{i}\hat{j}}$ **then**
9: $\quad\quad\quad \mathcal{I}(t) \leftarrow \{1, \ldots, q\} \setminus \{\hat{j}\}$
10: $\quad\quad \{\hat{i}, \hat{j}\} \leftarrow \arg\max_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
11: $\quad$ **for each** $i \in \mathcal{I}(t)$ **do**
12: $\quad\quad$ **if** $\|\frac{1}{4} K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{i}}(t))\|_2 > \frac{1}{2}\gamma_{min}$ **then**
13: $\quad\quad\quad$ **if** $\Omega_{i}^{i\hat{i}}$ **then**
14: $\quad\quad\quad\quad \mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{i\}$
15: $\quad\quad\quad$ **if** $\Omega_{\hat{i}}^{i\hat{i}}$ **then**
16: $\quad\quad\quad\quad \mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{\hat{i}\}$
17: $\quad\quad$ **if** $\|\frac{1}{4} K(t)(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,\hat{j}}(t))\|_2 > \frac{1}{2}\gamma_{min}$ **then**
18: $\quad\quad\quad$ **if** $\Omega_{i}^{i\hat{j}}$ **then**
19: $\quad\quad\quad\quad \mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{i\}$
20: $\quad\quad\quad$ **if** $\Omega_{\hat{j}}^{i\hat{j}}$ **then**
21: $\quad\quad\quad\quad \mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{\hat{j}\}$
22: $\quad\quad \{\hat{i}, \hat{j}\} \leftarrow \arg\max_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
23: $\quad$ **return** $\mathcal{I}(t)$

---

intersection of all constraints. In line 4, we first check whether $\mathcal{U}(t) = \emptyset$. In line 5, if $\mathcal{U}(t) = \emptyset$, we utilize $\mathcal{I}\_\text{Selection}$ in Algorithm 1 to identify and eliminate those $\mathcal{U}_{\gamma_i}(t)$ which result in $\mathcal{U}(t) = \emptyset$ and output $\mathcal{I}(t)$. In line 6, the algorithm invokes the existing solver, denoted as QCQP($\mathcal{I}(t)$), at each time t to solve the QCQP with the form

$$\min_{\mathbf{u}(t)} \mathbf{u}(t)^T R \mathbf{u}(t) + \hat{\mathbf{x}}(t)^T P(t) B \mathbf{u}(t) + \mathbf{s}(t)^T B \mathbf{u}(t)$$
$$\text{s.t. } \mathbf{u}(t) \in \mathcal{U}_{\gamma_i}(t),\ i \in \mathcal{I}(t) \tag{16}$$

Algorithm 2 Proposed control policy that guarantees safety and reachability constraints under multiple-adversary scenario.

1: **procedure** $\text{CONTROL\_POLICY}(q, \mathcal{U}_{\gamma_i}(t), i \in \{1, \ldots, q\})$
2: $\quad \mathcal{I}(t) \leftarrow \{1, \ldots, q\}$
3: $\quad \mathcal{U}(t) \leftarrow \bigcap_{i \in \mathcal{I}(t)} \mathcal{U}_{\gamma_i}(t)$
4: $\quad$ **if** $\mathcal{U}(t) == \emptyset$ **then**
5: $\quad\quad \mathcal{I}(t) \leftarrow \mathcal{I}\_\text{Selection}(q,\ K(t),\ \hat{\mathbf{x}}_{\alpha,i}(t),\ \hat{\mathbf{x}}_{\alpha,i,j}(t),$
$\quad\quad \gamma_{min}, \mathcal{U}_{\gamma_i}(t), i, j \in \{1, \ldots, q\}, i \neq j)$
6: $\quad \mathbf{u}(t) \leftarrow$ QCQP($\mathcal{I}(t)$) in Equation (16)
7: $\quad$ **return** $\mathbf{u}(t)$

When there is no attack, the controller attempts to minimize the objective function. Due to the existence of noise, $d_{i,j}$ may deviate from 0 for $\forall i, j \in \{1, \ldots, q\}$. This may lead to smaller

feasible region $\mathcal{U}(t)$, and suboptimal performance with respect to expected cost. If all $\mathbf{u}_{\alpha,i}(t)$ can be proved to be close to the optimal control $\mathbf{u}^*(t)$, the feasibility and performance of the proposed approach can be guaranteed.

