Secure State Estimation for Linear Time-varying Processes via Local Estimators

Liang Xu[1], Xiaoyu Mo[1], Yilin Mo[2], Xinghua Liu[3]

1. Nanyang Technological University, Singapore 639798, Singapore
E-mail: {lxu006, xiaoyu006}@e.ntu.edu.sg

2. Department of Automation, Tsinghua University, Beijing 100084, P. R. China
E-mail: ylmo@tsinghua.edu.cn

3. Department of Electrical Engineering, Xi'an University of Technology, Xi'an 710048, China
E-mail: liuxh@xaut.edu.cn

Abstract: This paper studies the secure state estimation problem of linear time-varying Gaussian processes in the presence of stochastic noises based on measurements from a set of sensors, a subset of which can be compromised by an attacker. The measurement of the compromised sensors can be arbitrarily manipulated by the attacker. We first show that in the absence of attacks, the Kalman filter can be decomposed into m local estimators and the Kalman estimate can be obtained by summing up the local estimates. We further show a least square interpretation to the fusion process and based on which, a convex optimization based secure state estimation scheme is proposed. The secure state estimation algorithm guarantees that when all the sensors are benign, the secure estimate coincides with the Kalman estimate. When less than half of the sensors are compromised, the secure state estimation scheme can still generate an estimate with bounded estimation error. Moreover, we demonstrate how to formulate the convex optimization problem to a conic programming problem to facilitate the application of the proposed secure state estimation algorithm in embedded systems. In the end, numerical simulations are conducted to verify the effectiveness of the proposed algorithm.

Key Words: Estimation, Kalman filtering, Time-varying systems, Cyber-physical security

1 Introduction

Networked embedded sensors are ubiquitous in monitoring dynamical systems due to their low cost and easy of installation. However, they are also vulnerable to attackers owing to their limited capacity and sparsely spatial deployment. Attackers might get access to sensors and arbitrary manipulate sensor measurements, or break the communication links between sensors and system operators to inject faked information. Therefore, the secure state estimation problem of linear dynamical systems under sparse sensor attacks has been extensively studied in the past few years. In the problem setting, it is usually assumed that a group of sensors are deployed to monitor the systems dynamics, of which a subset of sensors might be compromised and their measurements can be arbitrarily tampered. The problem of interests is to determine the conditions under which the system states can be reliably estimated and design secure estimators to generate reliable estimates.

When the linear dynamical system is free of process and measurement noises, the secure state estimation problem is studied in [1–3]. It is shown that when the number of compromised sensors is no larger than the maximal tolerable bound, which is a function of system matrices (A, C), the attacks can always be detected and isolated, and the system state can always be exactly recovered. Moreover, efficient algorithms using convex relaxation and even-triggered approach are proposed respectively to estimate the system state despite attacks in [2, 3]. When there exist process or measurement noises, the secure state estimation problem is further complicated by the fact that we have to distinguish between the noises and the attacks injected by an adversary. Two kinds of noises are considers in previous studies: 1) bounded nonstochastic noises and 2) stochastic noises. In the consideration of bounded noises, [4] presents an l_0 -based state estimator that can be formulated as a mixed-integer linear program and its convex relaxation based on the l_1 norm. For both state estimators, analytic bounds on the state-estimation errors caused by the presence of noise are analyzed. [5] further proposes Satisfiability Modulo Theory based techniques to exploit the geometric structure of the secure state estimation problem to efficiently reason about inconsistency of sensor measurements and improve the runtime performance. In the presence of Gaussian stochastic noises, [6] proposes state estimator which involves Kalman filters operating over subsets of sensors to search for a sensor subset which is reliable for state estimation. To further improve the subset searching time, the authors propose Satisfiability Modulo Theory-based techniques to exploit the combinatorial nature of searching over sensor subsets. [7, 8] propose convex optimization based approach to merge estimates of local estimators, which use only the measurement from a single sensor, to generate a secure state estimate. The proposed estimator coincides with the Kalman estimator with certain probability when all sensors are benign and is stable when less than half of the sensors are compromised. However, the above mentioned work on secure state estimation in the presence of sparse sensor attacks only consider linear time-invariant systems.

The main difference between the this paper and our previous work [7, 8] is that we consider a linear time varying system instead of an LTI system. This is motivated by our research on sensor fusion for autonomous vehicle, where the sensors have different sampling frequency and are not synchronized. We believe that this formulation has many real world applications beyond autonomous driving vehicles. The main contributions are as follows: 1) this paper proposes a decomposition method for the time-varying Kalman filter; 2) a convex optimization based secure state estimation scheme is proposed, which guarantees that when all the sensors are benign, the secure estimate can generate the Kalman estimate, when less than half of the sensors are under attack, the secure estimator can still generate a reliable estimate; 3) the secure state estimation algorithm is further formulated as a conic programming problem to facilitate its applications on embedded systems.

