Abstract—We investigate a linear quadratic Gaussian (LQG) tracking problem with safety and reachability constraints in the presence of an adversary who mounts a false data injection 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. 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 (FDI) attack, linear quadratic Gaussian (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 health care, 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. Wu et al. [15] assume 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 article, 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 article is twofold. 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 rest of this article is organized as follows. Section II states the system and adversary models and the problem formulation. Sections III and IV propose the control policy for the multiple- and single-adversary scenarios, respectively. Section V contains simulation results. Finally, Section VI concludes this article.

II. SYSTEM MODEL AND PROBLEM STATEMENT

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

Zhouchi Li, Student Member, IEEE, Luyao Niu, Student Member, IEEE, and Andrew Clark, Member, IEEE
A. System and Adversary Models

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

\[
\dot{x}(t) = Ax(t) + Bu(t) + w(t) \tag{1a}
\]

\[
y(t) = Cx(t) + v(t) + a(t). \tag{1b}
\]

In (1), \( w(t) \) and \( v(t) \) are independent Gaussian processes with means identically zero and autocorrelation functions \( R_w(\tau) = \Sigma_w \delta(\tau) \) and \( R_v(\tau) = \Sigma_v \delta(\tau) \), respectively, where \( \delta(\tau) \) denotes the Dirac delta function. We use \( \Sigma_w \) and \( \Sigma_v \) to denote the covariance matrices of \( w(t) \) and \( v(t) \) at each time \( t \). We assume \( (A, N_w) \) is stabilizable, where \( N_w N_w^T = \Sigma_w \). The initial state \( x(0) \) is equal to \( x_0 \). Denote \( \mathcal{S}(t) \) as the information available to the controller at time \( t \). We have \( \mathcal{S}(t) = \{y(t)|t' \leq t\} \cup \{u(t')|t' < t\} \) and \( \mathcal{S}(0) = y(0) \). The control policy of the system is defined as a function \( \mu(\mathcal{S}(t)) \in \mathcal{U} \).

In (1b), \( a(t) \) is the attack signal injected by the adversary. There exists a collection of attack patterns \( \{A_i : i \in \{1, \ldots, q\}\} \). Here, \( A_i \subseteq \{1, \ldots, p\} \) is a subset of sensors, in which it is possible that \( A_i \cap A_j \neq \emptyset \). The adversary chooses one \( A^* \) from \( A_1, \ldots, A_q \). The adversary then chooses \( a(t) \) with arbitrary values such that \( \text{support}(a(t)) \subseteq A^* \) for all time \( t \in [0, T] \). The controller knows the possible compromised sets \( A_1, \ldots, A_q \), but does not know which set \( A^* \) has been chosen by the adversary. At each time \( t \), the adversary knows the control policy \( \mu(\mathcal{S}(t)) \), the system state \( x(t) \), the output \( y(t) \), and the control input \( u(t) \) for all \( t' \leq t \). Denote the adversary policy \( \nu(t) \) as a function which maps \( \{x(t), u(t), y(t) : t' \leq t\} \) to \( a(t) \).

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

B. Problem Formulation

The problem studied in this work is

\[
\min_{\mu} \mathbb{E} \left[ (x(T) - r(T))^T F(x(T) - r(T)) + \int_0^T (u(t))^T R u(t) dt \right] + \mathbb{E} \left[ (x(t) - r(t))^T Q (x(t) - r(t)) dt \right] \tag{2}
\]

s.t. \( \max_{\nu} \{Pr(\mathcal{S} \in [0, T] : x(t) \notin U) | \mu, \nu \} \leq \epsilon_s \)

\[
\min_{\nu} \{Pr(x(T) \in G | \mu, \nu) \} \geq 1 - \epsilon_r. \tag{2}
\]

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 \( \epsilon_s \). 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 multiadversary 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 \( u_{\alpha,i}(t) \) that corresponds to the measurements from \( \{1, \ldots, p\} \setminus A_i \) for each attack pattern \( A_i \), then we can limit the impact from the adversary’s attack signal.

