*Electronic Research Archive*

https://www.aimspress.com/journal/era

ERA, 32(6): 4181–4198.
DOI: 10.3934/era.2024188
Received: 08 April 2024
Revised: 17 June 2024
Accepted: 24 June 2024
Published: 28 June 2024

*Research article*

# Maximum likelihood-based identification for FIR systems with binary observations and data tampering attacks

**Xinchang Guo**[1,2], **Jiahao Fan**[1,2] **and Yan Liu**[1,2,*]

[1] School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China

[2] Key Laboratory of Knowledge Automation for Industrial Processes, Ministry of Education, Beijing 100083, China

* **Correspondence:** Email: liuyan@ustb.edu.cn.

**Abstract:** The security issue of CPS (cyber-physical systems) is of great importance for their stable operation. Within the framework of system identification, this paper proposed a maximum likelihood estimation algorithm for FIR (finite impulse response) systems with binary observations and data tampering attacks. In the case of data transmission in the communication network being subjected to data tampering attacks after the FIR system sends out data, the objective of this study was to design an algorithm for estimating the system parameters and infer the attack strategies using the proposed algorithm. To begin, the maximum likelihood function of the available data was established. Then, parameter estimation algorithms were proposed for both known and unknown attack strategies. Meanwhile, the convergence condition and convergence proof of these algorithms were provided. Finally, the effectiveness of the designed algorithm was verified by numerical simulations.

**Keywords:** finite impulse response system; data tampering attack; maximum likelihood method; system parameter identification

## 1. Introduction

Cyber-physical system (CPS) is an emerging technology that integrates computation, communication, and physical devices. Introduction of network technology in CPS offers significant advantages in system efficiency, scalability, and maintainability. CPS is widely applied in various fields due to its robustness, high reliability, and fast operation speed [1–3]. Due to the close interaction among computation, sensing, communication, and actuation in CPS, it is highly susceptible to network security threats.Additionally, intelligent CPS presents new challenges and threats different from existing issues [4, 5]. Notably, CPS closely integrated with national infrastructure can lead to immeasurable

severe consequences if subjected to malicious attacks. Therefore, ensuring the secure operation of CPS-related devices is an urgent problem that needs to be addressed [6, 7].

There have been many security incidents of CPS in the world, which have brought huge losses [8,9]. In June 2010, Iran's nuclear facilities were attacked by the Stuxnet virus, which seriously damaged nuclear power plants and other facilities, seriously jeopardizing Iran's nuclear security. In 2014, the Havex Trojan attacked numerous European industrial manufacturing systems. In addition to attacks on industrial systems, attacks on the power grid also occur frequently. In 2015, the Ukrainian power grid suffered a Black-Energy attack. In 2016, the Israeli power grid suffered a serious cyber attack, and in 2019, several South American countries suffered a cyber attack on the power system. An attack on the power grid would lead to widespread power outages, which would render factories inoperable and infrastructure paralyzed, causing serious inconvenience and impact to society.

In recent years, scholars have conducted extensive research on the security of CPSs. Attack detection is one of the important strategies to ensure the safe operation of CPS, aiming to identify malicious behaviors such as network attacks and take appropriate countermeasures as early as possible to minimize or prevent significant losses [10, 11]. As the complexity of attacks in CPS increases, traditional anomaly detection methods have limitations and require the design of detection algorithms with specific characteristics for a particular domain [12,13]. Reference [14] tackles the design problem of intrusion detection systems by creatively combining feature-based intrusion detection system (SIDS) and anomaly-based intrusion detection system (AIDS) to form an improved stacked ensemble algorithm (ISEA). This algorithm significantly reduces the false positive rate (FPR) through a false positive elimination strategy (FPES). Reference [15] argues that in the era of Industry 4.0, a layered and distributed approach is required for intrusion detection. This approach includes perception-execution layer monitoring based on Kalman filters, network transmission layer monitoring based on recursive Gaussian mixture models, and application control layer monitoring based on sparse deep belief network models. It enables comprehensive and efficient identification of covert attacks and ensures security protection. Reference [16] proposes a federated deep learning scheme to address the attack problem in large-scale and complex industrial networked physical systems. This scheme utilizes a deep learning-based intrusion detection model combined with federated learning framework and secure communication protocols to enhance the privacy of industrial CPS while ensuring resilience against network threats.

Data tampering attacks are a prevalent and typical type of network attack targeting CPSs. They have also gained widespread attention in recent years [13, 17, 18]. The main method of data tampering attacks is to manipulate the data transmitted in the network, affecting the estimation and control center of CPS, leading to incorrect judgments or decisions, and issuing erroneous instructions, which may result in abnormal or even damaged physical devices [19–21]. Such attacks are often difficult to be detected by existing intrusion detection systems, thus they can quietly penetrate CPS systems and affect their stable operation [22, 23].

In recent years, the detection algorithms for data tampering attacks have received attention, and some scholars have conducted in-depth analysis and research on these attacks. Reference [24] proposes a solution to mitigate the computational cost and enhance privacy for smart grid aggregation faced with deletion and tampering attacks, targeted specifically at data tampering attacks. Reference [25] addresses firmware tampering attack defense and forensics issues by designing a detection method based on joint testing action groups and memory comparison to detect firmware tampering attacks. Reference [26] addresses the problem of the $\chi^2$ detector being difficult to detect false data injection

attacks with white noise. It proposes a novel summation (SUM) detector that not only utilizes current compromise information but also collects all historical information to reveal the threat. It also has good identification for improved false data injection. Reference [27] studies the identification problem of finite impulse response (FIR) systems with binary measurements under data tampering, and the optimal attack strategy and defense method are given. Reference [28] introduces a novel secure key aggregation searchable encryption scheme and anti-tampering blockchain technology to propose a data sharing system that selectively shares and retrieves vehicle sensor data, detecting unauthorized data tampering attacks.

This paper focuses on the data tampering attack problem in binary quantization FIR systems. Under the framework of system identification, a novel algorithm is designed to solve the system parameters and attack strategies using the maximum likelihood method and binary measurement data. The computation method is also provided. To begin, the maximum likelihood function of the measurement data is established. Then, parameter estimation algorithms are proposed for both known and unknown attack strategies. The closeness between the estimated system parameter values obtained from this estimation algorithm and the true values depends on the sample data size and whether the attack strategy is known or unknown. In the case of an unknown attack strategy, the difficulty in algorithm design increases due to the coupling between unknown parameters and attack strategies. The unknown variables in the maximum likelihood function are simplified to the system of equations. The Newton-Raphson iteration method is used to train the back propagation neural network (BPNN), and the attack strategy is estimated in advance. The estimated value of the attack strategy is then substituted into the algorithm to obtain the unknown parameter estimates. The results obtained from the algorithm show that with a small sample data size, the estimation algorithm produces large fluctuations in the solved system parameters. However, as the sample data size increases, the estimated values of the system parameters tend to become closer to the true values.