The paper is organized as follows: Section 2 is the problem formulation. The Kalman filter decomposition and the least square interpretation are given in Section 3. Section 4 introduces the secure information fusion scheme. The reformulation to a conic programming problem is provided in Section 5. The numerical simulations are given in Section 6 and this paper ends with some concluding remarks in Section 7.

Notations: $\mathbb{R}$ and $\mathbb{R}^n$ denote sets of real numbers and n-dimensional real vectors, respectively. $\mathbf{1}$ represents a vector with all elements to be 1. I denotes the identity matrix. A', A^{-1} denote the transpose and inverse of matrix A, respectively. $A \succ 0 (A \succeq 0)$ means that the matrix A is positive definite (positive semi-definite). $v \geqslant 0$ means that every element of the vector v is greater than or equal to zero. $\mathbb{E}\{\cdot\}$ denotes the expectation operator.

2 Problem Formulation

This paper studies the following linear time-varying process

$$x(k+1) = A(k)x(k) + w(k), \tag{1}$$

where $x(k) \in \mathbb{R}^n$ is the state and $w(k) \in \mathbb{R}^n$ is the process noise. We assume that the initial condition satisfies $x(0) \sim \mathcal{N}(0, \Sigma)$ with $\Sigma \succ 0$; the process noise satisfies $w(k) \sim \mathcal{N}(0, Q(k))$ and $w(k_1)$ and $w(k_2)$ are independent for any $k_1 \neq k_2$. m sensors are deployed to measure the process state. The measurement output at each sensor is

$$y_i(k) = C_i(k)x(k) + v_i(k) + a_i(k), \quad i = 1, \dots, m, \tag{2}$$

where $y_i(k) \in \mathbb{R}$ is the sensor measurement; $v_i(k) \in \mathbb{R}$ is the stochastic measurement noise and $a_i(k) \in \mathbb{R}$ is the deterministic bias injected by the attacker. (2) can be equivalently formulated as

$$y(k) = C(k)x(k) + v(k) + a(k), \tag{3}$$

where y, C, v, a are vectors/matrices formed by stacking y_i, C_i, v_i and a_i, respectively. We further assumed that $v(k) \sim \mathcal{N}(0, R(k))$; $v(k_1)$ and $v(k_2)$ are independent for any $k_1 \neq k_2$ and $w(k_1), v(k_2), x(0)$ are independent for any k_1, k_2.

Remark 1. *The dynamics* (1), (3) *can model the scenario that a continuous-time process is monitored by multiple sensors with asynchronous measurements or transmission packet losses. Consider the simple case that the continuous-time process is a linear system with $\dot{x}(t) = Ax(t)$, $y_i(t) = C_i x(t), i = 1, \dots, m$. Then $A(k) = \exp(A\tau)$, where τ is the time interval between two consecutive measurements. Moreover, $C(k) = [\tilde{C}_i', \dots, \tilde{C}_m']'$ with $\tilde{C}_i$ either be C_i if the i-th sensor's measurement is accessible at time instance k or* 0 *otherwise.*

Due to resource constraints of attackers, we assume that at most p out of m sensors can be compromised with arbitrary a_i. We try to propose a secure estimation scheme to estimate the system state despite attacks. In the following section, we show that when all the sensors are benign, the Kalman estimate can be obtained by merging estimates generated from m local estimators, which only use the measurement from a single sensor. Based on this result, we further propose a secure state estimation scheme in Section 4.

3 Kalman Filter Decomposition Using Local Estimate

If all sensors are benign, i.e., $a(k) = 0$ for all k, the optimal state estimator is the Kalman filter

$$\begin{aligned} \hat{x}(k) &= \hat{x}(k|k-1) + K(k)(y(k) - C(k)\hat{x}(k|k-1)), \\ P(k) &= P(k|k-1) - K(k)C(k)P(k|k-1) \end{aligned} \tag{4}$$

where

$$\begin{aligned} \hat{x}(k+1|k) &= A(k)\hat{x}(k), \\ P(k+1|k) &= A(k)P(k)A(k)' + Q(k), \\ K(k) &= P(k|k-1)C(k)'(C(k)P(k|k-1)C(k)' + R(k))^{-1} \end{aligned}$$

with initial conditions $\hat{x}(0|-1) = 0, P(0|-1) = \Sigma$.

We further make the following assumptions on the system parameters and the Kalman filter gain.