A. Control Policy Construction

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

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

\[
\dot{\hat{x}}_{\alpha,i}(t) = A \hat{x}_{\alpha,i}(t) + B u_{\alpha,i}(t) + \Theta_{\alpha,i}(t) (y_{\alpha,i}(t) - C_{\alpha,i} \hat{x}_{\alpha,i}(t)) \tag{3}
\]

\[
\Theta_{\alpha,i}(t) = \Phi_{\alpha,i}(t) C_{\alpha,i}^T \Sigma_{v_{\alpha,i}}^{-1} \tag{4}
\]

\[
\Phi_{\alpha,i}(t) = A \Phi_{\alpha,i}(t) + \Phi_{\alpha,i}(t) A^T + \Sigma_w - \Phi_{\alpha,i}(t) C_{\alpha,i}^T \Sigma_{v_{\alpha,i}}^{-1} C_{\alpha,i} \Phi_{\alpha,i}(t)^T \tag{5}
\]

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

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

\[
u_{\alpha,i}(t) = \frac{1}{2} K(t) \hat{x}_{\alpha,i}(t) - \frac{1}{2} R^{-1} B T^* s(t) \tag{6a}\]

\[
K(t) = -R^{-1} B T^* P(t) \tag{6b}\]

\[
\dot{s}(t) = \left( -A T^* + \frac{1}{2} P(t) B R^{-1} B^T \right) s(t) + 2 Q(t) P(t) \tag{6c}\]

where \( s(t) \) and \( P(t) \) have boundary conditions \( s(T) = -2 F R(T) \) and \( P(T) = 2 F \).

Denote \( \hat{x}_{\alpha,i}^*(t) \) as the KF estimate of \( x(t) \) based on \( y_{\alpha,i}^*(t) \) of sensors in \( A_i \setminus \{1, \ldots, p\} \). Dynamics of \( \hat{x}_{\alpha,i}^*(t) \) is analogous to (3)-(5). Similarly, we define \( u_{\alpha,i}^*(t) \) as the LQG tracking optimal control input based on \( y_{\alpha,i}^*(t) \).

Define the set of feasible control inputs at time \( t \) with respect to attack pattern \( A_i \) as \( U_{\alpha,i}(t) \triangleq \{u(t) : (u(t) - u_{\alpha,i}(t))^T (u(t) - u_{\alpha,i}(t)) \leq \gamma_i^2 \} \), where \( \gamma_i \geq 0 \) is a parameter that will be discussed in Section III-B. Define \( U^+(t) \triangleq \{u(t) : |u(t) - u_{\alpha,i}(t)| \leq \gamma_i \} \) and \( U(t) \triangleq \bigcap_{i=1}^q U_{\alpha,i}(t) \). Using this constraint instead of the constraint in (2), the problem becomes

\[
\min_{u(t)} \mathbb{E} \left[ \int_0^T ((x(t) - r(t))^T Q (x(t) - r(t)) + u(t)^T R u(t)) dt \right] + \mathbb{E} \left[ (x(t) - r(t))^T F(x(t) - r(t)) \right] \tag{6a}
\]

s.t. \( u(t) \in U(t) \) \( \forall t \in [0, T] \).
The solution of (6) can be computed by solving a stochastic Hamilton–Jacobi–Bellman (HJB) equation [25]

\[
0 = \min_{u(t),u(t)} \left\{ \langle x(t) - r(t) \rangle^T Q(x(t) - r(t)) \right. \\
+ V_k(x(t),Ax(t) + Bu(t)) + \frac{1}{2} \text{tr}(V_{xx}(t,x)\Sigma_w) \\
+ u(t)^T R u(t) + V_i(x(t)) \right\}
\]

(7)

where the optimal \( u(t) \) with respect to (7) is equal to the minimizer of (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 \( u(t) \in U(t) \). The value function is equal to [24]

\[
V(t,x) = \frac{1}{2} x(t)^T P(t)x(t) + \beta(t) + s(t)^T x(t) + s_0(t)
\]

(8)

where \( s_0(t) = \frac{1}{2} s(t)^T B R^{-1} B^T s(t) - \beta(t) + \frac{1}{2} \text{tr}(P(t)\Sigma_w) \).

