Hindawi
Journal of Sensors
Volume 2022, Article ID 2127102, 10 pages
https://doi.org/10.1155/2022/2127102

Research Article

A GMM-Based Secure State Estimation Approach against Dynamic Malicious Adversaries

Cui Zhu, Zile Wang, Zeyuan Zang, Yuxuan Li, and Huanming Zheng

Beijing Information Science and Technology University, School of Information and Communication Engineering, Beijing 100192, China

Correspondence should be addressed to Cui Zhu; cuizhu_lzy@bistu.edu.cn

Received 28 October 2021; Accepted 13 January 2022; Published 29 January 2022

Academic Editor: Xue-bo Jin

We consider the secure state estimation of linear time-invariant Gaussian systems subject to dynamic malicious attacks. An error compensator is proposed to reduce the impact of local error data on state estimation. Based on that, a new estimation algorithm based on the Gaussian mixture model (GMM) aiming at dynamic attacks is proposed, which can cluster the local state estimates autonomously and improve the remote estimation accuracy effectively. The superiority of the proposed algorithm is verified by numerical simulations.

1. Introduction

Cyberphysical systems (CPSs), such as transportation networks and smart grids, integrate sensing, computing, and control technologies with a communication infrastructure. Tight integration and cooperation between cyber and physical components are the features of CPSs [1]. However, CPSs are vulnerable to any successful attacks especially network attacks on the data and communication channels, which causes serious harms to the national economy and social security, for example, the Stuxnet storm reported in [2], StuxNet malware [3], power blackouts in Brazil [4], and Maroochy water bleach [5]. Due to the widespread application of CPSs in many real-life critical infrastructures [6], the security of CPSs has become an increasingly important issue which has attracted attention from many researchers in the past decades.

In the recent literature, the secure state estimation is an important research direction of CPSs security. In [7], a distributed state estimation method based on parallelized stream computing is proposed, which can not only significantly improve the speed of state estimation calculation but also reduce the interregional convergence correlation and the residual pollution. In [8], a new sequential estimation method is proposed to improve the estimation accuracy, which sequentially estimates states by the particle filter (PF) and parameters by the separable natural evolution strategy (SNES). The state estimation of three-phase power system models is studied in [9]. In [10], a Bayesian network based on the wireless power transfer (WPT) system state estimation algorithm is proposed, which can estimate the WPT system states in a distributed way using the Bayesian tree structure. In [11], a robust generalized maximum likelihood (GM) estimator, which leverages modified projection statistics and a Huber convex score function, is designed to bound the influence of observation outliers while maintaining its high statistical estimation efficiency. In [12], a distributed dynamic state estimation method for microgrids incorporating distributed energy resources is presented. In [13], a robust generalized maximum-likelihood Koopman operator-based Kalman filter (GM-KKF) is designed, which can estimate the rotor angle and speed of synchronous generators. In [14], a correlation-aided robust adaptive unscented Kalman filter (UKF) for power system decentralized dynamic state estimation with unknown inputs is presented, which has lower requirement of number of measurements for dynamic state estimation while achieving better robustness against bad data. In [15, 16], the state estimation method based on undamaged sensors is studied. In [17, 18], the state estimation for different systems is studied based on the convex optimization methods. In [19], by modeling and adopting a variety of models, a random Bayesian approach is proposed to solve the state estimation against switching patterns and signal attacks. In [20], the state estimation against fixed target attacks, switched target attacks with disturbance, and sparse sensor attacks are considered, and the sufficient condition for the existence of the switched observer is given. In [21], a fusion algorithm based on the Gaussian mixture model is presented to solve the estimation of a linear time-invariant Gaussian system under stealth attacks. However, the dynamic attacks are not considered. In [22], a dynamic combination strategy and a distributed Kalman filter are proposed, which improve the robustness of the system against random error data injection and replay attacks.

Most of the studies mentioned above have focused on static attacks. However, dynamic attacks are very common in real systems. Therefore, this paper considers the state estimation for a networked system suffering from dynamic adversaries as shown in Figure 1. The different sensors are attacked randomly at each time instant, and it is assumed that the number of attached sensors does not exceed half of the sensors.

Inspired by [21], we have designed an error compensator to reduce the impact of incorrect data on state estimation. Based on that, a new GMM-based state estimation algorithm is presented, which can effectively improve the state estimation accuracy against the dynamic adversaries. The contributions of this article are listed as follows:

(1) A new error compensator is proposed to alleviate the influence of wrong data on state estimation, which can judge whether the beliefs generated by the expectation-maximum (EM) algorithm are accurate based on the observability of the system, and correct the doubtful beliefs

(2) By introducing the error compensator, a new GMM-based estimation algorithm is presented, which can improve the estimation accuracy effectively. The proposed algorithm can fuse the local data by adopting the modified beliefs as the weights of the local data with the centralized Kalman filter

The rest of the paper is organized as follows. Section II formulates the model of the considered system and the problem of interest. Section III proposes the error compensator and the new GMM-based state estimation algorithm against dynamic adversaries. In Section IV, the effectiveness of the proposed algorithm is demonstrated by numerical simulations. Conclusions are given in Section V.

Notation: $\mathbb{N}$ and $\mathbb{R}$ are the sets of positive integers and real numbers, respectively. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. $\mathbb{S}_+^n(\mathbb{S}_{++}^n)$ is the set of $n \times n$ positive semidefinite (definite) matrices. We write $X \geq 0 (X > 0)$ when $X \in \mathbb{S}_+^n(\mathbb{S}_{++}^n)$. X' denotes the transpose of matrix X. $\mathbb{E}[\cdot]$ is the expectation of a random variable. $\mathcal{N}(\mu, \Sigma)$ is the Gaussian distribution with mean μ and covariance matrix Σ, and $X \sim \mathcal{N}(\mu, \Sigma)$ denotes X follows the Gaussian distribution $\mathcal{N}(\mu, \Sigma)$. $Diag\{\cdot\}$ denotes a block diagonal matrix.

