A Framework for Joint Attack Detection and Control Under False Data Injection

Luyao Niu(✉) and Andrew Clark

Worcester Polytechnic Institute, Worcester, MA 01609, USA
{lniu,aclark}@wpi.edu

Abstract. In this work, we consider an LTI system with a Kalman filter, detector, and Linear Quadratic Gaussian (LQG) controller under false data injection attack. The interaction between the controller and adversary is captured by a Stackelberg game, in which the controller is the leader and the adversary is the follower. We propose a framework under which the system chooses time-varying detection thresholds to reduce the effectiveness of the attack and enhance the control performance. We model the impact of the detector as a switching signal, resulting in a switched linear system. A closed form solution for the optimal attack is first computed using the proposed framework, as the best response to any detection threshold. We then present a convex program to compute the optimal detection threshold. Our approach is evaluated using a numerical case study.

Keywords: False data injection attacks · Control system · Detection threshold · LQG control · K-L divergence · Stealthiness

1 Introduction

Distributed sensors provide control systems with rich data. However, open and insecure communication between the sensors and plant exposes the system to threats from false data injection attacks. Control systems are vulnerable to false data injection attacks for the following reasons. Sensors might be physically unprotected and hence vulnerable to attacks. Compared to directly attacking the plant, the adversary incurs very low cost when attacking the sensors. Moreover, the false measurements can bias the decision of the controller and hence degrade the system performance [3] and cause safety risks [17].

The main challenge of mitigating false data injection attacks initiated by intelligent adversaries is that false data injection attacks are fundamentally different from stochastic disturbances whose distributions are typically assumed to be given and independent of the control policy [3]. The adversary, however, is strategic and hence its attack action will be tailored to the estimation and control policies that are used by the targeted system.

This work was supported by NSF grant CNS-1656981.

T. Alpcan et al. (Eds.): GameSec 2019, LNCS 11836, pp. 352–363, 2019.
https://doi.org/10.1007/978-3-030-32430-8_21

Due to the adversary's strategic response, designing a detection and control mechanism with fixed parameters could result in a degradation of control performance. An alternative approach is to develop a time-varying detection and randomized measurement selection strategy in order to increase the uncertainty of the adversary and thus reduce the impact of the attack. This approach is in the spirit of moving target defense [20], which has recently been proposed for control and cyber-physical systems. To the best of our knowledge, however, such detection strategies have not been proposed in the LQG setting.

In this paper, we focus on a system equipped with a Kalman filter, a detector and an LQG controller under false data attacks. We adopt the Stackelberg setting to capture the interplay between the controller and adversary. The adversary aims at degrading LQG control performance by introducing false measurements to a subset of sensors while being stealthy. The set of possibly compromised sensors is known to the controller, since some sensors (e.g., GPS signal [17]) are easier to tamper with, while others are more difficult to manipulate (e.g., inertial measurement unit serves as backup for GPS spoofing attack [14]). The controller computes a detection threshold at each time step to minimize the LQG cost function. Given the time varying threshold, the controller computes the control law at each time step by randomly using either all measurements or the measurements from the secured sensors to eliminate the impact of false data injected by the adversary. The proposed framework jointly models the attack, detection and LQG control, and consequently improves the system's resilience. We make the following specific contributions:

- We model the interaction between the system and adversary using a zero-sum Stackelberg game, in which the controller is the leader and the adversary is the follower. A switched linear system is used to model the system behavior, where switches between modes occur due to attack detection.
- We formulate a convex optimization problem for the attacker to compute the optimal attack sequence. By solving the convex program, we show that the optimal attack for the attacker is a zero-mean Gaussian noise. We derive a closed form solution for the covariance matrix of the optimal attack.
- We generalize our analysis of optimal attack under single stage case to multi-stage case. We show that the optimal attack sequence is a sequence of zero-mean Gaussian noise and give the closed form solution for the optimal covariance at each time step. We formulate a convex optimization problem to compute the optimal detection thresholds for the controller.
- A numerical case study is used to evaluate the proposed approach. The results show that the proposed approach outperforms the attack detector designed with fixed parameter.

The remainder of this paper is organized as follows. Section 2 presents related work. Section 3 gives the system model and problem formulation. Section 4 presents the proposed solution. Section 5 contains an illustrative case study. Section 6 concludes the paper.

2 Related Work

False data injection attacks have been extensively analyzed from the adversary's perspective in the existing literature. False data injection attack against networked control system equipped with Kalman filter and power system are analyzed in [12] and [10], respectively. In [7], the worst-case stealthy false data injection attack strategy is proposed against Kullback-Leibler (K-L) divergence based detector is proposed. In this work, we consider the interaction between the detector design and adversary. Hence we not only give the optimal attack strategy, but also present a game-theoretic approach to analyze how to design a resilient detector to counter false data injection attacks, which is absent in [7].

