This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

Secure State Estimation for Artificial Neural Networks With Unknown-But-Bounded Noises: A Homomorphic Encryption Scheme

Kaiqun Zhu, Zidong Wang, Derui Ding, Hongli Dong, and Cheng-Zhong Xu

***Abstract*—This paper is concerned with the secure state estimation problem for artificial neural networks (ANNs) subject to unknown-but-bounded noises, where sensors and the remote estimator are connected via open and bandwidth-limited communication networks. Using the encoding-decoding mechanism and the Paillier encryption technique, a novel homomorphic encryption scheme (HES) is introduced, which aims to ensure the secure transmission of measurement information within communication networks that are constrained by bandwidth. Under this encoding-decoding-based HES, the data being transmitted can be encrypted into ciphertexts comprising finite bits. The emphasis of this research is placed on the development of a secure set-membership state estimation algorithm, which allows for the computation of estimates using encrypted data without the need for decryption, thereby ensuring data security throughout the entire estimation process. Taking into account the unknown-but-bounded noises, the underlying ANN and the adopted HES, sufficient conditions are determined for the existence of the desired ellipsoidal set. The related secure state estimator gains are then derived by addressing optimization problems using the Lagrange multiplier method. Lastly, an example is presented to verify the effectiveness of the proposed secure state estimation approach.**

***Index Terms*—Artificial neural networks, secure state estimation, homomorphic encryption scheme, bandwidth constraints, set-membership state estimation.**

Abbreviations and Notations

ANN	Artificial neural network
EDM	Encoding-decoding mechanism
HES	Homomorphic encryption scheme
$\mathbb{R}^{m\times n}$	The set of all $m \times n$ real matrices
$\mathbb{R}^n$	The n-dimensional Euclidean space
$\mathbb{Z}$	The set of prime numbers
$\lvert * \rvert$	The absolute value of "$*$"
$[\![x]\!]$	The encryption function for an integer x
$\mathrm{lcm}(p, q)$	The least common multiple of p and q
$\mathrm{gcd}(p, q)$	The greatest common divisor of p and q
$\oplus$	The Minkowski sum of two sets
$\lambda_{\max}(A)$	The maximum eigenvalue of A
$\mathrm{Tr}(P)$	The trace of a matrix P
$Q > 0$	Q is a positive-definite matrix

I. Introduction

The structure and functionality of biological neural networks, especially the brain, are emulated by an artificial neural network (ANN). Characterized by its ability to approximate functions, the ANN showcases essential features such as self-learning and nonlinear mapping [6], [14], [16], [31], [32], [52], [55]. Structurally, the ANN consists of three layers: the input layer, hidden layer, and output layer. Each of these layers houses multiple neurons, and the connection weights among these neurons can be adjusted through learning from input data. Due to its unique advantages and architectural design, ANNs have been widely utilized across various sectors, encompassing signal processing, optimal control, pattern recognition, and expert systems, to name a few. In the past two decades, significant research efforts have been channeled towards the analysis and synthesis challenges (such as synchronization and state estimation) associated with ANNs, see e.g. [5], [8]–[10], [13], [22], [29], [35], [37], [39], [53].

In applications like industrial system modeling and optimal control, it is often necessary to acquire state information from each neuron so as to harness the full performance potential of neural networks [19], [40], [43]. Regrettably, due to limited sensing capabilities and the intricate internal coupling within neural networks, obtaining comprehensive and accurate state information becomes a challenging endeavor [1], [24], [26], [45], and this underscores the importance of devising suitable state estimators for ANNs to predict the actual states of the neurons [27], [46]. For instance, a state estimator has been crafted in [30] for neural networks influenced by stochastic

This work was supported in part by the National Natural Science Foundation of China under Grant 61933007 and Grant U21A2019; in part by the Science and Technology Development Fund of Macao SAR under Grants 0123/2022/AFJ and 0081/2022/A2; in part by the UM Talent Programme under Grant UMTP2023-PF01-0046; in part by the Shanghai Pujiang Program under Grant 22PJ1411700; in part by the China Postdoctoral Science Foundation under Grant 2023M732322; in part by the Hainan Province Science and Technology Special Fund of China under Grant ZDYF2022SHFZ105; in part by the Royal Society of the UK; and in part by the Alexander von Humboldt Foundation of Germany. *(Corresponding author: Cheng-Zhong Xu.)*

Kaiqun Zhu is with the Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China, and also with the State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau 999078, China. (Email: zkqun@163.com)

Zidong Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: Zidong.Wang@brunel.ac.uk)

Derui Ding is with the Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China. (Email: deruiding2010@usst.edu.cn)

Hongli Dong is with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China. (Email: shiningdhl@vip.126.com)

Cheng-Zhong Xu is with the State Key Laboratory of Internet of Things for Smart City, Department of Computer and Information Science, University of Macau, Macau 999078, China. (Email: czxu@um.edu.mo)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

system parameters. Subsequently, in the context of neural networks exposed to energy-bounded noises, both the ℓ_2-ℓ_∞ state estimator and the H_∞ state estimator have been developed with the assistance of the linear matrix inequality technique in [18] and [41], respectively. It is crucial to recognize that, when ANNs experience unknown-but-bounded noises, the above-mentioned estimation algorithms might not produce satisfactory results, and this gives rise to the need for an alternative estimation algorithm tailored to such conditions. As such, the primary objective of this paper is to introduce a *recursive* state estimator for ANNs within the set-membership estimation paradigm and to *optimize* the relevant parameters.