Lemma 3. *Let* $\mathbf{u}^*(t) = \frac{1}{2} K(t)\hat{\mathbf{x}}(t) - \frac{1}{2} R^{-1} B^T \mathbf{s}(t)$. *Define* $\lambda^* = \sup_t \{\lambda_{max}(\Sigma(t))\}$, *where* $\Sigma(t)$ *is the covariance matrix of* $(\mathbf{x}(t) - \hat{\mathbf{x}}(t))$. *Let* $\overline{\eta} = \max\{\eta^i : \forall i \in \mathcal{I}(t)\}$, *where* $\eta^i = (\lambda^* \Gamma + \lambda_i^* \Gamma_i) \overline{K}^2 / \gamma_{min}^2$ *and* $\Gamma = \mathbf{E}\left(\mathbf{e}(0)^T \Sigma(0)^{-1} \mathbf{e}(0)\right)$. *When* $\beta = 1$, *we have*

$$Pr(\sup_{t \in [0,T]} \|\mathbf{u}^*(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_{min}) \geq 1 - \overline{\eta}, \forall i \in \mathcal{I}(t),$$
$$Pr\left(\mathbf{u}^*(t) \in \mathcal{U}(t)\ \forall t \in [0,T]\right) \geq 1 - \Sigma_{i \in \mathcal{I}(t)}\ \eta^i$$

Proof. Based on the definitions of $\mathbf{u}^*(t)$ and $\mathbf{u}_{\alpha,i}(t)$, we have

$$Pr(\sup_{t \in [0,T]} \|\mathbf{u}^*(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \geq \gamma_{min})$$
$$= Pr(\sup_{t \in [0,T]} \|K(t)(\hat{\mathbf{x}}(t) - \hat{\mathbf{x}}_{\alpha,i}(t))\|_2 \geq 2\gamma_{min})$$

According to Theorem 2, we have

$$Pr(\sup_{t \in [0,T]} \|K(t)(\hat{\mathbf{x}}(t) - \hat{\mathbf{x}}_{\alpha,i}(t))\|_2 \geq 2\gamma_{min}) \leq \eta^i.$$

Thus,

$$Pr(\sup_{t \in [0,T]} \|\mathbf{u}^*(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_{min}) \geq 1 - \eta^i \tag{17}$$

We have

$$Pr(\sup_{t \in [0,T]} \|\mathbf{u}^*(t) - \mathbf{u}_{\alpha,i}(t)\|_2 \leq \gamma_{min}) \geq 1 - \overline{\eta}, \forall i \in \mathcal{I}(t). \tag{18}$$

Based on Equation (17) we can obtain

$$Pr\left(\mathbf{u}^*(t) \in \mathcal{U}(t)\ \forall t \in [0,T]\right)$$
$$= 1 - Pr(\cup_{i \in \mathcal{I}(t)} \mathbf{u}^*(t) \notin \mathcal{U}_{\gamma_i}(t)\ \forall t \in [0,T]))$$
$$\geq 1 - \Sigma_{i \in \mathcal{I}(t)}\ \eta^i \tag{19}$$
$\square$

Based on (18), the probability that in the non-adversary case $\bigcap_{i \in \mathcal{I}(t)} \mathcal{U}_{\gamma_i}(t) \neq \emptyset$ is lower bounded by $1 - \overline{\eta}$. Our proposed approach guarantees feasibility under benign environment. Equation (19) implies that the probability that our proposed approach provides the same utility as the best possible control when no adversary is present is lower bounded.

E. Safety and Reachability Guarantees

In this subsection, we present the safety and reachability guarantees provided by the control policy obtained by Algorithm 2. Define $\Omega_{sr} \triangleq (\bigcap_{t \in [0,T]} \{\mathbf{x}(t) \notin U\}) \bigcap \{\mathbf{x}(T) \in G\}$, $\Omega_{\mathcal{U}} \triangleq \bigcap_{t \in [0,T]} \{\mathbf{u}(t) \in \mathcal{U}_\gamma^*(t)\}$, and $\overline{\Omega}_{\mathcal{U}} \triangleq \bigcup_{t \in [0,T]} \{\mathbf{u}(t) \notin \mathcal{U}_\gamma^*(t)\}$. The safety and reachability analysis of our proposed control policy is based on bounding the probability $P_0 = Pr(\Omega_{sr})$. We define $P_1 \triangleq Pr(\Omega_{sr}|\Omega_{\mathcal{U}})$ as the probability that safety and reachability constraints are satisfied given that the control inputs are from $\mathcal{U}_\gamma^*(t)$. This probability has been discussed in Theorem 1. We denote $P_2 \triangleq Pr(\Omega_{\mathcal{U}})$ as the