Resilient control in adversarial environments has been extensively studied. Robust control and secure state estimation against false data injection attacks has been studied in [4,5,13,15] and references therein. In this work, we focus on the detection of false data injection attack under LQG setting. One alternative approach to thwart false data injection initiated by adversary that is knowledgeable in system model and detection and control strategies is to limit its information by committing to a time varying detection and control mechanism. A randomized detection threshold for K-L divergence based detectors is proposed in [9]. While [9] focuses on minimizing estimation error, in this work, we fill the gap between LQG control in adversarial environments and the detection strategy under false data injection attack. Moving target defense has been applied in literature to limit the adversary's knowledge of the system model, e.g., system dynamics [20]. The idea of [20] is to change the system dynamics randomly to limit the knowledge of the adversary, while this works aims at designing a time varying detection threshold with fixed system dynamics. Moreover, the metric in this work is set as the LQG cost function, while contributions [19,20] focuses on the information metric (e.g., Fisher information matrix) from the adversary's perspective. A resilient LQG control under false data injection attacks has been proposed for LTI system in [4]. In [4], a resilient control strategy is proposed so that the worst case damage introduced by the adversary is limited. However, no detection mechanism is considered in [4].

In addition to control-theoretic approaches, game theory is also used to study the interaction between the system and adversary [1,11,21]. These models consider the Nash setting, in this paper we consider a Stackelberg setting which is applicable to a variety of CPS domains [16]. Contribution [22] focuses on picking pre-designed detector among a configuration library. In this work, we investigate the problem of jointly modeling the attack, detection and LQG control performance. Stackelberg setting is adopted in [6,18] to compute a detector tuning. A fixed detection threshold is considered in [18], while a time-varying threshold is considered in this work. While an exhaustive search based approach is given [6] to select an adaptive detection threshold, we consider the LQG control performance in this work and show that the time-varying detection threshold can be obtained by solving a convex program.

3 System Model and Problem Formulation

In this section, we present the system model and problem formulation.

3.1 System Model

Consider a discrete-time LTI system with time index $k = 1, 2, \cdots$, as follows:

$$\mathbf{x}_{k+1} = A\mathbf{x}_k + B\mathbf{u}_k + \mathbf{w}_k, \quad \mathbf{y}_k = C\mathbf{x}_k + \mathbf{v}_k$$

where $\mathbf{x}_k \in \mathbb{R}^n$ is the system state, $\mathbf{u}_k \in \mathbb{R}^p$ is the input, $\mathbf{y}_k \in \mathbb{R}^m$ is the output, and $\mathbf{w}_k \in \mathbb{R}^n$ and $\mathbf{v}_k \in \mathbb{R}^m$ are i.i.d. stochastic disturbance with distributions $\mathbf{w}_k \sim \mathcal{N}(0, \Sigma_{\mathbf{w}})$ and $\mathbf{v}_k \sim \mathcal{N}(0, \Sigma_{\mathbf{v}})$, respectively. Matrices A, B and C are with proper dimensions. The initial state $\mathbf{x}_0$ is assumed to follow a distribution $\mathbf{x}_0 \sim \mathcal{N}(0, \Sigma_{\mathbf{x}})$. The disturbances $\mathbf{w}_k$ and $\mathbf{v}_k$ are assumed to be independent of each other and independent of the historical values of $\mathbf{w}$, $\mathbf{v}$, $\mathbf{u}$ and $\mathbf{y}$.

The state estimation $\hat{\mathbf{x}}_k$ is computed using a Kalman filter [8] as $\hat{\mathbf{x}}_{0|-1} = 0$, $\hat{\mathbf{x}}_{k+1|k} = A\hat{\mathbf{x}}_k + B\mathbf{u}_k$, $P_{0|-1} = \Sigma_{\mathbf{x}}$, $P_{k+1|k} = AP_kA^T + \Sigma_{\mathbf{w}}$, $K_k = P_{k|k-1}C^T(CP_{k|k-1}C^T + \Sigma_{\mathbf{v}})^{-1}$, $\hat{\mathbf{x}}_k = A\hat{\mathbf{x}}_{k|k-1} + K_k(\mathbf{y}_k - C\hat{\mathbf{x}}_{k|k-1})$, and $P_k = P_{k|k-1} - K_kCP_{k|k-1}$. The Kalman filter is assumed to be in steady state and the error covariance and Kalman gain are hence represented as $P = \lim_{k\to\infty} P_{k|k-1}, K = PC^T(CPC^T + \Sigma_{\mathbf{v}})^{-1}$ [8]. Denote the residue at each time step k as $\mathbf{z}_{k+1} = \mathbf{y}_{k+1} - C(A\hat{\mathbf{x}}_k + B\mathbf{u}_k)$. Then the state estimation can be rewritten as $\hat{\mathbf{x}}_{k+1} = A\hat{\mathbf{x}}_k + B\mathbf{u}_k + K[\mathbf{y}_{k+1} - C(A\hat{\mathbf{x}}_k + B\mathbf{u}_k)]$.

3.2 Adversary Model

We consider an intelligent adversary that can corrupt a subset of sensors by injecting false measurements. The injected false measurements provide the system biased outputs $\tilde{\mathbf{y}}_k$ at each time k and hence misleads the controller. At each time step k, the measurements perceived by the system can be characterized as follows: $\tilde{\mathbf{y}}_k = C\mathbf{x}_k + \mathbf{v}_k + \mathbf{a}_k$, where $\mathbf{a}_k$ is an arbitrary measurement injected by the adversary. The residue under false data injection attack is computed as $\tilde{\mathbf{z}}_{k+1} = \tilde{\mathbf{y}}_{k+1} - C(A\hat{\mathbf{x}}_k + B\mathbf{u}_k)$.