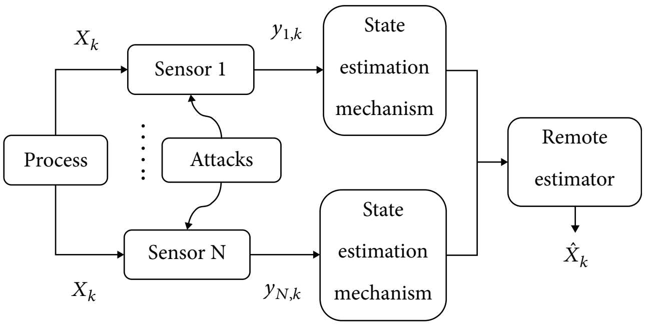

Figure 1: The networked system under attacks.

2. Problem Formulation

Consider the following networked system under attacks:

$$x_{k+1} = Ax_k + w_k, \tag{1}$$

$$y_{i,k} = C_i x_k + v_{i,k} + a_{i,k}, \tag{2}$$

where $x_k \in \mathbb{R}^n$ denotes the system state, $y_{i,k} \in \mathbb{R}^{m_i}$ represents the measured value from sensor i at time k, and $a_{i,k} \in \mathbb{R}^{m_i}$ is attack signal. The number of sensors is denoted by N. $w_k \in \mathbb{R}^n$ is the process noise, and $w_k \sim \mathcal{N}(0, Q)$. $v_{i,k} \in \mathbb{R}^{m_i}$ is the measurement noise, and $v_{i,k} \sim \mathcal{N}(0, R_i)$. Meanwhile, it is assumed that $\mathbb{E}[w_k w_l'] = \delta_{kl} Q \, (Q \geq 0)$, $\mathbb{E}[v_{i,k} v_{j,l}'] = \delta_{ij} \delta_{kl} R_i \;\; (R_i > 0)$, where $i = j (i \neq j)$, $\delta_{i,j} = 1 (\delta_{i,j} = 0)$. $\mathbb{E}[w_k v_{i,l}'] = 0$, $\forall k, l \in \mathbb{N}$, $i, j = 1, 2, \cdots, N$. The initial state x_0 is independent of w_k and $v_{i,k}$ for all $k \geq 0$ and $x_0 \sim \mathcal{N}(0, \Pi_0)$. (A, C_i) and $(A, \sqrt{Q})$ are detectable and controllable, respectively.

The malicious attack $a_{i,k} \in \mathbb{R}^{m_i}$ satisfies the following assumptions:

Assumption 1. Any s $(s \leq N/2)$ sensors can be corrupted by the adversary, and the output values of the sensors are changed. Only when sensor i is unattacked, $a_{i,k} = 0$.

Assumption 2. The number of attacked sensors s is unknown, stochastic, and variable.

Assumption 3. The system parameters and noise statistics are known for the adversary.

Assumption 4. $a_{i,k}$ is statistically independent of $\{w_{\mathcal{K}}\}_{\mathcal{K}>k}$ and $\{v_{i,\mathcal{K}}\}_{\mathcal{K}>k}$, respectively.

Remark 1. According to [23, 24], it is impossible to accurately reconstruct the state of a system when more than half the sensors are attacked. Thus, we assume that the maximum number of damaged sensors does not exceed N/2 in this paper, i.e., the upper limit of s is N/2.

When the system is not attacked, the measurements at time instant k can be stacked as

$$y_k = Cx_k + v_k, \tag{3}$$

where

$$\begin{aligned} y_k &\triangleq \left[y_{1,k}' y_{2,k}' \cdots y_{N,k}'\right]', \\ v_k &\triangleq \left[v_{1,k}' v_{2,k}' \cdots v_{N,k}'\right]', \\ C &\triangleq \left[C_1' C_2' \cdots C_N'\right]', \\ R &\triangleq \mathrm{Diag}\{R_1, R_2, \cdots, R_N\}. \end{aligned} \tag{4}$$

Then, we adopt a centralized Kalman filter as the remote estimator:

$$\begin{aligned} \hat{x}_k^- &= A\hat{x}_{k-1}, \\ P_k^- &= AP_{k-1}A' + Q, \\ K_k &= P_k^- C' \left(CP_k^- C' + R\right)^{-1}, \\ \hat{x}_k &= \hat{x}_k^- + K_k(y_k - C\hat{x}_k^-), \\ P_k &= (I - K_k C)P_k^-, \end{aligned} \tag{5}$$

where $\hat{x}_k^-$ and $\hat{x}_k$ are the priori and the posteriori estimation of the system state x_k, respectively. P_k^- and P_k are the priori and posteriori estimation error covariance, respectively. K_k is the Kalman filter gain.

From [21], we know that the information-form Kalman filter can be expressed as

$$\hat{x}_k = \hat{x}_k^- + P_k C' R^{-1}(y_k - C\hat{x}_k^-), \tag{6}$$

$$(P_k)^{-1} = (P_{k-1}^-)^{-1} + C' R^{-1} C. \tag{7}$$

Similarly, the local Kalman filter for sensor i can be written as

$$\begin{aligned} \hat{x}_{i,k} &= \hat{x}_{i,k}^- + P_{i,k} C_i' R_i^{-1}\left(y_{i,k} - C_i \hat{x}_{i,k}^-\right), \\ (P_{i,k})^{-1} &= \left(P_{i,k-1}^-\right)^{-1} + C_i' R_i^{-1} C_i. \end{aligned} \tag{8}$$

It is noted that P_k and $P_{i,k}$ can be calculated offline. According to [25], the Kalman filter converges from any initial condition exponentially when (A, C_i) and $(A, \sqrt{Q})$ are detectable and controllable, respectively. The steady-state values of local and centralized Kalman filter are defined as

$$\begin{aligned} \bar{P}_i &\triangleq \lim_{k \longrightarrow +\infty} P_{i,k}, \bar{P}_i^- \triangleq \lim_{k \longrightarrow +\infty} P_{i,k}^-, \\ P &\triangleq \lim_{k \longrightarrow +\infty} P_k, P^- \triangleq \lim_{k \longrightarrow +\infty} P_k^-. \end{aligned} \tag{9}$$

It is assumed that the system starts from the steady state with $P_{i,0} = \bar{P}_i$ and $P_0 = P$, and the fixed-gain of local and centralized Kalman filters can be represented as:

$$\begin{aligned} K_i &= \bar{P}_i C_i' R_i^{-1} = \bar{P}_i^- C_i' \left(C_i \bar{P}_i^- C_i' + R_i\right)^{-1}, \\ K &= PC' R^{-1} = P^- C' \left(CP^- C' + R\right)^{-1}. \end{aligned} \tag{10}$$

The objective of this paper is to design a new GMM-based estimation method for systems suffering from dynamic adversaries.