Assumption 2. *$A(k)$ and $A(k) - K(k+1)C(k+1)A(k)$ are invertible for all k.*

Remark 3. *If $A(k) = \exp(A\tau)$ is from discretizing a linear continuous-time system, $A(k)$ is automatically invertible. Then the invertibility of $A(k) - K(k+1)C(k+1)A(k)$ is equivalent to that of $I - K(k)C(k)$. If $Q(k) \succ 0, R(k) \succ 0$, we can prove that $I - K(k)C(k)$ is invertible. Since $P(k|k-1) \succ 0$, the invertibility of $I - K(k)C(k)$ is equivalent to that of $P(k|k-1) - K(k)C(k)P(k|k-1)$. Further from the matrix inversion lemma [9], we know that*

$$\begin{aligned} &P(k|k-1) - K(k)C(k)P(k|k-1) \\ &\qquad = (P(k|k-1)^{-1} + C(k)'R(k)^{-1}C(k))^{-1}, \end{aligned}$$

which implies that $I - K(k)C(k)$ is invertible.

Before giving the design of the local estimator, we need the following lemma, whose proof is given in Appendix A.

Lemma 4. *Under Assumption 2, for any given $\mathcal{S} \in \mathbb{R}^n$ with $1 + C_i(k+1)A(k)\mathcal{S} \neq 0$, $A(k) - \mathcal{L}_i C_i(k+1)A(k)$ is invertible with $\mathcal{L}_i = 1/(1 + C_i(k+1)A(k)\mathcal{S})A(k)\mathcal{S}$.*

In view of Lemma 4, let $F_i(0) = \frac{1}{m}I$, we can construct sequences $L_i(k), k \geq 1$ and $F_i(k), k \geq 1$ from

$$L_i(k+1) = \frac{1}{1 + C_i(k+1)A(k)S(k)} A(k)S(k), \tag{5}$$

$$\begin{aligned} F_i(k+1) &= (A(k) - K(k+1)C(k+1)A(k))F_i(k) \\ &\quad \times (A(k) - L_i(k+1)C_i(k+1)A(k))^{-1}, \end{aligned} \tag{6}$$

where

$$\begin{aligned} S(k) = F_i(k)^{-1}&(A(k) - K(k+1)C(k+1)A(k))^{-1} \\ &\times K_i(k+1), \end{aligned}$$

and $K_i(k+1)$ is the i-th column of $K(k+1)$.

We can verify from (5) and (6) that $L_i(k)$ and $F_i(k)$ satisfy the following relation

$$\begin{aligned} F_i(k+1)&(A(k) - L_i(k+1)C_i(k+1)A(k)) \\ &= (A(k) - K(k+1)C(k+1)A(k))F_i(k), \quad (7)\\ F_i(k+1)&L_i(k+1) = K_i(k+1). \quad (8)\end{aligned}$$

Moreover, $F_i(k)$ has the following property whose proof is given in Appendix B.

Lemma 5. *$F_i(k)$ satisfies $\sum_{i=1}^m F_i(k) = I$ for all k.*

The m local estimators with each one using only the measurement of a single sensor are designed as

$$\begin{aligned}\tilde{x}_i(k) = (A(k-1) - L_i(k)C_i(k)A(k-1))\tilde{x}_i(k-1)& \\ + L_i(k)y_i(k),& \quad (9)\end{aligned}$$

for $i = 1, \dots, m$, where $\tilde{x}_i(k)$ is the estimate of each local estimator initialized as $\tilde{x}_i(0) = \hat{x}(0) = K(0)y(0)$.

We then have that the Kalman estimate $\hat{x}(k)$ can be obtained as a weighted sum of the local estimates $\tilde{x}_i(k)$ as proved below.

Theorem 6. *Under Assumption 2, with the designed local estimators* (9)*, we have for all k that*

$$\hat{x}(k) = \sum_{i=1}^m F_i(k)\tilde{x}_i(k).$$

Proof. Left multiply $F_i(k)$ to (9), further from (7) and (8), we have

$$\begin{aligned}F_i(k)\tilde{x}_i(k) = (A(k-1) - K(k)C(k)A(k-1))F_i(k-1)& \\ \times \tilde{x}_i(k-1) + K_i(k)y_i(k).&\end{aligned}$$

Sum up the above equation over i, we have

$$\begin{aligned}\sum_{i=1}^m F_i(k)\tilde{x}_i(k) = (A(k-1) - K(k)C(k)A(k-1))& \\ \times \sum_{i=1}^m F_i(k-1)\tilde{x}_i(k-1) + K(k)y(k).&\end{aligned}$$

Therefore $\sum_{i=1}^m F_i(k)\tilde{x}_i(k)$ has the same dynamics as $\hat{x}(k)$. Since $\sum_{i=1}^m F_i(0)\tilde{x}_i(0) = \hat{x}(0)$, we know that $\hat{x}(k) = \sum_{i=1}^m F_i(k)\tilde{x}_i(k)$ for all k. □

In the following we show that we can also reconstruct $\hat{x}(k)$ in terms of $\tilde{x}_i(k)$ from a least square problem, which enables the introduction of a secure state estimation scheme in the next section.