probability that at any time t the control input $\mathbf{u}(t)$ satisfies the correct constraint $\mathcal{U}_\gamma^*(t)$. We have

$$
\begin{aligned}
P_0 &= Pr\left(\Omega_{sr}\right) \\
&= Pr(\Omega_{sr}|\Omega_{\mathcal{U}}) \cdot Pr(\Omega_{\mathcal{U}}) + Pr(\Omega_{sr}|\overline{\Omega}_{\mathcal{U}}) \cdot Pr(\overline{\Omega}_{\mathcal{U}}) \\
&\geq P_1 \cdot P_2
\end{aligned}
$$

Here P_0 denotes the probability that safety and reachability are guaranteed and the control input $\mathbf{u}(t)$ is in $\mathcal{U}_\gamma^*(t), \forall t$, and can be expressed using P_1 and P_2. If there exist lower bounds for both P_1 and P_2, the lower bound for P_0 exists.

The safety and reachability guarantees of the proposed control policy is presented by the following theorem.

Theorem 3. *The control strategy returned by Algorithm 2 satisfies the safety and reachability constraints in Equation (2).*

Proof. The probability that safety and reachability are guaranteed when the control input $\mathbf{u}(t)$ is in $\mathcal{U}_\gamma^*(t)$ for all t, with probability $P_0 = P_1 \cdot P_2$. P_1 is bounded below by Theorem 1. Assume $\mathcal{A}^* = \mathcal{A}_i$. P_2 is equivalent to the probability that $\mathcal{U}_{\gamma_i}(t)$ is never eliminated at each time t, which is bounded below by the probability that $\{\sup_{t\in[0,T]}||K(t)\left(\hat{\mathbf{x}}_{\alpha,i}(t) - \hat{\mathbf{x}}_{\alpha,i,j}(t)\right)||_2 \leq \gamma_{min} \ \forall j \in \{1,\ldots,q\}\setminus\{i\}\}$. Thus, we obtain

$$
\begin{aligned}
P_2 &= Pr(\cap_{j\in\{1,\ldots,q\}\setminus\{i\}} \sup_{t\in[0,T]}\overline{\Omega}_i^{ij}) \\
&= 1 - Pr(\cup_{j\in\{1,\ldots,q\}\setminus\{i\}} \sup_{t\in[0,T]}\Omega_i^{ij}) \\
&\geq 1 - \Sigma_{j\in\{1,\ldots,q\}\setminus\{i\}}Pr(\sup_{t\in[0,T]}\Omega_i^{ij}) \\
&\geq 1 - \Sigma_{j\in\{1,\ldots,q\}\setminus\{i\}}\eta^{i,j}, \quad (20)
\end{aligned}
$$
$$
P_0 \geq P_1 \cdot \left(1 - \Sigma_{j\in\{1,\ldots,q\}\setminus\{i\}}\eta^{i,j}\right). \quad (21)
$$

By choosing $\gamma_i, \forall i \in \{1,\ldots,q\}$ and γ_{min} properly, we can make $P_0 \geq \max\{1-\epsilon_s, 1-\epsilon_r\} \ \forall i \in \{1,\ldots,q\}$. $\square$

Theorem 3 implies that there exists a lower bound of the probability that the safety and reachability constraints can be satisfied for $\forall \mathcal{A}_i$. We observe that this lower bound given in Equation (20) depends on $\gamma_i \ \forall i \in \{1,\ldots,q\}$, γ_{min}, and the noise characteristics of the system. By choosing appropriate $\gamma_i \ \forall i \in \{1,\ldots,q\}$ and γ_{min}, and constructing corresponding set of feasible control inputs $\mathcal{U}_{\gamma_i}(t)$, we can attempt to make the lower bound be within $[\max\{1-\epsilon_s, 1-\epsilon_r\}, 1]$.