Substituting (8) into (7), we have

\[
0 = \min_{u(t),u(t)} \left\{ \langle x(t) - r(t) \rangle^T Q(x(t) - r(t)) + s_0(t) + \beta(t) \\
+ u(t)^T R u(t) + x(t)^T P(t)(Ax(t) + Bu(t)) + x(t)^T s(t) \\
+ \frac{1}{2} x(t)^T P(t)x(t) + s(t)^T (Ax(t) + Bu(t)) \right\}
\]

(9)

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

\[
\begin{align*}
\min_{u(t)} & \quad u(t)^T R u(t) + \dot{x}(t)^T P(t) (B u(t) + s(t)^T Bu(t)) \\
s.t. & \quad u(t) \in U(t) \quad \forall t \in [0,T]
\end{align*}
\]

(10)

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

### B. Safety and Reachability Verification

Parameters \( \gamma_i \) in \( U_i = \left\{ u(t) : \| u(t) - u_o,i(t) \|_2 \leq \gamma_i \right\} \) determines the size of the set of feasible control inputs at each time \( t \). Larger \( \gamma_i \) provides a larger feasible region of \( u(t) \), 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 \( \gamma_i \).

In [23], we developed a binary search algorithm to find the maximal feasible \( \gamma_i \) which satisfies the safety and reachability constraints in (2). We used the barrier function method to determine whether safety and reachability are guaranteed for each value of \( \gamma_i \). The idea is to construct a barrier function \( D_i(x) \) for each \( \gamma_i \) such that, for some \( L < K, D_i(x) \leq L, D_i(x) > K \) for all \( x(t) \in U \), and \( D_i(x) \) is decreasing over any feasible trajectories of \( x(t) \). Thus, if this \( D_i(x) \) exists for each \( \gamma_i \), \( x(t) \) will not enter the unsafe region.

Let \( \gamma_i = \min\{\gamma_i^a, \gamma_i^c\} \). Satisfying \( U_i(t) \) can guarantee safety and reachability if \( A_i^c = A_i \). This result is formally stated using the following theorem based on [23].

**Theorem 1:** If \( A_i^c = A_i \), there exist \( \gamma_i^a \) and \( \gamma_i^c \) such that satisfying \( \| u(t) - u_o,i(t) \|_2 \leq \gamma_i^a \) and \( \| u(t) - u_o,i(t) \|_2 \leq \gamma_i^c \) guarantee safety and reachability with probabilities \( 1 - \epsilon_s \) and \( 1 - \epsilon_r \), respectively.

### C. Selection of Constraints

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

**Proposition 1:** If there exists a ball of radius \( \gamma_{\min} \) such that \( u_o,i \in \{1, \ldots, q\} \) are in the ball, then \( U(t) \neq \emptyset \).

**Proof:** Suppose there exists such a ball with center \( u_0 \). We have \( \| u_0 - u_o,i \|_2 \leq \gamma_{\min} \leq \gamma_i \forall i \in \{1, \ldots, q\} \). Hence, \( u_0 \in U(t) \), and \( U(t) \neq \emptyset \).

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

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

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

By definition of \( u_o,i(t) \) and contraposition, if \( U(t) = \emptyset \), then

\[
\| K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 + K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \leq \gamma_{\min}
\]

(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 \( U(t) = \emptyset \), then either \( \| 1/K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \leq \gamma_{\min} \) or \( \| 1/K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \leq \gamma_{\min} \), or both of them hold.

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

\[
\| K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 + \| K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \\
\geq \frac{\| K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2}{4} + \frac{\| K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2}{4} \\
\geq \gamma_{\min}
\]

(12)

Inequality (12) is satisfied if at least one of \( \| 1/K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \) or \( \| 1/K(t)(\delta_{o,i}(t) - \delta_{o,j}(t))/4 \|_2 \) is satisfied.

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

Denote \( C_{o,i,j} \) as \( C \) with rows indexed by \( \{1, \ldots, p\} \setminus \{A_i \cup A_j\} \). We assume that all systems \( (A_i, C_{o,i,j}) \forall i, j \in \{1, \ldots, q\} \neq j \) are
obtainable. Introduce the KF state estimate $\hat{x}_{\alpha,i,j}(t)$, which is obtained via $y_{\alpha,i,j}(t)$, the output with the measurements indexed by $\{1, \ldots, p\} \setminus (A_{\alpha} \cup A_{j})$.