The structure of this paper is as follows. Section 2 describes the data tampering detection problem in binary quantization FIR systems; Section 3 presents the expression of the maximum likelihood function of the system; Section 4 discusses the use of maximum likelihood estimation to solve the system parameters in the case of a known attack strategy; Section 5 discusses the step-by-step solution of system parameters and attack strategies in the case of an unknown attack strategy; Section 6 validates the estimation algorithm through numerical simulations; and Section 7 provides a summary and outlook for this paper.

## 2. Problem formulation

Consider a single-input single-output discrete-time FIR system:

$$\begin{aligned} y_k &= a_1u_k + a_2u_{k-1} + \cdots + a_nu_{k-n-1} + d_k \\ &= \phi_k^T\theta + d_k, \quad k = 1, 2, \ldots, \end{aligned} \tag{1}$$

where $u_k$ is the quantized system input and its possible value is in $\{\mu_1, \mu_2, \ldots, \mu_r\}$, i.e., $u_k \in \{\mu_1, \mu_2, \ldots, \mu_r\}$; $\phi_k = [u_k, \ldots, u_{k-n-1}]^T$ is the regression vector composed of quantized inputs, since $u_k$ can only take $r$ different values, $\phi_k$ has $l = r^n$ possible values, which can be represented as $\pi_1, \pi_2, \ldots, \pi_l$, that is, $\phi_k \in \{\pi_1, \pi_2, \ldots, \pi_l\}$; $\theta = [a_1, \ldots, a_n]^T$ is the unknown parameters of the system; $d_k$ is the system noise; $y_k$ is the system output, measured by a binary sensor with threshold $C \in (-\infty, \infty)$, and it can be

represented by an indicator function as:

$$s_k^0 = I_{\{y_k \le C\}} = \begin{cases} 1, & y_k \le C; \\ 0, & \text{else.} \end{cases} \tag{2}$$

From here on, the superscript $^T$ denotes the transpose of a matrix or vector.

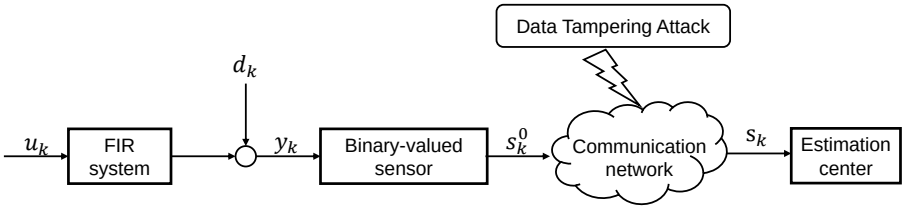


**Figure 1.** System block diagram.

As shown in Figure 1, $s_k^0$ is transmitted through a communication network to a data center, but it is susceptible to data tampering attacks during the communication process. The data received by the data center is denoted as $s_k$, and its relationship with $s_k^0$ is as follows:

$$\begin{cases} \Pr(s_k = 1 | s_k^0 = 0) = p_0; \\ \Pr(s_k = 0 | s_k^0 = 1) = p_1. \end{cases} \tag{3}$$

The above equation essentially describes a data tampering attack strategy, which is denoted as $(p_0, p_1)$.

In this paper, a maximum likelihood estimation method is used to provide an estimation algorithm for the unknown parameters $\theta$, and the convergence performance of the algorithm is also analyzed.

**Assumption 1.** *The system noise $\{d_k\}$ is an independent and identically distributed (i.i.d.) sequence of normal random variables with zero mean and variance $\sigma^2$, and its probability distribution function and probability density function are denoted as $F(\cdot)$ and $f(\cdot)$, respectively.*

**Remark 1.** 1) This paper is concerned with the binary observation. For the case of multi-threshold quantization, it can be converted into multiple binary values for processing [29]. 2) The attack process here is independent, and the existing literature often studies the cases where it is dependent and modeled as Markov processes [30]. The method in this paper can provide reference for the case of nonindependent attack process.

## 3. Maximum likelihood function of available data

Maximum likelihood estimate is a commonly used parameter estimation method in statistics that estimates model parameters by maximizing the likelihood function of the sample data. This section presents the maximum likelihood function of the data received at the receiving center, laying the foundation for the subsequent algorithm design.

From Eqs (1) and (2), we can determine the probability of $s_k^0 = 1$ being equal to

$$\begin{aligned}\Pr(y_k \le C) &= \Pr(\phi_k^T\theta + d_k \le C)\\ &= \Pr(d_k \le C - \phi_k^T\theta)\\ &= F(C - \phi_k^T\theta).\end{aligned} \tag{4}$$

Combining this with Eq (3) and using the law of total probability, we obtain:

$$\begin{aligned}&\Pr(s_k = 1)\\ =\ &\Pr(s_k = 1|s_k^0 = 0)\cdot\Pr(s_k^0 = 0) + \Pr(s_k = 1|s_k^0 = 1)\cdot\Pr(s_k^0 = 1)\\ =\ &p_0\cdot\Pr(y_k > C) + (1 - p_1)\cdot\Pr(y_k \le C)\\ =\ &p_0\cdot(1 - F(C - \phi_k^T\theta)) + (1 - p_1)\cdot F(C - \phi_k^T\theta) \overset{\text{def}}{=} g_k.\end{aligned} \tag{5}$$

Then,

$$\Pr(s_k) = g_k^{s_k}\cdot(1 - g_k)^{(1-s_k)}. \tag{6}$$

Based on Eq (5), $g_k$ can be simplified as:

$$g_k = (1 - p_0 - p_1)F(C - \phi_k^T\theta) + p_0. \tag{7}$$

Hence, for a data length of $N$, the maximum likelihood function of $s_1, s_2, \ldots, s_N$ is:

$$\begin{aligned}L(\theta|s_1, s_2, \ldots, s_N) &= \Pr(s_1, s_2, \ldots, s_N)\\ &= \Pr(s_1)\cdot\Pr(s_2)\cdot\cdots\cdot\Pr(s_N)\\ &= \prod_{k=1}^{N} g_k^{s_k}\cdot(1 - g_k)^{(1-s_k)}.\end{aligned} \tag{8}$$

## 4. Identification algorithm: the attack strategy is known

The principle of maximum likelihood estimation is based on the intuitive idea that a parameter is the most reasonable estimate if it gives the greatest probability that the sample data will occur. For the maximum likelihood function, the parameters at its maximum value are called the maximum likelihood estimates. In this section, the attack strategy $(p_0, p_1)$ is assumed to be known. Two functions are defined as follows:

$$h_1(x) = \frac{(1 - p_0 - p_1)f(C - x)}{(1 - p_0 - p_1)F(C - x) + p_0},\quad h_2(x) = \frac{(1 - p_0 - p_1)f(C - x)}{(p_0 + p_1 - 1)F(C - x) + 1 - p_0}. \tag{9}$$

Let

$$\frac{\partial}{\partial\theta}\ln L(s_1, s_2, \ldots, s_N) = 0. \tag{10}$$

The solution of the equation is denoted as $\widehat{\theta}_N = \widehat{\theta}_N(s_1, s_2, \ldots, s_N)$, which is the maximum likelihood estimate of $\theta$.