F. Selection of γ_i and γ_{min}

The parameters $\gamma_i \ \forall i \in \{1,\ldots,q\}$ and γ_{min} affect both P_1 and P_2. In P_1, smaller $\gamma_i \ \forall i \in \{1,\ldots,q\}$ can make the system be more difficult to be biased. In P_2, larger γ_{min} is more likely to make the correct constraint be kept. In order to guarantee safety and reachability for all $\mathcal{A}_i$, we need to keep $P_0 \geq \max\{1-\epsilon_s, 1-\epsilon_r\} \ \forall i \in \{1,\ldots,q\}$. Since the closed form expression of P_1 as a function of γ_i is not clear, we utilize a heuristic method to search for proper value of $\gamma_i \ \forall i \in \{1,\ldots,q\}$ and γ_{min} which satisfies $P_1 \cdot P_2 \geq \max\{1-\epsilon_s, 1-\epsilon_r\}$ for all $\mathcal{A}_i$. The intuition is that we initialize P_1 first to compute the corresponding γ_i to the candidate P_1, and calculate the corresponding $\gamma_{min} = \min_i \gamma_i$

Algorithm 3 Algorithm for computing the parameters $\{\gamma_i, i \in 1,\ldots,q\}$ and γ_{min} that ensures safety and reachability.

1: **procedure** $\gamma\_$SELECTION$(\epsilon_s, \epsilon_r, iter\_times, \overline{K}, \lambda_i^*, \lambda_{i,j}^*,$
$\quad i,j \in 1,\ldots,q\}, i \neq j)$
2: $\quad \overline{\epsilon} \leftarrow \max\{1-\epsilon_s, 1-\epsilon_r\}$
3: $\quad$ **for each** $i \in \{1,\ldots,q\}$ **do**
4: $\quad\quad \overline{P}_{1,i} \leftarrow 1, \ \underline{P}_{1,i} \leftarrow (\overline{P}_{1,i} - \overline{\epsilon})/iter\_times$
5: $\quad\quad \gamma_i \leftarrow$ Barrier_Certificate$(\overline{P}_{1,i})$
6: $\quad$ Update γ_{min} and i_{min}.
7: $\quad$ **for each** $i \in \{1,\ldots,q\}$ **do**
8: $\quad\quad \eta^{i,j} \leftarrow 4(\lambda_i^*\Gamma_i + \lambda_{i,j}^*\Gamma_{i,j})\overline{K}^2/\gamma_{min}^2$
9: $\quad\quad$ Update $\overline{P}_{2,i}$ and $\overline{P}_{0,i}$ via (20) and (21).
10: $\quad i \leftarrow 1$
11: $\quad$ **while** $i \leq iter\_times$ **do**
12: $\quad\quad \overline{P}_{1,i_{min}} \leftarrow \overline{P}_{1,i_{min}} - \underline{P}_{1,i_{min}}$
13: $\quad\quad \gamma_{i_{min}} \leftarrow$ Barrier_Certificate$(\overline{P}_{1,i_{min}})$
14: $\quad\quad$ Update γ_{min} and i_{min}.
15: $\quad\quad$ **for each** $i \in \{1,\ldots,q\}$ **do**
16: $\quad\quad\quad \eta^{i,j} \leftarrow 4(\lambda_i^*\Gamma_i + \lambda_{i,j}^*\Gamma_{i,j})\overline{K}^2/\gamma_{min}^2$
17: $\quad\quad\quad$ Update $\overline{P}_{2,i}$ and $\overline{P}_{0,i}$ via (20) and (21).
18: $\quad\quad$ **if** $\forall \overline{P}_{0,i} \geq \overline{\epsilon}$ **then**
19: $\quad\quad\quad$ break
20: $\quad\quad i \leftarrow i+1$
21: $\quad$ **if** $i > iter\_times$ **then**
22: $\quad\quad$ **return** null
23: $\quad$ **return** $\{\gamma_i, i \in 1,\ldots,q\}, \gamma_{min}$

---

for all $i \in \{1,\ldots,q\}$. Here we assume existence of a function Barrier_Certificate that returns the γ_i. Then we check the lower bound of P_0 for all $\mathcal{A}_i$ according to inequality (21). If the lower bound is greater than $\max\{1-\epsilon_s, 1-\epsilon_r\}$ for all $\mathcal{A}_i$, the safety and reachability constraints are satisfied. Otherwise, we enlarge γ_{min} by reducing the P_1 corresponding to the minimal γ_i, recalculating this γ_i under the updated P_1, and checking the lower bounds of P_0 for all $\mathcal{A}_i$ under new γ_{min}. We do this procedure iteratively until the lower bounds of P_0 for all $\mathcal{A}_i$ are greater than $\max\{1-\epsilon_s, 1-\epsilon_r\}$ for all $\mathcal{A}_i$. The proposed procedure is shown in Algorithm 3.