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

**Proof:** Applying triangle inequality, we have

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

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

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

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

We use inequalities (14) and (15) later to identify the $U_{i,j}$ that leads to infeasibility of QCQP (16). Intuitively, for a certain pair of $\{i, j\} \in \{1, \ldots, p\}$, if the measurements are only affected by the noises, $\| \hat{x}_{\alpha,i}(t) - \hat{x}_{\alpha,i,j}(t)\|_2$ should be smaller than some thresholds. If $A_{\alpha} = A_{i}$ or $A_{\alpha} = A_{j}$, $\hat{x}_{\alpha,i,j}(t)$ should not be biased by $a(t)$. Thus, when $\| \frac{1}{4} K(t)(\hat{x}_{\alpha,i}(t) - \hat{x}_{\alpha,i,j}(t))\|_2 > \frac{1}{4} \gamma_{\min}$, $\hat{x}_{\alpha,i,j}(t)$ can be utilized as a benchmark for checking whether $\hat{x}_{\alpha,i}(t)$ and $\hat{x}_{\alpha,j}(t)$ 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 $\| \frac{1}{4} K(t)(\hat{x}_{\alpha,i}(t) - \hat{x}_{\alpha,i,j}(t))\|_2 > \frac{1}{4} \gamma_{\min}$, which could result in measurements being excluded erroneously. We derive the following theorem to show the probability that $\| \frac{1}{4} K(t)(\hat{x}_{\alpha,i}(t) - \hat{x}_{\alpha,i,j}(t))\|_2 > \frac{1}{4} \gamma_{\min}$ holds during $t \in [0, T]$ is upper-bounded when no adversary is present. We will use this theorem later to eliminate $U_{i,j}(t)$ which may render $U(t) = \emptyset$.

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

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

where $\eta^{i,j} = 4(\lambda_{\max}^i \Gamma_1 + \lambda_{\max}^j \Gamma_2) \gamma_{\min} / \gamma_{\min}^2$, $\hat{x}_{\alpha,i}(t)$ and $\hat{x}_{\alpha,i,j}(t)$ are estimates calculated using KF and measurements indexed by $\{1, \ldots, p\} \setminus A_{\alpha}$ and $\{1, \ldots, p\} \setminus (A_{\alpha} \cup A_{j})$, respectively, $K = \sup_{t \in [0,T]} \{ K(t)\|_2 \}$, $\lambda_{\max}^i = \sup_{t \in [0,T]} \{ \lambda_{\max}(\Sigma_i(t)) \}$, $\lambda_{\max}^j = \sup_{t \in [0,T]} \{ \lambda_{\max}(\Sigma_j(t)) \}$, $\Sigma_i(t)$ and $\Sigma_j(t)$ are the covariance matrices of $(x(t) - \hat{x}_{\alpha,i}(t))$ and $(x(t) - \hat{x}_{\alpha,i,j}(t))$, respectively, $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue of a matrix, $\Gamma_i = E(\sigma_i(0)^T \Sigma_i(0)^{-1} \sigma_i(0))$, $\Gamma_j = E(\sigma_j(0)^T \Sigma_j(0)^{-1} \sigma_j(0))$, $\sigma_i(0) = \hat{x}_{\alpha,i}(0) - x_0$, and $\sigma_j(0) = \hat{x}_{\alpha,i,j}(0) - x_0$.

**Proof:** The proof is analogous to the proof of [23, Th. 1] and we omit the proof due to space constraints.

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

Algorithm 1: Algorithm for Selecting Constraints $U_{i,j}(t)$ that can guarantee Safety and Reachability Properties with Desired Probability.

1: procedure $\mathcal{I}$ Selection($g(K(t), \hat{x}_{\alpha,i}(t), \hat{x}_{\alpha,j}(t), \gamma_{\min}$, $U_{i,j}(t), i,j \in \{1, \ldots, p\}, i \neq j$)
2: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
3: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
4: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
5: while $d_{i,j} > 2\gamma_{\min}$ do
6: if $\Omega^{i,j}$ then
7: $\mathcal{I}(t) \leftarrow \{1, \ldots, q\} \setminus \{i\}$
8: if $\Omega^{i,j}$ then
9: $\mathcal{I}(t) \leftarrow \{1, \ldots, q\} \setminus \{j\}$
10: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
11: for each $i \in \mathcal{I}(t)$ do
12: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
13: if $\Omega^{i,j}$ then
14: $\mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{i\}$
15: if $\Omega^{i,j}$ then
16: $\mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{j\}$
17: if $\Omega^{i,j}$ then
18: $\mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{i\}$
19: if $\Omega^{i,j}$ then
20: $\mathcal{I}(t) \leftarrow \mathcal{I}(t) \setminus \{j\}$
21: if $\Omega^{i,j}$ then
22: $\{i,j\} = \text{arg \ max}_{i,j \in \mathcal{I}(t)} \{d_{i,j}\}$
23: return $\mathcal{I}(t)$

