2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Secure State Estimation with Asynchronous Measurements against Malicious Measurement-data and Time-stamp Manipulation

Zishuo Li[1], Anh Tung Nguyen[2], André M. H. Teixeira[2], Yilin Mo[1], Karl H. Johansson[3]

***Abstract*— This paper proposes a secure state estimation scheme with asynchronous non-periodic measurements for continuous LTI systems under false data attacks on measurement transmission channels. Each sensor transmits the measurement information in a triple comprised of its sensor index, the time-stamp, and the measurement value to the fusion center via unprotected communication channels. A malicious attacker can corrupt a subset of sensors by (i) manipulating the time-stamp and the measurement value, (ii) blocking transmitted measurement triples, or (iii) injecting fake measurement triples. To deal with such attacks, we propose a secure state estimator by designing decentralized local estimators and fusing all the local states by the median operator. The local estimators receive the sampled measurements and update their local state in an asynchronous manner, while the fusion center triggers the fusion and generates a secure estimation in the presence of a local update. We prove that local estimators of benign sensors are unbiased with stable error covariance. Moreover, the fused secure estimation error has bounded expectation and covariance against at most p corrupted sensors as long as the system is $2p$-sparse observable. The efficacy of the proposed scheme is demonstrated through a benchmark example of the IEEE 14-bus system.**

I. Introduction

Recent reports have shown the disastrous consequences of malware for an industrial control system in Iran and a Ukrainian power grid [1], [2]. Motivated by these and many other examples in [2], security is an essential element of cyber-physical systems. In particular, the challenge of securely estimating unmeasured states under malicious activities has been widely addressed [3]–[9], given the crucial role of state estimation in control systems. This challenge, known as secure state estimation of control systems, is mainly addressed through considering asynchronous non-periodic sampled systems in this paper.

In asynchronous non-periodic sampled systems, where measurement data is sampled at different rates, data packages of the measurement, sent to the estimator over unprotected communication channels, are vulnerable to malicious attackers. In this paper, we propose a novel model of false data attacks on the asynchronous non-periodic sampled system (see Fig. 1). This novel attack includes both integrity attacks such as false-data injection [7], and availability attacks such as denial-of-service attacks [8], [9]. Moreover, we investigate the influence of time-stamp manipulation caused by malicious attackers. Apart from those attacks, injecting fake data packages into authentic measurement streams is also a serious threat to the asynchronous non-periodic sampled system due to its stealthiness. Our introduced attack model unifies all the above attacks into one framework without excluding the possibility of their combinations. To deal with the problem of secure state estimation against false data injection attacks, three research directions consisting of the sliding window method, the estimator switching method, and the local decomposition-fusion method, have been mainly developed in recent years [3]–[6]. On the other hand, to handle Denial-of-Service attacks, which are conducted on multiple transmission channels, a class of partial observers that provide reliable partial state estimates is proposed in [8]. One of the most ubiquitous techniques used to effectively deal with DoS attacks is event-triggered mechanisms [9].

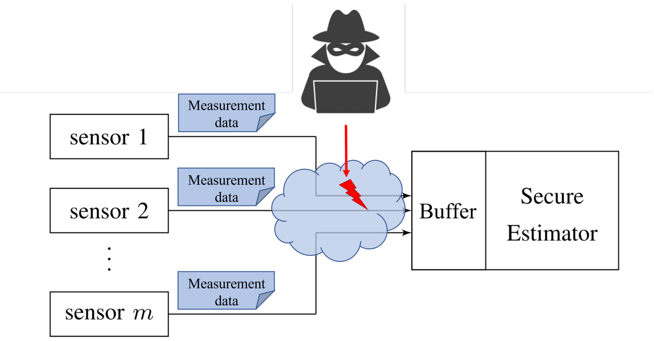

Fig. 1. The general state estimation scheme with a measurement buffer dealing with out-of-order sequence [10] where some communication channels are compromised by a malicious attacker.

To the best of our knowledge, comparatively little progress has been made toward studying the negative influence of time-stamp manipulation on the state estimation performance, especially on asynchronous sampled systems. Li et al. [11] and Guo et al. [12] propose Kalman filter-based algorithms for non-uniformly sampled multi-rate systems. To deal with the problem of the asynchronous linear and nonlinear sampled systems, the authors in [13] propose a class of continuous-discrete observers, resulting in a differential Riccati equation. They show the stability of such a differen-

This work is supported by the Swedish Research Council under the grants 2018-04396 and 2021-06316, by the Swedish Foundation for Strategic Research, and by the National Natural Science Foundation of China under grant no. 62273196.

[1] Zishuo Li and Yilin Mo are with the Department of Automation, Tsinghua University, Beijing, 100084, China. {lizs19@mails, ylmo@mail}.tsinghua.edu.cn

[2] Anh Tung Nguyen and André M. H. Teixeira are with the Department of Information Technology, Uppsala University, PO Box 337, SE-75105, Uppsala, Sweden. {anh.tung.nguyen, andre.teixeira}@it.uu.se

[3] Karl H. Johansson is with School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm SE-100 44, Sweden. kallej@kth.se

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

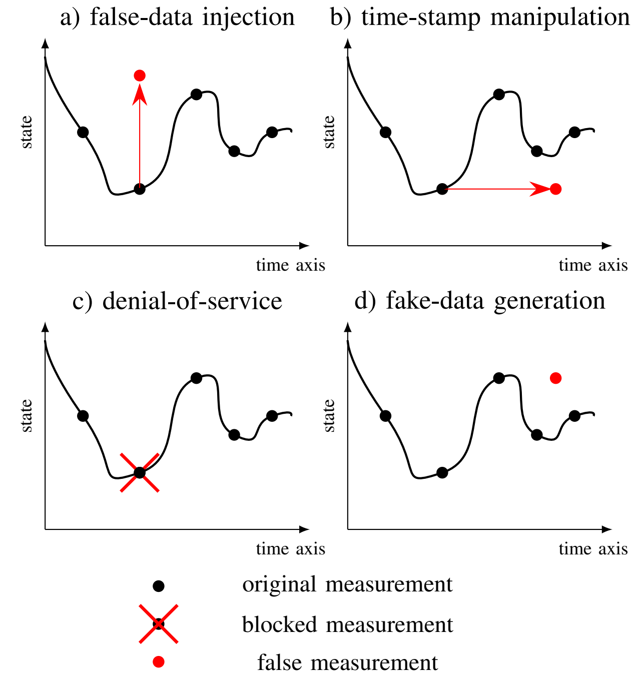

Fig. 2. Examples of the spatio-temporal false data attack that can manipulate both the time-stamp value and the measurement value.

tial Riccati equation, which guarantees the convergence of the observers. Ding et al. [14] and Muhammad et al. [15] analyze the observability degradation problem of multi-rate and non-periodic sampled systems. For time-stamp-related attacks, the negative impact of Time Synchronization Attack (TAS) on smart grids is studied by the authors in [16].