For the realization of remote estimation and control tasks, network communication technology has become an integral component of automation control systems [4], [12], [25], [34], [38], [47]. In these networked configurations, measurement data is relayed to the remote estimator through an open communication channel that is constrained by bandwidth [17], [20], [51], [54]. It is important to highlight that transmitting system data across open network communication channels exposes it to potential eavesdropping threats. Such vulnerabilities can jeopardize the integrity of the conveyed data, which could consequently undermine the system's estimation or control performance [7], [28], [48], [56]. Given this scenario, there emerges a critical need to investigate data transmission mechanisms and state estimation algorithms that incorporate security features [49]. Presently, two predominant security protection mechanisms are employed in networked systems. One revolves around data-perturbation strategies such as differential privacy method, while the other centers on encryption techniques exemplified by the Paillier encryption method [11], [23].

In the data-perturbation-based strategy, security is achieved by introducing random noises to the data prior to transmission, thus obscuring the original data [21], [50]. However, the integration of these random noises might compromise the system's desired performance. On the other hand, the encryption-based approach ensures data transmission security through intricate algebraic operations. Notably, leveraging the homomorphic attributes of the encryption algorithm also secures the parameter-solving process [36], [42]. It should be pointed out that studies centered on encryption-based estimation remain nascent. As such, we aim to develop an *encrypted* set-membership state estimation algorithm that safeguards both the data transmission and parameter computation phases. Furthermore, given the bandwidth constraints on networked ANNs, it becomes imperative to introduce a novel framework dedicated to the co-design of data encoding and encryption mechanisms, which further drives our research motivation.

In this paper, our primary focus is the secure set-membership state estimation for ANNs using the homomorphic encryption scheme (HES). The central *challenges* are delineated as follows:

1) How can an efficient data security protection mechanism be designed that seamlessly integrates encoding and encrypting capabilities for transmitted data?
2) How can an apt encrypted state estimation scheme be crafted that addresses the intricacies posed by bandwidth limitations, the HES, and the presence of unknown-but-bounded noises?
3) In the midst of ensuring security, how can the estimator parameters be optimized during the state estimate calculation process?

In light of the aforementioned challenges, the primary *contributions* of this paper are articulated as follows.

1) Leveraging the encoding-decoding mechanism (EDM) in tandem with the Paillier encryption technique, an innovative HES is introduced. This approach, for the first time, concurrently lightens the communication load and ensures information security.
2) An encrypted set-membership state estimator tailored for ANNs under bandwidth constraints is developed, and the associated estimator parameters are subsequently optimized.
3) By capitalizing on the additive homomorphic attribute of the EDM-based encryption strategy, the security of the state estimation computation process is affirmed.

The structure of this paper unfolds as follows. In Section II, we introduce both the EDM-based HES and the encrypted state estimator. Moving to Section III, utilizing the EDM-based encryption mechanism, a secure set-membership state estimation scheme tailored for ANNs facing unknown-but-bounded noises is delineated, and the optimization of estimator parameters is explored. Section IV offers a simulation example to corroborate the effectiveness of our findings. The paper culminates with conclusions in Section V.

II. System Description and Preliminaries

A. Description of Artificial Neural Networks

For the purpose of problem formulation, we first give the following definitions.

Definition 1: [2] An ellipsoidal set is defined as

$$\mathscr{S}(c,\pi P) \triangleq \{x|(x-c)^{\mathrm{T}}P^{-1}(x-c)\leq \pi\} \tag{1}$$

where c is the center of the ellipsoidal set, P is the positive definite matrix that determines the shape of the set, and π is the positive scalar.

Definition 2: [44] The function $\sigma:\mathbb{R}^m\mapsto\mathbb{R}^m$ is said to satisfy the offset sector-bounded condition around x_* if

$$(\sigma(x)-\sigma(x_*)-\tau(x-x_*))^{\mathrm{T}}(\sigma(x)-\sigma(x_*))\leq 0 \tag{2}$$

where τ is the positive scalar, and $x\in\mathbb{R}^m$ and $x_*\in\mathbb{R}^m$ are vectors.

Now, consider a time-varying ANN of the following form:

$$x_{t+1}=\Phi_t x_t+W_t\sigma(x_t)+w_t \tag{3}$$

where $x_t \triangleq \begin{bmatrix}x_{1,t} & x_{2,t} & \cdots & x_{m,t}\end{bmatrix}^{\mathrm{T}}\in\mathbb{R}^m$ is the state vector; $\sigma(x_t) \triangleq \begin{bmatrix}\sigma_1(x_{1,t}) & \sigma_2(x_{2,t}) & \cdots & \sigma_m(x_{m,t})\end{bmatrix}^{\mathrm{T}}$ is the neuron activation function which satisfies the offset sector-bounded condition; Φ_t and W_t are known time-varying matrices with appropriate dimensions; and $w_t\in\mathbb{R}^m$ represents the unknown-but-bounded noise with

$$w_t\in\mathscr{S}(0,Q_t)\triangleq\{w_t|w_t^{\mathrm{T}}Q_t^{-1}w_t\leq 1\}. \tag{4}$$

Here, Q_t is the positive definite matrix.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

The measurement output of ANN system (3) is characterized as follows:

$$y_t = C_t x_t + v_t \tag{5}$$

where $y_t \triangleq \begin{bmatrix} y_{1,t} & y_{2,t} & \cdots & y_{l,t} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^l$ is the measurement output, C_t is the known time-varying matrix with appropriate dimension, and $v_t \in \mathbb{R}^l$ is the unknown-but-bounded noise with

$$v_t \in \mathscr{S}(0, R_t) \triangleq \{v_t | v_t^{\mathrm{T}} R_t^{-1} v_t \leq 1\}. \tag{6}$$

Here, R_t is the positive definite matrix.