IV. CONTROL STRATEGY FOR SINGLE-ADVERSARY SCENARIO

In this section, we consider a special case where there exists a unique attack pattern, denoted as $\mathcal{A}_1$. Both the controller and the adversary have the knowledge of $\mathcal{A}^* = \mathcal{A}_1$. However, the controller does not know which sensors in $\mathcal{A}_1$ are compromised by the adversary.

In the single-adversary scenario, Equation (6) in the multiple-adversary scenario becomes

$$
\min_{\mathbf{u}(t)} \mathbf{E}[\int_0^T ((\mathbf{x}(t)-\mathbf{r}(t))^T Q(\mathbf{x}(t)-\mathbf{r}(t)) + \mathbf{u}(t)^T R\mathbf{u}(t))dt
$$
$$
+ (\mathbf{x}(T)-\mathbf{r}(T))^T F(\mathbf{x}(T)-\mathbf{r}(T))] \quad (22)
$$
s.t. $\mathbf{u}(t) \in \mathcal{U}_{\gamma_1}(t), \forall t \in [0,T]$.

When solving (7), we do not know which $\mathcal{A}_i$ is $\mathcal{A}^*$, and $\mathcal{I}(t)$ is changing at each time step t. Thus, we have to relax the

constraints $\mathcal{U}_{\gamma_i}(t)$ for all $i \in \mathcal{I}(t)$. Since $\mathcal{A}^* = \mathcal{A}_1$ is known in the single-adversary scenario, we use the method of Lagrange multipliers to construct the dual problem of Equation (22) rather than relax the constraint $\mathcal{U}_{\gamma_1}(t)$ when solving the HJB equation. Denote the Lagrange multiplier corresponding to constraint $\mathcal{U}_{\gamma_1}(t)$ as $\lambda(t)$. The dual problem of (22) is [28]

$$\max_{\lambda(t)} \min_{\mathbf{u}(t)} \mathbf{E}\left\{\int_0^T [(\mathbf{x}(t) - \mathbf{r}(t))^T Q(\mathbf{x}(t) - \mathbf{r}(t)) \right.$$
$$+ \mathbf{u}(t)^T R\mathbf{u}(t) - \lambda(t)\left(\gamma_1^2 - \|\mathbf{u}(t) - \mathbf{u}_{\alpha,1}(t)\|_2^2\right)]dt$$
$$\left. + (\mathbf{x}(T) - \mathbf{r}(T))^T F(\mathbf{x}(T) - \mathbf{r}(T))\right\} \quad (23a)$$

$$\text{s.t. } \lambda(t) \geq 0, \forall t \in [0, T] \quad (23b)$$

Choosing the value of $\lambda(t)$ at each time step t is challenging, so we relax the problem by assuming $\lambda(t) \equiv \lambda \geq 0$ for all $t \in [0, T]$. The following analysis can be repeated for different values of λ to obtain a lower bound on the solution to (20), and hence a lower bound on the value function. The inner minimization problem of Equation (23) can be rewritten as

$$\min_{\mathbf{u}(t)} \mathbf{E}\left\{\int_0^T [(\widetilde{\mathbf{x}}(t) - \widetilde{\mathbf{r}}(t))^T \widetilde{Q}(t)(\widetilde{\mathbf{x}}(t) - \widetilde{\mathbf{r}}(t)) \right.$$
$$+ \mathbf{u}(t)^T (\lambda I + R)\mathbf{u}(t) - \widetilde{\mathbf{x}}(t)^T M(t)\mathbf{u}(t) - \lambda\gamma_1^2]dt$$
$$\left. + (\widetilde{\mathbf{x}}(T) - \widetilde{\mathbf{r}}(T))^T \widetilde{F}(\widetilde{\mathbf{x}}(T) - \widetilde{\mathbf{r}}(T))\right\}, \quad (24)$$

where $\widetilde{\mathbf{x}}(t) = [\mathbf{x}(t)^T, \hat{\mathbf{x}}_{\alpha,1}(t)^T, \mathbf{s}(t)^T]^T$, $\widetilde{\mathbf{r}}(t) = [\mathbf{r}(t)^T, 0, 0]^T$,