In this paper, we first propose a novel spatio-temporal false data attack model, as depicted in Fig. 2. Then, we design a secure estimation algorithm to recover the system state in the presence of such a spatio-temporal false data attack on a fixed number of sensors (say p corrupted sensors). The algorithm has the following merits:

(1) The proposed algorithm adopts an asynchronous non-periodic sampling framework. Thus, the algorithm is capable of including synchronous sampling and multi-rate sampling scenarios.
(2) The negative impact of the spatio-temporal false data attack is transformed into the value change of local state estimations. This transformation enables us to handle such an attack by using a resilient fusion algorithm that can generate secure state estimation.
(3) Given the $2p$-sparse observability of the system, we show that the proposed estimation has a stable error. Moreover, we give explicit estimation error expectation and covariance bounds in the presence of spatio-temporal false data attacks.

We conclude this section by introducing the notation that will be utilized throughout this paper.
Notation: The sets of positive integers, non-negative integers, and non-negative real numbers are denoted as $\mathbb{Z}_{>0}, \mathbb{Z}_{\geq 0}$, and $\mathbb{R}_{\geq 0}$, respectively. The cardinality of a set $\mathcal{S}$ is denoted as $|\mathcal{S}|$. Denote the span of row vectors of matrix A as $\mathrm{rowspan}(A)$. All-zero and all-one matrices with an appropriate size are denoted as $\mathbf{0}$ and $\mathbf{1}$, respectively. We denote I as an identity matrix with an appropriate dimension. The spectral radius of matrix A is denoted as $\rho(A)$. For a vector x, $[x]_j$ stands for its j-th entry. We denote the continuous time index in a pair of parenthesis $(\cdot)$ and the discrete-time index in a pair of brackets $[\cdot]$.

II. Problem Formulation and Preliminaries

In this section, we first introduce the system, the modeling of asynchronous measurements, and several assumptions that will be used throughout this paper. Secondly, we present a novel spatio-temporal false data attack. Finally, the secure estimation problem is formulated.

A. State Estimation with Asynchronous Measurements

We consider a continuous LTI system:

$$\dot{x}(t) = Ax(t) + w(t), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the system state and the process noise $w(t)$ is a Wiener process. The process noise from time t_1 to t_2 is denoted as $w(t_1, t_2)$ and the corresponding covariance is $Q \cdot (t_2 - t_1)$ where Q is a positive semi-definite matrix. The initial state $x(0)$ is assumed to be a Gaussian random vector with a known expectation and is independent of the measurement noise. We introduce the following assumption on A to prevent system observability degradation problems.

Assumption 1. *The geometric multiplicity of all the eigenvalues of A is 1.*

Without loss of generality, Assumption 1 enables us to assume that A is in the Jordan canonical form. Let us denote the sensor index set as $\mathcal{I} \triangleq \{1, 2, \dots, m\}$ and the state index set as $\mathcal{J} \triangleq \{1, 2, \dots, n\}$. We consider a general asynchronous non-periodic sampling scenario where the estimation operator receives measurement triples from sensor $i \in \mathcal{I}$, which has the following form:

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

where i is the sensor index, t is the time-stamp, and $y_i(t)$ is the measurement value given by sensor i. Sensor i provides scalar measurement values with the measurement model as

$$y_i(t) = C_i x(t) + v_i(t), \tag{2}$$

where $C_i \in \mathbb{R}^{1 \times n}$ is the measurement matrix and $v_i(t) \in \mathbb{R}$ is Gaussian measurement noise with time-varying covariance $R_i(t)$ which is under the following assumption.

Assumption 2. *For every sensor $i \in \mathcal{I}$, its corresponding measurement noise covariance $R_i(t)$ satisfies the following:*

$$0 \leq R_i(t) \leq \bar{r}, \quad \forall t \in \mathbb{R}_{\geq 0},$$

where $\bar{r}$ is a given positive constant scalar.

For convenience, let us define $C \triangleq [C_1^\top, \cdots, C_m^\top]^\top$. We employ the following assumption, which is conventional in literature (e.g. [5]), to facilitate our design of a secure state estimation algorithm in the subsequent section.

Assumption 3. *The system (A, C) is $2p$-sparse observable, i.e., the system $(A, C_{\mathcal{I}\setminus\mathcal{M}})$ is observable*[1] *for any subset $\mathcal{M} \subset \mathcal{I}$ where $|\mathcal{M}| = 2p$.*

Define the set of sampling time-stamps from sensor i as Γ_i. Without loss of generality, the time when the estimation starts working is set as $t_0 = 0$. In order to guarantee system observability under non-uniform asynchronous measurements, we introduce the following notation and assumptions. Define the set of sampling time intervals and cumulative sampling time from sensor i as follows

$$\mathcal{T} \triangleq \bigcup_{i=1}^{m} \mathcal{T}_i,\ \mathcal{T}_i \triangleq \{t_k - t_{k-1} \mid t_k, t_{k-1} \in \Gamma_i, k \in \mathbb{Z}_{>0}\},$$

$$\widetilde{\mathcal{T}} \triangleq \bigcup_{i=1}^{m} \widetilde{\mathcal{T}}_i,\ \widetilde{\mathcal{T}}_i \triangleq \{t_k - t_j \mid t_k, t_j \in \Gamma_i, k > j, k, j \in \mathbb{Z}_{\geq 0}\}.$$

Define the system pathological sampling interval set [14] as

$$\mathcal{T}^* \triangleq \{T > 0 \mid \exp(\lambda_i T) = \exp(\lambda_j T),\ i \neq j,\ \lambda_i, \lambda_j \in \mathrm{sp}(A) \subseteq \mathbb{C}\}.$$

To prevent system observability degradation problems due to discrete-time samplings, the following assumption, which is also seen in [14], [15], is introduced.

Assumption 4 (non-pathological sampling time)**.** *The sampling time interval set $\mathcal{T}$ satisfies the following conditions:*

$$\sup \mathcal{T} \leq T_{\max} \text{ and } \widetilde{\mathcal{T}} \cap \mathcal{T}^* = \varnothing.$$

B. Measurement-data and time-stamp manipulation

In this section, we introduce a novel spatio-temporal false data attack that generalizes integrity attacks and availability attacks (see Fig. 2 for more detail). For the convenience of denotation about the measurement sampling process, we introduce the measurement triple generation set as all the measurement triples with time-stamp t:

$$\mathcal{S}(t) = \{(i, t, y_i(t)) \mid i \in \mathcal{I}\}.$$

Moreover, $\mathcal{S}^a(t)$ denotes the set of measurement triples with time-stamp t after being manipulated by the attacker. Denote the set of corrupted sensors as $\mathcal{C}$, which is fixed over time. The spatio-temporal false data attack is defined as follows:

Definition 1 (spatio-temporal false data attack)**.** *The attacker can manipulate measurement triples given by corrupted sensor $i \in \mathcal{C}$ in the following four ways:*

(i) false-data injection $(i, t, y_i^a(t)) \leftarrow (i, t, y_i(t))$,

(ii) time-stamp manipulation $(i, t^a, y_i(t)) \leftarrow (i, t, y_i(t))$,

where $(i, t, y_i(t)) \in \mathcal{S}(t)$. The notation $y_i^a(t)$ and t^a stand for the attacked data.