B. EDM-based Homomorphic Encryption Scheme

When system data traverses the sensor-to-estimator communication channel, the data transmission rate might be curtailed due to communication bandwidth limitations. Concurrently, given the open nature of the communication network, the transmitted data remains susceptible to eavesdropping attacks, potentially compromising data security. To address these concerns, this section introduces a novel EDM-based HES through leveraging the dynamic EDM so as to fortify both data transmission and computation processes, see Algorithm 1 for more details.

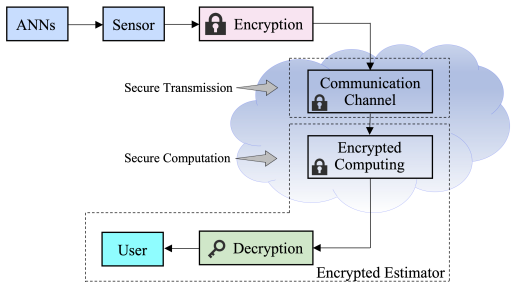


Fig. 1. Architecture of the secure state estimation for ANNs under the HES.

Encoding: First, for converting the continuous-amplitude system signal into the discrete-amplitude data, the dynamic encoding rule is given as follows:

$$\begin{cases} z_{\iota,t} = \alpha_t z_{\iota,t-1} + \beta_t \hat{y}_{\iota,t} \\ \hat{y}_{\iota,t} = \mathscr{Q}\big(\frac{1}{\beta_t}(y_{\iota,t} - \alpha_t z_{\iota,t-1})\big) \end{cases} \tag{7}$$

for $\iota = 1, 2, \ldots, l$, where $\hat{y}_{\iota,t} \in \mathbb{R}$ is the encoded data, $z_{\iota,t} \in \mathbb{R}$ is the internal variable, α_t and β_t are known scalars, and $\mathscr{Q}(\cdot)$ is the quantization function. Here, for $r > 0$, the quantization rule is given as

$$\mathscr{Q}(y) \triangleq \left\lceil \frac{2^{b-1} y}{r} \right\rceil \frac{r}{2^{b-1}} \tag{8}$$

with b being the length of binary bits for y and $\lceil \cdot \rceil$ being the function rounding upward to the nearest integer.

Encryption: Next, the Paillier encryption technique is utilized to convert the plaintext into the ciphertext, which includes three steps, namely, key generation, encryption and decryption [33]. In the key generation step, the public key (n, g) and the secrete key (λ, μ) are generated. Then, the encryption process is given as follows:

$$[\![\check{y}_{\iota,t}]\!] \triangleq \mathrm{Enc}\Big[\frac{2^{b-1}}{r}\hat{y}_{\iota,t}\Big] = g^{\frac{2^{b-1}}{r}\hat{y}_{\iota,t}} \gamma^n \bmod n^2 \tag{9}$$

where $\mathrm{Enc}[\cdot]$ is the encryption function, γ is a random integer and

$$\check{y}_{\iota,t} \triangleq \frac{2^{b-1}}{r}\hat{y}_{\iota,t}.$$

Decryption: In the decryptor side, the ciphertext $[\![\check{y}_{\iota,t}]\!]$ is decrypted by the following rule:

$$\mathrm{Dec}\big[[\![\check{y}_{\iota,t}]\!]\big] = \frac{([\![\check{y}_{\iota,t}]\!]^{\lambda} \bmod n^2 - 1)\mu}{n} \bmod n \tag{10}$$

where $\mathrm{Dec}[\cdot]$ is the decryption function.

Decoding: The $\hat{y}_{\iota,t}$ is decoded according to

$$\acute{y}_{\iota,t} \triangleq \hbar(\hat{y}_{\iota,t}) = \alpha_t \acute{y}_{\iota,t-1} + \beta_t \hat{y}_{\iota,t} \tag{11}$$

where $\hbar(\cdot)$ is the decoding function and $\acute{y}_{\iota,t} \in \mathbb{R}$ is the decoded data with the initial condition $\acute{y}_{\iota,0} = z_{\iota,0}$.

Algorithm 1 EDM-based Paillier Encryption

procedure KEY GENERATION
  Randomly select two large prime numbers p and q such that $\gcd(pq, (p-1)(q-1)) = 1$.
  Compute $n = pq$.
  Compute $\lambda = \mathrm{lcm}(p-1, q-1)$.
  Randomly select a value g such that $g \in \mathbb{Z}_{n^2}^*$ and ensure the existence of $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where $L(\alpha) \triangleq \frac{\alpha-1}{n}$ and $\mathbb{Z}_{n^2}^* \triangleq \{\beta | \beta \in \mathbb{Z}, 0 \leq \beta < n^2, \gcd(\beta, n^2) = 1\}$.
  Public key: (n, g).
  Secret key: (λ, μ).
end procedure
procedure ENCRYPTION
  Select a random γ from $\mathbb{Z}_{n^2}^*$.
  Compute ciphertext $[\![\check{y}_{\iota,t}]\!] = g^{\frac{2^{b-1}}{r}\hat{y}_{\iota,t}} \gamma^n \bmod n^2$.
  Return $[\![\check{y}_{\iota,t}]\!]$ as the encrypted message.
end procedure
procedure DECRYPTION
  Compute $\mu L([\![\check{y}_{\iota,t}]\!]^{\lambda} \bmod n^2) \bmod n$.
  Return the result as the decrypted plaintext message.
end procedure

Letting $\delta_{\iota,t} \triangleq \acute{y}_{\iota,t} - y_{\iota,t}$ be the decoding error, one has

$$\begin{aligned} \delta_{\iota,t} &\triangleq \acute{y}_{\iota,t} - y_{\iota,t} \\ &= \beta_t \Big(\mathscr{Q}\big(\frac{1}{\beta_t}(y_{\iota,t} - \alpha_t z_{\iota,t-1})\big) - \frac{1}{\beta_t}(y_{\iota,t} - \alpha_t \acute{y}_{\iota,t-1}) \Big). \end{aligned} \tag{12}$$