D. Control Strategy Design

Our proposed control design is summarized in Algorithm 2. In lines 2 and 3, we initialize $\mathcal{I}(t)$ and $U(t)$ as the indexes and intersection of all constraints. In line 4, we first check whether $U(t) = \emptyset$. In line 5, if $U(t) = \emptyset$, we utilize $\mathcal{I}$ Selection in Algorithm 1 to identify and eliminate those $U_{i,j}(t)$ which result in $U(t) = \emptyset$ and output $\mathcal{I}(t)$. In line 6, the algorithm involves the existing solver, denoted as QCQP($\mathcal{I}(t)$),
Algorithm 2: Proposed Control Policy that Guarantees Safety and Reachability Constraints under Multiple-Adversary Scenario.

1: procedure Control_Policy(q, Ut_i(t), i ∈ {1, ..., q})
2: I_i(t) ← {1, ..., q}
3: Ut_i(t) ← ∩t∈I_i(t) Ut_i(t)
4: if Ut_i(t) = ∅ then
5: I_i(t) ← I_Selection(q, K_i(t), x_{a,i,t}, x_{a,i,j,t}, γ_{min}, Ut_i(t), i, j ∈ {1, ..., q}, i ≠ j)
6: u(t) ← QCQP(I_i(t)) in (16)
7: return u(t)

at each time t to solve the QCQP with the form

$$\min_{u(t)} \mathbf{u}(t)^T R(t) \mathbf{u}(t) + \mathbf{x}(t)^T P(t) B(t) \mathbf{u}(t) + s(t)^T B(t) \mathbf{u}(t)$$

s.t. $\mathbf{u}(t) \in U_{t_i}(t), i \in I_i(t).$

When there is no attack, the controller attempts to minimize the objective function. Due to the existence of noise, $d_{a,j}$ may deviate from 0 for all $i, j \in \{1, \ldots, q\}$. This may lead to smaller feasible region $U(t)$, and suboptimal performance with respect to expected cost. If all $u_{a,i}(t)$ can be proved to be close to the optimal control $u^*(t)$, the feasibility and performance of the proposed approach can be guaranteed.

Lemma 3: Let $u^*(t) = \frac{1}{2} K_i(t) \hat{x}(t) - \frac{1}{2} R^{1/2} B(t)^T s(t)$. Define $\lambda^2 = \max\{\lambda_{max}(\Sigma(t))\}$, where $\Sigma(t)$ is the covariance matrix of $\hat{x}(t) - \hat{x}(t)$. Define $\eta_i^2 = (\lambda^2 + \lambda_{min}(\Sigma_{t_i}))^{1/2}$ and $\Gamma = \mathbb{E}(e(0)^T \Sigma(t)^{-1} e(t))$. When $\beta = 1$, we have

$$\Pr(\sup_{t \in [0, T]} \|u^*(t) - u_{a,i}(t)\|_2 \leq \gamma_{min}) \geq 1 - \eta_i^2 \quad \forall i \in I_i(t).$$

Proof: Based on the definitions of $u^*(t)$ and $u_{a,i}(t)$, we have

$$\Pr(\sup_{t \in [0, T]} \|u^*(t) - u_{a,i}(t)\|_2 \geq \gamma_{min}) = \Pr(\sup_{t \in [0, T]} \|K_i(t) \mathbf{x}(t) - x_{a,i}(t)\|_2 \geq 2 \gamma_{min}).$$

According to Theorem 2, we have

$$\Pr(\sup_{t \in [0, T]} \|K_i(t) \mathbf{x}(t) - x_{a,i}(t)\|_2 \geq 2 \gamma_{min}) \leq \eta_i^4.$$
Algorithm 3: Algorithm for Computing the Parameters $\{\gamma_i, i \in 1, \ldots, q\}$ and $\gamma_{\text{min}}$ that Ensures Safety and Reachability.