The adversary can perform false data injection attacks on a certain set of sensors Υ. Thus the support of injected false measurements $\text{supp}(\mathbf{a}_k) \subseteq \Upsilon$. We assume that Υ is fixed and known to both the system and adversary. The reason that the adversary can only corrupt the measurements of sensors in Υ is that the adversary might only be co-located with a subset of sensors, and it is only capable of corrupting the sensors that are exposed and unattended (e.g., distributed sensors in networked control system [12,17]). For instance, in [14], inertial measurements are used as a secure backup in the event of a GPS spoofing attack. For notation simplicity, we denote the set of sensors Υ as compromised sensors and the set of sensors outside Υ as the secured sensors.

Denote the information available to the adversary at time k as $I_k^{\mathcal{A}}$. Then the information set is represented as $I_k^{\mathcal{A}} = \{\mathbf{u}_0, \cdots, \mathbf{u}_k\} \cup \{\mathbf{y}_0^{\mathcal{A}}, \cdots, \mathbf{y}_k^{\mathcal{A}}\} \cup$

$\{\mathbf{x}_0, \cdots, \mathbf{x}_k\}$, where $\mathbf{y}_k^{\mathcal{A}}$ is the measurement from the compromised sensors. The information $I_k^{\mathcal{A}}$ captures the worst-case adversary model. Denote the set of all possible information set available to the adversary as $\mathcal{I}_k^{\mathcal{A}}$. An attack policy for the adversary $\tau_k : \mathcal{I}_k^{\mathcal{A}} \mapsto \mathbb{R}^{\text{supp}(\mathbf{a}_k)}$ is a function mapping the set of possible information to the set of false measurements at time k. Let $\boldsymbol{\tau} = \{\tau_k : k = 0, 1, \cdots, \}$ be the sequence of attack policies over time.

3.3 Controller Model

Assume the matrices A, B, C, $\Sigma_{\mathbf{w}}$ and $\Sigma_{\mathbf{v}}$ are known to the system and adversary. Denote the information available to the system at each time step k as I_k. The system knows the control inputs up to time k and the outputs up to time k. Therefore, the information set I_k is represented as $I_k = \{\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_k\} \cup \{\tilde{\mathbf{y}}_0, \tilde{\mathbf{y}}_1, \cdots, \tilde{\mathbf{y}}_k\}$. Denote the set of all possible I_k at time k as $\mathcal{I}_k$.

The system implements LQG control $\mathbf{u}_k = -L_k \hat{\mathbf{x}}_k$ to minimize a cost function in quadratic form as follows:

$$J = \mathbb{E}\left\{\sum_{k=0}^{N} \left(\mathbf{x}_k^T Q_k \mathbf{x}_k + \mathbf{u}_k^T R_k \mathbf{u}_k\right)\right\}, \tag{1}$$

where Q_k and R_k are symmetric positive definite matrices for all k, respectively, and L_k is the controller gain. The state estimation $\hat{\mathbf{x}}_k$ is determined by the measurements that the system uses. Based on the detection result, which is further jointly determined by the system's strategy and adversary's strategy, the system decides if it will only consider the measurements from secured sensors or it will consider measurements from all sensors. Taking the detection result as a switching signal, we model the system's choices over sensors by formulating the following switched linear system: $\mathbf{x}_{k+1} = A\mathbf{x}_k + B\mathbf{u}_k + \mathbf{w}_k, \mathbf{y}_k = C_{\theta_k}\mathbf{x}_k + \mathbf{v}_k$, where $\theta_k \in \Theta = \{0, 1\}$ is the mode index defined as $\theta_k = 0$ if no alarm is triggered from the detector and $\theta_k = 1$ if an alarm is triggered from the detector. Matrix C_{θ_k} models the selection of the sensor measurements for each time step k. Let $C[i]$ denote the ith row of matrix C. Then for each row i and time k, matrix C_{θ_k} is defined as follows: $C_{\theta_k}[i] = \mathbf{0}_n$ if $\theta_k = 0$ and $C_{\theta_k}[i] = C[i]$ if $\theta_k = 1$, with $\mathbf{0}_n$ being zero vector of length n. Using matrix C_{θ_k}, the jump between modes of the switched linear system captures the system's choice over sensors. If no alarm is sounded, then the output $\mathbf{y}_k$ is computed using the measurements from all sensors. In this mode, the control performance could be potentially degraded since the adversary can inject false measurements and bias the system's control decision. If an alarm is triggered by the detector, then the output $\mathbf{y}_k$ is computed using the measurements obtained from the subset of sensors that are secured. In this mode, although the false measurements injected by the adversary are eliminated, system performance would degrade under benign environment since the state estimation $\hat{\mathbf{x}}$ might be inaccurate when only using measurements from a subset of sensors. Thus, the system needs to carefully design its detection threshold and henceforth determine the mode θ_k at each time step.