3.1 Least Square Interpretation

Let $e(k) = [e_1(k)', \dots, e_m(k)']'$ with $e_i(k) = \tilde{x}_i(k) - x(k)$. Let $\Sigma_e(k) = \mathbb{E}\{e(k)e(k)'\}$. Then we have

$$\tilde{x}(k) = Hx(k) + e(k), \quad (10)$$

where $\tilde{x}(k) = [\tilde{x}_1(k)', \dots, \tilde{x}_m(k)']'$ and $H = [I', \dots, I']'$.

Define the following least square problem

$$\min_{\check{x}, \check{e}} \frac{1}{2}\check{e}'\Sigma_e(k)^{-1}\check{e} \quad s.t. \quad \tilde{x}(k) = H\check{x} + \check{e}. \quad (11)$$

Denote the optimal variables to the above least square problem as $\check{x}^*$, $\check{e}^*$. Then,we have the following theorem.

Theorem 7. *The solution to the least square problem* (11) *is given by*

$$\begin{aligned}\check{x}^* &= \hat{x}(k) = [F_1(k), \dots, F_m(k)]\tilde{x}(k),\\ \check{e}^* &= (I - H[F_1(k), \dots, F_m(k)])e(k).\end{aligned}$$

Proof. We can verify that the Kalman estimation error covariance matrix $P(k)$ and the Kalman filter gain $K(k)$ satisfy the following relation

$$\begin{aligned}P(k+1) = (A(k) - K(k+1)C(k+1)A(k))P(k)A(k)'& \\ + (I - K(k+1)C(k+1))Q(k),&\end{aligned}$$

$$\begin{aligned}K(k+1)R(k+1) =&(A(k) - K(k+1)C(k+1)A(k)) \\ &\times P(k)A(k)'C(k+1)' \\ &+ (I - K(k+1)C(k+1)) \\ &\times Q(k)C(k+1)'.\end{aligned}$$

Then, for any compatible matrix $\mathcal{L}$, we have the following relation

$$\begin{aligned}P(k+1) =&(A(k) - K(k+1)C(k+1)A(k))P(k) \\ &\times (A(k) - \mathcal{L}C(k+1)A(k))' \\ &+ (I - K(k+1)C(k+1))Q(k) \\ &\times (I - \mathcal{L}C(k+1))' \\ &+ K(k+1)R(k+1)\mathcal{L}'.\end{aligned}$$

Let $[\Sigma_e(k)]_{ij} = \mathbb{E}\{e_i(k)e_j(k)'\}$. Then we have that

$$\begin{aligned}[\Sigma_e(k+1)]_{ij} =&(A(k) - L_i(k+1)C_i(k+1)A(k))[\Sigma_e(k)]_{ij} \\ &\times (A(k) - L_j(k+1)C_j(k+1)A(k))' \\ &+ (L_i(k+1)C_i(k+1) - I)Q(k) \\ &\times (L_j(k+1)C_j(k+1) - I)' \\ &+ r_{ij}(k)L_i(k+1)L_j(k+1)',\end{aligned}$$

where $r_{ij}(k) = \mathbb{E}\{v_i(k)v_j(k)'\}$. Therefore we have that

$$\begin{aligned}&F_i(k+1)[\Sigma_e(k+1)]_{ij} = \\ &(A(k) - K(k+1)C(k+1)A(k))F_i(k)[\Sigma_e(k)]_{ij} \\ &\quad \times (A(k) - L_j(k+1)C_j(k+1)A(k))' \\ &+ (K_i(k+1)C_i(k+1) - F_i(k+1))Q(k) \\ &\quad \times (L_j(k+1)C_j(k+1) - I)' \\ &+ r_{ij}(k)K_i(k+1)L_j(k+1)'.\end{aligned}$$

Let $\tilde{S}_j(k) = \sum_{i=1}^m F_i(k)[\Sigma_e(k)]_{ij}$, we have that

$$\begin{aligned}\tilde{S}_j(k+1) =&(A(k) - K(k+1)C(k+1)A(k))\tilde{S}_j(k) \\ &\times (A(k) - L_j(k+1)C_j(k+1)A(k))' \\ &+ (K(k+1)C(k+1) - I)Q(k) \\ &\times (L_j(k+1)C_j(k+1) - I)' \\ &+ \sum_{i=1}^m r_{ij}(k)K_i(k+1)L_j(k+1)'.\end{aligned}$$

