Secure Filtering against Spatio-Temporal False Data Attacks under Asynchronous Sampling

Zishuo Li, Anh Tung Nguyen, André M. H. Teixeira, Yilin Mo, Karl H. Johansson

***Abstract*— This paper [1] addresses the secure state estimation problem for continuous linear time-invariant systems with non-periodic and asynchronous sampled measurements, where the sensors need to transmit not only measurements but also sampling time-stamps to the fusion center. This measurement and communication setup is well-suited for operating large-scale control systems and, at the same time, introduces new vulnerabilities that can be exploited by adversaries through (i) manipulation of measurements, (ii) manipulation of time-stamps, (iii) elimination of measurements, (iv) generation of completely new false measurements, or a combination of these attacks. To mitigate these attacks, we propose a decentralized estimation algorithm in which each sensor maintains its local state estimate asynchronously based on its measurements.**

I. Introduction & Problem Formulation

Many real-world large-scale systems, such as power systems, water distribution networks, and transportation networks, are examples of cyber-physical systems where physical processes are tightly coupled with digital devices. These systems are monitored and controlled via wired or wireless communications, leaving the systems vulnerable to malicious attackers. The asynchronous and non-periodic sampling scheme opens up new opportunities for the adversaries. The challenge of securely estimating states under malicious activities will be addressed in this paper, given their crucial role in control systems.

Let us denote the state index set as $\mathcal{J} \triangleq \{1, 2, \dots, n\}$ and the sensor index set as $\mathcal{I} \triangleq \{1, 2, \dots, m\}$. The LTI system is modeled as follows:

$$\dot{x}(t) = Ax(t) + w(t), \ w(t) \sim \mathcal{N}(0, Q) \tag{1}$$

$$y_i(t) = C_i x(t) + v_i(t), \ \forall\, i \in \mathcal{I}, \tag{2}$$

where $v(t) \sim \mathcal{N}(0, R)$. The sensors sample and send data packets to an estimator in a non-periodic and asynchronous manner, which contain not only measurements but also their sensor indices and sampling time-stamps. More specifically, the estimator receives measurement triples from sensor $i \in \mathcal{I}$, which has the following form:

$$\textbf{measurement triple: } (i,\ t,\ y_i(t)), \tag{3}$$

This work is supported by the National Natural Science Foundation of China under grant no. 62273196, the Swedish Research Council under the grant 2021-06316, the Swedish Foundation for Strategic Research, the Swedish Research Council Distinguished Professor grant 2017-01078, and the Knut and Alice Wallenberg Foundation Wallenberg Scholar grant.

Zishuo Li and Yilin Mo are with the Department of Automation, Tsinghua University, China. Anh Tung Nguyen and André M. H. Teixeira are with the Department of Information Technology, Uppsala University, Sweden. Karl H. Johansson is with School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Sweden. He is also affiliated with Digital Futures.

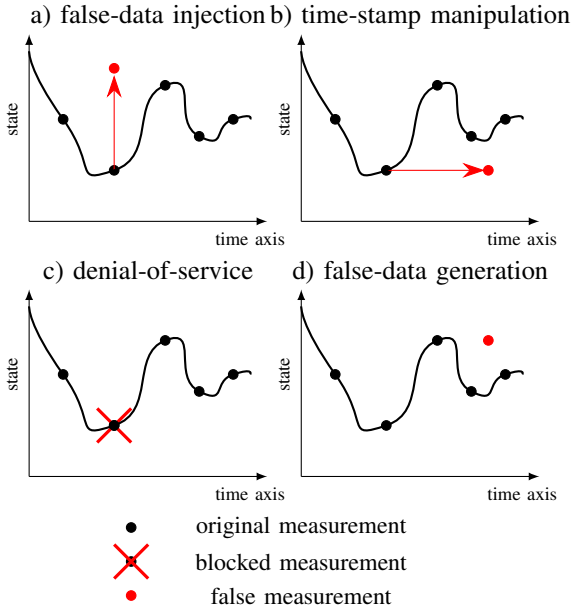

Fig. 1: Examples of spatio-temporal false data attacks that can manipulate both time-stamps and measurements.

where i is the sensor index, t is the sampling time-stamp, and $y_i(t)$ is the measurement given by sensor i. In this paper, we propose a novel false data attack model for such systems which manipulate elements in the measurement triple (3) (see Fig. 1). This attack model includes both integrity attacks such as false-data injection, and availability attacks such as DoS attacks. To deal with such false data attacks, we propose an estimation scheme in the next section.