Since Eq (10) is highly nonlinear, an explicit solution generally doesn't exist. Here, an approximate solution method is presented. Taking the logarithm of Eq (8), we have

$$\begin{aligned}
&\ln L(\theta|s_1, s_2, \ldots, s_N) \\
&= \sum_{k=1}^{N} \left[ s_k \cdot \ln g_k + (1 - s_k) \cdot \ln(1 - g_k) \right] \\
&= \sum_{k=1}^{N} s_k \cdot \ln \left[ F(C - \phi_k^T \theta)(1 - p_0 - p_1) + p_0 \right] \\
&\quad + \sum_{k=1}^{N} (1 - s_k) \cdot \ln \left[ F(C - \phi_k^T \theta)(p_0 + p_1 - 1) + 1 - p_0 \right].
\end{aligned} \tag{11}$$

Taking the partial derivative of the above equation with respect to $\theta$, we get

$$\begin{aligned}
&\frac{\partial}{\partial \theta} \ln L(\theta|s_1, s_2, \ldots, s_N) \\
&= \sum_{k=1}^{N} s_k \cdot \frac{(1 - p_0 - p_1) f(C - \phi_k^T \theta) \cdot (-\phi_k^T)}{(1 - p_0 - p_1) F(C - \phi_k^T \theta) + p_0} \\
&\quad + \sum_{k=1}^{N} (s_k - 1) \cdot \frac{(1 - p_0 - p_1) f(C - \phi_k^T \theta) \cdot (-\phi_k^T)}{(p_0 + p_1 - 1) F(C - \phi_k^T \theta) + 1 - p_0}.
\end{aligned} \tag{12}$$

By Eq (9), Eq (12) can be expressed as:

$$\frac{\partial}{\partial \theta} \ln L(\theta) = \sum_{k=1}^{N} s_k h_1(\phi_k^T \theta)(-\phi_k^T) + \sum_{k=1}^{N} (s_k - 1) h_2(\phi_k^T \theta)(-\phi_k^T). \tag{13}$$

Since $\phi_k^T$ can take the values $\pi_1, \pi_2, \ldots, \pi_l$, grouping the above expression based on these values, we can rearrange it as:

$$\begin{aligned}
\frac{\partial}{\partial \theta} \ln L(\theta) = &\sum_{k=1, \phi_k^T = \pi_1}^{N} s_k h_1(\pi_1 \theta)(-\pi_1) + \sum_{k=1, \phi_k^T = \pi_1}^{N} (s_k - 1) h_2(\pi_1 \theta)(-\pi_1) \\
&+ \sum_{k=1, \phi_k^T = \pi_2}^{N} s_k h_1(\pi_2 \theta)(-\pi_2) + \sum_{k=1, \phi_k^T = \pi_2}^{N} (s_k - 1) h_2(\pi_2 \theta)(-\pi_2) \\
&+ \cdots \\
&+ \sum_{k=1, \phi_k^T = \pi_l}^{N} s_k h_1(\pi_l \theta)(-\pi_l) + \sum_{k=1, \phi_k^T = \pi_l}^{N} (s_k - 1) h_2(\pi_l \theta)(-\pi_l).
\end{aligned} \tag{14}$$

In Eq (15), if we have

$$\sum_{k=1, \phi_k^T = \pi_i}^{N} s_k h_1(\pi_i \theta) + \sum_{k=1, \phi_k^T = \pi_i}^{N} (s_k - 1) h_2(\pi_i \theta) = 0, \quad i = 1, 2, \ldots, l, \tag{15}$$

then $\frac{\partial}{\partial\theta}\ln L(\theta) = 0$. Thus, the problem of solving the equation $\frac{\partial}{\partial\theta}\ln L(\theta) = 0$ is reduced to solving the system of Eq (15).

By rearranging (15), we get

$$[h_1(\pi_i\theta) + h_2(\pi_i\theta)] \sum_{k=1,\phi_k^T=\pi_i}^{N} s_k = h_2(\pi_i\theta) \sum_{k=1,\phi_k^T=\pi_i}^{N} 1.$$

As a result, we obtain

$$\frac{\sum_{k=1}^{N} s_k I\{\phi_k^T = \pi_i\}}{\sum_{k=1}^{N} I\{\phi_k^T = \pi_i\}} = \frac{h_2(\pi_i\theta)}{h_1(\pi_i\theta) + h_2(\pi_i\theta)} = H(\pi_i\theta), \tag{16}$$

where $H(x) = \frac{h_2(x)}{h_1(x)+h_2(x)}$, $h_1(x)$, and $h_2(x)$ are given by (9). Let the $H(x)$ reverse function be $H^{-1}(x)$, and we have

$$\begin{aligned} & H(x) = (1 - p_0 - p_1)F(C - x) + p_0 \\ \Rightarrow\ & H(x) - p_0 = (1 - p_0 - p_1)F(C - x) \\ \Rightarrow\ & \frac{H(x) - p_0}{1 - p_0 - p_1} = F(C - x) \qquad (17) \\ \Rightarrow\ & F^{-1}\left(\frac{H(x) - p_0}{1 - p_0 - p_1}\right) = C - x. \qquad (18) \end{aligned}$$

Therefore, from (16), we have

$$\pi_i\theta = C - F^{-1}\left(\frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_i\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_i\}}} - p_0}{1 - p_0 - p_1}\right), \quad i = 1, 2, \ldots, l.$$

Expressing the above equation set in matrix form, we have

$$\begin{bmatrix} \pi_1 \\ \vdots \\ \pi_l \end{bmatrix}\theta = \begin{bmatrix} C - F^{-1}\left(\frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_1\}}} - p_0}{1-p_0-p_1}\right) \\ \vdots \\ C - F^{-1}\left(\frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_l\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_l\}}} - p_0}{1-p_0-p_1}\right) \end{bmatrix}. \tag{19}$$

Let $\Phi = [\pi_1^T, \pi_2^T, \ldots, \pi_l^T]^T$, $\eta_{N,i} = C - F^{-1}\left(\frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_i\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_i\}}} - p_0}{1-p_0-p_1}\right)$, $i = 1, 2, \ldots, l$. The maximum likelihood estimate of $\theta$ is obtained as:

$$\widehat{\theta_N} = \Phi^{+}[\eta_{N,1}, \ldots, \eta_{N,l}]^T, \tag{20}$$

where $^+$ denotes the Moore-Penrose inverse of the matrix.

**Remark 2.** From the above, it can be seen that the distribution function of the system noise plays an important role in the algorithm design. For the unknown case, an estimation algorithm can be designed to estimate it, and then the estimated value can be used instead of the true value, so as to realize the adaptive identification of unknown parameters [29].