1: procedure \text{Selection}(\varepsilon_i, \varepsilon_r, \text{iter\_times}, K, \lambda^i, \lambda^i_{ij},
      i, j \in 1, \ldots, q, i \neq j)
2: \begin{align*}
\bar{t} &\leftarrow \max\{1 - \varepsilon_i, 1 - \varepsilon_r\} \\
\text{for each } &\bar{t} \in \{1, \ldots, q\} \text{ do}
3: &\bar{P}_{1, \bar{t}} \leftarrow 1, \bar{P}_{1, \bar{t}} \leftarrow (\bar{P}_{1, \bar{t}} - \bar{t})/\text{iter\_times} \\
4: &\gamma_0 \leftarrow \text{Barrier\_Certificate}(\bar{P}_{1, \bar{t}}) \\
5: &\text{Update } \gamma_{\text{min}} \text{ and } i_{\text{min}}. \\
6: &\text{for each } i \in \{1, \ldots, q\} \text{ do}
7: &\eta^{i, \bar{t}} \leftarrow 4(\lambda^i_i \Gamma_t + \lambda^i_{ij} \Gamma_{ij}) R_t^2/\gamma_{\text{min}}^2 \\
8: &\text{Update } \bar{P}_{2, i} \text{ and } \bar{P}_{0, i} \text{ via (20) and (21)}. \\
9: &i \leftarrow i + 1 \\
10: &\text{while } i \leq \text{iter\_times} \text{ do}
11: &\bar{P}_{1, i_{\text{min}}} \leftarrow \bar{P}_{1, i_{\text{min}}} - \bar{P}_{1, \bar{t}} \\
12: &\gamma_{\text{min}} \leftarrow \text{Barrier\_Certificate}(\bar{P}_{1, i_{\text{min}}}) \\
13: &\text{Update } \gamma_{\text{min}} \text{ and } i_{\text{min}}. \\
14: &\text{for each } i \in \{1, \ldots, q\} \text{ do}
15: &\eta^{i, i_{\text{min}}} \leftarrow 4(\lambda^i_i \Gamma_t + \lambda^i_{ij} \Gamma_{ij}) R_t^2/\gamma_{\text{min}}^2 \\
16: &\text{Update } \bar{P}_{2, i} \text{ and } \bar{P}_{0, i} \text{ via (20) and (21)}. \\
17: &\text{if } \sqrt{\bar{P}_{0, i}} \geq \bar{t} \text{ then}
18: &\text{break} \\
19: &i \leftarrow i + 1 \\
20: &\text{if } i > \text{iter\_times} \text{ then}
21: &\text{return } \{\gamma_i, i \in 1, \ldots, q\}, \gamma_{\text{min}}. 
\end{align*}

Since the closed form expression of $P_1$ as a function of $\gamma_i$ is not clear, we utilize a heuristic method to search for proper value of $\gamma_i \forall i \in \{1, \ldots, q\}$ and $\gamma_{\text{min}}$ which satisfies $P_1 \cdot P_2 \geq \max\{1 - \varepsilon_i, 1 - \varepsilon_r\}$ for all $A_i$. The intuition is that we initialize $P_1$ first to compute the corresponding $\gamma_i$ to the candidate $P_1$, and calculate the corresponding $\gamma_{\text{min}} = \min \gamma_i$ for all $i \in \{1, \ldots, q\}$. Here, we assume existence of a function \text{Barrier\_Certificate} that returns the $\gamma_i$. Then we check the lower bound of $P_0$ for all $A_i$ according to inequality (21). If the lower bound is greater than $\max\{1 - \varepsilon_i, 1 - \varepsilon_r\}$ for all $A_i$, the safety and reachability constraints are satisfied. Otherwise, we enlarge $\gamma_{\text{min}}$ by reducing the $P_1$ corresponding to the minimal $\gamma_i$, recalculating this $\gamma_i$ under the updated $P_1$, and checking the lower bounds of $P_0$ for all $A_i$ under new $\gamma_{\text{min}}$. We do this procedure iteratively until the lower bounds of $P_0$ for all $A_i$ are greater than $\max\{1 - \varepsilon_i, 1 - \varepsilon_r\}$ for all $A_i$. 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 $A_i$. Both the controller and the adversary have the knowledge of $A^* = A_i$. However, the controller does not know which sensors in $A_i$ are compromised by the adversary.