Then, with the aid of the mathematical induction method, one has $z_{\iota,t} = \acute{y}_{\iota,t}$, which further indicates that

$$|\delta_{\iota,t}| \leq \frac{r}{2^{b-1}} |\beta_t|. \tag{13}$$

Note that the EDM-based homomorphic encryption technique operates on integers. Consequently, within the estimator, any operations involving encrypted data must be executed in integer form. In this paper, the form of the encrypted set-membership state estimator is delineated as follows:

$$\vec{x}_{t+1} = \Phi_t \hat{x}_t + W_t \sigma(\hat{x}_t) \tag{14}$$

$$\hat{x}_{t+1} = G_{t+1} \vec{x}_{t+1} + \vec{F}_{t+1} \hbar\Big(\frac{r}{2^{b-1}} \mathrm{Dec}\big[[\![\check{y}_{t+1}]\!]\big] \Big) \tag{15}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

where

$$G_t \triangleq I - \vec{F}_t C_t,$$

$\vec{x}_t \in \mathbb{R}^m$ is the one-step prediction, $\hat{x}_t \in \mathbb{R}^m$ is the estimate of x_t, and $\vec{F}_t$ is the quantized state estimator gain to be determined with

$$\vec{F}_t \triangleq \mathscr{Q}(F_t) = F_t + \Delta_t.$$

Here, F_t is the state estimator gain before being quantized and Δ_t is the quantization error.

Remark 1: This paper proposes a novel HES that draws upon the EDM and the Paillier encryption technique, thereby marking significant strides in the realm of secure estimation. The bespoke EDM-based encryption mechanism proffers several benefits including: 1) mitigating the communication overhead, 2) fortifying the security of data transmission, and 3) upholding the integrity of the homomorphic encryption computation process. Furthermore, it is imperative to highlight that, under this HES, operations pertaining to ciphertexts $[\![\check{y}_{\iota,t}]\!]$ must be conducted on integers. As a result, the state estimator gain requires quantization, and this complicates the tasks of parameter determination for the estimator and the analysis of its performance.

The main objectives of this paper are outlined as follows.

1) Determine state estimator gains for ANNs such that, under the influence of bandwidth constraints and HES, the system state x_t is confined to the following ellipsoidal set over a finite-horizon $t \in [0,\ \mathcal{T}]$:

$$x_t \in \mathscr{S}(\hat{x}_t, \pi_t P_t) \tag{16}$$

where $\mathcal{T}$ is the time horzion, π_t is the positive scalar, and $P_t > 0$ is the shape-defining matrix for the ellipsoidal set.

2) Develop a secure state estimation scheme for ANNs utilizing the EDM-based homomorphic encryption technique in order to ensure both a data transmission process fortified with security and a protected parameter computation procedure.

III. Main Results

The following lemmas are necessary for deriving our main results.

Lemma 1: [15] For $k = 1, 2, \ldots, K$, let $\mathscr{S}(c_k, P_k)$ be given ellipsoidal sets. The Minkowski sum of the given ellipsoidal sets are bounded by the ellipsoidal set $\mathscr{S}(c, P)$, that is:

$$\mathscr{S}(c_1, P_1) \oplus \mathscr{S}(c_2, P_2) \oplus \cdots \oplus \mathscr{S}(c_K, P_K) \subseteq \mathscr{S}(c, P)$$

where the center c and the shape-defining matrix $P > 0$ of the ellipsoidal set satisfy

$$c = \sum_{k=1}^{K} c_k, \quad P = \sum_{k=1}^{K} \varrho_k^{-1} P_k, \quad \sum_{k=1}^{K} \varrho_k = 1, \quad \varrho_k > 0.$$

A. Design of the Encrypted State Estimator

In the following theorem, a sufficient condition is derived, which guarantees the existence of the ellipsoidal set (16).

Theorem 1: Let positive scalars $\rho_{1,t}$, $\rho_{2,t}$, $\rho_{3,t}$, ϱ_t be given and $x_0 \in \mathscr{S}(\hat{x}_0, \pi_0 P_0)$. For $t \in [0,\ \mathcal{T}]$, consider the ANN (3), the EDM-based HES (7)–(11), and the encrypted set-membership state estimator (14), (15). Suppose that

$$x_t \in \mathscr{S}(\hat{x}_t, \pi_t P_t). \tag{17}$$

Compute shape-defining matrices $\vec{P}_{t+1}$ and P_{t+1} as per

$$\vec{P}_{t+1} = \rho_{1,t}\pi_t \Phi_t P_t \Phi_t^{\mathrm{T}} + \rho_{2,t} W_t \Xi_t W_t^{\mathrm{T}} + \rho_{3,t} Q_t \tag{18}$$

$$P_{t+1} = (1 - \varrho_{t+1})^{-1}(I - F_{t+1} C_{t+1}) \vec{P}_{t+1}. \tag{19}$$