Let $\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k) = \int f_{\tilde{\mathbf{z}}}(\mathbf{t}) \log \frac{f_{\tilde{\mathbf{z}}}(\mathbf{t})}{f_{\mathbf{z}}(\mathbf{t})} \, \mathrm{d}\mathbf{t}$ be the K-L divergence between compromised residue $\tilde{\mathbf{z}}_k$ and residue $\mathbf{z}_k$ [9,21]. The K-L divergence represents how the realized residue under attack differs from the expected residue without attack. From the adversary's perspective, the K-L divergence should be small to fool the controller who cannot distinguish the deviation caused by measurement noise $\mathbf{v}_k$ and attack $\mathbf{a}_k$. Given a detection threshold γ_k at time step k, an alarm will be triggered from the detector if $\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k) > \gamma_k$, and correspondingly the operation mode $\theta_k = 1$. Otherwise no alarm will be triggered and $\theta_k = 0$. Thus we have that the mode at each time k is determined as $\theta_k = 0$ if $\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k) \leq \gamma_k$ and $\theta_k = 1$ if $\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k) > \gamma_k$. To implement the detector, we need to evaluate the K-L divergence $\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k)$, which requires the probability distributions of the residue $\mathbf{z}_k$ of the legitimate system and the residue $\tilde{\mathbf{z}}_k$ under false data injection attack. The distribution of the residue $\mathbf{z}_k$ is identical to that of the additive noise $\mathbf{v}_k$, i.e., $\mathbf{z}_k \sim \mathcal{N}(0, \Sigma_{\mathbf{v}})$. The probability distribution of the compromised residue $\tilde{\mathbf{z}}_k$ can be evaluated numerically by observing the historical residue [2]. While the residues of the sensors under attack have unknown distribution, we can leverage Theorem 1 in Sect. 4, which states that the optimal attack strategy is a zero-mean ergodic Gaussian random process. Hence, without loss of generality (since we assume that the adversary chooses the optimal strategy), we assume that the residue sequence $\{\tilde{\mathbf{z}}_k\}$ is ergodic and the K-L divergence can be computed using known detection algorithms [2].

A deterministic control policy $\mu_k : \mathcal{I}_k \mapsto \mathbb{R}$ at each time step k is a function mapping the set of information $\mathcal{I}_k$ to a detection threshold γ_k. Let $\boldsymbol{\mu} = \{\mu_k : k = 0, 1, \cdots, \}$ be the sequence of control policies over time. Then the objective of the system is to compute a sequence of control policies $\boldsymbol{\mu}$ such that the cost function (1) is minimized.

3.4 Problem Formulation

The problem we investigate is formulated as $\min_{\boldsymbol{\mu}} \max_{\boldsymbol{\tau}} \mathbb{E}\{\sum_{k=0}^{N}(\mathbf{x}_k^T Q_k \mathbf{x}_k + \mathbf{u}_k^T R_k \mathbf{u}_k)\}$, where the expectation is over $\mathbf{w}_k$, $\mathbf{v}_k$, θ_k, and $\mathbf{x}_0$. The formulation can be interpreted as a two-player zero-sum Stackelberg game, in which the system computes a sequence of detection threshold, and the adversary chooses the set of false measurements to inject. In the following section, we solve the problem by computing the Stackelberg equilibrium.

4 Solution Approach

In this section, we give the proposed solution approach. First, we rewrite the system dynamics for state vector $\bar{\mathbf{x}}_k = [\mathbf{x}_k, \hat{\mathbf{x}}_k]^T \in \mathbb{R}^{2n}$ as $\bar{\mathbf{x}}_{k+1} = \bar{A}_k \bar{\mathbf{x}}_k + W_k$, where $\bar{A}_k = \begin{bmatrix} A & -BL_k \\ KC_{\theta_{k+1}} A & A - BL_k - KC_{\theta_{k+1}} A \end{bmatrix}$, and $W_k = [\mathbf{w}_k, KC_{\theta_{k+1}} \mathbf{w}_k + K\mathbf{v}_{k+1} + K(1 - I_{\theta_{k+1}})\mathbf{a}_{k+1}]^T$, where indicator function $I_{\theta_{k+1}} = 0$ when $\theta_{k+1} = 0$ and $I_{\theta_{k+1}} = 1$ when $\theta_{k+1} = 1$. Denote the matrices $\bar{A}_k$ and W_k when $\theta_{k+1} = \theta$ as $\bar{A}_k^{\theta}$ and W_k^{θ}, respectively. Let $\Sigma_k = \mathbb{E}\{\bar{\mathbf{x}}_k \bar{\mathbf{x}}_k^T\}$. Given $\mathbf{u}_k = -L_k \hat{\mathbf{x}}_k$, the cost

function (1) can be rewritten as $J = \sum_{k=0}^{N} \mathbb{E}\left\{\bar{\mathbf{x}}_k^T H_k \bar{\mathbf{x}}_k\right\} = \sum_{k=0}^{N} \mathrm{tr}\left(H_k \Sigma_k\right)$ where $H_k = \begin{bmatrix} Q_k & \mathbf{0} \\ \mathbf{0} & L_k^T R_k L_k \end{bmatrix}$, and $\mathrm{tr}(\cdot)$ is the trace operator. The evolution of matrix Σ_k is given by

$$\Sigma_{k+1} = \mathbb{E}\left\{\left(\bar{A}_k \bar{\mathbf{x}}_k + W_k\right)\left(\bar{A}_k \bar{\mathbf{x}}_k + W_k\right)^T\right\} = G(\Sigma_k) + \bar{W}_k + F(\Lambda_{k+1}),$$