3. The GMM-Based State Estimation

In this section, an error compensator and the GMM-based state estimation algorithm against dynamic adversaries are proposed.

3.1. Modeling and the EM Algorithm. For a Gaussian mixture model with $\mathbb{Q}$ components [21], the mean and covariance of the q-th component $\mathcal{Q}_q$ $(q \in \{1, 2, \cdots, \mathbb{Q}\})$ are expressed as $\mu^{(q)}$ and $\Sigma^{(q)}$, respectively. $\pi^{(q)}$ is the mixture component weights of $\mathcal{Q}_q$, and $\sum_{q=1}^{\mathbb{Q}} \pi^{(q)} = 1$. In this case, the mixture density of a Gaussian mixture model can be expressed as

$$p(x) = \sum_{q=1}^{\mathbb{Q}} p\left(x \mid \mathcal{Q}_q\right) \Pr\left(\mathcal{Q}_q\right) = \sum_{q=1}^{\mathbb{Q}} \pi^{(q)} f\left(x ; \mu^{(q)}, \Sigma^{(q)}\right), \tag{11}$$

where $p(x \mid \mathcal{Q}_q)$ and $\Pr(\mathcal{Q}_q)$ are the Gaussian distribution density and weight of the q-th component, respectively. Function $f(x ; \mu, \Sigma)$ is the probability density function (pdf) for Gaussian random variables:

$$f(x ; \mu, \Sigma) = \frac{1}{\sqrt{(2\pi)^n |\Sigma|}} \exp\left(-\frac{1}{2}(x - \mu)' \Sigma^{-1}(x - \mu)\right). \tag{12}$$

At time instant k, we denote the means of the state variables for sensor i as $\mu_k^{(1)}$ under the unattacked scenario and $\mu_k^{(2)}$ under the attacked-scenario, respectively. $\Sigma_k^{(1)}$ and $\Sigma_k^{(2)}$ represent the covariance when sensor i is unattacked and attacked, respectively. The local state estimation $\hat{x}_{i,k}$ follows different distributions depending on whether sensor i is attacked or not. According to the definition of GMM and the analysis of Kalman filtering in [25], it can be known that when sensor i is unattacked (defined as the first component),

$\widehat{x}_{i,k}$ follows the Gaussian distribution with the mean $\mu_k^{(1)}$ and the fixed covariance $\Sigma_k^{(1)} = \bar{P}_i$, i.e., $p(\widehat{x}_{i,k} \mid \mathcal{Q}_1) \sim \mathcal{N}(\mu_k^{(1)}, \bar{P}_i)$, $\forall i \in N$. When sensor i is attacked (defined as the second component), the exact distribution of $\widehat{x}_{i,k}$ is unknown since the specific type and the starting time of attacks are unknown. In this case, similar to [21], we can adopt a Gaussian distribution with the first and second moments, i.e., $p(\widehat{x}_{i,k} \mid \mathcal{Q}_2) \sim \mathcal{N}(\mu_k^{(2)}, \Sigma_k^{(2)})$, $\forall i \in N$, to approximate the distribution of all local estimates in the second component. Then, $\widehat{x}_{i,k}$ can be described by the following 2-component Gaussian mixture model:

$$\begin{aligned} p(\widehat{x}_{i,k}) &= \sum_{q=1}^{2} p\left(\widehat{x}_{i,k} \mid \mathcal{Q}_q\right) \Pr\left(\mathcal{Q}_q\right) \\ &= \pi_k^{(1)} p(\widehat{x}_{i,k} \mid \mathcal{Q}_1) + \pi_k^{(2)} p(\widehat{x}_{i,k} \mid \mathcal{Q}_2) \\ &= \pi_k^{(1)} f\left(\widehat{x}_{i,k} ; \mu_k^{(1)}, \bar{P}_i\right) + \pi_k^{(2)} f\left(\widehat{x}_{i,k} ; \mu_k^{(2)}, \Sigma_k^{(2)}\right), \end{aligned} \tag{13}$$

where $\pi_k^{(1)}$ and $\pi_k^{(2)}$ are the weights of the first and second components at time k, respectively.

The observation data set is defined as $\mathcal{X}_k = \{\widehat{x}_{i,k}\}_{i=1}^{N}$. According to [26, 27], it is known that the expectation-maximization (EM) algorithm can be adopted to find the maximum likelihood estimates for the parameter $\Phi_k = \{\pi_k^{(q)}, \mu_k^{(q)}, \Sigma_k^{(2)}\}_{q=1}^{2}$ using $\mathcal{X}_k = \{\widehat{x}_{i,k}\}_{i=1}^{N}$. The log likelihood is shown as

$$\begin{aligned} \mathcal{L}(\Phi_k ; \mathcal{X}_k) = \sum_{i=1}^{N} \log \Big(&\pi_k^{(1)} f\left(\widehat{x}_{i,k} ; \mu_k^{(1)}, \bar{P}_i\right) \\ &+ \pi_k^{(2)} f\left(\widehat{x}_{i,k} ; \mu_k^{(2)}, \Sigma_k^{(2)}\right)\Big). \end{aligned} \tag{14}$$