(iii) denial-of-service $\mathcal{S}^a(t) \leftarrow \mathcal{S}(t) \setminus (i, t, y_i(t))$,

(iv) fake-data generation $\mathcal{S}^a(t) \leftarrow \mathcal{S}(t) \cup \left(i, t^f, y_i^f(t)\right)$,

where $(i, t, y_i(t)) \in \mathcal{S}(t)$, $(i, t^f, y_i^f(t)) \notin \mathcal{S}(t)$, the superscript "$f$" means "fake" (not real measurement).

If the set of corrupted sensors satisfies $|\mathcal{C}| \leq p$, malicious activities are called p-sparse spatio-temporal false data attacks.

Remark 1. *The system operator does not know set $\mathcal{C}$ or the integer p, and thus the algorithm will be proposed later regardless of $\mathcal{C}$ or p. However, if the system has knowledge of p, we can check the observability redundancy offline. If the sparse observability index is larger than $2p$, then the algorithm is guaranteed to be secure. Otherwise, the system operator can resort to other methods to increase system resilience such as introducing more sensors.*

In the scope of this paper, we study the p-sparse spatio-temporal false data attack. The manipulated time-stamp set Γ^a is defined as follows:

$$\Gamma^a \triangleq \bigcup_{i=1}^{m} \Gamma_i^a, \qquad \Gamma_i^a \triangleq \{t \mid (i, t, y_i(t)) \in \mathcal{S}^a(t)\}. \tag{3}$$

Due to various delays, received measurement time-stamps may not be in increasing order, resulting in the out-of-sequence problem [10], [17], [18]. This problem is generally dealt with by utilizing the *Buffering* method. The buffer simply stores all the measurements from a time window of length d before sending them to the estimator, where d is the maximum delay of a measurement sample [10], [17], [18]. Measurements, delayed more than d, are seen as non-informative and discarded from the buffer. In this way, the measurement sequence after the buffer is sorted in the correct order. In this paper, we assume a similar buffering system is working before the secure estimator (see Fig. 1), yielding the following assumption.

Assumption 5. *The incoming manipulated time-stamp is in a strictly increasing order, i.e., $\Gamma^a = \{t_0, t_1, t_2, \cdots\}$ and $0 = t_0 < t_i < t_{i+1},\ \forall i \in \mathbb{Z}_{>0}$.*

Now, we are ready to formulate the secure state estimation problem with asynchronous measurements in the following.

C. Secure state estimation problem

The communication protocol among sensors and the buffer depicted in Fig. 1 leaves the system vulnerable to spatio-temporal false data attacks in Definition 1. To estimate the system states under such attacks, this paper will deal with a secure state estimation problem, which is defined below.

Problem 1 (Secure state estimation)**.** *Find an estimator that is a measurable time-varying function $f_t(\cdot)$ of all manipulated measurement triples:*

$$\hat{x}(t) = f_t(\mathcal{S}^a(\tau), 0 \leq \tau \leq t)$$

[1] The matrix $C_{\mathcal{I}\setminus\mathcal{M}}$ represents the matrix composed of rows of C with row index in $\mathcal{I} \setminus \mathcal{M}$.

such that the estimation error expectation and covariance are uniformly bounded at sampling instants:

$$\sup_{t\in\Gamma^a} \|\mathbb{E}\left[\hat{x}(t)-x(t)\right]\|_\infty \le \gamma_e(A,C,Q,\bar{r}),$$
$$\sup_{t\in\Gamma^a} \operatorname{Cov}\left[\hat{x}(t)-x(t)\right] \preceq \gamma_c(A,C,Q,\bar{r})\cdot I,$$

where $\gamma_e(A,C,Q,\bar{r})$ and $\gamma_c(A,C,Q,\bar{r})$ are scalars determined by system parameters $A,C,Q,\bar{r}$ and independent of attacks. The notation $\mathbb{E}[\cdot]$ and $\operatorname{Cov}[\cdot]$ are the expectation and the covariance with respect to the probability measure generated by the Gaussian noise, respectively.

Remark 2. *In Problem 1, we only consider the estimation error at sampling times $t_k \in \Gamma^a$, because the estimation between sampling times $t \notin \Gamma^a$ is trivially provided by the following prediction for t in interval $\left(t_k, t_{k+1}\right)$, where t_k and $t_{k+1} \in \Gamma^a$:*

$$\hat{x}(t) = \hat{x}(t_k) + \exp(A(t-t_k)),$$

and the estimation error are determined by $\hat{x}(t_k)$.

With the help of the above assumptions and definitions, we are ready to deal with Problem 1 by designing a secure state estimation algorithm in the following section.

III. Secure Estimation Design

In this section, we first introduce some preliminaries on the local observable subspace decomposition. Secondly, the design of secure state estimation with the consideration of asynchronous measurement is presented. Finally, The analysis of resilient state estimation concludes the section.

A. Local Observable Subspace Decomposition

Consider the system (1) and the output measurement (2) corresponding to sensor i, define the observability matrix with respect to sensor i as

$$O_i \triangleq \begin{bmatrix} C_i^\top & (C_iA)^\top & \cdots & \left(C_iA^{n-1}\right)^\top \end{bmatrix}^\top. \tag{4}$$

Then, the local observable subspace of sensor i is defined as

$$\begin{aligned}\mathbb{O}_i &\triangleq \operatorname{rowspan}(O_i)\\ &= \operatorname{span}\left(C_i^\top, (C_iA)^\top, \cdots, \left(C_iA^{n-1}\right)^\top\right).\end{aligned}$$

Denote the dimension of the linear space $\mathbb{O}_i$ as n_i. The global observable space of the entire system is given by $\mathbb{O} \triangleq \cup_{i\in\mathcal{I}}\mathbb{O}_i$. Define $\mathbf{e}_j$ as a canonical basis vector with dimension n where 1 is on the j-th entry and 0 is on all the other entries. Recalling Assumption 1 about the Jordan canonical form of matrix A, this assumption enables us to define the index set of states that can be observed by sensor i as

$$\mathcal{Q}_i \triangleq \{j \in \mathcal{J} \mid O_i\mathbf{e}_j \neq \mathbf{0}\}. \tag{5}$$

The following theorem characterizes the structure of $\mathbb{O}_i$.