II. Secure State Estimation

A. Asynchronous sampled-data Kalman filter

We define the measurement availability index $\phi_i[k] \in \{0, 1\}$ where $\phi_i[k] = 1$ if sensor i has a measurement with time-stamp t_k and $\phi_i[k] = 0$ otherwise. At each sampling instant k, we have the following asynchronous sampled-data Kalman filter (KF):

Prediction steps:

$$\hat{x}_{\text{-}}[k] = A[k-1]\hat{x}[k-1], \tag{4a}$$

$$P_{\text{-}}[k] = A[k-1]P[k-1]A^{\top}[k-1] + Q[k-1], \tag{4b}$$

Update steps:

$$K[k] = P_{\text{-}}[k]C^{\top}[k]\big(C[k]P_{\text{-}}[k]C^{\top}[k] + R[k]\big)^{\dagger}, \tag{4c}$$

$$P[k] = (I - K[k]C[k])P_{\text{-}}[k], \tag{4d}$$

$$\hat{x}[k] = \hat{x}_{\text{-}}[k] + K[k]\left(y[k] - C[k]\hat{x}_{\text{-}}[k]\right), \tag{4e}$$

B. Linear decomposition

Define

$$\Pi[k-1] \triangleq A[k-1] - K[k]CA[k-1]. \tag{5}$$

$$G_i[k] \triangleq \Pi[k-1]G_i[k-1]A^{-1}[k-1] + K_i[k]C_i. \tag{6}$$

$$\boldsymbol{W}[k+1] \triangleq \boldsymbol{\Pi}[k]\boldsymbol{W}[k]\boldsymbol{\Pi}^{\top}[k] + \boldsymbol{Q}[k], \tag{7}$$

where $\boldsymbol{Q}[k]$ is based on system parameters. The local estimator at sensor i is defined as:

$$\zeta_i[k] \triangleq \Pi[k-1]\zeta_i[k-1] + K_i[k]y_i[k], \tag{8}$$

which is initialized as $\zeta_i[0] = \mathbf{0}$. From (4e), (5), and (8), one obtains the following property

$$\hat{x}[k] = \sum_{i=1}^{m} \zeta_i[k]. \tag{9}$$

C. Least-square fusion

The state estimation provided by the sampled-data KF (4e) can be recovered by the minimizer $x_{\rm ls}$ to the following optimization problem [1, Thm. 1]:

$$\underset{x_{\rm ls}[k],\theta[k]}{\text{minimize}} \quad \frac{1}{2}\theta[k]^{\top}\boldsymbol{W}^{-1}[k]\theta[k] \tag{10a}$$

$$\text{subject to} \quad \boldsymbol{\zeta}[k] = \boldsymbol{G}x_{\rm ls}[k] + \theta[k] \tag{10b}$$

D. Secure least-square fusion

All the false data attacks in Fig. 1 can be isolated into local estimator (8) whose corresponding sensor is under attack [1, Sec. IV]. This enables us to introduce the following ℓ_1-regularization least-square optimization problem:

$$\underset{\check{x}[k],\,\mu[k],\,\vartheta[k]}{\text{minimize}} \quad \frac{1}{2}\mu[k]^{\top}\boldsymbol{W}^{-1}[k]\,\mu[k] + \gamma\,\|\vartheta[k]\|_1 \tag{11a}$$

$$\text{subject to} \quad \boldsymbol{\zeta}[k] = \boldsymbol{G}\check{x}[k] + \mu[k] + \vartheta[k]. \tag{11b}$$

The following theorem provides a sufficient condition on the parameter γ in (11) under which the solutions to (10) and (11) are identical in the absence of attacks.

Theorem 1: Consider the least square problems (10) and (11) with a given $\gamma > 0$, let $(x_{\rm ls}[k],\, \theta[k])$ be the minimizer for the problem (10) and $(\check{x}[k],\, \mu[k],\, \vartheta[k])$ be the minimizer for the problem (11). In the absence of the attacks, if the following condition holds

$$\gamma > \|\tilde{\boldsymbol{W}}^{-1}[k]\theta[k]\|_{\infty}, \tag{12}$$

then $\check{x}[k] = x_{\rm ls}[k]$, $\mu[k] = \theta[k]$, and $\vartheta[k] = 0$. ◁

Let us make use of the following definition of a function that will help us in evaluating the minimizer $\check{x}[k]$ of (11) against spatio-temporal attacks in the subsequent theorem.

Definition 1: Given an n-dimensional vector $x \in \mathbb{R}^n$ and a positive integer a, we define a function $h_a : \mathbb{R}^n \to \mathbb{R}$ such that $h_a(x)$ takes the a-th largest value of the vector x.