Then, we have

$$x_{t+1} \in \mathscr{S}(\hat{x}_{t+1}, \pi_{t+1} P_{t+1}) \tag{20}$$

and the estimator parameter is calculated by

$$F_{t+1} = (1 - \varrho_{t+1})^{-1} \vec{P}_{t+1} C_{t+1}^{\mathrm{T}} O_{t+1}^{-1} \tag{21}$$

where

$$O_{t+1} = \varrho_{t+1}^{-1} \vec{R}_{t+1} + (1 - \varrho_{t+1})^{-1} C_{t+1} \vec{P}_{t+1} C_{t+1}^{\mathrm{T}} \tag{22}$$

$$\begin{aligned} \pi_{t+1} = {} & \frac{1}{1 - \varpi_{t+1}} + \frac{m l r^2 \beta_{t+1}^2 \theta_{t+1}}{2^{2b-2} \varpi_{t+1}} \mathrm{Tr}(P_{t+1}^{-1}) \\ & - \frac{\varrho_{t+1}(1 - \varrho_{t+1}) \theta_{t+1} \mathrm{Tr}(\vec{R}_{t+1}^{-1})}{(1 - \varpi_{t+1})\big(1 - \varrho_{t+1} + \varrho_{t+1} \lambda_{\max}(\Psi_{t+1})\big)} \end{aligned} \tag{23}$$

$$\sum_{i=1}^{3} \rho_{i,t}^{-1} = 1, \quad \rho_{i,t} > 0, \quad i = 1, 2, 3$$

$$\Xi_t \triangleq \tau^2 \pi_t P_t, \quad 0 \le \varrho_t < 1, \quad \gamma_{1,t}^{-1} + \gamma_{2,t}^{-1} = 1$$

$$\gamma_{1,t} > 0, \quad \gamma_{2,t} > 0, \quad \vec{R}_t \triangleq \gamma_{1,t} R_t + \gamma_{2,t} \Lambda_t$$

$$\Lambda_t \triangleq \frac{l r^2 \beta_t^2}{2^{2b-2}} I, \quad \theta_t \triangleq 2\mathrm{Tr}(C_t^{\mathrm{T}} C_t \vec{P}_t + R_t) + \frac{l r^2 \beta_t^2}{2^{2b-3}}$$

$$\Psi_t \triangleq \acute{R}_t C_t \vec{P}_t C_t^{\mathrm{T}} \acute{R}_t^{\mathrm{T}}, \quad \vec{R}_t^{-1} = \acute{R}_t^{\mathrm{T}} \acute{R}_t, \quad 0 < \varpi_t < 1.$$

Moreover, the quantized set-membership state estimator gain is determined by

$$\vec{F}_t = \begin{bmatrix} \lceil \frac{F_{11,t}}{\flat} \rceil \flat & \lceil \frac{F_{12,t}}{\flat} \rceil \flat & \cdots & \lceil \frac{F_{1l,t}}{\flat} \rceil \flat \\ \lceil \frac{F_{21,t}}{\flat} \rceil \flat & \lceil \frac{F_{22,t}}{\flat} \rceil \flat & \cdots & \lceil \frac{F_{2l,t}}{\flat} \rceil \flat \\ \vdots & \vdots & \vdots & \vdots \\ \lceil \frac{F_{m1,t}}{\flat} \rceil \flat & \lceil \frac{F_{m2,t}}{\flat} \rceil \flat & \cdots & \lceil \frac{F_{ml,t}}{\flat} \rceil \flat \end{bmatrix} \tag{24}$$

with $\flat \triangleq 2^{1-b} r$ and $\lceil \cdot \rceil$ being the function rounding upward to the nearest integer.

Proof: First, let's handle the neuron activation function in (3). According to Definition 2, we have

$$(\xi_t - \tau(x_t - \hat{x}_t))^{\mathrm{T}} \xi_t \le 0 \tag{25}$$

where

$$\xi_t \triangleq \sigma(x_t) - \sigma(\hat{x}_t).$$

Utilizing the elementary inequality, it follows from (25) that

$$\begin{aligned} \xi_t^{\mathrm{T}} \xi_t &\le \tau (x_t - \hat{x}_t)^{\mathrm{T}} \xi_t \\ &\le \frac{\tau \varepsilon}{2} \xi_t^{\mathrm{T}} \xi_t + \frac{\tau}{2\varepsilon} (x_t - \hat{x}_t)^{\mathrm{T}} (x_t - \hat{x}_t) \end{aligned} \tag{26}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

which further indicates

$$\xi_t^{\mathrm{T}}\xi_t \leq \frac{\tau\varepsilon^{-1}}{2-\tau\varepsilon}(x_t-\hat{x}_t)^{\mathrm{T}}(x_t-\hat{x}_t). \tag{27}$$

It is obvious that $\frac{\tau\varepsilon^{-1}}{2-\tau\varepsilon}$ is minimized if $\varepsilon=\tau^{-1}$. Then, it follows from (17) and (27) that

$$\xi_t\xi_t^{\mathrm{T}} \leq \tau^2\pi_t P_t \tag{28}$$

which results in

$$\xi_t \in \mathscr{S}(0,\Xi_t) \tag{29}$$

with $\Xi_t \triangleq \tau^2\pi_t P_t$.

Next, according to the definition of Minkowski sum [15], it follows from (3), (4) and (17) that the system state x_{t+1} is confined to the following set:

$$\begin{aligned} x_{t+1} &= \Phi_t x_t + W_t\sigma(x_t) + w_t \\ &= \Phi_t x_t + W_t\sigma(\hat{x}_t) + W_t\xi_t + w_t \\ &\in \Phi_t\mathscr{S}(\hat{x}_t,\pi_t P_t) \oplus W_t\sigma(\hat{x}_t) \\ &\quad \oplus W_t\mathscr{S}(0,\Xi_t) \oplus \mathscr{S}(0,Q_t). \end{aligned} \tag{30}$$