Let $\mathcal{L}_j(k) = [0, \dots, 0, L_j(k), 0, \dots, 0]$, we have

$$\begin{aligned}\tilde{S}_j(k+1) =&(A(k) - K(k+1)C(k+1)A(k))\tilde{S}_j(k) \\ &\times (A(k) - \mathcal{L}_j(k+1)C(k+1)A(k))' \\ &+ (K(k+1)C(k+1) - I)Q(k) \\ &\times (\mathcal{L}_j(k+1)C(k+1) - I)' \\ &+ K(k+1)R(k+1)\mathcal{L}_j(k+1)'.\end{aligned}$$

Since $\tilde{S}_j(0) = P(0)$, we then have $\tilde{S}_j(k) = P(k)$. Therefore

$$[F_1(k), \dots, F_m(k)]\Sigma_e(k) = P(k)H'.$$

Then we have

$$H'\Sigma_e(k)^{-1} = P(k)^{-1}[F_1(k), \dots, F_m(k)],$$
$$H'\Sigma_e(k)^{-1}H \overset{(a)}{=} P(k)^{-1},$$

where (a) follows from Lemma 5. It is known that the least square problem (11) admits the solutions that

$$\check{x}^* = (H'\Sigma_e(k)^{-1}H)^{-1}H'\Sigma_e(k)^{-1}\tilde{x}(k),$$

which further gives $\check{x}^* = [F_1(k), \dots, F_m(k)]\tilde{x}(k)$. Then we have that

$$\begin{aligned} e^* &= \tilde{x}(k) - H\check{x}^* \\ &= (I - H[F_1(k), \dots, F_m(k)])\tilde{x}(k) \\ &\overset{(a)}{=} (I - H[F_1(k), \dots, F_m(k)])e(k), \end{aligned}$$

where (a) follows from Lemma 5. The proof is completed. □

The above least square interpretation to the Kalman fusion leads us to the proposition of a convex optimization based secure state estimation scheme in the next section.

4 Secure Information Fusion

In the presence of attacks, we have

$$\begin{aligned} e_i(k+1) =& (A(k) - L_i(k+1)C_i(k+1)A(k))e_i(k) \\ &+ (L_i(k+1)C_i(k+1) - I)w(k) \\ &+ L_i(k+1)v_i(k+1) + L_i(k+1)a_i(k+1). \end{aligned}$$

Define $\mu_i(k), \nu_i(k)$ as follows

$$\begin{aligned} \mu_i(k+1) =& (A(k) - L_i(k+1)C_i(k+1)A(k))\mu_i(k) \\ &+ (L_i(k+1)C_i(k+1) - I)w(k) \\ &+ L_i(k+1)v_i(k+1), \qquad (12) \\ \nu_i(k+1) =& (A(k) - L_i(k+1)C_i(k+1)A(k))\nu_i(k) \\ &+ L_i(k+1)a_i(k+1). \end{aligned}$$

Then we have

$$e_i(k) = \mu_i(k) + \nu_i(k).$$

Therefore, in the presences of attacks, the error $e(k)$ can be decomposed as the error caused by noise and the error caused by bias injected by attackers. As a result, we proposed a LASSO [10] based secure fusion scheme as a counterpart to the least square problem (11)

$$\begin{aligned} \min_{\check{x}_s, \mu, \nu} \quad & \frac{1}{2}\mu'\Sigma_e(k)^{-1}\mu + \gamma\|\nu\|_1 \qquad (13) \\ s.t., \quad & \tilde{x}(k) = H\check{x}_s + \mu + \nu \end{aligned}$$

where $\Sigma_e(k)$ is the same one as used in (11), and its value can be recursively calculated from (12).

Then following similar line of arguments as in the proof of Lemma 3 in [7], we have the following lemma characterizing the solution to the optimization problem (13).

Lemma 8. *Let $\check{x}_s^*$, μ^*, ν^* be the minimizer to the LASSO problem* (13)*, and let $\check{x}^*$, $\check{e}^*$ be the minimizer to the least square problem* (11)*. Then the following statements hold*

- *the following inequality holds*

$$\|\Sigma_e(k)^{-1}\mu^*\|_\infty \leq \gamma.$$

- *if $\|\Sigma_e(k)^{-1}\check{e}^*\|_\infty < \gamma$, then*

$$\check{x}_s^* = \check{x}^*, \mu^* = \check{e}^*, \nu^* = 0.$$

Furthermore, when all the sensors are benign, in view of Theorem 7 and Lemma 8, we have the following result.

Theorem 9. *When all the sensors are benign, if the following conditions hold,*

$$\|\Sigma_e(k)^{-1}(I - H[F_1(k), \dots, F_m(k)])\mu(k)\|_\infty < \gamma,$$

where $\mu = [\mu_1, \dots, \mu_m]'$, the LASSO estimate $\check{x}_s^*$ gives the Kalman estimate $\hat{x}(t)$.