**Theorem 1.** *Consider the system (1) and the binary observation (2) under the data tampering attack (3). If Assumption 1 holds, the matrix* $\Phi$ *generated by the system input is full rank, and* $\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_i\}} \to \infty$ *as* $N \to \infty$ *for* $i = 1, 2, \ldots, l$*, then the maximum likelihood-based parameter estimate* $\widehat{\theta}_N$ *given by (20) converges strongly to the true value* $\theta$*, i.e.,*

$$\widehat{\theta}_N \to \theta, \ \ N \to \infty, \ \ \text{w.p.1.}$$

*Proof.* By (5), it is known that

$$\begin{aligned} \mathbb{E}(s_k I_{\{\phi_k^T=\pi_i\}}) &= p_0 \cdot (1 - F(C - \pi_i\theta)) + (1 - p_1) \cdot F(C - \pi_i\theta) \\ &= p_0 + (1 - p_0 - p_1)F(C - \pi_i\theta). \end{aligned}$$

According to the Law of Large Numbers, for $i = 1, 2, \ldots, l$, we have

$$\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_1\}}} \to p_0 + (1 - p_0 - p_1)F(C - \pi_i\theta), \ \ N \to \infty, \tag{21}$$

which implies that

$$C - F^{-1}\left(\frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_1\}}} - p_0}{1 - p_0 - p_1}\right) \to \pi_i\theta, \ \ N \to \infty. \tag{22}$$

Since $\Phi$ is full rank, from (19) and (20), the theorem is proved.

## 5. Identification algorithm: the attack strategy is unknown

In the previous section, an identification algorithm with unknown parameters was designed under the assumption of known attack strategies. In the case of unknown attack strategies, the design of the identification algorithm becomes more difficult. This is mainly because the unknown parameters and attack strategies are coupled together. This section primarily addresses this problem.

Using the maximum likelihood function, Eq (11) is used to obtain the maximum likelihood estimates of $\theta$, $p_0$, and $p_1$, which results in a system of equations consisting of $n + 2$ equations involving $\theta$, $p_0$, and $p_1$. Solving this system of equations yields the estimates $\hat{\theta}$, $\hat{p_0}$, and $\hat{p_1}$. However, solving a system of $n + 2$ dimensional equations numerically will be challenging and time-consuming. The solution process is illustrated in Figure 2, divided into three steps below.

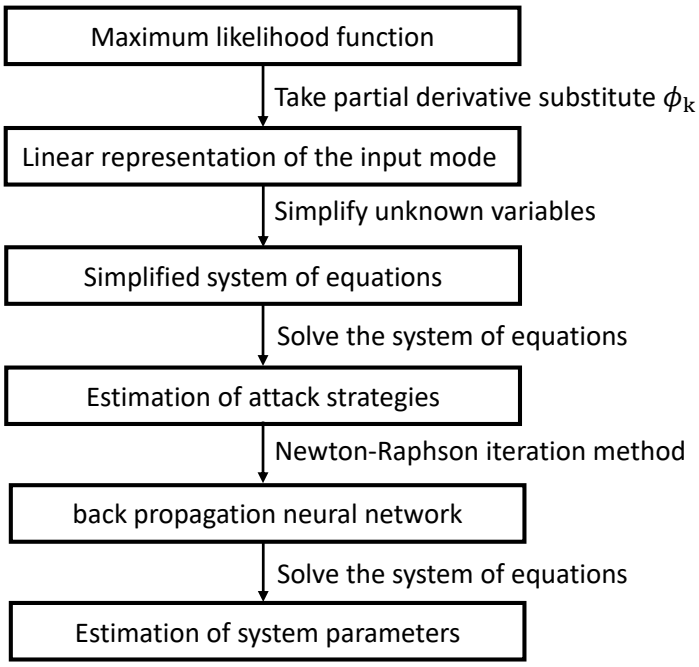


**Figure 2.** Solution steps.

**Step 1: Construction of system of equations for $\theta$ and $(p_0, p_1)$**

Based on the analysis process, when the attack strategies are known, the likelihood function $L(\theta|s_1, s_2, \ldots, s_N)$ is first logarithmically transformed into a logarithmic form and then differentiated. From Eqs (16) and (17), it can be determined that the problem of solving the extremum of the maximum likelihood function is equivalent to the problem of solving the following system of equations:

$$\begin{cases} F(C-\pi_1\theta) = \dfrac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_1\}}} - p_0}{1-p_0-p_1}; \\ F(C-\pi_2\theta) = \dfrac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_2\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_2\}}} - p_0}{1-p_0-p_1}; \\ \vdots \\ F(C-\pi_l\theta) = \dfrac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_l\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_l\}}} - p_0}{1-p_0-p_1}. \end{cases} \tag{23}$$

If $\pi_i\theta$ is treated as an unknown variable, then the above system of equations has $l+2$ unknowns but only $l$ equations. Therefore, it is generally unsolvable. To address this, the correlation between $\pi_i$ is utilized, which leads to the second step.

**Step 2: Solve the system of equations for $\theta$ and $(p_0, p_1)$, and obtain the estimated values of the attack strategies $(\widehat{p}_{N,0}, \widehat{p}_{N,1})$**

Let the number of maximal linearly independent sets of $\pi_1, \pi_2, \ldots, \pi_l$ be denoted as $l_0$. Without loss of generality, assume that $\pi_1, \pi_2, \ldots, \pi_{l_0}$ form a maximal linearly independent set of $\pi_1, \pi_2, \ldots, \pi_l$.

Then, each $\pi_i$ can be expressed as a linear combination of $\pi_1, \pi_2, \ldots, \pi_{l_0}$, as follows:

$$\pi_i = \sum_{j=1}^{l_0} \alpha_{i,j}\pi_j, \quad i = 1, 2, \ldots, l. \tag{24}$$

Substituting the above equation into Eq (23), we get

$$\begin{cases} F(C - \sum_{j=1}^{l_0} \alpha_{1,j}\pi_j\theta) = \frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T = \pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T = \pi_1\}}} - p_0}{1 - p_0 - p_1}; \\ F(C - \sum_{j=1}^{l_0} \alpha_{2,j}\pi_j\theta) = \frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T = \pi_2\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T = \pi_2\}}} - p_0}{1 - p_0 - p_1}; \\ \quad \vdots \\ F(C - \sum_{j=1}^{l_0} \alpha_{l,j}\pi_j\theta) = \frac{\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T = \pi_l\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T = \pi_l\}}} - p_0}{1 - p_0 - p_1}. \end{cases} \tag{25}$$

The above system of equations consists of $l$ equations, and the number of unknowns is reduced to $l_0 + 2$. Solving the above system of equations, denoted as $g(s_1, s_2, \ldots, s_N) = (g_1, g_2, \ldots, g_{l_0+2})$, which gives the estimated values of $\pi_1\theta, \pi_2\theta, \ldots, \pi_{l_0}\theta$, and $(p_0, p_1)$ as follows:

$$\widehat{\pi_1\theta}_N = g_1(s_1, s_2, \ldots, s_N); \tag{26}$$

$$\vdots \tag{27}$$

$$\widehat{\pi_{l_0}\theta}_N = g_{l_0}(s_1, s_2, \ldots, s_N); \tag{28}$$

$$\widehat{p}_{N,0} = g_{l_0+1}(s_1, s_2, \ldots, s_N); \tag{29}$$

$$\widehat{p}_{N,1} = g_{l_0+2}(s_1, s_2, \ldots, s_N). \tag{30}$$

Equations (29) and (30) provide the estimated values of the attack strategies.