where $G(\Sigma_k) = \mathbb{E}\{\bar{A}_k \bar{\mathbf{x}}_k \bar{\mathbf{x}}_k^T \bar{A}_k^T\} = p_k^0(q_{k+1}^{01} \bar{A}_k^1 \Sigma_k \bar{A}_k^{1^T} + q_{k+1}^{00} \bar{A}_k^0 \Sigma_k \bar{A}_k^{0^T}) + p_k^1 (q_{k+1}^{11} \bar{A}_k^1 \Sigma_k \bar{A}_k^{1^T} + q_{k+1}^{10} \bar{A}_k^0 \Sigma_k \bar{A}_k^{0^T})$, $\bar{W}_k = \mathbb{E}\{W_k W_k^T\} = p_k^0(q_{k+1}^{01} \underline{W}^1 + q_{k+1}^{00} \underline{W}^0) + p_k^1(q_{k+1}^{11} \underline{W}^1 + q_{k+1}^{10} \underline{W}^0)$, $F(\Lambda_{k+1}) = (p_k^0 q_{k+1}^{00} + p_k^1 q_{k+1}^{10}) \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & K \Lambda_{k+1} K^T \end{bmatrix}$, $\underline{W}^1 = \begin{bmatrix} \Sigma_{\mathbf{w}} & \underline{P}^1 \\ \underline{P}^1 & \bar{P}^1 \end{bmatrix}$, $\underline{W}^0 = \begin{bmatrix} \Sigma_{\mathbf{w}} & \underline{P}^0 \\ \underline{P}^0 & \bar{P}^0 \end{bmatrix}$, $\underline{P}^1 = K C^1 \Sigma_{\mathbf{w}} C^{1^T} K^T, \bar{P}^1 = \underline{P}^0 + K \Sigma_{\mathbf{v}} K^T$, $\underline{P}^0 = K C^0 \Sigma_{\mathbf{w}} C^{0^T} K^T$, $\bar{P}^0 = \underline{P}^0 + K \Sigma_{\mathbf{v}} K^T$, p_k^θ is the probability of the system being at mode θ at time k, $q_{k+1}^{\theta\theta'}$ is the transition probability from mode θ to θ', and Λ_{k+1} is the covariance matrix for injected false measurement $\mathbf{a}_{k+1}$.

In the following, we derive the optimal attack strategy and controller's strategy. At time step k', the adversary solves the following problem:

$$\max_{\mathbf{a}_{k':N}} \quad \sum_{k=k'}^{N} \mathrm{tr}\left(H_k \Sigma_k\right) \tag{2a}$$

$$\text{subject to} \quad \Sigma_k = G(\Sigma_{k-1}) + \bar{W}_k + F(\Lambda_k),\ \forall k = k', \cdots, N \tag{2b}$$

$$\mathcal{D}(\tilde{\mathbf{z}}_k || \mathbf{z}_k) \le \gamma_k,\ \forall k = k', \cdots, N \tag{2c}$$

$$\Sigma_k \succeq 0,\ \forall k = k', \cdots, N \tag{2d}$$

The objective of the adversary is to maximize the cost function J. Constraint (2b) models the evolution of matrix Σ. Constraint (2c) requires the adversary to design its attack signal such that the system stays in mode *0* so that the injected false measurements can bias the system. Constraint (2d) guarantees the covariance matrix Σ is well defined. Substituting constraint (2b) into the objective function (2a), we observe that the adversary maximizes the cost J in two ways: (i) increase the probability of being at mode *0*, and (ii) increase the covariance matrix Λ. The following theorem characterizes the optimal attack [7].

Theorem 1. *The optimal attacks* $\mathbf{a}_{0:N}^* = [\mathbf{a}_0^*, \cdots, \mathbf{a}_N^*]^T$ *are zero-mean and Gaussian.*

Given Theorem 1, the K-L divergence $\mathcal{D}(\tilde{\mathbf{z}}||\mathbf{z})$ can be represented as $\mathcal{D}(\tilde{\mathbf{z}}||\mathbf{z}) = \frac{1}{2}\left(\mathrm{tr}\left(\Sigma_{\mathbf{v}}^{-1}\Lambda\right) - m + \log\left(\det(\Sigma_{\mathbf{v}})/\det(\Lambda)\right)\right)$. Assume mode switch reaches stationary probability distribution. Then we simply denote the probability of being at mode *0* and *1* at time k as p_k^0 and p_k^1, respectively. Substituting constraint (2b) into (2a), we can convert problem (2) to a convex program

$$\max_{\mathbf{\Lambda}_{k':N}} \quad p^0_{k'}\mathrm{tr}\left(H_{k'}\bar{\Lambda}_{k'}\right) + p^0_{k'+1}p^0_{k'}\mathrm{tr}\left(H_{k'+1}\bar{A}^0_k\bar{\Lambda}_{k'}\bar{A}^{0^T}_{k'}\right)$$
$$+ p^1_{k'+1}p^1_{k'}\mathrm{tr}\left(H_{k'+1}\bar{A}^1_k\bar{\Lambda}_{k'}\bar{A}^{1^T}_{k'}\right) + \underline{J}_{k'} \tag{3a}$$

$$\text{subject to} \quad \frac{1}{2}\left(\mathrm{tr}\left(\Sigma^{-1}_{\mathbf{v}}\Lambda\right) - m + \log\left(\frac{\det(\Sigma_{\mathbf{v}})}{\det(\Lambda)}\right)\right) \leq \gamma_k,\ \forall k = k', \cdots, N \tag{3b}$$

$$\Lambda_k \succeq 0,\ \forall k = k', \cdots, N \tag{3c}$$

where $\underline{J}_{k'}$ contains the terms that are independent of $\Lambda_{k'}$.

Solving optimization problem (3), then the covariance of optimal attack at time k is characterized using the following theorem.