The above theorem implies that a larger γ is preferred in practical applications, since in the absence of attacks, a larger γ can guarantee that the secure state estimate has a larger possibility to be equal to the Kalman estimate.

Define the following operator: $f_i : \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} \to \mathbb{R}$, such that $f_i(\beta_1, \dots, \beta_m)$ equals to the i-th smallest element in the set $\{\beta_1, \dots, \beta_m\}$. Assuming that $d_1, \dots, d_m \in \mathbb{R}^n$ are vectors. With slightly abuse of notations, we define $f_i(d_1, \dots, d_m)$ as a vector where each of its entry is the i-th smallest element among the corresponding entries in $e_1, \dots, e_m$. We further define $f_{i+1/2} = (f_i + f_{i+1})/2$. When the system is under attack, we have the following theorem. The proof is similar to the proof of Theorem 3 in [7] and is omitted here.

Theorem 10. *Suppose that $p < \frac{m}{2}$ sensors are compromised, then the error of the secure state estimate is bounded by*

$$\begin{aligned} f_{(m+1)/2-p}(\mu_1(k), \dots, \mu_m(k)) - \gamma\|\Sigma_e(k)\|_\infty \leq x(k) - \check{x}_s^* \\ \leq f_{(m+1)/2+p}(\mu_1(k), \dots, \mu_m(k)) + \gamma\|\Sigma_e(k)\|_\infty. \end{aligned}$$

The above theorem implies that in the presence of attacks, a smaller γ is preferred in practical applications, since a smaller γ can guarantee that the bound for the secure estimation error is smaller.

Remark 11. *Since observability is not well defined for time-varying systems, we do not impose any observability requirements on applying the algorithm. Indeed, from Theorem 10, we can observe that the estimation error $x_k - \check{x}_k^*$ is bounded by $\|\Sigma_e(k)\|_\infty$, which can be any value and even unbounded depending on the observability condition.*

5 LASSO to Conic Programming

The formulated LASSO problem can be solved via CVX [11]. However, the secure state estimation algorithm is usually implemented in resource constrained devices, such as embedded devices. It is desired to transform (13) to a form that is convenient for implementation. ECOS is a conic programming solver designed for embedded systems [12]. In the following we propose to formulate LASSO as a conic programming problem to facilitate the application of proposed secure state estimation scheme in embedded systems with ECOS.

First of all, since the l_1 norm of ν has the following expression

$$\begin{aligned}\|\nu\|_1 &= \min_{\nu_1,\nu_2} \mathbf{1}'\nu_1 + \mathbf{1}'\nu_2 \\ s.t. \quad & \nu = \nu_1 - \nu_2, \nu_1 \geqslant 0, \nu_2 \geqslant 0,\end{aligned}$$

(13) is equivalent to the following optimization problem

$$\begin{aligned}\min_{\check{x}_s,\mu,\nu_1,\nu_2,t} & \frac{1}{2}t + \gamma\mathbf{1}'\nu_1 + \gamma\mathbf{1}'\nu_2 \\ s.t., \quad & \nu_1 \geqslant 0, \nu_2 \geqslant 0, \\ & \tilde{x}(k) = H\check{x}_s + \mu + \nu_1 - \nu_2, \\ & \|\Sigma_e(k)^{-\frac{1}{2}}\mu\|_2^2 \leq t.\end{aligned}$$

The constraint $\|\Sigma_e(k)^{-\frac{1}{2}}\mu\|_2^2 \leq t$ implies that the vector $[\frac{1}{2}, t, (\Sigma_e(k)^{-\frac{1}{2}}\mu)']'$ belongs to the rotated quadratic cone $\mathcal{Q}_r^{2+n\times p}$. The rotated quadratic cone is defined as

$$\mathcal{Q}_r^n = \left\{x \in \mathbb{R}^n | 2x_1x_2 \geq x_3^2 + \ldots + x_n^2, x_1, x_2 \geq 0\right\}.$$

Therefore the vector $T_{2+n\times p}[\frac{1}{2}, t, (\Sigma_e(k)^{-\frac{1}{2}}\mu)']' = [\frac{\sqrt{2}}{4} + \frac{\sqrt{2}}{2}t, \frac{\sqrt{2}}{4} - \frac{\sqrt{2}}{2}t, (\Sigma_e(k)^{-\frac{1}{2}}\mu)']'$ belongs to the second order cone $\mathcal{Q}^{2+n\times p}$, where

$$T_n = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & \\ & & I_{n-2} \end{bmatrix},$$

$$\mathcal{Q}^n = \left\{x \in \mathbb{R}^n | x_1 \geq \sqrt{x_2^2 + \ldots + x_n^2}\right\}.$$