$$\widetilde{Q}(t) = \begin{bmatrix} Q & 0 & 0 \\ 0 & \lambda K(t)^T K(t) & -\frac{1}{2}\lambda K(t)^T R^{-1} B^T \\ 0 & -\frac{1}{2}\lambda B R^{-1} K(t) & \frac{1}{4}\lambda B R^{-1} R^{-1} B^T \end{bmatrix}$$

$$M(t) = \begin{bmatrix} 0 \\ 2\lambda K(t)^T \\ -\lambda B R^{-1} \end{bmatrix}, \widetilde{F}(t) = \begin{bmatrix} F & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The solution of Equation (24) can be obtained by solving a stochastic HJB equation [25]. Solving that HJB equation yields

$$\mathbf{u}^*(t) = -\frac{1}{2}(R + \lambda I)^{-1}(\widetilde{B}^T \widetilde{P}(t) - M(t)^T)\widetilde{\mathbf{x}}(t)$$
$$-\frac{1}{2}(R + \lambda I)^{-1}\widetilde{B}^T \widetilde{\mathbf{s}}(t), \quad (25)$$

where $\widetilde{B} = \begin{bmatrix} B & B & 0 \end{bmatrix}^T$,

$$-\dot{\widetilde{P}}(t) = \widetilde{A}^T \widetilde{P}(t) + \widetilde{P}(t)\widetilde{A} + 2\widetilde{Q}$$
$$-\frac{1}{2}(\widetilde{B}^T \widetilde{P}(t) - M(t)^T)^T (R + \lambda I)^{-1}(\widetilde{B}^T \widetilde{P}(t) - M(t)^T)$$
$$\dot{\widetilde{\mathbf{s}}}(t) = (-\widetilde{A}^T + \frac{1}{2}\widetilde{P}(t)\widetilde{B}(R + \lambda I)^{-1}\widetilde{B}^T$$
$$-\frac{1}{2}M(t)\widetilde{B})\widetilde{\mathbf{s}}(t) + (2\widetilde{Q} - \widetilde{P}(t)H)\widetilde{\mathbf{r}}(t)$$

with boundary conditions $\widetilde{\mathbf{s}}(T) = -2\widetilde{F}\widetilde{\mathbf{r}}(T)$ and $\widetilde{P}(T) = 2\widetilde{F}$.

Define the optimal value of Equation (22) as $\mathcal{V}_1$, the value of Equation (22) using the solution of QCQP (10) as $\mathcal{V}_2$, and the value of Equation (22) using Equation (25) as $\mathcal{V}_3$. Based on the weak duality [28], $\mathcal{V}_3 \leq \mathcal{V}_1$. Note that when $\lambda = 0$,
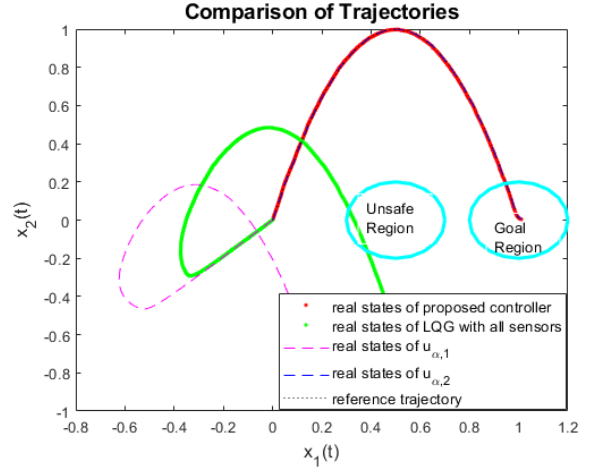