Theorem 1. *If Assumption 1 holds, then the local observable space $\mathbb{O}_i$ can be represented as the linear span of the following canonical basis vectors:*

$$\mathbb{O}_i = \operatorname{span}\{\mathbf{e}_j, j\in\mathcal{Q}_i\}.$$

Proof. The proof directly follows our previous results [19, Appendix A]. □

We stack the basis of $\mathbb{O}_i$ in a matrix $H_i \in \mathbb{R}^{n_i\times n}$:

$$H_i \triangleq \begin{bmatrix}\mathbf{e}_{j_1} & \mathbf{e}_{j_2} & \cdots & \mathbf{e}_{j_{n_i}}\end{bmatrix}^\top. \tag{6}$$

where $\{j_1,\cdots,j_{n_i}\} = \mathcal{Q}_i$. Therefore, matrix H_i represents the transformation from $\mathbb{O}$ to $\mathbb{O}_i$, and plays a crucial role in our design of the decentralized observers. We further define the following local system matrices. Define the state transition matrix from time t to t' as

$$\Lambda(t'-t) = \exp(A\cdot(t'-t)). \tag{7}$$

Define

$$\tilde{A}_i(t) \triangleq H_i\Lambda(t)H_i^\top \in \mathbb{C}^{n_i\times n_i}, \tag{8}$$
$$\tilde{C}_i \triangleq C_iH_i^\top \in \mathbb{C}^{1\times n_i}. \tag{9}$$

The following properties of the transformation matrix H_i are important to the design of local estimators.

Lemma 1. *If Assumption 1 holds, then the following properties hold for every sensor $i\in\mathcal{I},\ t\in\mathbb{R}_{\ge 0}$:*

$$H_i\Lambda(t) = \tilde{A}_i(t)H_i, \tag{10}$$
$$C_i\Lambda(t) = \tilde{C}_i\tilde{A}_i(t)H_i. \tag{11}$$

Moreover, if (A,C) is observable, the pair $(\tilde{A}_i(t),\tilde{C}_i)$ is observable for every sensor $i\in\mathcal{I}, t\in\mathbb{R}_{\ge 0}$.

Proof. Notice that if A is in Jordan canonical form, then $\exp(At), t>0$ is also in Jordan canonical form. Thus, the result directly follows our previous result [19, Lemma 2]. □

Lemma 1 affords us to design local state estimators of the decentralized observer when asynchronous non-periodic sensor measurements are considered in the next subsection.

B. Secure estimation with asynchronous measurements

In the following, we propose a local estimator that maintains an estimate of $H_ix(t)$, i.e., the system state $x(t)$ is projected on local subspace $\mathbb{O}_i$. For the convenience of denotation about whether sensor i receives a measurement triple with time-stamp t, we introduce the index function $\psi_i(t)$ as follows:

$$\psi_i(t) = \begin{cases}1, & \text{if } (i,t,y_i(t)) \in \mathcal{S}^a(t)\\ 0, & \text{if } (i,t,y_i(t)) \notin \mathcal{S}^a(t)\end{cases}.$$

The index function $\psi_i(t)$ is utilized to indicate whether sensor i has a new measurement with time-stamp t. This local information $\psi_i(t)$ is only available to the local estimator i. Our proposed algorithm is based on two steps:

(1) Local state update: At each sampling time t_k, the dynamics of local estimate $\eta_i[k]$ corresponding to sensor i is defined as

$$\begin{aligned}\eta_i[k] &= \tilde{A}_i(t_k-t_{k-1})\eta_i[k-1]\\ &\quad+\psi_i(t_k)L_i[k]\left(y_i(t_k)-\tilde{C}_i\tilde{A}_i(t_k-t_{k-1})\eta_i[k-1]\right).\end{aligned} \tag{12}$$

The local estimate η_i is initialized as $\eta_i[0] = H_i\mathbb{E}[x(0)]$. Here, we assume that the expected initial state $\mathbb{E}[x(0)]$ is known. If it is unknown, we still have stable estimation results (see Remark 3). If sensor i does not have a measurement at time t_k, i.e., $\psi_i(t_k) = 0$, the local state update (12) degenerates into pure prediction $\eta_i[k] = \tilde{A}_i(t_k - t_{k-1})\eta_i[k-1]$. The design process of gain $L_i[k]$ will be provided in the next subsection after introducing the following state fusion protocol.

(2) State fusion: Due to the simple form of H_i, the fusion of all local estimates is done by taking the median:

$$[\hat{x}[k]]_j \triangleq \text{med}\{\left[H_i^\top \eta_i[k]\right]_j, i \in \mathcal{F}_j\}, \tag{13}$$

where $\mathcal{F}_j$ is designed as the index set of sensors that can observe state j as follows:

$$\mathcal{F}_j \triangleq \{i \in \mathcal{I} \mid O_i\mathbf{e}_j \neq \mathbf{0}\}. \tag{14}$$

C. Design of local observer gain

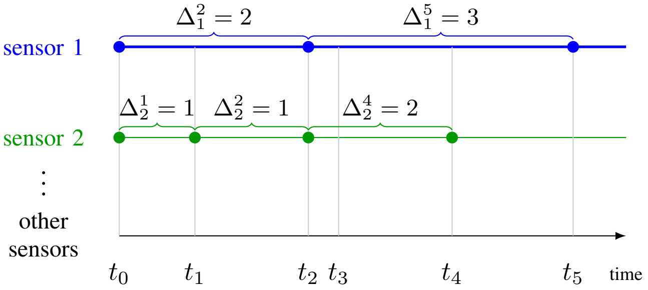

Fig. 3. An illustration of the time interval notation. The round dot denotes the time-stamp when the corresponding sensor samples the measurement. Integer Δ_i^k represents the total number of intervals between time-stamps, from the last measurement sampled at sensor i to the current time-stamp t_k. For example, when sensor 1 receives a measurement with time-stamp t_5, it will recall its last time-stamp t_2 and record $\Delta_1^5 = 5 - 2 = 3$. The time difference since last sample is thus denoted by $t_5 - t_{5-\Delta_1^5} = t_5 - t_2$.