We can then formulate (13) to the following conic programming problem

$$\begin{aligned}\min_{\check{x}_s,\mu,\nu_1,\nu_2,t} & \frac{1}{2}t + \gamma\mathbf{1}'v_1 + \gamma\mathbf{1}'v_2 \\ s.t., \quad & v_1 \geqslant 0, v_2 \geqslant 0, \\ & \tilde{x}(k) = H\check{x}_s + \mu + v_1 - v_2, \\ & \left[\frac{\sqrt{2}}{4} + \frac{\sqrt{2}}{2}t, \frac{\sqrt{2}}{4} - \frac{\sqrt{2}}{2}t, (\Sigma_e(k)^{-\frac{1}{2}}\mu)'\right]' \in \mathcal{Q}^{2+n\times p}.\end{aligned}$$

6 Numerical Illustrations

In this section, we conduct simulations to verify the derived results. We assume that the linear discrete-time system (1) is obtained from sampling a continuous-time linear process $\dot{x}(t) = Ax(t)$, where $A = \begin{bmatrix} 1 & 0 \\ 0 & -0.5 \end{bmatrix}$, and the sampling interval is $0.1s$. The initial system state covariance matrix is given by $\Sigma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Moreover, we assume that three sensors are deployed to measure the dynamic process, and their measurement matrices are

$$C_1 = [1, 5], C_2 = [3, -1], C_3 = [1, 2].$$

We assume that the process and measurement noise covariance matrices are $Q = 3I, R = 4I$.

We consider the asynchronous measurement case. We assume that at every sampling time, the measurement from sensor 1 and sensor 2 are available. However, the measure from sensor 3 are only available every $0.2s$ [1]. This models the case that certain sensors, for example the GPS sensors, requires small sensing and computational resources and their measurements are available almost instantly. However, some other sensors, such as the vision based localization sensors, might require time for computation. Therefore, their measurements are only available at a low frequency.

In the first simulation, we assume that the first sensor is attacked with $a_1(k) = 10$ for all k. Let $\gamma = 0.8$ in the secure state estimation algorithm. The estimate from the proposed secure estimation algorithm and from the Kalman estimator are plotted in Fig. 1.

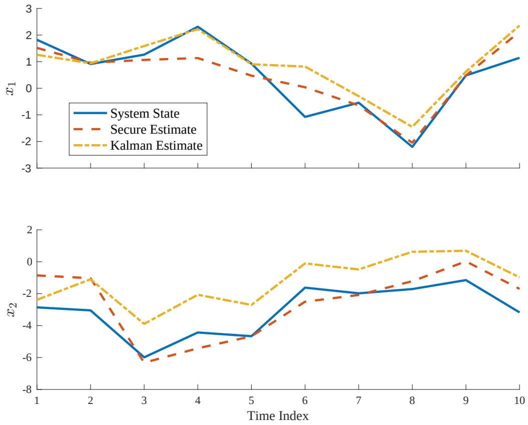

Fig. 1: Secure estimate v.s. Kalman estimate

Moreover, the accumulated estimation error defined as $\sum_{k=1}^{T} \|x(k) - \hat{x}(k)\|^2$ for the Kalman estimator and the secure estimator are 42.13 and 17.71, respectively. Therefore, in the presence of attacks, the secure estimation algorithm provides a more reliable estimate with a smaller estimation error as compared to the Kalman estimator.

In the second simulation, we consider two scenarios, 1) all the sensors are benign and 2) the first sensor is under attack and $a_1(k) = 10$ for all k. We compute the empirical Mean Squared Error (MSE) of the secure estimator for each scenario and for different choices of γ. Define relative MSE as the MSE of the secure state estimator divided by the MSE of the Kalman filter without attacks. Fig. 2 is the plot of relative MSE verses different values of γ. It is clear that when there are no attacks, a larger γ guarantees a smaller estimation error. While in the presence of attacks, the relative MSE achieves the minimum at around $\gamma = 0.6$.

7 Conclusions

This paper studies the secure state estimation problem of a linear time-varying process in the presence of sparse sensor attacks and stochastic noises. We first propose a method to decompose the Kalman filter using only local sensor measurements. Based on this decomposition, a convex optimization based secure state estimation scheme is proposed. The performance of this secure state estimation scheme both with and without attacks is analyzed. The reformulation of the

[1] In the simulation, we only consider the periodic measurement case. However, our proposed method also applies to the aperiodic measurement case by invoking the modeling approach noted in Remark 1.