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

$$\begin{align*}
\min_{u(t)} &\mathbb{E}\left[\int_0^T ((x(t) - r(t))^T Q (x(t) - r(t)) + u(t)^T R u(t)) dt + (x(T) - r(T))^T F (x(T) - r(T))\right] \\
\text{s.t. } &u(t) \in \mathcal{U}_{\gamma_i}(t), \forall t \in [0, T].
\end{align*}$$

(22)

When solving (7), we do not know which $A_i$ is $A^*$, and $I(t)$ is changing at each time step $t$. Thus, we have to relax the constraints $\mathcal{U}_{\gamma_i}(t)$ for all $i \in I(t)$. Since $A^* = A_i$ is known in the single-adversary scenario, we use the method of Lagrange multipliers to construct the dual problem of (22) rather than relax the constraint $\mathcal{U}_{\gamma_i}(t)$ when solving the HJB equation. Denote the Lagrange multiplier corresponding to constraint $\mathcal{U}_{\gamma_i}(t)$ as $\lambda(t)$. The dual problem of (22) is [28]

$$\begin{align*}
\max_{u(t)} &\min_{\lambda(t)} \mathbb{E}\left[\int_0^T ((x(t) - r(t))^T Q (x(t) - r(t)) + u(t)^T R u(t) - \lambda(t) \gamma_i^2 - ||u(t) - u_{\text{opt}}(t)||_2^2) dt \\
&+ (x(T) - r(T))^T F (x(T) - r(T))\right] \\
\text{s.t. } &\lambda(t) \geq 0, \forall t \in [0, T].
\end{align*}$$

(23a)

(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 $\lambda$ to obtain a lower bound on the solution to (20), and hence a lower bound on the value function. The inner minimization problem of (23) can be rewritten as

$$\begin{align*}
\min_{u(t)} &\mathbb{E}\left[\int_0^T ((\bar{x}(t) - \bar{r}(t))^T \bar{Q}(t)(\bar{x}(t) - \bar{r}(t)) \\
&+ u(t)^T (\lambda I + R) u(t) - \bar{x}(t)^T M(u(t) u(t) - \lambda \gamma_i^2) dt \\
&+ (\bar{x}(T) - \bar{r}(T))^T \bar{F}(\bar{x}(T) - \bar{r}(T))\right]
\end{align*}$$

(24)

where $\bar{x}(t) = [x(t)^T, \bar{x}^i(t)^T, s(t)^T]^T, \bar{r}(t) = [r(t)^T, 0, 0]^T$.

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

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

$$\begin{align*}
u^*(t) = &- \frac{1}{2} (R + \lambda I)^{-1} (B^T \bar{P}(t) - M(t)^T) \bar{x}(t) \\
&- \frac{1}{2} (R + \lambda I)^{-1} B^T \bar{s}(t)
\end{align*}$$

(25)

where $\bar{B} = \begin{bmatrix} B & B & 0 \end{bmatrix}^T$.

$$\begin{align*}
\bar{P}(t) = &\begin{bmatrix} A^T \bar{P}(t) + \bar{P}(t) A + 2Q \\ - \frac{1}{2} \bar{B}^T \bar{P}(t) - M(t)^T (R + \lambda I)^{-1} (B^T \bar{P}(t) - M(t)^T) \\
\hat{s}(t) = &\begin{bmatrix} - \bar{A}^T + \frac{1}{2} \bar{P}(t) \bar{B} (R + \lambda I)^{-1} B^T \\ - \frac{1}{2} M(t)^T \bar{B} \end{bmatrix} \tilde{s}(t) + (2\tilde{Q} - \tilde{P}(t) H) \tilde{r}(t)
\end{align*}$$

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

Define the optimal value of (22) as $V_1$, the value of (22) using the solution of QCQP (10) as $V_2$, and the value of (22) using (25) as...
I, A. The worst case probability that the safety and/or reachability constraints are violated is designed as \( V_3 \). Based on the weak duality [28], \( V_3 \leq V_1 \). Note that when \( \lambda = 0 \), \( V_3 = V_2 \). Since 0 is a feasible solution of \( \lambda \) and (23a) maximizes over \( \lambda \), we have that \( V_3 \leq V_3 \), which further yields that \( V_3 \) is a tighter bound over \( V_1 \) than \( V_2 \).