Define the stamp step index before sensor i receives measurement with time-stamp t_k as $t_{k-\Delta_i^k}$ (see Fig. 3) where

$$\Delta_i^k \triangleq \min\{\Delta \in \mathbb{Z}_{>0} | \psi_i(t_{k-\Delta}) = 1\}. \tag{15}$$

Notice that Δ_i^k is valid only when k and i satisfy $\psi_i(t_k) = 1$. The value of Δ_i^k only requires local information of the last stamp step index at sensor i (as depicted in Fig. 3). In the design of local estimators (12), the estimator gain $L_i[k]$ should satisfy the following condition when a new measurement comes, i.e. when $\psi_i(t_k) = 1$:

$$\rho\left((I - L_i[k]\tilde{C}_i)\tilde{A}_i\left(t_k - t_{k-\Delta_i^k}\right)\right) \leq \bar{\rho} < 1, \tag{16}$$

where $\bar{\rho}$ is a predefined design parameter to balance the weight between historical estimation and new measurements. Since t_k and $t_{k-\Delta_i^k}$ are local knowledge known to sensor i, with prescribed parameter $\bar{\rho}$ known, the inequality (16) only requires local information and the calculation of $L_i[k]$ can be done in a decentralized manner. Since $\left(\tilde{A}_i(t), \tilde{C}_i\right)$ is observable from Lemma 1 and $\tilde{A}_i(t)$ is non-singular for $t \in \mathbb{R}_{>0}$, the system $\left(\tilde{A}_i(t), \tilde{C}_i\tilde{A}_i(t)\right)$ is also observable. According to the Pole Assignment Theorem [20], there **always exists** $L_i[k]$ such that inequality in (16) is satisfied. The following lemma ensures that such $L_i[k]$ not only exists but also has a uniformly bounded ℓ_2-norm.

Lemma 2. *Suppose Assumptions 1-5 hold. There always exist a constant scalar $\bar{l} > 0$ determined by $A, C, \bar{\rho}$, and an estimator gain L_i such that the following inequality holds for all $t \in (0,\ T_{\max})$ with $T_{\max} > 0$ from Assumption 4:*

$$\rho\left((I - L_i\tilde{C}_i)\tilde{A}_i\,(t)\right) \leq \bar{\rho} < 1,\ \|L_i\|_2^2 \leq \bar{l}. \tag{17}$$

The proof of Lemma 2 is in Appendix A of the full version [21]. The calculation of $\bar{l}$ is also in proof of Lemma 2 and omitted here for space limit. Our proposed secure state estimation algorithm based on local observers is summarized in Algorithm 1. In the following subsection, we will give the main theorem of this paper and provide its proof.

Algorithm 1 Secure estimation for asynchronous non-periodic measurements under attack

```
Input: Design constant scalar parameter $\bar{\rho} > 0$ and associated scalar $\bar{l} > 0$ (see Lemma 2).
Output: Secure estate estimation $\hat{x}[k]$.
Receive a set of measurements with time-stamp $t_k$
for every sensor $i$ do
    if $\psi_i(t_k) = 1$ then
        Recall $t_{k-\Delta_i^k}$ when sensor $i$ has a measurement and calculate $\tilde{A}_i\big(t_k - t_{k-\Delta_i^k}\big)$
        Obtain $L_i[k]$ with $\|L_i[k]\|_2^2 \leq \bar{l}$ such that inequality (16) is satisfied
    end if
    Update $\eta_i[k]$ by (12)
end for
Calculate each entry of $\hat{x}[k]$ by (13).
```

D. Main result

The following theorem is our main contribution of the paper. It claims that our proposed estimator is secure under the spatio-temporal false data attack. Let us define the following constants:

$$N_i = \int_0^{+\infty} s^i \cdot \mathrm{d}[\Phi^m(s)], i \in \{1, 2\}, \tag{18}$$

where $\Phi(s)$ is the cumulative density function of the standard Gaussian random variable. Define the initial estimation covariance spectral radius, which is unknown to the estimator, as follows:

$$\sigma_0 \triangleq \rho(\text{Cov}(\hat{x}(0) - x(0))). \tag{19}$$

Theorem 2 (secure estimation)**.** *Suppose Assumptions 1-5 are satisfied. The estimation error expectation is upper bounded by*

$$\|\mathbb{E}[\hat{x}[k] - x(t_k)]\|_\infty \leq \left(\bar{\rho}^{2k}\sigma_0\bar{a}^2 + \frac{(\bar{r}\bar{l} + \bar{q})\bar{a}^2}{1 - \bar{\rho}^2}\right)N_1, \tag{20}$$

and the error covariance is bounded by

$$\rho\left(\mathrm{Cov}[\hat{x}[k]-x(t_k)]\right) \le \left(\bar{\rho}^{2k}\sigma_0\bar{a}^2 + \frac{(\bar{r}\bar{l}+\bar{q})\bar{a}^2}{1-\bar{\rho}^2}\right)^2 N_2,$$

where $\bar{r}$ is given from Assumption 2, $\bar{l}$ is given from Lemma 2, $\bar{q} \triangleq T_{\max}\rho(Q)(\bar{l}\cdot\max_{i\in\mathcal{I}}\|C_i\|_2+1)^2$, $\bar{a} \triangleq \sup_{0<t<T_{\max}}\rho(\exp(At))$, and $T_{\max}$ is given from Assumption 4, and $\bar{\rho}$ is the design parameter in (16).

We will prove Theorem 2 in this subsection. The proof is based on the following two facts:

(1) The local estimation error $\eta_i[k]-H_ix(t_k)$ is bounded for benign sensors.

(2) The estimation error of the median number is smaller than the maximum error of the benign sensors as long as the system is $2p$-observable.

We first prove the first statement by the following theorem. The second statement will be evident in the proof of Theorem 2 given later. Define local estimation error as

$$\epsilon_i[k] = \eta_i[k]-H_ix(t_k),\ \forall i\in\mathcal{I}. \tag{21}$$

The following theorem claims that the local estimation errors $\epsilon_i[k]$ of benign sensors are unbiased and stable.

Theorem 3. *Consider benign sensors $i\in\mathcal{I}\setminus\mathcal{C}$. If Assumptions 1-5 are satisfied and there exists $L_i[k]$ such that the following inequalities hold:*

$$\rho\left((I-L_i[k]\tilde{C}_i)\tilde{A}_i\left(t_k-t_{k-\Delta_i^k}\right)\right)\le\bar{\rho},\ \|L_i[k]\|_2^2\le\bar{l}.$$

Then, the local estimation errors of benign sensors are unbiased and have uniformly upper bounded covariance:

$$\mathbb{E}(\epsilon_i[k]) = 0, \tag{22}$$

$$\rho(\mathrm{Cov}(\epsilon_i[k])) \le \bar{\rho}^{2k}\sigma_0\bar{a}^2+\frac{(\bar{r}\bar{l}+\bar{q})\bar{a}^2}{1-\bar{\rho}^2}. \tag{23}$$

Proof. Define $\tilde{A}_i[k]\triangleq\tilde{A}_i(t_k-t_{k-1})$ for notation simplicity. For a benign sensor $i\in\mathcal{I}\setminus\mathcal{C}$, if a measurement triple from sensor i is received with time-stamp t_k, the results in (10)-(11) and the local estimate (12) give us

$$\begin{aligned}\epsilon_i[k] =& \eta_i[k]-H_ix(t_k)\\ =& \left(\tilde{A}_i[k]-L_i[k]\tilde{C}_i\tilde{A}_i[k]\right)\epsilon_i[k-1]+L_i[k]v_i(t_k)\\ &+(L_i[k]C_i-H_i)w(t_{k-1},t_k).\end{aligned}$$