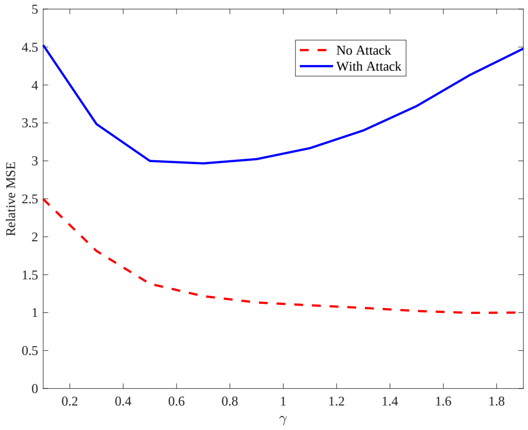

Fig. 2: Relative MSE v.s. different values of γ

secure state estimation scheme to implementable forms are also studied. In the end, simulations are conducted to verify the derived result.

Appendix

A. Proof of Lemma 4

Proof. Since

$$\begin{aligned}&A(k)-\mathcal{L}_iC_i(k+1)A(k)\\&=A(k)-\frac{1}{1+C_i(k+1)A(k)\mathcal{S}}A(k)\mathcal{S}C_i(k+1)A(k)\\&=A(k)(I-\frac{1}{1+C_i(k+1)A(k)\mathcal{S}}\mathcal{S}C_i(k+1)A(k)),\end{aligned}$$

the invertibility of $A(k)-\mathcal{L}_iC_i(k+1)A(k)$ is equivalent to that of $I-\frac{\mathcal{S}C_i(k+1)}{1+C_i(k+1)A(k)\mathcal{S}}A(k)$. We will prove this by contradiction. Suppose that $I-\frac{\mathcal{S}C_i(k+1)}{1+C_i(k+1)A(k)\mathcal{S}}A(k)$ is not invertible, then there is a non-zero vector z such that

$$(I-\frac{\mathcal{S}C_i(k+1)}{1+C_i(k+1)A(k)\mathcal{S}}A(k))z=0.$$

Then

$$z=\frac{C_i(k+1)A(k)z}{1+C_i(k+1)A(k)\mathcal{S}}\mathcal{S}.$$

Therefore we have that $C_i(k+1)A(k)z\neq 0$. Since

$$C_i(k+1)A(k)z=\frac{C_i(k+1)A(k)z}{1+C_i(k+1)A(k)\mathcal{S}}C_i(k+1)A(k)\mathcal{S},$$

we have

$$1=\frac{C_i(k+1)A(k)\mathcal{S}}{1+C_i(k+1)A(k)\mathcal{S}}.$$

However, this is not possible. Therefore, $I-\frac{\mathcal{S}C_i(k+1)}{1+C_i(k+1)A(k)\mathcal{S}}A(k)$ is invertible. The proof is completed. □

B. Proof of Lemma 5

Proof. We prove this using induction. Suppose $\sum_{i=1}^m F_i(k)=I$. From (7) and (8), we have

$$\begin{aligned}&F_i(k+1)A(k)-K_i(k+1)C_i(k+1)A(k)\\&=(A(k)-K(k+1)C(k+1)A(k))F_i(k).\end{aligned}$$

Sum up the above equation over i, we obtain that

$$\begin{aligned}&\sum_{i=1}^m F_i(k+1)A(k)-K(k+1)C(k+1)A(k)\\&=(A(k)-K(k+1)C(k+1)A(k))\sum_{i=1}^m F_i(k).\end{aligned}$$

Since $\sum_{i=1}^m F_i(k)=I$, we then have from the above that

$$\sum_{i=1}^m F_i(k+1)A(k)=A(k).$$

Since $A(k)$ is invertible, we further have that $\sum_{i=1}^m F_i(k+1)=I$. Since $\sum_{i=1}^m F_i(0)=I$, we know that $\sum_{i=1}^m F_i(k)=I$ for all k. □

References

[1] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

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

[3] Y. Shoukry and P. Tabuada, “Event-triggered state observers for sparse sensor noise/attacks,” *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[4] M. Pajic, I. Lee, and G. J. Pappas, “Attack-resilient state estimation for noisy dynamical systems,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2017.

[5] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, “Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach,” *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[6] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, “Secure state estimation against sensor attacks in the presence of noise,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2017.

[7] Y. Mo and E. Garone, “Secure dynamic state estimation via local estimators,” in *Proceedings of the 55th IEEE Conference on Decision and Control*, pp. 5073–5078, IEEE, 2016.

[8] X. Liu, Y. Mo, and E. Garone, “Secure dynamic state estimation by decomposing Kalman filter,” *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7351–7356, 2017.

[9] D. S. Bernstein, *Matrix mathematics: theory, facts, and formulas*. Princeton, N.J.: Princeton University Press, 2009.

[10] R. Tibshirani, “Regression shrinkage and selection via the lasso,” *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 267–288, 1996.

[11] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming, version 2.1.” http://cvxr.com/cvx, Mar. 2014.

[12] A. Domahidi, E. Chu, and S. Boyd, “ECOS: An SOCP solver for embedded systems,” in *2013 European Control Conference*, pp. 3071–3076, IEEE, 2013.