Theorem 2 (Secure fusion): Consider the least square problems (10) and (11) with a given $\gamma > 0$, let $(x_{\rm ls}[k],\, \theta[k])$ be the minimizer for the problem (10) in the absence of attacks and $(\check{x}[k],\, \mu[k],\, \vartheta[k])$ be the minimizer for the problem (11) in the presence of attacks. In the presence of attacks, the error between $x_{\rm ls}[k]$ and $\check{x}[k]$ has the following upper bound:

$$\left|\left[\check{x}[k]\right]_j - \left[x_{\rm ls}[k]\right]_j\right| \le \max\left\{\left|h_c\big(\eta^j[k]\big)\right|,\ \left|-h_c\big(-\eta^j[k]\big)\right|\right\},$$

where $\eta^j[k]$ is a $|\mathcal{E}_j \setminus \mathcal{C}|$-dimensional vector where its i-th element $[\eta^j[k]]_i \triangleq [\theta_i[k]]_j + \gamma\, \boldsymbol{e}^{\top}_{n(i-1)+j}\tilde{\boldsymbol{W}}[k]\check{\vartheta}[k]$ $(\forall\, i \in \mathcal{E}_j \setminus \mathcal{C})$, with

$$\check{\vartheta}[k] \in \partial\|\boldsymbol{V}[k]\boldsymbol{\zeta}^f[k] - \vartheta[k]\|_1,\ c \triangleq \left\lceil \frac{|\mathcal{E}_j \setminus \mathcal{C}| - |\mathcal{E}_j \bigcap \mathcal{C}|}{2} \right\rceil.$$

◁

III. Simulation Results

We show an example of state estimation problem in electricity monitoring in Fig. 2 (left). To validate the efficiency of the proposed state estimation in the previous section, we implement it in the IEEE 14-bus system with false data attacks on buses 2-5 (see Fig. 2 right-top corner). The estimation error is shown in Fig. 2 right-bottom corner where the state estimate provided by (11) is resilient to attacks.

References

[1] Z. Li, A. T. Nguyen, A. M. Teixeira, Y. Mo, and K. H. Johansson, "Secure filtering against spatio-temporal false data attacks under asynchronous sampling," *arXiv preprint arXiv:2411.19765*, 2024.

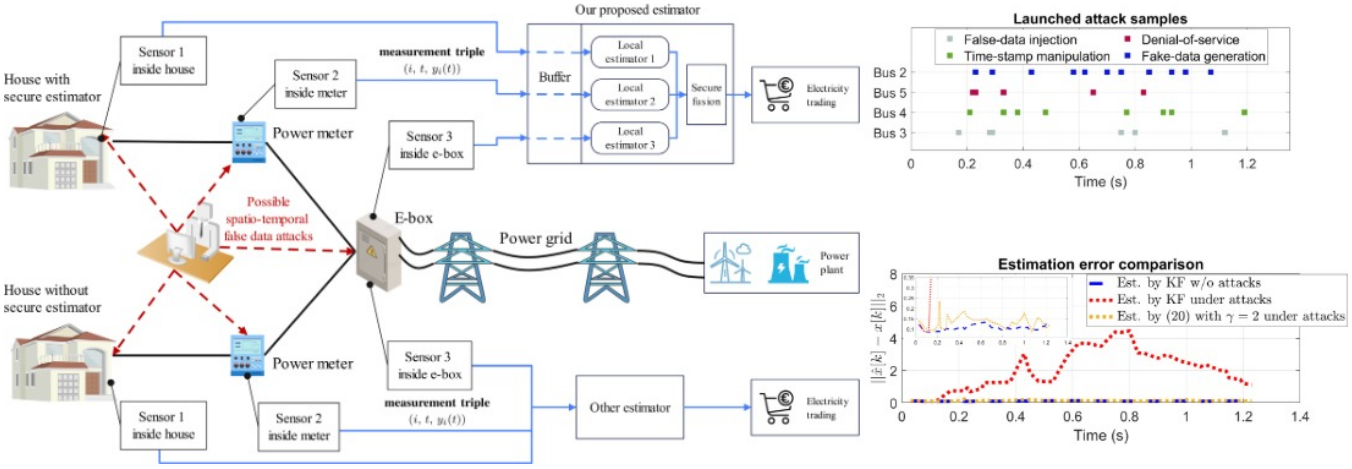

Fig. 2: An example in electricity consumption monitoring (left) and simulation results (right).