The most critical part is how to obtain the expression of $g(s_1, s_2, \ldots, s_N)$, which can be divided into two cases. One case is when the system of Eq (25) has an analytical solution, in which case the expression of $g(\cdot)$ can be obtained through mathematical operations. The other case is when (25) does not have an analytical solution, in which case the expression of $g(\cdot)$ can be approximated using numerical methods and neural networks. The process is as follows.

Consider the following system of equations:

$$\begin{cases} F(C - \sum_{j=1}^{l_0} \alpha_{1,j}x_j) = \frac{\beta_1 - x_{l_0+1}}{1 - x_{l_0+1} - x_{l_0+2}}; \\ F(C - \sum_{j=1}^{l_0} \alpha_{2,j}x_j) = \frac{\beta_2 - x_{l_0+1}}{1 - x_{l_0+1} - x_{l_0+2}}; \\ \quad \vdots \\ F(C - \sum_{j=1}^{l_0} \alpha_{l,j}x_j) = \frac{\beta_l - x_{l_0+1}}{1 - x_{l_0+1} - x_{l_0+2}}, \end{cases} \tag{31}$$

where $X = [x_1, x_2, \ldots, x_{l_0+2}]^T \in \mathbb{R}^{l_0+2}$ is the unknown variable, and $\beta_1, \beta_2, \ldots, \beta_l$ are known parameters.

Given a step size $\Delta \in (0, 1)$, we uniformly sample the interval $[0, 1]$ to obtain a set

$$\Gamma = \{(j-1)\Delta : j = 1, 2, \ldots, \lceil \frac{1}{\Delta} \rceil\}, \tag{32}$$

where $\lceil\cdot\rceil$ denotes the ceiling function. We randomly take any element $\boldsymbol{\beta} = [\beta_1, \beta_2, \ldots, \beta_l]$ from $\Gamma^l$ and substitute it into Eq (31). Then, we solve the Eq (31) using the Newton-Raphson iteration method to obtain the solution $X = X(\boldsymbol{\beta})$. Specifically, let $\varpi_i(x_1, x_2, \ldots, x_{l_0+2}) = F(C - \sum_{j=1}^{l_0} \alpha_{i,j} x_j) - \frac{\beta_i - x_{l_0+1}}{1 - x_{l_0+1} - x_{l_0+2}}$, $i = 1, 2, \ldots, l$. Then, the system of Eq (31) can be equivalently written as:

$$\Omega(X) = \begin{bmatrix} \varpi_1(x_1, x_2, \ldots, x_{l_0+2}) \\ \varpi_2(x_1, x_2, \ldots, x_{l_0+2}) \\ \vdots \\ \varpi_l(x_1, x_2, \ldots, x_{l_0+2}) \end{bmatrix} = 0. \tag{33}$$

The Jacobian matrix of the above equations is given by:

$$\begin{aligned} J(X) &= \begin{bmatrix} \frac{\partial \varpi_1}{\partial x_1} & \cdots & \frac{\partial \varpi_1}{\partial x_{l_0+2}} \\ \vdots & \ddots & \vdots \\ \frac{\partial \varpi_l}{\partial x_1} & \cdots & \frac{\partial \varpi_l}{\partial x_{l_0+2}} \end{bmatrix} \\ &= \begin{bmatrix} -\alpha_{1,1} f(C - \sum_{j=1}^{l_0} \alpha_{1,j} x_j) & \cdots & \frac{1-\beta_1 - x_{l_0+2}}{(1-x_{l_0+1}-x_{l_0+2})^2} & \frac{\beta_1 + x_{l_0+1}}{(1-x_{l_0+1}-x_{l_0+2})^2} \\ \vdots & \ddots & \vdots & \vdots \\ -\alpha_{l,1} f(C - \sum_{j=1}^{l_0} \alpha_{1,j} x_j) & \cdots & \frac{1-\beta_l - x_{l_0+2}}{(1-x_{l_0+1}-x_{l_0+2})^2} & \frac{\beta_l + x_{l_0+1}}{(1-x_{l_0+1}-x_{l_0+2})^2} \end{bmatrix}. \end{aligned} \tag{34}$$

Given an initial value $X_0$, let $X_t = [x_1^{\{t\}}, x_2^{\{t\}}, \ldots, x_{l_0+2}^{\{t\}}]^T$ represent the zero of the system of equations for the solution of Eq (33) obtained at the $t$-th iteration. Then,

$$X_t = X_{t-1} - J^{-1}(X_{t-1})\Omega(X_{t-1}). \tag{35}$$

Repeat the above process and iteratively calculate until $\|X_t - X_{t-1}\| < \varepsilon$ is satisfied, where $X(\beta) = X_t$ is the solution to the system of Eq (31), $\|\cdot\|$ denotes the norm of a vector, and $\varepsilon > 0$ is a given constant called the iteration stopping tolerance.

Repeat the above process, letting $\boldsymbol{\beta}$ traverse $\Gamma^l$, and simultaneously obtaining the solution $X = X(\boldsymbol{\beta})$ for Eq (31). This way, a set of data $\{\boldsymbol{\beta}, X(\boldsymbol{\beta}) : \boldsymbol{\beta} \in \Gamma^l\}$ is obtained. Treat $\boldsymbol{\beta}$ as the input and $X(\boldsymbol{\beta})$ as the output of a BPNN*, and train the neural network as $g^0(\beta_1, \beta_2, \ldots, \beta_l)$. As a result, $g(s_1, s_2, \ldots, s_N)$ can be computed as follows:

$$g(s_1, s_2, \ldots, s_N) = g^0\left(\frac{\sum_{k=1}^N s_k I_{\{\phi_k^T = \pi_1\}}}{\sum_{k=1}^N I_{\{\phi_k^T = \pi_1\}}}, \ldots, \frac{\sum_{k=1}^N s_k I_{\{\phi_k^T = \pi_l\}}}{\sum_{k=1}^N I_{\{\phi_k^T = \pi_l\}}}\right). \tag{36}$$

The above process can be summarized into the following algorithm:

*Here we choose BPNN as the fitting algorithm, mainly to show our thinking and method. In specific use, one can also choose other regression algorithms, such as random forest and so on.