Then, with the aid of the (14), (18) and by applying Lemma 1 to (30), the Minkowski sum of the above-mentioned sets can be bounded by an ellipsoidal set of the following form:

$$\begin{aligned} &\Phi_t\mathscr{S}(\hat{x}_t,\pi_t P_t) \oplus W_t\sigma(\hat{x}_t) \\ &\quad \oplus W_t\mathscr{S}(0,\Xi_t) \oplus \mathscr{S}(0,Q_t) \\ &\subseteq \mathscr{S}(\vec{x}_{t+1},\vec{P}_{t+1}) \end{aligned} \tag{31}$$

which implies that the system state is confined to the following ellipsoidal set:

$$x_{t+1} \in \mathscr{S}(\vec{x}_{t+1},\vec{P}_{t+1}). \tag{32}$$

In next steps, with the aim of further improving the estimation performance, the measurement information $\acute{y}_t$ is used to correct the shape of the ellipsoidal set (32). According to (5) and (12), one has

$$\begin{aligned} &\acute{y}_{t+1} - C_{t+1}x_{t+1} = \delta_{t+1} + v_{t+1} \\ &\in \mathscr{S}(0,\Lambda_{t+1}) \oplus \mathscr{S}(0,R_{t+1}) \end{aligned} \tag{33}$$

where

$$\Lambda_t \triangleq \frac{lr^2\beta_t^2}{2^{2b-2}}I.$$

By leveraging Lemma 1, one obtains an ellipsoidal set that covers the set (33):

$$\mathscr{S}(0,\Lambda_{t+1}) \oplus \mathscr{S}(0,R_{t+1}) \subseteq \mathscr{S}(0,\vec{R}_{t+1}) \tag{34}$$

where $\vec{R}_t \triangleq \gamma_{1,t}R_t + \gamma_{2,t}\Lambda_t$. Obviously, it follows from (33) and (34) that

$$\begin{aligned} x_{t+1} \in \mathscr{S}_{\acute{y}_{t+t}} \triangleq \{x_{t+1} | &(\acute{y}_{t+t} - C_{t+1}x_{t+1})^{\mathrm{T}}\vec{R}_{t+1}^{-1} \\ &\times (\acute{y}_{t+t} - C_{t+1}x_{t+1}) \leq 1\}. \end{aligned} \tag{35}$$

From (32) and (35), it is known that the system state x_{t+1} is confined in the intersection of ellipsoidal set $\mathscr{S}(\vec{x}_{t+1},\vec{P}_{t+1})$ and ellipsoidal set $\mathscr{S}_{\acute{y}_{t+t}}$:

$$x_{t+1} \in \mathscr{S}(\vec{x}_{t+1},\vec{P}_{t+1}) \cap \mathscr{S}_{\acute{y}_{t+t}}.$$

That is

$$\begin{cases} (x_{t+1}-\vec{x}_{t+1})^{\mathrm{T}}\vec{P}_{t+1}^{-1}(x_{t+1}-\vec{x}_{t+1}) \leq 1 \\ (\acute{y}_{t+1}-C_{t+1}x_{t+1})^{\mathrm{T}}\vec{R}_{t+1}^{-1}(\acute{y}_{t+1}-C_{t+1}x_{t+1}) \leq 1 \end{cases}$$

which yields

$$(1-\varrho_{t+1})\vec{\zeta}_{t+1}^{\mathrm{T}}\vec{P}_{t+1}^{-1}\vec{\zeta}_{t+1} + \varrho_{t+1}\eta_t^{\mathrm{T}}\vec{R}_{t+1}^{-1}\eta_t \leq 1 \tag{36}$$

with $\vec{\zeta}_t \triangleq x_t - \vec{x}_t$, $\eta_t \triangleq \acute{y}_t - C_t x_t$ and $0 \leq \varrho_t \leq 1$.

By substituting $\acute{y}_t - C_t x_t = \acute{y}_t - C_t\vec{x}_t - C_t\vec{\zeta}_t$ into (36), it is easy to derive that

$$\begin{aligned} &\vec{\zeta}_{t+1}^{\mathrm{T}}\big((1-\varrho_{t+1})\vec{P}_{t+1}^{-1} + \varrho_{t+1}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}C_{t+1}\big)\vec{\zeta}_{t+1} \\ &- 2\varrho_{t+1}\vec{\zeta}_{t+1}^{\mathrm{T}}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} + \varrho_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \leq 1 \end{aligned} \tag{37}$$

where $\vec{\eta}_t \triangleq \acute{y}_t - C_t\vec{x}_t$.

Further applying the matrix inverse lemma [3] to (37), it follows from (19) that

$$\begin{aligned} &\vec{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\vec{\zeta}_{t+1} - 2\varrho_{t+1}\vec{\zeta}_{t+1}^{\mathrm{T}}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \\ &+ \varrho_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \leq 1. \end{aligned} \tag{38}$$

Next, according to (15), one has

$$\begin{aligned} \vec{\zeta}_{t+1} &= \hat{\zeta}_{t+1} + \vec{F}_{t+1}\vec{\eta}_{t+1} \\ &= \hat{\zeta}_{t+1} + F_{t+1}\vec{\eta}_{t+1} + \nu_{t+1} \end{aligned} \tag{39}$$

where $\hat{\zeta}_t \triangleq x_t - \hat{x}_t$ and $\nu_t \triangleq \Delta_t\vec{\eta}_t$. Then, it is easy to verify that

$$\nu_t^{\mathrm{T}}\nu_t \leq \tilde{\beta}_t\vec{\eta}_t^{\mathrm{T}}\vec{\eta}_t \tag{40}$$