Fig. 1. The states of the proposed policy and $\mathbf{u}_{\alpha,2}(t)$ converge to the goal region without reaching the unsafe region in spite of a constant attack. Meanwhile the state of the LQG controller using all measurements and $\mathbf{u}_{\alpha,1}(t)$ violates safety and/or reachability constraints.
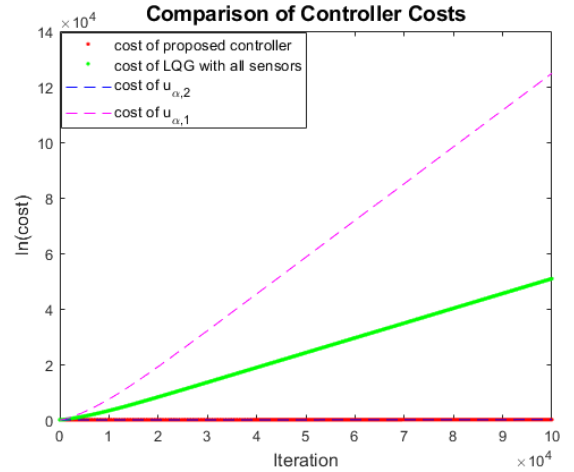

Fig. 2. The average costs of the proposed policy and $\mathbf{u}_{\alpha,2}(t)$ are 31.8519 and 29.6224, respectively, which are lower than those of the LQG controller using all measurements and $\mathbf{u}_{\alpha,1}(t)$.

$\mathcal{V}_3 = \mathcal{V}_2$. Since 0 is a feasible solution of λ and Equation (23a) maximizes over λ, we have that $\mathcal{V}_2 \leq \mathcal{V}_3$, which further yields that $\mathcal{V}_3$ is a tighter bound to $\mathcal{V}_1$ than $\mathcal{V}_2$.

V. CASE STUDY

In this section, we evaluate the proposed policy via a numerical case study. Consider a system with 2 states, 2 inputs, and 6 sensors. There are $q = 3$ attack patterns, denoted as $\mathcal{A}_1 = \{1, 4\}$, $\mathcal{A}^* = \mathcal{A}_2 = \{2, 5\}$, and $\mathcal{A}_3 = \{3, 6\}$. The adversary selects $\mathbf{a}(t) = (0, 1, 0, 0, 1, 0)^T$. Matrices A and B are set to be identity matrices I with proper dimensions. Matrix $C = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}^T$. The noises $\mathbf{w}(t)$ and $\mathbf{v}(t)$ are Gaussian with means 0 and covariances $\Sigma_\mathbf{w} = 0.1I$ and $\Sigma_\mathbf{v} = 0.1I$. The cost matrices are selected as $Q = I$, $F = 0.03I$, and $R = 1 \times 10^{-3}I$ with proper dimensions.

The system tracks a parabolic reference trajectory with the form $x_2(t) = -4 \times (x_1(t) - 0.5001)^2 + 0.9999$, where $x_1(t)$

and $x_2(t)$ denote the first and second dimensions of the state at time t. The initial state $\mathbf{x}_0 = (0.0001, -0.0001)^T$. We choose that $\Phi_{\alpha,i}(0) = 10I$ and $\hat{\mathbf{x}}_{\alpha,i}(0) = (0,0)^T$. The system is required to avoid the set of unsafe states $U = \{\mathbf{x} : 0.2^2 - (x_1 - 0.5001)^2 - (x_2 + 0.0001)^2 > 0\}$ and reach the set of the goal states $G = \{\mathbf{x} : 0.2^2 - (x_1 - 1.0001)^2 - (x_2 + 0.0001)^2 > 0\}$ at $T = 10$. The worst case probability that the safety and reachability constraints are violated are designed as $\epsilon_s = 0.3$ and $\epsilon_r = 0.3$.

The proposed policy is compared with three LQG controllers. One LQG controller utilizes the measurements of all sensors, while the other two LQG controllers $\mathbf{u}_{\alpha,1}(t)$ and $\mathbf{u}_{\alpha,2}(t)$ which eliminate the measurements of sensors indexed by $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. The performances of the four controllers are shown in Fig. 1 and 2. As shown in Fig. 1, the proposed controller and $\mathbf{u}_{\alpha,2}(t)$ can satisfy the safety and reachability constraints, while the LQG controller using all measurements and $\mathbf{u}_{\alpha,1}(t)$ are biased by the attack and violate the constraints. From Fig. 2, we see that the cost of proposed controller converges to the cost of $\mathbf{u}_{\alpha,2}(t)$, which is less than the costs of the LQG controller using all measurements and $\mathbf{u}_{\alpha,1}(t)$. From the results shown in Fig. 1 and 2, the proposed controller guarantees safety and reachability, and at the same time provides comparable cost performance with $\mathbf{u}_{\alpha,2}(t)$. This results from the fact that after the function $\mathcal{I}\_Selection$ eliminates the contraints $\mathcal{U}_{\gamma_1}(t)$ and $\mathcal{U}_{\gamma_3}(t)$, the controller is not biased by the adversary. The LQG controller $\mathbf{u}_{\alpha,2}(t)$ is optimal, but the attack pattern $\mathcal{A}^* = \mathcal{A}_2$ is not known by the controller a prior. Thus, in real world, $\mathbf{u}_{\alpha,2}(t)$ is not realizable because $\mathcal{A}^* = \mathcal{A}_2$ is only known by the adversary.