In this scenario, the expectation and covariance dynamics are

$$\begin{aligned}\mathbb{E}[\epsilon_i[k]] =& \left(\tilde{A}_i[k]-L_i[k]\tilde{C}_i\tilde{A}_i[k]\right)\mathbb{E}[\epsilon_i[k-1]],\\ \mathrm{Cov}(\epsilon_i[k]) =& (I-L_i[k]\tilde{C}_i)\tilde{A}_i\left(t_k-t_{k-\Delta_i^k}\right)\times\\ &\mathrm{Cov}(\epsilon_i[k-\Delta_i^k])\tilde{A}_i\left(t_k-t_{k-\Delta_i^k}\right)^\top(I-L_i[k]\tilde{C}_i)^\top\\ &+L_i[k]R_i(t_k)L_i[k]^\top\\ &+(L_i[k]C_i-H_i)Q(t_k-t_{k-1})(L_i[k]C_i-H_i)^\top.\end{aligned}$$

Based on Assumption 2 and Lemma 2, we have

$$\rho\left(L_i[k]R_i(t_k)L_i[k]^\top\right)\le\bar{r}\rho\left(L_i[k]L_i[k]^\top\right)\le\bar{r}\bar{l}.$$

From Assumption 4, we have $t_k-t_{k-1}<T_{\max}$. Moreover, the form of H_i in (6) implies that

$$\begin{aligned}&\rho((L_i[k]C_i-H_i)Q\cdot(t_k-t_{k-1})(L_i[k]C_i-H_i)^\top)\\ \le&\ \rho(Q\cdot(t_k-t_{k-1}))\cdot(\|L_i[k]\|_2\|C_i\|_2+\|H_i\|_2)^2\le\bar{q}.\end{aligned}$$

From (19), one has $\rho(\mathrm{Cov}(\epsilon_i[0]))\le\rho(\mathrm{Cov}(\hat{x}(0)-x(0)))=\sigma_0$. Thus, if $\psi_i(t_k)=1$, the design condition (16) implies that

$$\begin{aligned}\rho(\mathrm{Cov}(\epsilon_i[k])) \le&\ \bar{\rho}^{2k}\sigma_0+\sum_{t=0}^{k-1}\bar{\rho}^{2t}(\bar{r}\bar{l}+\bar{q})\\ \le&\ \bar{\rho}^{2k}\sigma_0+\frac{\bar{r}\bar{l}+\bar{q}}{1-\bar{\rho}^2}.\end{aligned}\tag{24}$$

If no measurement triple from sensor i is received with time-stamp t_k, based on (10), the local estimation errors satisfy

$$\begin{aligned}\mathbb{E}[\epsilon_i[k]] =& \left(\tilde{A}_i[k]-L_i[k]\tilde{C}_i\tilde{A}_i[k]\right)\mathbb{E}[\epsilon_i[k-1]]\\ \epsilon_i[k] =& \eta_i[k]-H_ix(t_k)\\ =& \tilde{A}_i\left(t_k-t_{k-\Delta_i^k}\right)\epsilon_i[k-\Delta_i^k].\end{aligned}$$

Thus, if $i\notin\psi(t_k)$, since $\psi(t_{k-\Delta_i^k})=1$ according to (24), we have

$$\rho(\mathrm{Cov}(\epsilon_i[k])) \le \bar{\rho}^{2k}\sigma_0\bar{a}^2+\frac{(\bar{r}\bar{l}+\bar{q})\bar{a}^2}{1-\bar{\rho}^2}. \tag{25}$$

Firstly, $\mathbb{E}[\epsilon_i[0]]=\mathbb{E}[\eta_i[0]-H_ix(0)]=H_i\mathbb{E}[x(0)]-H_i\mathbb{E}[x(0)]=0$ implies $\mathbb{E}[\epsilon_i[k]]=0$ for all $k\in\mathbb{Z}_{\ge0}$. Moreover, the results in (24) and (25) complete the proof. □

Remark 3. *Since matrix $\tilde{A}_i[k]-L_i[k]\tilde{C}_i\tilde{A}_i[k]$ is Schur stable, the equality*

$$\mathbb{E}[\epsilon_i[k]]=\left(\tilde{A}_i[k]-L_i[k]\tilde{C}_i\tilde{A}_i[k]\right)\mathbb{E}[\epsilon_i[k-1]]$$

implies that the expected local estimation error converges to zero, even if $\mathbb{E}[x(0)]$ is unknown and $\eta_i[0]\ne H_i\mathbb{E}[x(0)]$. In other words, the expected local estimation is asymptotically unbiased when the expected initial state $\mathbb{E}[x(0)]$ is unknown, otherwise it is unbiased.

We are now ready to present the proof of Theorem 2.

Proof of Theorem 2. Let us define the following sequence order operator: $f_i(x_1,\cdots,x_L)$ equals to the i-th smallest element in the set $\{x_1,\cdots,x_L\}$. For even number i, we further define

$$f_{\frac{i+1}{2}}=\frac{1}{2}\left(f_{\frac{i}{2}}+f_{\frac{i}{2}+1}\right).$$

Thus, the function $f_{(L+1)/2}\left(x_l, l\in\{1,\cdots,L\}\right)$ is the median number of set $\{x_1,\ldots,x_L\}$, giving us the following formulation, which is equivalent to (13), as follows:

$$[\hat{x}[k]-x(t_k)]_j=f_{(|\mathcal{F}_j|+1)/2}\left([H_i^\top\eta_i[k]-x(t_k)]_j, i\in\mathcal{F}_j\right).$$

Define the η_i^o as the local estimate of benign sensor i, which is not manipulated by the attacker. Since the system is $2p$-sparse observable and there are at most p corrupted sensors, we have

$$\min_{i\in\mathcal{F}_j}\left\{[H_i^\top \eta_i^o[k]-x(t_k)]_j\right\}\leq[\hat{x}[k]-x(t_k)]_j$$
$$\leq\max_{i\in\mathcal{F}_j}\left\{[H_i^\top \eta_i^o[k]-x(t_k)]_j\right\}.$$