Generally, the EM algorithm is divided into two steps: the expectation and maximization step. First, initializing the parameter Φ_k at each time k, then the expectation step generates a belief $\gamma_{i,k}^{(q)}\,(q = 1, 2)$ based on Φ_k and $\widehat{x}_{i,k}$ for each sensor:

$$\gamma_{i,k}^{(1)} = \frac{\pi_k^{(1)} f\left(\widehat{x}_{i,k} ; \mu_k^{(1)}, \Sigma_k^{(1)}\right)}{\pi_k^{(1)} f\left(\widehat{x}_{i,k} ; \mu_k^{(1)}, \Sigma_k^{(1)}\right) + \pi_k^{(2)} f\left(\widehat{x}_{i,k} ; \mu_k^{(2)}, \Sigma_k^{(2)}\right)}, \tag{15}$$

$$\gamma_{i,k}^{(2)} = 1 - \gamma_{i,k}^{(1)}, \tag{16}$$

where $\gamma_{i,k}^{(1)}$ and $\gamma_{i,k}^{(2)}$ represent the probability of sensor i belonging to the component $\mathcal{Q}_1$ and $\mathcal{Q}_2$, respectively.

Given all beliefs $\gamma_{i,k}^{(1)}$ and $\gamma_{i,k}^{(2)}$, the parameters $\{\pi_k^{(q)}, \mu_k^{(q)}, \Sigma_k^{(2)}\}_{q=1}^{2}$ are reestimated in the maximization step:

$$\pi_k^{(q)} = \frac{\sum_{i=1}^{N} \gamma_{i,k}^{(q)}}{N}, \tag{17}$$

$$\mu_k^{(q)} = \frac{\sum_{i=1}^{N} \gamma_{i,k}^{(q)} \widehat{x}_{i,k}}{\sum_{i=1}^{N} \gamma_{i,k}^{(q)}}, \tag{18}$$

$$\Sigma_k^{(2)} = \frac{\sum_{i=1}^{N} \gamma_{i,k}^{(2)} \left(\widehat{x}_{i,k} - \mu_k^{(2)}\right) \left(x\Lambda_{i,k} - \mu_k^{(2)}\right)'}{\sum_{i=1}^{N} \gamma_{i,k}^{(2)}}. \tag{19}$$

The expectation and maximization steps iterate until they converge to a certain value. This iterative procedure maximizes the concave lower bound of the log likelihood in (14).

3.2. The Error Compensator. In this subsection, an error compensator is proposed to reduce the influence of incorrect data on the state estimation.

According to 3.1, the EM algorithm can be used to calculate the GMM parameters and find the maximum likelihood estimation. However, the convergence and clustering results of the EM algorithm are affected by the initial parameters. In this paper, the first and second moments are adopted as the initial parameters of the second cluster. Due to the randomness of dynamic adversary and its specific type is unknown, the output of some attacked sensors may be similar to that of normal sensors at some moments. In this case, $\gamma_{i,k}^{(1)}$ will be miscalculated as $\gamma_{i,k}^{(2)}$ in the iterative process (15)-(19), since the observed data are considered to be closer to the second cluster by the EM algorithm. When the above case occurs, the estimation accuracy will be reduced seriously because the number of data available for fusion is less than $N/2$. On the other hand, the measurements that are similar to the true measurements can provide useful information for the remote state estimation, which means that the data belonging to the second cluster can be adopted to estimate system state. Hence, a compensator is designed to solve the above problem.

$\bar{\gamma}_k^{(2)}$ represents the average of all $\gamma_{i,k}^{(2)}$ at time instant k, which can be calculated as follows:

$$\bar{\gamma}_k^{(2)} = \frac{\sum_{i=1}^{N} \gamma_{i,k}^{(2)}}{N}. \tag{20}$$

According to the EM algorithm, $\gamma_{i,k}^{(2)}$ tends to 1 if and only if sensor i is attacked, and the expectation step is accurate, which causes $\sum_{i=1}^{N} \gamma_{i,k}^{(2)}$ to approach s. When the expectation step is miscalculated, $\sum_{i=1}^{N} \gamma_{i,k}^{(2)}$ tends to $N - s$ since $\gamma_{i,k}^{(2)}$ approachs 0 for the attacked sensor i. According to Assumptions 1–4, the maximum number of damaged sensors does not exceed $N/2$ (namely, $s \leq N/2$), which means $N - s > N/2$. Hence, it can be known that $\gamma_{i,k}^{(1)}$ and $\gamma_{i,k}^{(2)}$ are miscalculated if $\sum_{i=1}^{N} \gamma_{i,k}^{(2)} > N/2$. Based on the above analysis, the compensator is designed as follows:

$$\begin{aligned} \widehat{\gamma}_{i,k}^{(1)} &= \begin{cases} \gamma_{i,k}^{(1)}, & \bar{\gamma}_k^{(2)} \leq \varepsilon \\ \gamma_{i,k}^{(2)}, & \bar{\gamma}_k^{(2)} > \varepsilon \end{cases}, \\ \widehat{\gamma}_{i,k}^{(2)} &= 1 - \widehat{\gamma}_{i,k}^{(1)}, \end{aligned} \tag{21}$$

```
// Run Kalman filter to steady state.
Initialize $\widehat{x}_{i,-\infty} = 0, P_{i,-\infty} = \Pi_i, \widehat{x}_{-\infty} = 0, P_{-\infty} = \Pi$;
for $k = -\infty : 0$ do
    // Local data reaches steady state.
    For $i = 1 : N$ do
        $P_{i,k} = [(AP_{i,k-1}A' + Q)^{-1} + C_i'R_i^{-1}C_i]^{-1}$ ;
        $\widehat{x}_{i,k} = A\widehat{x}_{i,k-1} + P_{i,k}C_i'R^{-1}(y_{i,k} - C_iA\widehat{x}_{i,k-1})$ ;
    end for
    // The remote estimator reaches steady state.
    $P_k = [(AP_{k-1}A' + Q)^{-1} + C'R^{-1}C]^{-1}$ ;
    $\widehat{x}_k = A\widehat{x}_{k-1} + P_kC'R^{-1}(y_k - CA\widehat{x}_{k-1})$ ;
end for
// GMM clustering by the EM algorithm.
Set $\bar{P}_i = P_{i,0}, \Sigma_i^{(1)} = P_{i,0}$
for $k = 1 : +\infty$ do
    for $i = 1 : N$ do
        $\widehat{x}_{i,k} = A\widehat{x}_{i,k-1} + \bar{P}_iC_i'R_i^{-1}(y_{i,k} - C_iA\widehat{x}_{i,k-1})$;
    end for
    // the EM algorithm.
    Initialize $\pi_k^{(1)}, \pi_k^{(2)}, \mu_k^{(1)}, \mu_k^{(2)}, \Sigma_k^{(2)}$ ;
    while $\mathscr{L}(\Phi_{k;}\mathscr{Z}_k)$ not achieve the maximum likelihood estimates do
        The expectation step: calculate $\gamma_{i,k}^{(1)}$ and $\gamma_{i,k}^{(2)}$ according to Equation (15)-(16).
        The maximization step: calculate $\{\pi_k^{(q)}, \mu_k^{(q)}, \Sigma_k^{(2)}\}_{q=1}^{2}$ by Equation (17)-(19).
    end while
    // the error compensator.
    $\bar{\gamma}_k^{(2)} = \sum_{i=1}^N \gamma_{i,k}^{(2)}/N$
    for $i = 1 : N$do
        if $\bar{\gamma}_k^{(2)} > \varepsilon$  $(\varepsilon \geqslant (|s|/N))$ then
            $\widehat{\gamma}_{i,k}^{(1)} = \gamma_{i,k}^{(2)}$;
            $\widehat{\gamma}_{i,k}^{(2)} = \gamma_{i,k}^{(1)}$;
        else
            $\widehat{\gamma}_{i,k}^{(1)} = \gamma_{i,k}^{(1)}$;
            $\widehat{\gamma}_{i,k}^{(2)} = \gamma_{i,k}^{(2)}$;
        end if
    end for
    // Remote state estimation.
    $\widehat{x}_k^- = A\widehat{x}_{k-1}$ ;
    $P_k^- = AP_{k-1}A' + Q$;
    $\widehat{x}_k = \widehat{x}_k^- + \sum_{i=1}^N \widehat{\gamma}_{i,k}^{(1)} P_kC_i'R_i^{-1}(y_{i,k} - C_i\widehat{x}_k^-)$ ;
    $P_k = [(P_k^-)^{-1} + \sum_{i=1}^N \gamma\wedge_{i,k}^{(1)} C_i'R_i^{-1}C_i]^{-1}$ ;
end for
```

Algorithm 1: The GMM-based state estimation against dynamic attacks.

where $\widehat{\gamma}_{i,k}^{(1)}$ and $\widehat{\gamma}_{i,k}^{(2)}$ are the modified beliefs, and $\varepsilon \geq s/N$ represents a threshold, which can be adjusted according to the performance requirements of the actual system.

3.3. The GMM-Based State Estimation Approach against Dynamic Attacks.

In this subsection, a GMM-based estimation algorithm is proposed to deal with the dynamic attacks, which can improve the estimation accuracy effectively.

$$\widehat{x}_k^- = A\widehat{x}_{k-1}, \tag{22a}$$

$$P_k^- = AP_{k-1}A' + Q, \tag{22b}$$

$$\widehat{x}_k = \widehat{x}_k^- + \sum_{i=1}^{N} \widehat{\gamma}_{i,k}^{(1)} P_kC_i'R_i^{-1}\left(y_{i,k} - C_i\widehat{x}_k^-\right), \tag{22c}$$

$$P_k = \left[(P_k^-)^{-1} + \sum_{i=1}^{N} \gamma\wedge_{i,k}^{(1)} C_i'R_i^{-1}C_i\right]^{-1}, \tag{22d}$$

where the initial values $\widehat{x}_0$ and P_0 are the steady-state values of the remote estimator when $k \leq 0$.

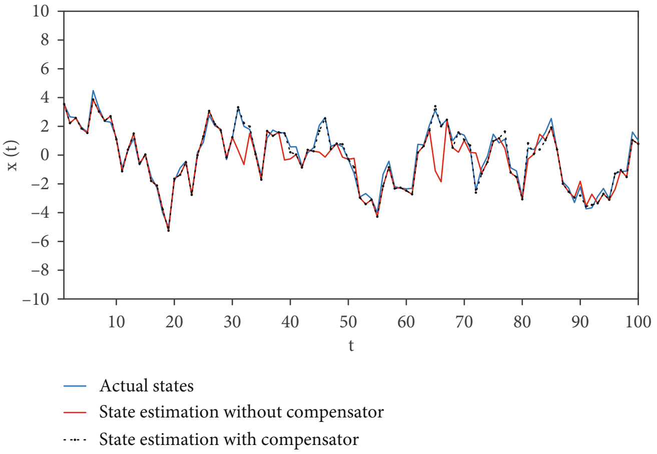

Figure 2: The actual states and its remote estimation with different approaches.

Theorem 2. *Consider the linear time-invariant system (1)-(2) and the dynamic adversary satisfying Assumptions 1–4, and the remote state estimation $\hat{x}_k$ can be calculated by*

Proof. According to the Definition 2 in [16, 28], if $s(s \le N/2)$ sensors are attacked, the following system is still observable in the absence of attacks:

$$\begin{aligned} x_{k+1} &= Ax_k + w_k, \\ y_{\bar{s},k} &= C_{\bar{s}}x_k + v_{\bar{s},k}, \end{aligned} \tag{23}$$

where $\bar{s} \subseteq \{1, 2, \cdots, N\}$ is the set of unattacked sensors, and $y_{\bar{s},k}$ is the measurement stacked by the set $\bar{s}$. Similarly, $C_{\bar{s}}$ and $v_{\bar{s},k}$ are the system parameter and the measurement noise stacked by the set $\bar{s}$, respectively. The pair $(A, C_{\bar{s}})$ is observable.