where

$$\tilde{\beta}_t \triangleq \frac{mlr^2\beta_t^2}{2^{2b-2}}.$$

By substituting (39) into (38), we obtain that

$$\begin{aligned} &\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\hat{\zeta}_{t+1} + \vec{\eta}_{t+1}^{\mathrm{T}}F_{t+1}^{\mathrm{T}}P_{t+1}^{-1}F_{t+1}\vec{\eta}_{t+1} + \nu_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\nu_{t+1} \\ &+ 2\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}F_{t+1}\vec{\eta}_{t+1} + 2\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\nu_{t+1} + 2\vec{\eta}_{t+1}^{\mathrm{T}}F_{t+1}^{\mathrm{T}} \\ &\times P_{t+1}^{-1}\nu_{t+1} - 2\varrho_{t+1}\hat{\zeta}_{t+1}^{\mathrm{T}}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} - 2\varrho_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}F_{t+1}^{\mathrm{T}} \\ &\times C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} - 2\varrho_{t+1}\nu_{t+1}^{\mathrm{T}}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \\ &+ \varrho_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \leq 1. \end{aligned} \tag{41}$$

It follows from (21), (22) and (41) that

$$\begin{aligned} &\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\hat{\zeta}_{t+1} \\ &\leq \varrho_{t+1}^2\vec{\eta}_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}C_{t+1}P_{t+1}C_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} \\ &\quad - \varrho_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}\vec{R}_{t+1}^{-1}\vec{\eta}_{t+1} - \nu_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\nu_{t+1} \\ &\quad - 2\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\nu_{t+1} + 1 \\ &\leq 1 - \vec{\eta}_{t+1}^{\mathrm{T}}O_{t+1}^{-1}\vec{\eta}_{t+1} + (\varpi_{t+1}^{-1}-1)\nu_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\nu_{t+1} \\ &\quad + \varpi_{t+1}\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\hat{\zeta}_{t+1} \end{aligned} \tag{42}$$

which, together with (40), results in

$$\begin{aligned} &\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\hat{\zeta}_{t+1} \\ &\leq \frac{1}{1-\varpi_{t+1}}(1 - \vec{\eta}_{t+1}^{\mathrm{T}}O_{t+1}^{-1}\vec{\eta}_{t+1} + \tilde{\beta}_{t+1}\vec{\varpi}_{t+1}\vec{\eta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\vec{\eta}_{t+1}) \\ &= \frac{1}{1-\varpi_{t+1}}(1 + \mathrm{Tr}(\tilde{\beta}_{t+1}\vec{\varpi}_{t+1}P_{t+1}^{-1} - O_{t+1}^{-1})\vec{\eta}_{t+1}^{\mathrm{T}}\vec{\eta}_{t+1}) \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

$$\leq \frac{1}{1-\varpi_{t+1}}(1+\theta_{t+1}\mathrm{Tr}(\tilde{\beta}_{t+1}\vec{\varpi}_{t+1}P_{t+1}^{-1}-O_{t+1}^{-1})) \tag{43}$$

where

$$\vec{\varpi}_t \triangleq \varpi_t^{-1}-1, \quad 0<\varpi_t<1$$
$$\theta_t \triangleq 2\mathrm{Tr}(C_t^{\mathrm{T}}C_t\vec{P}_t)+2\mathrm{Tr}(R_t)+\frac{lr^2\beta_t^2}{2^{2b-3}}.$$

According to (22), one has

$$\begin{aligned}
&O_{t+1}^{-1}\\
&=(\varrho_{t+1}^{-1}\vec{R}_{t+1}+(1-\varrho_{t+1})^{-1}C_{t+1}\vec{P}_{t+1}C_{t+1}^{\mathrm{T}})^{-1}\\
&=\varrho_{t+1}(1-\varrho_{t+1})((1-\varrho_{t+1})\vec{R}_{t+1}+\varrho_{t+1}C_{t+1}\vec{P}_{t+1}C_{t+1}^{\mathrm{T}})^{-1}\\
&=\varrho_{t+1}(1-\varrho_{t+1})\acute{R}_{t+1}^{\mathrm{T}}((1-\varrho_{t+1})I+\varrho_{t+1}\acute{R}_{t+1}C_{t+1}\vec{P}_{t+1}\\
&\quad\times C_{t+1}^{\mathrm{T}}\acute{R}_{t+1}^{\mathrm{T}})^{-1}\acute{R}_{t+1}\\
&\geq \frac{\varrho_{t+1}(1-\varrho_{t+1})\vec{R}_{t+1}^{-1}}{1-\varrho_{t+1}+\varrho_{t+1}\lambda_{\max}(\Psi_{t+1})}
\end{aligned} \tag{44}$$

where

$$\Psi_t \triangleq \acute{R}_tC_t\vec{P}_tC_t^{\mathrm{T}}\acute{R}_t^{\mathrm{T}}$$

with $\acute{R}_t$ being the factorization of $\vec{R}_t^{-1}$, i.e.,

$$\vec{R}_t^{-1}=\acute{R}_t^{\mathrm{T}}\acute{R}_t.$$

Then, it follows from (43) and (44) that

$$\begin{aligned}
&\hat{\zeta}_{t+1}^{\mathrm{T}}P_{t+1}^{-1}\hat{\zeta}_{t+1}\\
&\leq \frac{1}{1-\varpi_{t+1}}+\frac{\tilde{\beta}_{t+1}\theta_{t+1}}{\varpi_{t+1}}\mathrm{Tr}(P_{t+1}^{-1})\\
&\quad-\frac{\varrho_{t+1}(1-\varrho_{t+1})\theta_{t+1}\mathrm{Tr}(\vec{R}_{t+1}^{-1})}{(1-\varpi_{t+1})\big(1-\varrho_{t+1}+\varrho_{t+1}\lambda_{\max}(\Psi_{t+1})\big)}
\end{aligned} \tag{45}$$

which means that (20) is ensured. Based on mathematical induction method, it is obvious that the (20) is always ensured over a finite-horizon $t\in[0,\ \mathcal{T}]$, and the proof is now complete. ■

B. Optimization of the Parameters

From Theorem 1, it becomes clear that the state estimation performance is contingent upon the parameters $\vec{P}_t$, $\vec{R}_t$ and π_t. These parameters signify the volume of the ellipsoidal set. Subsequent theorems furnish methodologies to minimize this ellipsoidal set's volume in terms of the matrix trace.