**Algorithm 1** Algorithm for computing function $g(\ldots)$

1. Initial values: sample step size $\Delta$ of $(0, 1)$; set $D = \emptyset$; iteration tolerance $\varepsilon > 0$ for stopping Newton-Raphson iteration.
2. Set $\Gamma$ based on (32), then obtain set $\Gamma^l$ with $m$ elements denoted as $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_m$
3. Loop: $i = 1, 2, \ldots, m$
   3.1. Substitute $\boldsymbol{\beta}_i$ into system of Eq (31)
   3.2. Initialize $X_0$, and use Newton-Raphson iteration to solve (31), obtain solution $X_i = X_i(\boldsymbol{\beta}_i)$
   3.3. Update data set $D = D \cup \{(\boldsymbol{\beta}_i, X_i)\}$
4. End loop
5. Train the BPNN $g^0(\beta_1, \beta_2, \ldots, \beta_l)$ based on data set $D$
6. Calculate $g(\ldots)$ based on (36)

**Step 3: Obtain the estimated values of the unknown parameters $\widehat{\theta}_N$**

Express the $\widehat{\pi_1\theta}_N, \widehat{\pi_2\theta}_N, \ldots, \widehat{\pi_{l_0}\theta}_N$ obtained in Step 2 in vector form. Based on Eqs (26) and (28), we have:

$$\begin{bmatrix} \pi_1 \\ \vdots \\ \pi_{l_0} \end{bmatrix} \widehat{\theta}_N = \begin{bmatrix} g_1(s_1, s_2, \ldots, s_N) \\ \vdots \\ g_{l_0}(s_1, s_2, \ldots, s_N) \end{bmatrix}.$$

Letting $[\pi_1^T, \ldots, \pi_{l_0}^T]^T = \overline{\Phi}$, we can obtain the estimate of $\theta$ as:

$$\widehat{\theta}_N = \overline{\Phi}^{+} \begin{bmatrix} g_1(s_1, s_2, \ldots, s_N) \\ \vdots \\ g_{l_0}(s_1, s_2, \ldots, s_N) \end{bmatrix}. \tag{37}$$

In the above equation, the expressions of $g_1, \ldots, g_{l_0}$ may contain the attack strategies $(p_0, p_1)$ as parameters. In this case, replace them with their estimated values from (29) and (30).

**Theorem 2.** *Under the condition of Theorem 1, if the matrix $\overline{\Phi}$ generated by the system input is full rank, the function $g(\cdot)$ given by Algorithm 1 is the solution to the Eq (33), then the maximum likelihood-based parameter estimate $\widehat{\theta}_N$ given by (37) converges strongly to the true value $\theta$, i.e.,*

$$\widehat{\theta}_N \to \theta, \quad N \to \infty, \quad \text{w.p.1.}$$

*Proof.* According to the conditions of the theorem and by (23) and (25), it is known that the solution to (31) is

$$\begin{aligned} X &= X([p_0 + (1 - p_0 - p_1)F(C - \pi_1\theta), \ldots, p_0 + (1 - p_0 - p_1)F(C - \pi_l\theta)]^T) \\ &= [\pi_1\theta, \ldots, \pi_{l_0}\theta]^T. \end{aligned} \tag{38}$$

From (21), we have

$$
\begin{aligned}
& g^0\left(\frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_1\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_1\}}}, \ldots, \frac{\sum_{k=1}^{N} s_k I_{\{\phi_k^T=\pi_l\}}}{\sum_{k=1}^{N} I_{\{\phi_k^T=\pi_l\}}}\right) \\
\rightarrow \quad & g^0(p_0 + (1-p_0-p_1)F(C-\pi_1\theta), \ldots, p_0 + (1-p_0-p_1)F(C-\pi_l\theta)), \quad N \rightarrow \infty,
\end{aligned}
$$

which together with (36) gives

$$
g(s_1, \ldots, s_N) \rightarrow g^0(p_0 + (1-p_0-p_1)F(C-\pi_1\theta), \ldots, p_0 + (1-p_0-p_1)F(C-\pi_l\theta))
$$

as $N \rightarrow \infty$. Combining the above and (38), by (37), it can be seen that

$$
\widehat{\theta_N} = \overline{\Phi}^{+} \begin{bmatrix} g_1(s_1, s_2, \ldots, s_N) \\ \vdots \\ g_{l_0}(s_1, s_2, \ldots, s_N) \end{bmatrix} \rightarrow \overline{\Phi}^{+} \begin{bmatrix} \pi_1\theta \\ \vdots \\ \pi_{l_0}\theta \end{bmatrix}, \quad N \rightarrow \infty. \tag{39}
$$

Considering that $\overline{\Phi}$ is full rank, the proof is completed.

## 6. Numerical simulation

Consider the system

$$
\begin{cases} y_k &= \phi_k^T\theta + d_k; \\ s_k^0 &= I_{\{y_k \le C\}}; \end{cases}
$$

with the system parameters $\theta = [a_1, \ldots, a_n]^T = [-2, 4, 8]^T$ and the system input $u_k \in \{1, 3, 5\}$; the threshold for the binary sensor output is $C = 30$; and the system noise follows an independent and identically distributed normal random variable sequence $d_k \sim (0, 40^2)$. The system output is transmitted to the data center through a communication network and is subjected to data tampering attacks with attack strategy $(p_0, p_1) = (0.4, 0.2)$.

The data center receives the tampered data $s_k$ after the original data $s_k^0$ has been attacked. The relationship between the data is shown in Figure 3. The original data $s_k^0$ has been randomly altered.

Experiments are conducted on algorithms (10)–(22) to compute the estimated system parameter values $\widehat{\theta_N}$, where the length of the data sample is $N = 80,000$. The results are shown in Figure 4, which indicate that: when the data sample size $N$ is small, the estimated parameter values $\widehat{\theta_N}$ have large convergence biases; When the data sample size $N$ exceeds a critical value, the estimated parameter values $\widehat{\theta_N}$ are close to the true values $\theta$; as the data sample size $N$ further increases, the deviation between the estimated parameter values $\widehat{\theta_N}$ and the true values decreases.