According to Section II, Equation (6) can be expanded as

$$\begin{aligned} \hat{x}_k &== \hat{x}_k^- + P_k C' R^{-1}\left(y_k - C\hat{x}_k^-\right) \\ &= \hat{x}_k^- + P_k \begin{bmatrix} C_1' \\ \vdots \\ C_N' \end{bmatrix}' \begin{bmatrix} R_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & R_N \end{bmatrix}^{-1} \left(\begin{bmatrix} y_{1,k} \\ \vdots \\ y_{N,k} \end{bmatrix} - \begin{bmatrix} C_1' \\ \vdots \\ C_N' \end{bmatrix} \hat{x}_k^- \right) \\ &= \hat{x}_k^- + P_k \begin{bmatrix} C_1' R_1^{-1} \\ \vdots \\ C_N' R_N^{-1} \end{bmatrix}' \begin{bmatrix} y_{1,k} - C_1'\hat{x}_k^- \\ \vdots \\ y_{N,k} - C_N'\hat{x}_k^- \end{bmatrix} \\ &= \hat{x}_k^- + \sum_{i=1}^{N} P_k C_i' R_i^{-1}\left(y_{i,k} - C_i\hat{x}_k^-\right), \end{aligned} \tag{24}$$

where the default weight of each sensor is equal to 1 when the sensor is not attacked. □

Based on the above analysis, we can calculate the remote state estimation $\hat{x}_k$ by adopting the undamaged sensors. The belief $\hat{\gamma}_{i,k}^{(1)}$ represents the probability that the sensor i is undamaged. Then, we can fuse the local data by adopting $\hat{\gamma}_{i,k}^{(1)}$ as the new weight of the local data, and then the Equations (22a)-(22d) can be obtained.

The system is assumed to reach steady state before time $k = 0$. The adversary can launch dynamic attacks at any time when $k \ge 1$. Starting from time $k = 1$, the local state estimation $\hat{x}_{i,k}$ is calculated utilizing the measurement of sensor i at each time instant k. Based on that, the remote estimator clusters the local state estimates and calculates the parameter Φ_k by the EM algorithm according to Equation (15)-(19). Then, the error compensator is used to correct the error beliefs. Finally, based on the modified belief $\hat{\gamma}_{i,k}^{(1)}$, the local data can be fused by Theorem 2 to obtain the state estimation $\hat{x}_k$. The whole process is summarized in Algorithm 1.

4. Numerical Simulation

In this section, the effectiveness of the GMM-based estimation algorithm is verified through numerical simulations. Similar to literature [21], we consider a linear time-invariant dynamic process which is measured by 15 sensors. The system parameters A and Q are randomly generated from intervals [0.4, 0.99] and [0.5, 2], respectively. Matrices C_i and R_i, $i \in N$, are randomly generated from intervals [1, 2]. The system reaches steady state before $t = 30$, and the attack signal starts from time $t = 31$, assuming that s $(1 \le s \le 6)$ sensors are attacked by $a_{i,k}$ at each time instant $t(t \ge 31)$.

4.1. Example 1.

In this example, the estimation accuracy of GMM-based method with and without compensator against dynamic attacks has been compared. Similar to [15], the attack signal $a_{i,k}$ can be assumed to be a linear function of the measurement noise:

$$a_{i,k} = \beta v_{i,k} + \Theta, \tag{25}$$

where β and Θ are real number from the interval [-5, 5] and [-10, 10], respectively. Meanwhile, $a_{i,k}$ satisfies Assumptions 1–4.

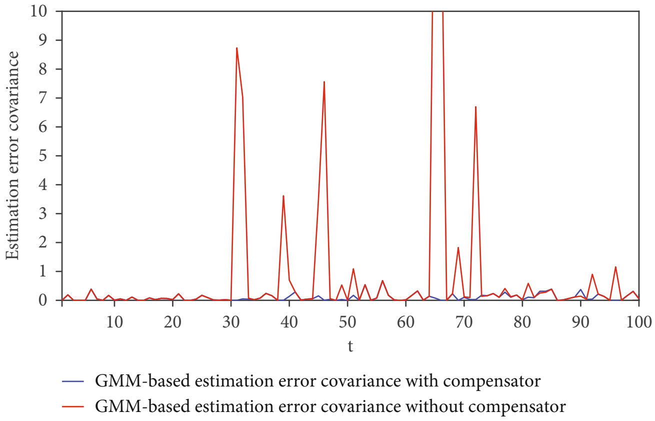

FIGURE 3: Remote estimation error covariance of the GMM-based method with and without compensator.

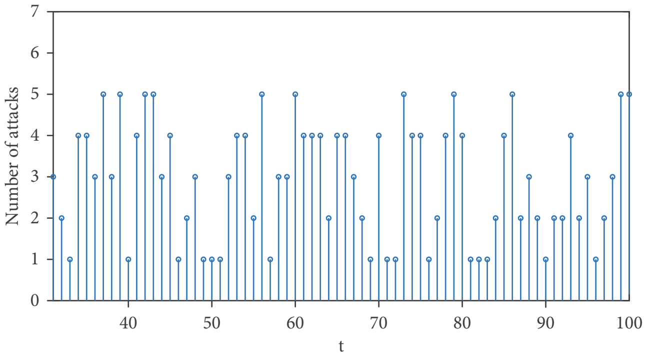

FIGURE 4: The number of attacked sensors at each moment when $T \geqslant 31$.