VI. CONCLUSION

This paper considered the LQG tracking problem with safety and reachability constraints and unknown FDI attack. We assumed that the adversary can compromise a subset of sensors. The controller only knows a collection of possible compromised sensor sets, but has no information about which set of sensors is under attack. We computed a control policy by bounding the control input with a collection of quadratic constraints, each of which corresponds to a possible compromised sensor set. We used a barrier certificate based algorithm to constrain the feasible region of the control policy. We proved that the proposed policy satisfies safety and reachability constraints with desired probability. We provided rules to resolve the possible conflicts between the quadratic constraints. We validated the proposed policy with a simulation study.

REFERENCES

[1] S. Mitra, T. Wongpiromsarn, and R. M. Murray, "Verifying cyber-physical interactions in safety-critical systems," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 28–37, 2013.

[2] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proc. of the IEEE*, vol. 100, no. 1, pp. 283–299, 2011.

[3] C. Kwon and I. Hwang, "Reachability analysis for safety assurance of cyber-physical systems against cyber attacks," *IEEE Trans. on Automatic Control*, vol. 63, no. 7, pp. 2272–2279, 2017.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[5] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. of the 1st Int. Conf. on High Confidence Networked Systems*, pp. 55–64, 2012.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[7] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[8] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Preprints of the 1st workshop on Secure Control Systems*, pp. 1–6, 2010.

[9] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[11] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2014.

[12] R. Zhang and P. Venkitasubramaniam, "A game theoretic approach to analyze false data injection and detection in LQG system," in *IEEE Conf. on Communications and Network Security*, pp. 427–431, IEEE, 2017.

[13] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, 2018.

[14] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.

[15] Z. Wu, F. Albalawi, J. Zhang, Z. Zhang, H. Durand, and P. D. Christofides, "Detecting and handling cyber-attacks in model predictive control of chemical processes," *Mathematics*, vol. 6, no. 10, p. 173, 2018.

[16] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[17] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada, "SMT-based observer design for cyber-physical systems under sensor attacks," *ACM Trans. on Cyber-Physical Systems*, vol. 2, no. 1, pp. 1–27, 2018.

[18] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Trans. on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2016.

[19] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[20] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Preserving physical safety under cyber attacks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6285–6300, 2018.

[21] K. Gheitasi, M. Ghaderi, and W. Lucia, "A novel networked control scheme with safety guarantees for detection and mitigation of cyber-attacks," in *18th European Control Conf. (ECC)*, pp. 1449–1454, IEEE, 2019.

[22] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial iot," *IEEE Trans. on Industrial Informatics*, vol. 16, no. 4, pp. 2716–2725, 2019.

[23] L. Niu, Z. Li, and A. Clark, "LQG reference tracking with safety and reachability guarantees under false data injection attacks," in *American Control Conf.*, pp. 2950–2957, IEEE, 2019.

[24] B. D. Anderson and J. B. Moore, *Optimal Control: Linear Quadratic Methods*. Courier Corporation, 2007.

[25] D. E. Kirk, *Optimal Control Theory: an Introduction*. Courier Corporation, 2004.

[26] A. Domahidi, A. U. Zgraggen, M. N. Zeilinger, M. Morari, and C. N. Jones, "Efficient interior point methods for multistage problems arising in receding horizon control," in *51st IEEE Conf. on decision and control (CDC)*, pp. 668–674, IEEE, 2012.

[27] G. Torrisi, S. Grammatico, R. S. Smith, and M. Morari, "A projected gradient and constraint linearization method for nonlinear model predictive control," *SIAM Journal on Control and Optimization*, vol. 56, no. 3, pp. 1968–1999, 2018.

[28] A. Shapiro, "On duality theory of convex semi-infinite programming," *Optimization*, vol. 54, no. 6, pp. 535–543, 2005.