23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Secure Estimation for Linear Time-varying Process via Local Estimators

Liang Xu, Xinghua Liu and Yilin Mo

Abstract— **We are interested in the secure estimation problem of a linear time-varying Gaussian process. m sensors are deployed to measure the process state and p out of m sensors might undergo integrity attack, which means their measurements can be arbitrarily manipulated by attackers. We first show that the Kalman filter can be decomposed into m local estimators and then summed up to obtain the Kalman estimate. Then we show a least square interpretation to the fusion process and based on which a convex optimization based secure estimation scheme is proposed. The secure estimation algorithm guarantees that when all the sensors are benign, the secure estimate coincides with the Kalman filter. When less than half of the sensors are compromised, the secure estimation scheme can still generate an estimate with bounded error. Moreover, numerical simulations are conducted to verify the effectiveness of the proposed algorithm.**

Keywords: **secure estimation, Kalman filtering, convex optimization**

AMS subject classications: **93E03, 93E10, 90C25**

I. Introduction

The security problem has been studied in computer science for several decides, where attacks mostly affect software systems only and do not incur large physical impact. However, attacks on the cyber-physical systems, for example attacks on power systems, transportation networks, industrial control processes and critical infrastructures, has large impact on the physical world and everyday life. Therefore the security issues for cyber-physical systems have been extensively studied in recent years.

Traditionally, the fault detection and isolation has been widely studied to handle random failures, see [1]. However, these methods are not suitable for dealing with intelligent attacks [2]. Moreover, detecting and isolating attacks is also computationally hard [3], [4]. Therefore it is more suitable to design secure estimators that can tolerate a small portion of sensory data being attacked.

The traditional Kalman filter is not robust to sensor attacks, since the attack can accumulated in the estimation process and the adversary can exploit this fact to introduce a large estimation error [5], [6]. [7], [3] propose a moving horizon approach, which only use finite sensor data, not the entire historical data, to estimate system states to avoid the accumulation of attack signals. [8], [9] further generalize the result to consider bounded and random noises. However, since these secure estimators only use finite measurements, they have an estimation performance loss even in the case of no attacks. [10], [11] propose a convex optimization based secure estimation scheme, which can guarantee that when all the sensors are benign, the secure estimation scheme coincides with the Kalman estimate. Instead of relaxing with convex optimization techniques, [12] proposes Satisfiability Modulo Theory based techniques to exploit the combinatorial nature of searching over sensor subsets. However, the above works only consider time-invariant systems.

This extended abstract extends the result in [10], [11] to consider the secure estimation problem of linear time-varying systems. The main contributions are as follows: 1) this extended abstract propose a decomposition method for the Kalman filter; 2) a least square interpretation to the fusion scheme is demonstrated; 3) a convex optimization based secure estimation scheme is also proposed, and it is show 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 bounded estimate.

The extended abstract is organized as follows: Section II is the problem formulation. The Kalman filter decomposition and the least square interpretation are given in Section III. Section IV introduces the secure information fusion scheme. The numerical simulations are provided in Section V and this extended abstract ends with some concluding remarks in Section VI.

II. Problem Formulation

This extended abstract studies the following 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 $w(k)$ is the process noise. We assume that the initial condition satisfies $x(0) \sim \mathcal{N}(0, \Sigma)$ with $\Sigma > 0$; 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; $v_i(k)$ is the stochastic measurement noise and $a_i(k)$ 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 $y(k) = [y_1(k), \dots, y_m(k)]'$, $C(k) = [C_1(k)', \dots, C_m(k)']'$ and $a(k) = [a_1(k), \dots, a_m(k)]'$. 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.

Liang Xu, Xinghua Liu and Yilin Mo are with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Email: {xu_liang, liuxh, ylmo}@ntu.edu.sg

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 $\dot{x}(t) = Ax(t)$, $y_i(t) = C_i x(t), i = 1, \ldots, m$. Then $A(k) = \exp(A\tau)$, where τ is the time interval between two consecutive measurements. Moreover, $C(k) = [\tilde{C}'_i, \ldots, \tilde{C}'_m]'$ 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 the resource constraints of the attacker, we assume that at most p sensors can be compromised with arbitrarily chosen a_i. We try to propose a secure estimation scheme using the potentially compromised sensor measurement (3) such that when all the sensors are benign, the secure estimation scheme provides satisfactory estimation performance. In the case that p out of m senors are compromised, the secure estimation scheme can still guarantee a bounded estimation error for arbitrary attack signal a_i.