Theorem 2. *The covariance Λ^*_k of the optimal attack $\mathbf{a}^*_k$ is computed as*

$$\Lambda^*_k = \left(-\frac{1}{\beta_k}\Phi_k + \Sigma^{-1}_{\mathbf{v}}\right)^{-1}, \tag{4}$$

where $\underline{A}^0 = A - BL_k - KC^0A$, $\underline{A}^1 = A - BL_k - KC^1A$,

$$\Phi_k = 2p^0_k K^T L^T R_k L^T K + 2p^0_{k+1}p^0_k K^T\Big(L^T_k B^T Q_{k+1}BL_k + \underline{A}^{0^T}L^T_{k+1}R_{k+1}$$
$$L_{k+1}\underline{A}^{0^T}\Big)K + 2p^1_{k+1}p^1_k K^T\Big(L^T_k B^T Q_{k+1}BL_k + \underline{A}^{1^T}L^T_{k+1}R_{k+1}L_{k+1}\underline{A}^{1^T}\Big)K,$$

p^θ_k is the probability of system being in mode θ at time k, and β_k satisfies

$$\sum_i\left[\frac{\beta_k}{\beta_k - \Lambda_{k,i}} + \log\left(\frac{\beta_k - \Lambda_{k,i}}{\beta_k}\right)\right] = m + 2\gamma, \tag{5}$$

and $\Lambda_{k,i}$ are the eigenvalues of $\Phi_k\Sigma_{\mathbf{v}}$.

Before proving Theorem 2, we first present the a preliminary proposition.

Proposition 1. *Let $\{\lambda_i : \lambda_i \geq 0\}$ be a set of non-negative real numbers and sorted in descending order. Consider function $g(\beta) : (-\infty, 0) \cup (\Lambda_1, +\infty) \mapsto (0, +\infty)$ defined as $g(\beta) = \sum_i\left[\frac{\beta}{\beta-\Lambda_i} + \log\left(\frac{\beta-\Lambda_i}{\beta}\right)\right]$. Then given any positive number $\bar{g}$, there exists some $\beta > 0$ such that $g(\beta) = \bar{g}$.*

Proof. Proposition 1 follows from the fact that function $g(\beta)$ is continuous and monotone decreasing with respect to β. □

Proof. (Proof of Theorem 2.) We prove by induction backwards. First, (4) and (5) hold for time $k = N$ since $H_{k+1} = \mathbf{0}$.

Next, suppose (4) and (5) hold up to time $k' + 1$. We then induct one time step backwards. We prove (4) and (5) hold at time k' by verifying the KKT conditions of (3) at time k'.

We start with the stationarity condition. The Lagrangian is represented as

$$\mathcal{L}_{k'} = -p^0_{k'}p^0_{k'+1}\mathrm{tr}\left(H_{k'+1}\bar{A}^0_{k'}\bar{\Lambda}_{k'}\bar{A}^{0^T}_{k'}\right) - p^0_{k'}p^1_{k'+1}\mathrm{tr}\left(H_{k'+1}\bar{A}^1_{k'}\bar{\Lambda}_{k'}\bar{A}^{1^T}_{k'}\right)$$
$$-p^0_{k'}\mathrm{tr}\left(H_{k'}\bar{\Lambda}_{k'}\right) + \underline{J}_{k'} + \frac{\beta_{k'}}{2}\left(\mathrm{tr}\left(\Sigma_{\mathbf{v}}^{-1}\Lambda_{k'}\right) - m + \log\left(\frac{\det(\Sigma_{\mathbf{v}})}{\det(\Lambda_{k'})}\right) - 2\gamma\right),$$

where $\beta_{k'}$ is the Lagrangian multiplier associated with constraint $\mathcal{D}(\tilde{\mathbf{z}}_{k'}||\mathbf{z}_{k'}) \leq \gamma_{k'}$. Take the partial derivative of $\mathcal{L}_{k'}$ with respect to $\Lambda_{k'}$ and let it be zero. Then we have $\Phi_{k'} + \beta_{k'}\Sigma_{\mathbf{v}}^{-1} - \beta_{k'}\Lambda_{k'}^{-1} = 0$. When $-\frac{1}{\beta_k}\Phi_k + \Sigma_{\mathbf{v}}^{-1}$ is positive definite, we have (4) holds. By (4), we have $\Lambda^*_{k'}$ is symmetric. Moreover, $\Lambda^*_{k'}$ can be rewritten as $\left(-\Phi_{k'}/\beta_{k'} + \Sigma_{\mathbf{v}}^{-1}\right)^{-1} = \Sigma_{\mathbf{v}}\left(I - \Phi_{k'}\Sigma_{\mathbf{v}}/\beta_{k'}\right)^{-1}$, which is a product of two positive definite matrices. Hence, we have $\Lambda^*_{k'}$ defined in (4) is positive definite, implying primal feasibility defined by (3c) is satisfied.

We then verify dual feasibility $\beta_k \geq 0$. First, we show that $\beta_k \neq 0$. Suppose $\beta_k = 0$. Then the derivative of Lagrangian implies $-p^0 K^T L^T RLK = 0$. Since $K^T L^T RLK \succ 0$, we must have $p^0 = 0$. Therefore the system stays in mode *1* forever, implying that constraint (2c) is violated. By Proposition 1, we have that given any $\gamma_k \geq 0$, there exists a unique $\beta_k > 0$ such that (5) is satisfied. Hence, (5) guarantees dual feasibility $\beta \geq 0$.