V. Case Study

In this section, we evaluate the proposed policy via a numerical case study. Consider a system with two states, two inputs, and six sensors. There are \( q = 3 \) attack patterns, denoted as \( A_1 = \{1, 4\} \), \( A_2 = \{2, 5\} \), and \( A_3 = \{3, 6\} \). The adversary selects \( u(t) = 0 \) with proper dimensions. Matrix \( C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \). The noises \( w(t) \) and \( v(t) \) are Gaussian with means 0 and covariances \( \Sigma_w = 0.1I \) and \( \Sigma_v = 0.1I \). 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 \( x_0 = (0.0001, -0.0001)^T \). We choose that \( \Phi_{\alpha,1}(0) = 10I \) and \( \Phi_{\alpha,2}(0) = (0, 0)^T \). The system is required to avoid the set of unsafe states \( U = \{ x : 0.2^2 - (x_1 - 0.5001)^2 - (x_2 + 0.0001)^2 > 0 \} \) and reach the set of goal states \( G = \{ x : 0.2^2 - (x_1 - 1.0001)^2 - (x_2 + 0.0001)^2 \geq 0 \} \) at \( T = 10 \). The worst case probability that the safety and reachability constraints are violated are designed as \( \epsilon = 0.3 \) 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 \( u_{1,2}(t) \) and \( u_{1,2}(t) \) which eliminate the measurements of sensors indexed by \( A_1 \) and \( A_2 \), respectively. The performances of the four controllers are shown in Figs. 1 and 2. As shown in Fig. 1, the proposed controller and \( u_{1,2}(t) \) can satisfy the safety and reachability constraints, while the LQG controller using all measurements and \( u_{1,2}(t) \) are biased by the attack and violate the constraints. From Fig. 2, we can see that the cost of proposed controller converges to the cost of \( u_{1,2}(t) \), which is less than the costs of the LQG controller using all measurements and \( u_{1,2}(t) \). From the results shown in Figs. 1 and 2, the proposed controller guarantees safety and reachability, and at the same time provides comparable cost performance with \( u_{1,2}(t) \). This results from the fact that after the function \( L \)_Selection eliminates the constraints \( U_{1,2}(t) \) and \( U_{1,2}(t) \), the controller is not biased by the adversary. The LQG controller \( u_{1,2}(t) \) is optimal, but the attack pattern \( A^* = A_2 \) is not known by the controller a priori. Thus, in real world, \( u_{1,2}(t) \) is not realizable because \( A^* = A_2 \) is only known by the adversary.

VI. Conclusion

This article 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 Secur. Privacy, vol. 11, no. 4, pp. 28–37, Jul./Aug. 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. IEEE, vol. 100, no. 1, pp. 283–299, Jan. 2012.
[3] C. Kwon and I. Hwang, “Reachability analysis for safety assurance of cyber-physical systems against cyber attacks,” IEEE Trans. Autom. Control, vol. 63, no. 7, pp. 2272–2279, Jul. 2018.
[4] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Trans. Inf. Syst. Secur., 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. 1st Int. Conf. High Confidence Networked Syst., 2012, pp. 55–64.
[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. Power Syst., vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
[7] Z.-H. Yu and W.-L. Chin, “Blind false data injection attack using PCA approximation method in smart grid,” *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[8] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in *Proc. Preprints 1st workshop Secure Control Syst.*, 2010, pp. 1–6.

[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. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

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

[11] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[12] R. Zhang and P. Venkitasubramaniam, “A game theoretic approach to analyze false data injection and detection in LQG system,” in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2017, pp. 427–431.

[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, 2020, Art. no. 109117.

[15] Z. Wu, F. Albaiw, 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, 2018, Art. no. 173.

[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. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[17] Y. Shoukry et al., “SMT-based observer design for cyber-physical systems under sensor attacks,” *ACM Trans. Cyber-Phys. Syst.*, 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. Control Netw. Syst.*, vol. 4, no. 1, pp. 82–92, Mar. 2017.

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

[20] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, “Preserving physical safety under cyber attacks,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6285–6300, Aug. 2019.

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

[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. Ind. Inform.*, vol. 16, no. 4, pp. 2716–2725, Apr. 2020.

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

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

[25] D. E. Kirk, *Optimal Control Theory: An Introduction*. Chelmsford, MA, USA: 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 *Proc. 51st IEEE Conf. Decis. Control*, 2012, pp. 668–674.

[27] G. Torrisi, S. Grammatico, R. S. Smith, and M. Morari, “A projected gradient and constraint linearization method for nonlinear model predictive control,” *SIAM J. Control Optim.*, 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.