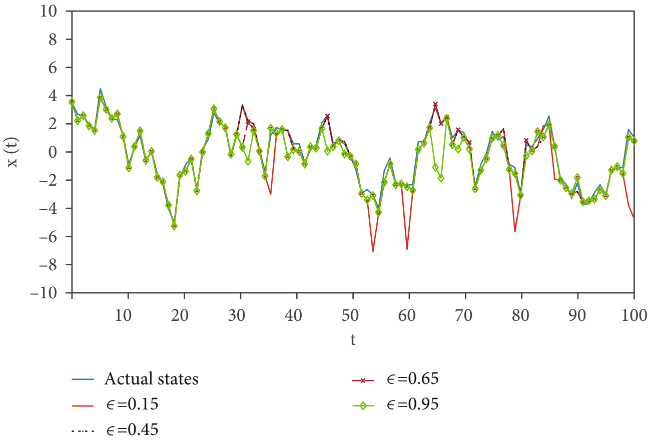

FIGURE 5: Comparison of the state estimation with different thresholds.

Set the threshold $\varepsilon = 0.45$ in the following example. In Figure 2, the trajectories of the actual state and the states estimated by the GMM-based estimation method with and without compensator are plotted. It is shown that the estimated states of the GMM-based method with compensator (dotted line) are closer to the actual state than that without compensator (red line). Figure 3 shows the estimation error covariance for the GMM-based method with and without compensator, respectively. It is observed that the estimation error covariance of the method without compensator (red line) is larger than that with compensator (black line), which means that the error compensator proposed in this paper can effectively reduce the impact of faulty data on state estimation. According to Figures 2 and 3, the estimation accuracy of the GMM-based estimation method with the compensator is higher than that without the compensator against dynamic attacks.

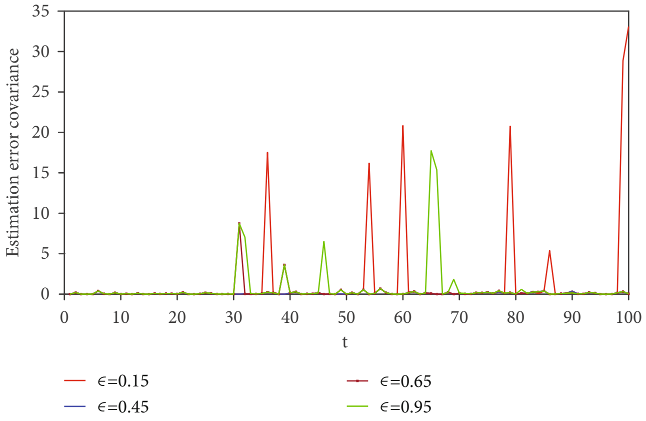

Figure 6: Remote estimation error covariance with different thresholds.

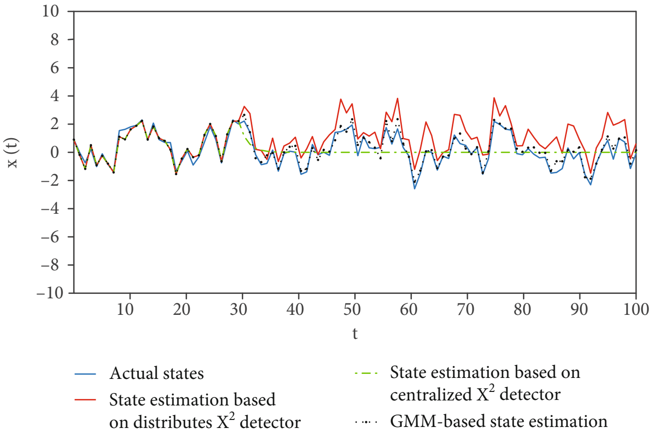

Figure 7: The actual states and its remote estimation based on different methods.

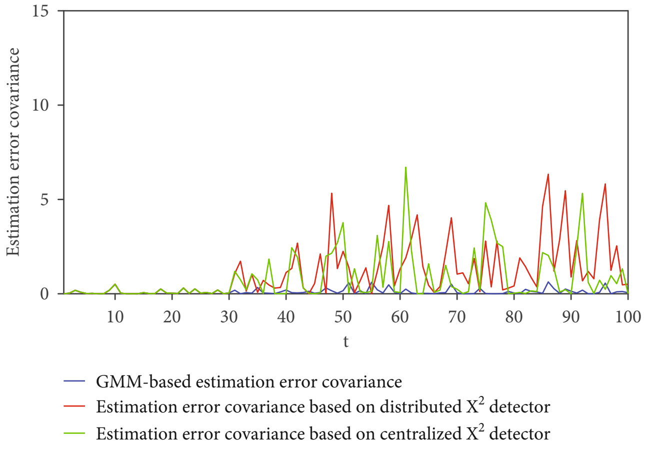

Figure 8: Remote estimation error covariance based on different methods.

The number of attacked sensors at each moment when $T \geq 31$ is plotted in Figure 4, and the state estimation and corresponding error covariance of the GMM-based algorithm when the compensator takes different thresholds are shown in Figures 5 and 6, respectively. It is seen that the state estimation accuracy is higher when $\varepsilon = 0.45$ and 0.65 than $\varepsilon = 0.15$ and 0.95, which is indicated that the performance of the remote estimator will deteriorate while ε is too large or too small. Hence, the threshold can be adjusted according to the actual performance requirements of the real system.

4.2. Example 2. Distributed and centralized χ^2 false-data detectors are common, and they determine whether an attack exists based on the statistical characteristics of the innovation $y_{i,k} - C_i\widehat{x}_{i,k}^-$ and $y_k - C\widehat{x}_k^-$, respectively. From [21], a well-designed dynamic attack can successfully bypass the distributed χ^2 detector but fails to remain stealthy to the centralized χ^2 false-data detector. In this subsection, we have compared the proposed approach and the estimation methods based on different χ^2 false-data detectors.

Similar to [21], the attack signal $a_{i,k}$ is set as

$$a_{i,k} = -2y_{i,k} + 2C_i\widehat{x}_k^-, \tag{26}$$

where $a_{i,k}$ satisfies Assumptions 1–4.