We finally verify primal feasibility and complementary slackness. We take the partial derivative of $\mathcal{L}_{k'}$ with respect to $\beta_{k'}$ and set it as zero. Then we have $\mathrm{tr}\left(\Sigma_{\mathbf{v}}^{-1}\Lambda_{k'}\right) + \log\det(\Sigma_{\mathbf{v}}) - \log\det(\Lambda_{k'}) = m + 2\gamma$. Substituting (4) into the equation above, we have (5) holds. □

By Theorem 2, the controller can compute the best response from the adversary, i.e., given any detection threshold γ, it can estimate the covariance matrix selected by the adversary. By Theorem 1, we have that the mode switch probability follows χ^2 distribution. Using the tail bounds of χ^2 random variable to approximate the mode switch probability, we have $Pr\left(\mathcal{D}(\tilde{\mathbf{z}}_k||\mathbf{z}_k) \leq \gamma\right) \leq \exp\left(-\frac{(m-\gamma)^2}{4m}\right)$. We remark that the cost obtained using the tail bound is an upper bound, and hence models the worst-case cost. Although Theorem 1 coincides with the result reported in [7], Theorem 2 differs from [7] since the adversary's objective is different and its strategy is not restricted to linear attack strategy. In the following, we also show how the system computes the detection threshold to optimize the LQG control performance, which is not reported in [7].

Given the optimal attacks characterized by Theorems 1 and 2, in the following, we derive the optimal mode switch thresholds. The system solves the following optimization problem

$$\min_{\gamma_{0:N}} \quad \sum_{k=0}^{N} \mathrm{tr}\left(H_k\Sigma_k\right) \tag{6a}$$
$$\text{subject to} \quad \Sigma_k = G(\Sigma_{k-1}) + \bar{W}_k + F(\Lambda_k),\ \forall k \tag{6b}$$
$$\Sigma_k \succeq 0,\ \forall k \tag{6c}$$

Theorem 3. *The optimal mode switch thresholds can be obtained by solving a convex program.*

Proof. By Theorem 2, problem (6) can be expressed as follows:

$$\min_{\gamma_{0:N},\Psi} \quad \Psi \tag{7a}$$

$$\text{subject to} \quad \max_{\Lambda_{0:N}} \left\{ \sum_{k=0}^{N} \text{tr}(H_k \Sigma_k) : \Lambda_k \text{ satisfies } \mathcal{D}(\tilde{\mathbf{z}}_k || \mathbf{z}_k) \leq \gamma_k \right\} \leq \Psi \tag{7b}$$

$$\Sigma_k = G(\Sigma_{k-1}) + \bar{W}_k + F(\Lambda_k), \ \forall k \tag{7c}$$

$$\Sigma_k \succeq 0, \ \forall k \tag{7d}$$

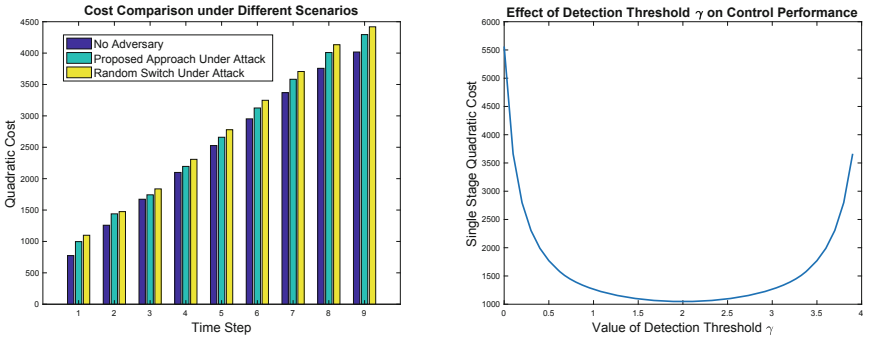
Constraint (7b) is linear with respect to Ψ and logarithmically convex with respect to γ_k. Thus problem (7) is jointly convex with respect to γ_k and Ψ. □

5 Simulation

In this section, we present a case study to demonstrate our proposed method. The proposed approach is evaluated using Matlab.

We consider a robot moving along a straight line [12]. The state of the robot contains its position and velocity, which are measured by two sensors. The dynamics is given by $\mathbf{x}_{k+1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \mathbf{x}_k + \begin{bmatrix} 1 \\ 0.5 \end{bmatrix} \mathbf{u}_k + \mathbf{w}_k, \mathbf{y}_k = \mathbf{x}_k + \mathbf{v}_k + \mathbf{a}_k$. The adversary can compromise the measurements from the position sensor, while it cannot tamper with the measurements from velocity sensor. Therefore, the output model is expressed using a switched system as $\mathbf{y}_k = \mathbf{x}_k + \mathbf{v}_k + \mathbf{a}_k$ if $\theta_t = 0$, and $\mathbf{y}_k = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{x}_k + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{v}_k$, if $\theta_t = 1$. Three scenarios are considered in our simulation: (i) LQG control in benign environment, (ii) design the detection threshold using the proposed approach, (iii) randomly generate one detection threshold without considering the presence of adversary and the adversary optimally responds to it. We demonstrate the effectiveness of the proposed approach by evaluating their LQG control performances, as shown in Fig. 1a. In the first scenario, the system does not need to switch between different modes and the cost incurred is the optimal LQG cost. This scenario gives the minimum cost among the three scenarios. Using the proposed approach, although the system still incurs additional cost comparing to the LQG cost incurred under benign environment due to the presence of the adversary, the cost increment is limited. In the third scenario, the system does not consider the presence of adversary and simply fix a mode switch threshold $\gamma = 3.3$ for all time instants. This scheme gives the highest cost among all scenarios. The strategic adversary can introduce much higher cost comparing to our proposed approach.