The following inequality is from Lemma 3 in the full version [21]:

$$-\sigma_{\max}[k]N_1\mathbf{1}\leq\mathbb{E}[\hat{x}[k]-x(t_k)]\leq\sigma_{\max}[k]N_1\mathbf{1},$$

where

$$\sigma_{\max}[k]=\max_{i\in\mathcal{I},j\in\{1,\cdots,n_i\}}\mathrm{Cov}([\epsilon_i[k]]_j),$$

resulting in (20). Due to

$$\mathrm{Cov}[\hat{x}[k]-x(t_k)]=\mathbb{E}[(\hat{x}[k]-x(t_k))^2]-(\mathbb{E}[\hat{x}[k]-x(t_k)])^2,$$

we have

$$\rho\left(\mathrm{Cov}[\hat{x}[k]-x(t_k)]\right)\leq$$
$$\max\left\{\mathbb{E}(\max\{\hat{x}[k]-x(t_k)\})^2,\mathbb{E}(\min\{\hat{x}[k]-x(t_k)\})^2\right\}$$
$$\leq(\sigma_{\max}[k])^2N_2.$$

Here the notation $\max\{\hat{x}[k]-x(t_k)\}$ and $\min\{\hat{x}[k]-x(t_k)\}$ represent the maximum and the minimum values of the vectors $\hat{x}[k]-x(t_k)$, respectively, while $\max\{a,b\}$ means the larger scalar between a and b. Since $\sigma_{\max}[k]\leq\bar{\rho}^{2k}\sigma_0\bar{a}^2+\frac{(\bar{r}\bar{l}+\bar{q})\bar{a}^2}{1-\bar{\rho}^2}$ from Theorem 3, the results are obtained. □

In the following section, we show numerical simulation results on the IEEE 14-bus system to demonstrate the effectiveness of our proposed method.

IV. Numerical Results

To verify the obtained results, we apply our proposed estimation scheme (Algorithm 1) to the IEEE 14-bus system under the novel spatio-temporal attack presented in Definition 1 (see Fig. 4). Let the generator bus index set be $\mathcal{V}_g=\{1,2,3,6,8\}$ and the load bus index set be $\mathcal{V}_l=\{2,3,4,5,6,9,10,11,12,13,14\}$. We adopt the continuous LTI system dynamics as in the following equations [22]:

$$\dot{\theta}_i(t)=\omega_i(t),$$
$$\dot{\omega}_i(t)=-\frac{1}{m_i}\left[D_i\omega_i(t)+\sum_{j\in\mathcal{N}_i}\left(P_{\text{tie}}^{ij}(t)-P_i(t)\right)+w_i(t)\right],$$

where $\theta_i(t)$ and $\omega_i(t)$ are the phase angle and angular frequency on bus i, respectively, m_i is the angular momentum of i, and w_i is the process disturbance. The parameter D_i is the load change sensitivity w.r.t. the frequency [22, Section 10.3]. The power flow between neighboring buses i and j is given by $P_{\text{tie}}^{ij}(t)=-P_{\text{tie}}^{ji}(t)=t_{ij}\left(\theta_i(t)-\theta_j(t)\right)$, where t_{ij} is the inverse of resistance between buses i and j. The power $P_i(t)$ denotes the difference between the mechanical power and power demand at bus i, which is known by the system operator. Every bus is equipped with three sensors: one electric power sensor, one phase sensor, and one angular velocity sensor. Measurements are sampled non-periodically with sampling intervals uniformly distributed in $[0.001,0.05]$. Each sensor has a probability of 0.6 of successful sampling at each time-stamp (see Fig. 5). The covariances of measurement noises are $Q=0.001I$ and $R=0.01I$.

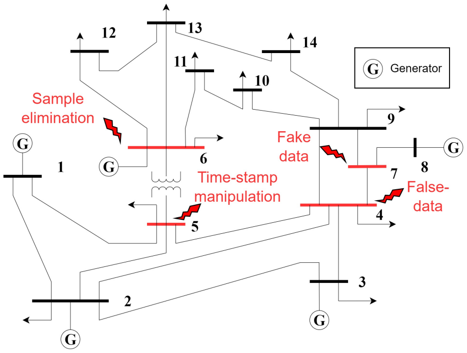

Fig. 4. The IEEE 14-bus system consists of five generators on buses 1, 2, 3, 6, and 8. Examples of spatio-temporal attacks: i) false-data attacks on bus 4; ii) time-stamp manipulation on bus 5; iii) sample elimination on bus 6; and iv) fake data on bus 7.

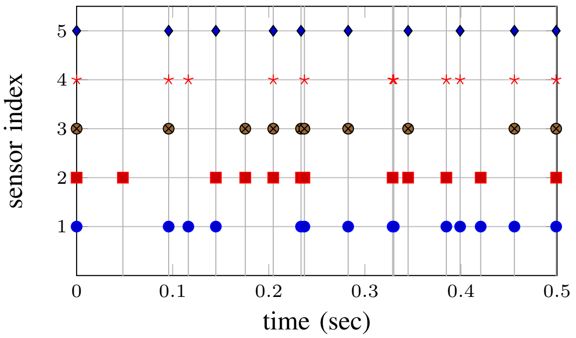

Fig. 5. Sensor measurement availability of asynchronous non-periodic sampling. For conciseness, only show sensors 1-5 in the time interval of 0-0.5 seconds.

Fig. 6 shows the estimation performance without an attacker. Even though the estimation holds stable, the estimation errors are relatively large due to the conservativeness of the median fusion algorithm. Attacks are launched on angular velocity sensors of buses $4, 5, 6$, and 7 (see Fig. 4). At bus 4, random false data is injected into its measurements. At bus 5, the time-stamp is randomly shifted (and thus the order of samples is changed). At bus 6, the successfully transmitted samples are eliminated with a probability of 0.5. At bus 7, new fake data with random measurements and random time-stamps are generated. Fig. 7 demonstrates the estimation performance on buses 5-7 under the aforementioned attacks. The estimation error is slightly larger than the scenario without attack but still remains stable despite various spatio-temporal false data attacks.

V. Conclusion

This paper introduced a novel framework for analyzing the time-stamp and measurement value manipulations from an adversary, named the spatial-temporal false data attack. The attack manipulates the data stream in communication

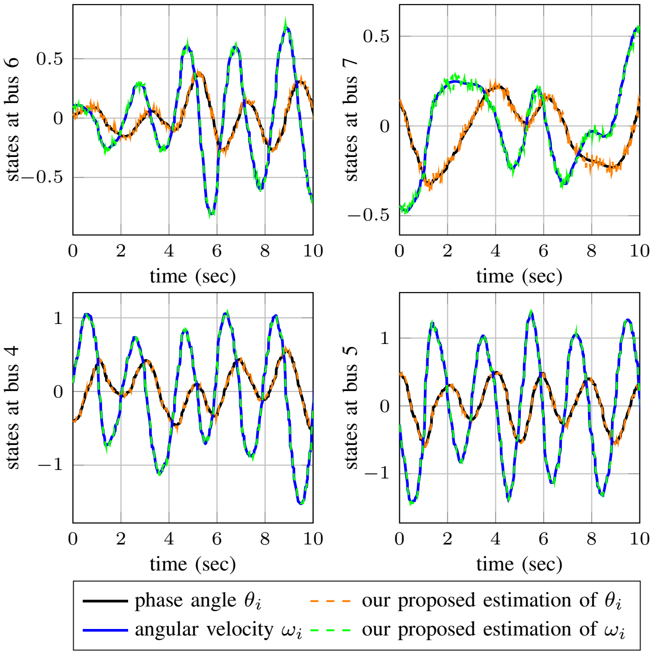

Fig. 6. Estimation of states without attack.