III. Kalman filter decomposition using local estimate

In this section, we assume that all the sensors are benign and propose a method to decompose the Kalman filter, which contains m local estimators using only local measurements and a fusion schemes to merge local estimates to obtain the Kalman estimate. We then show that the fusion procedure can be recast as a least square problem, based on which we further propose a secure estimation scheme in the next section.

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

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

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 condition

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

We further make the following assumptions,

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, then it is automatically invertible. Then the condition is equivalent to the invertibility of $I - K(k)C(k)$. If $Q(k) > 0, R(k) > 0$, we can show that $I - K(k)C(k)$ is also invertible. Since $P(k|k-1) > 0$, 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, we know that $P(k|k-1) - K(k)C(k)P(k|k-1) = (P(k|k-1)^{-1} + C(k)'R(k)^{-1}C(k))^{-1}$. Therefore $I - K(k)C(k)$ is invertible.

Under Assumption 2, let $F_i(0) = \frac{1}{m}I$, we can construct sequences $L_i(k), t \geq 1$ and $F_i(k), t \geq 1$ from

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

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

where

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

The local estimators are then defined as

$$\begin{aligned} \tilde{x}_i(k) = {} & (A(k-1) - L_i(k)C_i(k)A(k-1))\tilde{x}_i(k-1)\\ & + L_i(k)y_i(k), i = 1, \ldots, m, \end{aligned} \quad (7)$$

where $\tilde{x}_i(k)$ is the local estimate with initial condition $\tilde{x}_i(0) = \hat{x}(0) = K(0)y(0)$.

We then can show that the Kalman estimate is a weighted sum of the local estimate. The theorem can be proved by simply deriving the dynamics of $\sum_i^m F_i(k)\tilde{x}_i(k)$ and show that it is the same as that of the Kalman estimate (4).

Theorem 4: Under Assumption 2, with the designed local estimators (7), we have that

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

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

A. Least Square Interpretation

Let $e(k) = [e_1(k)', \ldots, e_m(k)']'$ with $e_i(k) = \tilde{x}_i(k) - x(k)$. Let $\Sigma_e(k) = E\{e(k)e(k)'\}$. From the definition of $e(k)$, we know that

$$\tilde{x}(k) = Hx(k) + e(k), \quad (8)$$

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

Define the following least square problem

$$\begin{aligned} &\min_{\check{x}, \check{e}} \frac{1}{2}\check{e}'\Sigma_e(k)^{-1}\check{e} \quad (9)\\ &s.t. \quad \tilde{x}(k) = H\check{x} + \check{e} \end{aligned}$$

Let the optimal variables be $\check{x}^*$, $\check{e}^*$. Then, after some algebraic manipulations, we can show that

Theorem 5: The solution to the least square problem (9) is given by

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

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

IV. Secure Information Fusion

In the presence of attacks, we have

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

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

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

Then we have

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

Therefore, in the presences of attacks, we can show that 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 based secure fusion scheme as a counterpart to the least square problem (9), which introduce a l_1 norm regularization term to promote sparsity of the estimated attack signal.

$$\begin{aligned} &\min_{\check{x}_s,\mu,\nu} \frac{1}{2}\mu'\Sigma_e(k)^{-1}\mu + \gamma\|\nu\|_1 \\ &s.t., \quad \tilde{x}(k) = H\check{x}_s + \mu + \nu \end{aligned} \tag{10}$$

Then following similar line of arguments as the proof of Lemma 3 in [10], we have the following lemma characterizing the solution to the optimization problem (10).

Lemma 6: Let $\check{x}_s^*$, μ^*, ν^* be the minimizer to the LASSO problem (10), and let $\check{x}^*$, $\check{e}^*$ be the minimizer to the least square problem (9). Then the following statements hold

- the following inequality holds
$$\|\Sigma_e(k)^{-1}\mu^*\|_\infty \le \gamma.$$
- 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 5 and Lemma 6, we have the following result.