We illustrate the relationship between the cost function and γ in Fig. 1. We consider the single time step case and choose γ from 1 to 4. When γ is close to the single stage optimal solution $\gamma^* = 2.1$, the cost is minimized. When the threshold deviates from the optimal value γ^*, the system incurs more cost.



(a) (b)

Fig. 1. (a) presents cost functions incurred in different scenarios: optimal LQG cost in benign environment, cost incurred using proposed mode switch, and cost incurred using fixed mode switch threshold without considering the presence of adversary. (b) shows the relationship between the cost function and the value of threshold γ.

6 Conclusion

In this paper, we focused on a control system conducting LQG control under false data injection attacks. Using the signal issued by the detector whose detection threshold is carefully designed as a switch signal, the system was modeled as a switched linear system with two modes. We investigated the optimal attack strategy and gave a closed form solution for the covariance of optimal attack. Furthermore, we showed the optimal detection threshold for the detection, and the corresponding optimal mode switch policy can be computed using a convex program. The proposed approach was evaluated using a numerical case study.

References

1. Alpcan, T., Basar, T.: An intrusion detection game with limited observations. In: International Symposium on Dynamic Games and Applications (2006)
2. Bai, C.Z., Gupta, V.: On Kalman filtering in the presence of a compromised sensor: Fundamental performance bounds. In: American Control Conference (ACC), pp. 3029–3034. IEEE (2014)
3. Cárdenas, A.A., Amin, S., Sastry, S.: Research challenges for the security of control systems. In: Summit on Hot Topics in Security (HotSec). USENIX (2008)
4. Clark, A., Niu, L.: Linear quadratic gaussian control under false data injection attacks. In: American Control Conference (ACC), pp. 5737–5743. IEEE (2018)
5. Fawzi, H., Tabuada, P., Diggavi, S.: Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. Autom. Control **59**(6), 1454–1467 (2014)
6. Ghafouri, A., Abbas, W., Laszka, A., Vorobeychik, Y., Koutsoukos, X.: Optimal thresholds for anomaly-based intrusion detection in dynamical environments. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds.) GameSec 2016.

LNCS, vol. 9996, pp. 415–434. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47413-7_24
7. Guo, Z., Shi, D., Johansson, K.H., Shi, L.: Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica **89**, 117–124 (2018)
8. Kalman, R.E.: A new approach to linear filtering and prediction problems. ASME J. Basic Eng. **82**(1), 35–45 (1960)
9. Kung, E., Dey, S., Shi, L.: Optimal stealthy attack under KL divergence and countermeasure with randomized threshold. 20th IFAC World Congr. **50**(1), 9496–9501 (2017)
10. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. (TISSEC) **14**(1), 13 (2011)
11. Miao, F., Zhu, Q.: A moving-horizon hybrid stochastic game for secure control of cyber-physical systems. In: Conference on Decision and Control (CDC), pp. 517–522. IEEE (2014)
12. Mo, Y., Garone, E., Casavola, A., Sinopoli, B.: False data injection attacks against state estimation in wireless sensor networks. In: Conference on Decision and Control (CDC), pp. 5967–5972. IEEE (2010)
13. Pajic, M., et al.: Robustness of attack-resilient state estimators. In: ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), pp. 163–174. IEEE (2014)
14. Psiaki, M.L., Humphreys, T.E.: GNSS spoofing and detection. Proc. IEEE **104**(6), 1258–1270 (2016)
15. Shoukry, Y., Nuzzo, P., Puggelli, A., Sangiovanni-Vincentelli, A.L., Seshia, S.A., Tabuada, P.: Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach. IEEE Trans. Autom. Control **62**(10), 4917–4932 (2017)
16. Tambe, M.: Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned. Cambridge University Press, Cambridge (2011)
17. Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B., Capkun, S.: On the requirements for successful GPS spoofing attacks. In: ACM Conference on Computer and Communications Security, pp. 75–86. ACM (2011)
18. Umsonst, D., Sandberg, H.: A game-theoretic approach for choosing a detector tuning under stealthy sensor data attacks. In: 2018 IEEE Conference on Decision and Control (CDC), pp. 5975–5981. IEEE (2018)
19. Weerakkody, S., Sinopoli, B.: Detecting integrity attacks on control systems using a moving target approach. In: 54th IEEE Conference on Decision and Control (CDC), pp. 5820–5826. IEEE (2015)
20. Weerakkody, S., Sinopoli, B.: A moving target approach for identifying malicious sensors in control systems. In: Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 1149–1156. IEEE (2016)
21. Zhang, R., Venkitasubramaniam, P.: A game theoretic approach to analyze false data injection and detection in lqg system. In: Conference on Communications and Network Security (CNS), pp. 427–431. IEEE (2017)
22. Zhu, Q., Başar, T.: Dynamic policy-based IDS configuration. In: Conference on Decision and Control, pp. 8600–8605. IEEE (2009)