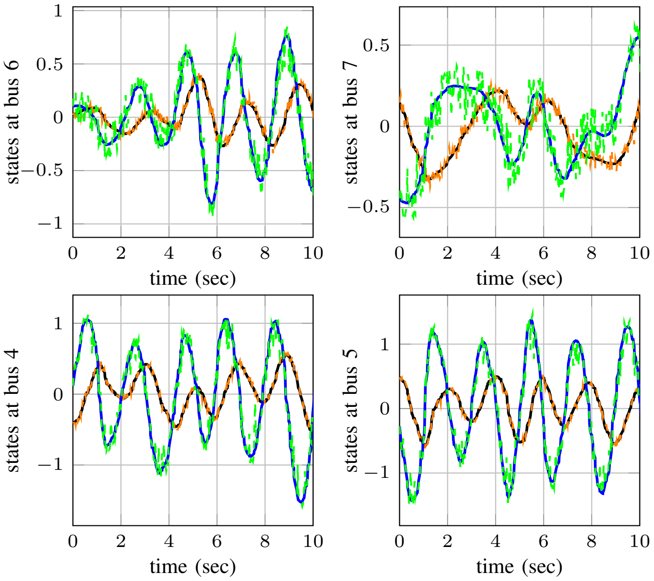

Fig. 7. Estimation performance under attack. The legend is the same as Fig. 6.

channels of an asynchronous non-periodic sampled system. A decentralized estimation scheme was proposed to isolate the negative impact of corrupted sensors. The proposed algorithm exhibited a median operator to fuse local estimates, which provides the resilient state estimation in the presence of the spatial-temporal false data attack. The effectiveness of the proposed algorithm was validated through a benchmark of the IEEE-14 bus system.

This analysis framework revealed that the manipulation of time-stamps has some intrinsic relations with false data injection attacks. Thus, the hitherto under-explored time-stamp manipulation strategy can be mapped to the well-studied false data injection strategies, while these two attacks have the same influence on a linear system. We believe this will facilitate the understanding and handling of timestamp-related problems (such as delays and asynchronicity) which are ubiquitous in real-world scenarios.

References

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, symantec corp., security response*, vol. 5, no. 6, p. 29, 2011.

[2] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[3] X. Liu, Y. Mo, and E. Garone, "Local decomposition of kalman filters and its application for secure state estimation," *IEEE Transactions on Automatic Control*, vol. 66, no. 10, pp. 5037–5044, 2020.

[4] Z. Li and Y. Mo, "Efficient secure state estimation against sparse integrity attack for regular linear system," *International Journal of Robust and Nonlinear Control*, vol. 33, no. 1, pp. 209–236, 2023.

[5] 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, 2015.

[6] Y. Nakahira and Y. Mo, "Attack-resilient $\mathcal{H}_2$, $\mathcal{H}_\infty$, and ℓ_1 state estimator," *IEEE Transactions on Automatic Control*, vol. 63, no. 12, pp. 4353–4360, 2018.

[7] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176 – 183, 2018.

[8] A.-Y. Lu and G.-H. Yang, "Resilient observer-based control for cyber-physical systems with multiple transmission channels under denial-of-service," *IEEE Transactions on Cybernetics*, vol. 50, no. 11, pp. 4796–4807, 2019.

[9] Y. Liu and G.-H. Yang, "Resilient event-triggered distributed state estimation for nonlinear systems against dos attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 9, pp. 9076–9089, 2021.

[10] K. J. Uribe-Murcia, Y. S. Shmaliy, C. K. Ahn, and S. Zhao, "Unbiased fir filtering for time-stamped discretely delayed and missing data," *IEEE Transactions on Automatic Control*, vol. 65, no. 5, pp. 2155–2162, 2020.

[11] W. Li, S. L. Shah, and D. Xiao, "Kalman filters in non-uniformly sampled multirate systems: For fdi and beyond," *Automatica*, vol. 44, no. 1, pp. 199–208, 2008.

[12] G. Hui-dong, Z. Xin-hua, X. Lin-zhou, S. Yuan, X. Ce, and T. Shao-bo, "Asynchronous multisensor data fusion based on minimum trace of error covariance," in *2006 9th International Conference on Information Fusion*, 2006, pp. 1–5.

[13] A. Feddaoui, N. Boizot, E. Busvelle, and V. Hugel, "High-gain extended kalman filter for continuous-discrete systems with asynchronous measurements," *International Journal of Control*, vol. 93, no. 8, pp. 2001–2014, 2020.

[14] F. Ding, L. Qiu, and T. Chen, "Reconstruction of continuous-time systems from their non-uniformly sampled discrete-time systems," *Automatica*, vol. 45, no. 2, pp. 324–332, 2009.

[15] Muhammad, G. Mustafa, A. Q. Khan, and M. Abid, "On the observability of non-uniformly sampled systems," in *2014 12th International Conference on Frontiers of Information Technology*, 2014, pp. 87–90.

[16] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[17] N. Kaempchen and K. C. J. Dietmayer, "Data synchronization strategies for multi-sensor fusion," in *World Congress on Intelligent Transport Systems*, 2003.

[18] A. Westenberger, M. Gabb, M. Muntzinger, M. Fritzsche, and K. Dietmayer, "State and existence estimation with out-of-sequence measurements for a collision avoidance system," in *2013 IEEE Intelligent Vehicles Symposium (IV)*, 2013, pp. 612–617.

[19] Z. Li, M. U. B. Niazi, C. Liu, Y. Mo, and K. H. Johansson, "Secure state estimation against sparse attacks on a time-varying set of sensors," 2022. [Online]. Available: https://arxiv.org/abs/2211.05566

[20] W. Wonham, "On pole assignment in multi-input controllable linear systems," *IEEE Transactions on Automatic Control*, vol. 12, no. 6, pp. 660–665, 1967.

[21] Z. Li, A. T. Nguyen, A. Teixeira, Y. Mo, and K. H. Johansson, "Secure state estimation with asynchronous measurements against malicious measurement-data and time-stamp manipulation," *arXiv preprint arXiv:2303.17514*, 2023.

[22] G. B. S. Allen J. Wood, Bruce F. Wollenberg, *Power Generation, Operation, and Control*, 3rd ed. Spriger, 2013.