Theorem 7: When all the sensors are benign, if the following conditions hold,

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

the LASSO estimate $\check{x}_s^*$ gives the Kalman estimate $\hat{x}(t)$.

The above theorem implies that a larger γ is preferred, since in the absence of attacks, a larger γ can guarantee that the secure 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 $e_1, \dots, e_m \in \mathbb{R}^n$ are vectors. With slightly abuse of notations, we define $f_i(e_1, \dots, e_m)$ 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 [10] and is omitted here.

Theorem 8: Suppose that $p < \frac{m}{2}$ sensors are compromised, then the error of the secure state estimate is bounded by

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

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

V. 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.

[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.

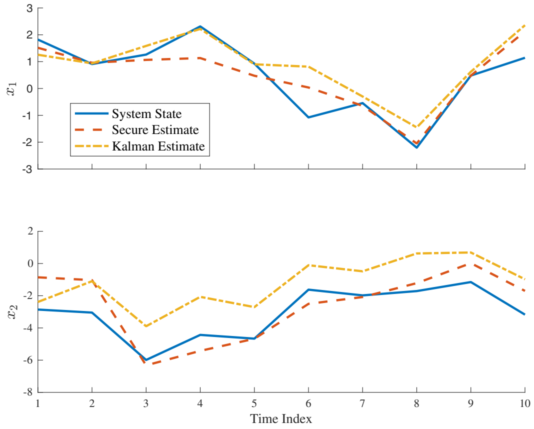

Fig. 1. Secure estimate v.s. Kalman estimate

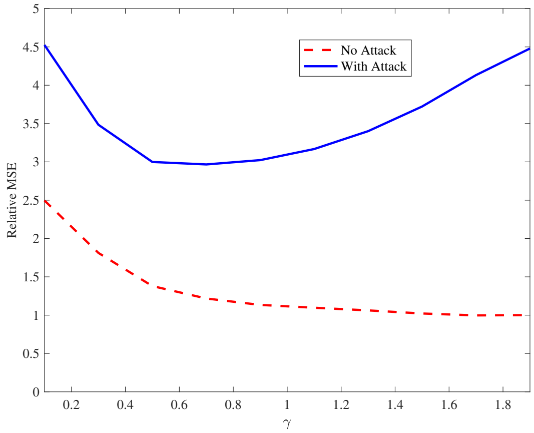

Fig. 2. Relative MSE v.s. different values of γ

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 $\gamma = 0.6$.

VI. Conclusions

This extended abstract studies the secure estimation problem of a time-varying linear process observed by multiple sensors. We first propose a method to decompose the Kalman filter using only local sensor measurements. Based on this decomposition, a convex optimization based secure estimation scheme is proposed. The performance of this secure estimation scheme both with and without attacks is analyzed. In the end, simulations are conducted to verify the derived result.

References

[1] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, “A survey of fault detection, isolation, and reconfiguration methods,” *IEEE Transactions on Control Systems Technology*, vol. 18, no. 3, pp. 636–653, 2010.

[2] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.

[3] 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.

[4] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus computation in unreliable networks: A system theoretic approach,” *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[5] Y. Mo and B. Sinopoli, “False data injection attacks in cyber physical systems,” in *First Workshop on Secure Control Systems*, 2010.

[6] Y. Mo and B. Sinopoli, “On the performance degradation of cyber-physical systems under stealthy integrity attacks,” *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[7] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure state-estimation for dynamical systems under active adversaries,” in *Proceedings of the 49th Annual Allerton Conference on Communication, Control, and Computing*, pp. 337–344, IEEE, 2011.

[8] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, “Robustness of attack-resilient state estimators,” in *Proceedings the 5th International Conference on Cyber-Physical Systems*, pp. 163–174, IEEE Computer Society, 2014.

[9] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, “Attack-resilient state estimation in the presence of noise,” in *Proceedings of the 54th Annual Conference on Decision and Control*, pp. 5827–5832, IEEE, 2015.

[10] 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.

[11] 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.

[12] 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.