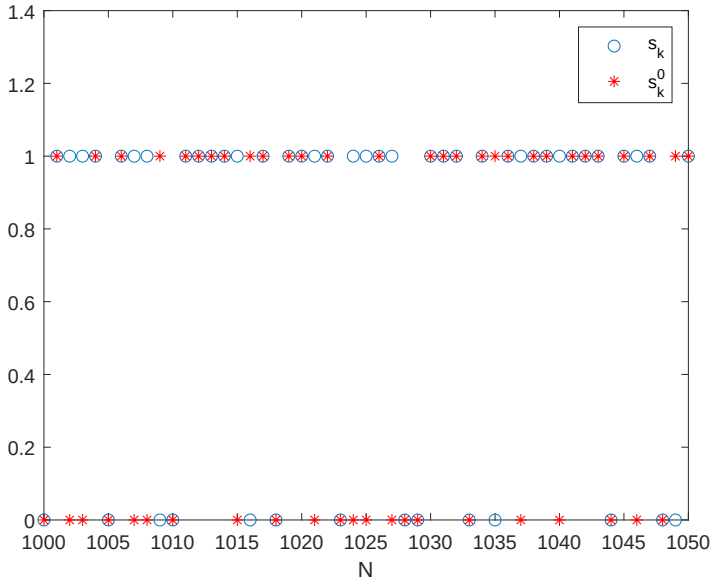


**Figure 3.** Comparison between original data and data after random attacks.

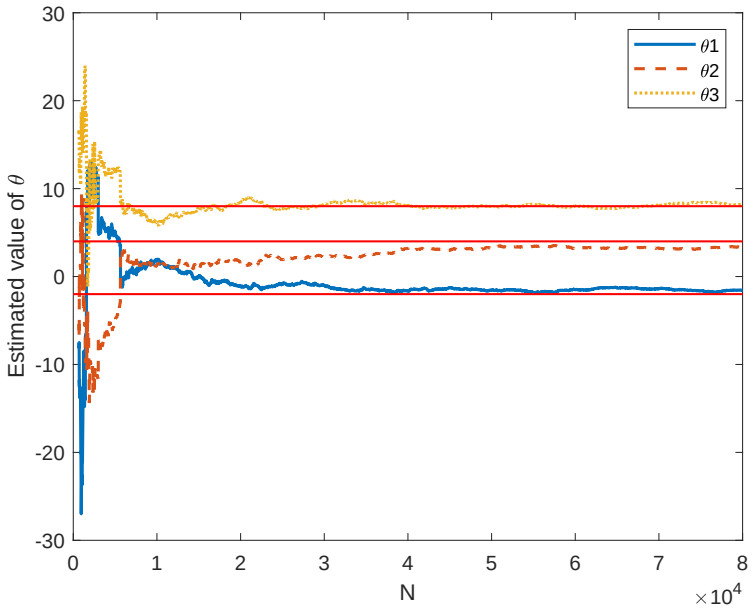


**Figure 4.** Estimation of system parameters when the attack strategy is known.

Experiments are conducted on algorithms (23)–(39) for $T = 150$ times, and the average results of each experiment are computed to obtain $\widehat{\theta_N}$, $p_0$, and $p_1$, where the length of the data sample is $N = 60,000$. The results are shown in Figures 5 and 6, which indicate that: As the data sample size $N$ increases, the estimated system parameter values $\widehat{\theta_N}$ approach the true values, and the estimated attack strategy values $\widehat{p_0}$ and $\widehat{p_1}$ also approach the true values. Moreover, due to the large number of experiments $T$, the convergence of each parameter improves as the data sample size $N$ increases.

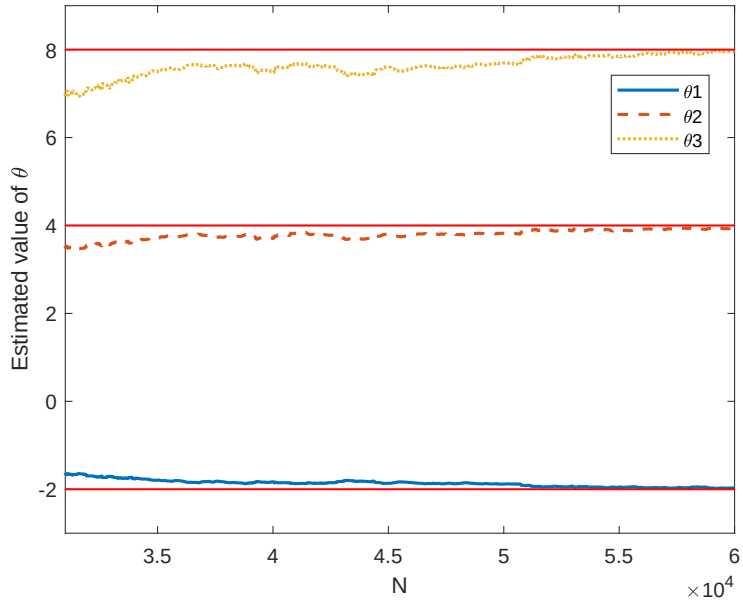


**Figure 5.** Estimation of system parameters when the attack strategy is unknown.

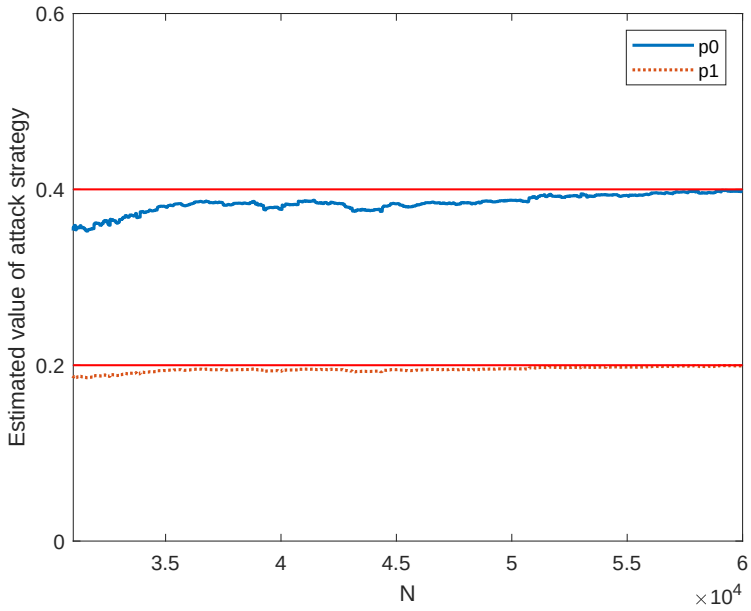


**Figure 6.** Estimation of the attack strategy when the attack strategy is unknown.

## 7. Conclusions

In the framework of system identification, this paper carried out the research of security issue based on the maximum likelihood estimation method. For FIR systems with binary observations and data tampering attacks, the parameter estimation algorithms are proposed in the two cases of known and unknown attack strategy, and the convergence condition and convergence proof of these algorithms

are given.

The maximum likelihood estimation is a very classical and effective method. This paper explores its application in CPS security identification. In the future, this method can be extended to nonlinear systems, multi-threshold observations, colored noise, and other more general cases.

## Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

## Acknowledgments

This research was supported in part by the National Natural Science Foundation of China (62173030) and in part by the Beijing Natural Science Foundation (4222050).

## Conflict of interest

The authors declare there is no conflict of interest.