In Figure 7, the trajectories of the actual state and the state estimated by estimation methods based on different detectors are plotted, respectively. It is seen that the GMM-based state estimation (black line) is closer to the actual state than the state estimation based on the distributed and centralized χ^2 detector (red and green). Figure 8 shows the estimation error covariance of the corresponding methods, and it is observed that the GMM-based estimation error covariance is much smaller than that based on the distributed and centralized χ^2 detector. It can be seen that the GMM-based estimation approach proposed in this paper can improve the performance effectively.

5. Conclusion

This paper studies the state estimation problem against dynamic malicious attacks. An error compensator is presented, which can reduce the influence of local error data on state estimation effectively. Based on that, a new GMM-based state estimation algorithm is proposed to improve the estimation accuracy for the system suffering from dynamic attacks. Finally, the effectiveness of the proposed algorithm is verified by numerical simulations. We will extend the GMM-based approach further to systems with parametric uncertainties in the future.

Data Availability

Some or all data, models, or code generated or used during the study are available from the corresponding author by request (Cui Zhu).

Conflicts of Interest

The authors declare that they have no conflicts of interest related to this work.

Acknowledgments

The author would like to thank the tutor and anonymous reviewers for their suggestions, which improved the quality of work. This work was supported by the National Natural Science Foundation of China (grant numbers 61603047, 61773334), the Scientific Research Project of Beijing Municipal Educational Commission (grant number KM201911232014), the Key Research Cultivation Program of Beijing Information Science and Technology University (grant number 2121YJPY221), and the Qin Xin Talents Cultivation Program, Beijing Information Science and Technology University (grant number QXTCPC202110).

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: milestones and research challenges," *Computer Communications*, vol. 36, no. 1, pp. 1–7, 2012.

[2] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," *IEEE Security and Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[3] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[4] J. P. Conti, "The day the samba stopped [power blackouts]," *Engineering and Technology*, vol. 5, no. 4, pp. 46-47, 2010.

[5] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *IFIP Advances in Information and Communication Technology*, vol. 253, pp. 73–82, 2007.

[6] K. Kim and P. R. Kumar, "Cyber–physical systems: a perspective at the centennial," *Proceedings of the IEEE*, vol. 100, pp. 1287–1308, 2012.

[7] L. Shan, J. Yu, J. Zhang, Y. Li, E. Zhou, and L. Zhao, "Distributed state estimation based on the realtime dispatch and control cloud platform," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–6, Beijing, China, 2018.

[8] Y. Kobayashi and I. Ono, "Sequential estimation of states and parameters of nonlinear state space models using particle filter and natural evolution strategy," in *2020 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1–8, Glasgow, UK, 2020.

[9] I. Polyakov, A. Pazderin, and O. Polyakova, "Computational performance comparing of the state estimation problem statementes in polar and rectangular coordinates," in *2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA)*, pp. 1–4, Varna, Bulgaria, June 2019.

[10] M. M. Rana and N. Dahotre, "Bayesian network and semidefinite programming based wireless power transfer manufacturing system state estimation and regulation," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, pp. 237–241, PyeongChang, Korea (South), Feb. 2021.

[11] J. Zhao, G. Zhang, Z. Y. Dong, and M. La Scala, "Robust forecasting aided power system state estimation considering state correlations," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2658–2666, 2018.

[12] M. M. Rana, W. Xiang, and E. Wang, "IoT-based state estimation for microgrids," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1345-1346, 2018.

[13] M. Netto and L. Mili, "A robust data-driven Koopman Kalman filter for power systems dynamic state estimation," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 7228–7237, 2018.

[14] J. Zhao, Z. Zheng, S. Wang et al., "Correlation-aided robust decentralized dynamic state estimation of power systems with unknown control inputs," *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 2443–2451, 2020.

[15] 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.

[16] W. Ao, Y. Song, C. Wen, and J. Lai, “Finite time attack detection and supervised secure state estimation for CPSs with malicious adversaries,” *Information Sciences*, vol. 451–452, pp. 67–82, 2018.

[17] X. Liu, Y. Mo, and E. Garone, “Secure dynamic state estimation by decomposing Kalman filter,” *IFAC (International Federation of Automatic Control)*, vol. 50, no. 1, pp. 7351–7356, 2017.

[18] X. Liu, Y. Mo, and X. Ren, “Security analysis of continuous-time cyber-physical system against sensor attacks,” in *2017 13th IEEE Conference on Automation Science and Engineering (CASE)*, pp. 1586–1591, Xi'an, China, Aug. 2017.

[19] N. Forti, G. Battistelli, L. Chisci, and B. Sinopoli, “Secure state estimation of cyber-physical systems under switching attacks,” *IFAC PapersOnLine*, vol. 50, no. 1, pp. 4979–4986, 2017.

[20] A. Y. Lu and G. H. Yang, “Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer,” *Information Sciences*, vol. 417, pp. 454–464, 2017.

[21] Z. Guo, D. Shi, D. E. Quevedo, and L. Shi, “Secure State Estimation against Integrity Attacks: a Gaussian Mixture Model Approach,” *IEEE Transactions on Signal Processing*, vol. 67, no. 1, pp. 194–207, 2019.

[22] F. Wen and Z. Wang, “Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks,” *Digital Signal Processing*, vol. 78, pp. 92–97, 2018.

[23] 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.

[24] M. Pajic, J. Weimer, N. Bezzo et al., “Robustness of attack-resilient state estimators,” in *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pp. 163–174, Berlin, Germany, April 2014.

[25] B. D. Anderson and J. B. Moore, *Optimal Filtering*, Courier Corporation, 2012.

[26] C. M. Bishop, *Pattern Eecognition and Machine Learning*, Springer, 2006.

[27] T. K. Moon, “The expectation-maximization algorithm,” *IEEE Signal Processing Magazine*, vol. 13, no. 6, pp. 47–60, 1996.

[28] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in *Proceedings of the American Control Conference*, pp. 2439–2444, Chicago, IL, USA, 2015.