## References

1. Y. Ju, M. Yang, C. Chakraborty, L. Liu, Q. Pei, M. Xiao, et al., Reliability–security trade-off analysis in mmWave Ad Hoc–based CPS, *ACM Trans. Sens. Netw.*, **20** (2024), 1–23. https://doi.org/10.1145/3582556
2. S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, et al., A review of current research trends in power-electronic innovations in cyber–physical systems, *IEEE J. Emerging Sel. Top. Power Electron.*, **9** (2021), 5146–5163. https://doi.org/10.1109/jestpe.2021.3051876
3. J. Guo, J. D. Diao, Prediction-based event-triggered identification of quantized input FIR systems with quantized output observations, *Sci. China Inf. Sci.*, **63** (2020), 112201. https://doi.org/10.1007/s11432-018-9845-6
4. S. M. Nagarajan, G. G. Deverajan, A. K. Bashir, R. P. Mahapatra, M. S. Al-Numay, IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems, *Comput. Commun.*, **188** (2022), 81–89. https://doi.org/10.1016/j.comcom.2022.02.022
5. R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, V. Terzija, A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid – Part – I: Background on CPPS and necessity of CPPS testbeds, *Int. J. Electr. Power Energy Syst.*, **136** (2022), 107718. https://doi.org/10.1016/j.ijepes.2021.107718
6. S. Kim, K. J. Park, C. Lu, A survey on network security for cyber–physical systems: From threats to resilient design, *IEEE Commun. Surv. Tutorials*, **24** (2022), 1534–1573. https://doi.org/10.1109/COMST.2022.3187531
7. J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, et al., A review of cyber–physical security for photovoltaic systems, *IEEE J. Emerging Sel. Top. Power Electron.*, **10** (2022), 4879–4901. https://doi.org/10.1109/jestpe.2021.3111728

8. R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE Secur. Privacy*, **9** (2011), 49–51. https://doi.org/10.1109/MSP.2011.67

9. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, et al., A review of cyber security risk assessment methods for scada systems, *Comput. Secur.*, **56** (2016), 1–27. https://doi.org/10.1016/j.cose.2015.09.009

10. A. V. Jha, B. Appasani, A. N. Ghazali, P. Pattanayak, D. S. Gurjar, E. Kabalci, et al., Smart grid cyber-physical systems: Communication technologies, standards and challenges, *Wireless Netw.*, **27** (2021), 2595–2613. https://doi.org/10.1007/s11276-021-02579-1

11. S. Tan, J. M. Guerrero, P. Xie, R. Han, J. C. Vasquez, Brief survey on attack detection methods for cyber-physical systems, *IEEE Syst. J.*, **14** (2020), 5329–5339. https://doi.org/10.1109/jsyst.2020.2991258

12. W. Duo, M. Zhou, A. Abusorrah, A survey of cyber attacks on cyber physical systems: Recent advances and challenges, *IEEE/CAA J. Autom. Sin.*, **9** (2022), 784–800. https://doi.org/10.1109/jas.2022.105548

13. D. Ding, Q. L. Han, X. Ge, J. Wang, Secure state estimation and control of cyber-physical systems: A survey, *IEEE Trans. Syst. Man Cybern.: Syst.*, **51** (2021), 176–190. https://doi.org/10.1109/tsmc.2020.3041121

14. S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, O. Jogunola, Federated deep learning for zero-day botnet attack detection in IoT-edge devices, *IEEE Internet Things J.*, **9** (2021), 3930–3944. https://doi.org/10.1109/JIOT.2021.3100755

15. J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, et al., Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection, *Expert Syst. Appl.*, **158** (2020), 113578. https://doi.org/10.1016/j.eswa.2020.113578

16. B. Li, Y. Wu, J. Song, R. Lu, T. Li, L. Zhao, DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems, *IEEE Trans. Ind. Inf.*, **17** (2021), 5615–5624. https://doi.org/10.1109/tii.2020.3023430

17. J. Guo, X. Wang, W. Xue, Y. Zhao, System identification with binary-valued observations under data tampering attacks, *IEEE Trans. Autom. Control*, **66** (2021), 3825–3832. https://doi.org/10.1109/tac.2020.3029325

18. H. Liang, L. Zhu, F. R. Yu, X. Wang, A cross-layer defense method for blockchain empowered CBTC systems against data tampering attacks, *IEEE Trans. Intell. Transp. Syst.*, **24** (2022), 501–515. https://doi.org/10.1109/tits.2022.3211020

19. D. W. Huang, W. Liu, J. Bi, Data tampering attacks diagnosis in dynamic wireless sensor networks, *Comput. Commun.*, **172** (2021), 84–92. https://doi.org/10.1016/j.comcom.2021.03.007

20. M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, M. Gidlund, A machine-learning-based technique for false data injection attacks detection in industrial IoT, *IEEE Internet Things J.*, **7** (2020), 8462–8471. https://doi.org/10.1109/jiot.2020.2991693

21. K. Yang, H. Wang, H. Wang, L. Sun, An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks, *Comput. Ind.*, **138** (2022), 103613. https://doi.org/10.1016/j.compind.2022.103613

22. M. Elsisi, M. Altius, S. F. Su, C. L. Su, Robust kalman filter for position estimation of automated guided vehicles under cyberattacks, *IEEE Trans. Instrum. Meas.*, **72** (2023), 1–12. https://doi.org/10.1109/tim.2023.3250285

23. X. Y. Kong, G. H. Yang, An intrusion detection method based on self-generated coding technology for stealthy false data injection attacks in train-ground communication systems, *IEEE Trans. Ind. Electron.*, **70** (2023), 8468–8476. https://doi.org/10.1109/tie.2022.3213899

24. J. Zhang, C. Dong, Privacy-preserving data aggregation scheme against deletion and tampering attacks from aggregators, *J. King Saud Univ. Comput. Inf. Sci.*, **35** (2023), 100–111. https://doi.org/10.1016/j.jksuci.2023.03.002

25. Y. Zhang, Y. Li, Z. Li, Aye: A trusted forensic method for firmware tampering attacks, *Symmetry*, **15** (2023), 145. https://doi.org/10.3390/sym15010145

26. D. Ye, T. Y. Zhang, Summation detector for false data-injection attack in cyber-physical systems, *IEEE Trans. Cybern.*, **50** (2019), 2338–2345. https://doi.org/10.1109/TCYB.2019.2915124

27. J. Guo, R. Jia, R. Su, Y. Zhao. Identification of FIR systems with binary-valued observations against data tampering attacks, *IEEE Trans. Syst. Man Cybern.: Syst.*, **53** (2023), 5861–5873. https://doi.org/10.1109/TSMC.2023.3276352

28. J. Sun, H. Xiong, S. Zhang, X. Liu, J. Yuan, R. H. Deng, A secure flexible and tampering-resistant data sharing system for vehicular social networks, *IEEE Trans. Veh. Technol.*, **69** (2020), 12938–12950. https://doi.org/10.1109/tvt.2020.3015916

29. J. Guo, L. Y. Wang, G. Yin, Y. Zhao, J. F. Zhang, Asymptotically efficient identification of FIR systems with quantized observations and general quantized inputs, *Automatica*, **57** (2015), 113–122. https://doi.org/10.1016/j.automatica.2015.04.009

30. H. T. Sun, C. Peng, T. C. Yang, H. Zhang, W. L. He, Resilient control of networked control systems with stochastic denial of service attacks, *Neurocomputing*, **270** (2017), 170–177. https://doi.org/10.1016/j.neucom.2017.02.093


AIMS Press