Theorem 2: The trace $\mathrm{Tr}(\vec{P}_t)$ is minimized when

$$\rho_{i,t}=\frac{\sum_{i=1}^{3}\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}}{\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}} \tag{46}$$

where

$$\mathscr{P}_{1,t}\triangleq\pi_t\Phi_tP_t\Phi_t^{\mathrm{T}}, \quad \mathscr{P}_{2,t}\triangleq W_t\Xi_tW_t^{\mathrm{T}}, \quad \mathscr{P}_{3,t}\triangleq Q_t.$$

Proof: The minimum of $\mathrm{Tr}(\vec{P}_t)$ is computed by solving the following constrained optimization problem:

$$\begin{aligned}
&\min_{\rho_{i,t}}\ \mathrm{Tr}(\vec{P}_t)\\
&\text{s.t.}\ \sum_{i=1}^{3}\rho_{i,t}^{-1}=1 \text{ and } \rho_{i,t}>0
\end{aligned} \tag{47}$$

where

$$\begin{aligned}
\mathrm{Tr}(\vec{P}_t)\triangleq\ &\rho_{1,t}\mathrm{Tr}(\pi_t\Phi_tP_t\Phi_t^{\mathrm{T}})+\rho_{2,t}\mathrm{Tr}(W_t\Xi_tW_t^{\mathrm{T}})\\
&+\rho_{3,t}\mathrm{Tr}(Q_t).
\end{aligned}$$

First, we define a Lagrangian function of the following form:

$$\mathscr{L}(\rho_{i,t},\lambda_t)=\mathrm{Tr}(\vec{P}_t)+\lambda_t\big(1-\sum_{i=1}^{3}\rho_{i,t}^{-1}\big) \tag{48}$$

where λ_t is a variable called the Lagrange multiplier.

Next, by resorting to the Lagrange multiplier approach, one obtains the minimal value of $\mathrm{Tr}(\vec{P}_t)$ by solving:

$$\begin{cases}\frac{\partial\mathscr{L}(\rho_{i,t},\lambda_t)}{\partial\rho_{i,t}}=0\\ \frac{\partial\mathscr{L}(\rho_{i,t},\lambda_t)}{\partial\lambda_t}=0.\end{cases} \tag{49}$$

Then, solving equations in (49), it is easy to calculate that

$$\begin{cases}\rho_{i,t}=\frac{\sum_{i=1}^{3}\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}}{\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}}\\ \lambda_t=\Big(\sum_{i=1}^{3}\sqrt{\mathrm{Tr}(\pi_t\Phi_tP_t\Phi_t^{\mathrm{T}})}\Big)^2.\end{cases} \tag{50}$$

Moreover, by substituting (50) into (18), one has

$$\vec{P}_t=\sum_{i=1}^{3}\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}\sum_{i=1}^{3}\frac{\mathscr{P}_{i,t}}{\sqrt{\mathrm{Tr}(\mathscr{P}_{i,t})}} \tag{51}$$

which completes the proof. ■

Theorem 3: The trace $\mathrm{Tr}(\vec{R}_t)$ is minimized when

$$\gamma_{1,t}=\frac{\sqrt{\mathrm{Tr}(R_t)}+\sqrt{\mathrm{Tr}(\Lambda_t)}}{\sqrt{\mathrm{Tr}(R_t)}} \tag{52}$$

$$\gamma_{2,t}=\frac{\sqrt{\mathrm{Tr}(R_t)}+\sqrt{\mathrm{Tr}(\Lambda_t)}}{\sqrt{\mathrm{Tr}(\Lambda_t)}}. \tag{53}$$

Proof: The proof of this theorem is similar to that of Theorem 2 and is thus omitted here. ■

Theorem 4: The variable π_t is minimized when

$$\varrho_t=\frac{1}{1+\sqrt{\lambda_{\max}(\Psi_t)}}. \tag{54}$$

Proof: First, computing the first- and second-order derivatives of the variable ϱ_t in the function π_t:

$$\frac{\mathrm{d}\pi_t}{\mathrm{d}\varrho_t}=\frac{\varrho_t^2\lambda_{\max}(\Psi_t)-(1-\varrho_t)^2}{(1-\varrho_t+\varrho_t\lambda_{\max}(\Psi_t))^2}\vec{\theta}_t \tag{55}$$

$$\frac{\mathrm{d}^2\pi_t}{\mathrm{d}\varrho_t^2}=\frac{2\lambda_{\max}(\Psi_t)}{(1-\varrho_t+\varrho_t\lambda_{\max}(\Psi_t))^3}\vec{\theta}_t \tag{56}$$

where

$$\vec{\theta}_t\triangleq\frac{\theta_t\mathrm{Tr}(\vec{R}_t^{-1})}{1-\varpi_t}.$$

It follows from (55)–(56) that, for any $0\leq\varrho_t<1$,

$$\frac{\mathrm{d}^2\pi_t}{\mathrm{d}\varrho_t^2}\geq 0 \tag{57}$$

which means that the first-order derivative of the function π_t is non-decreasing as ϱ_t increases. Then, by further utilizing (55)–(56), one acquires that

$$\begin{cases}\left.\frac{\mathrm{d}\pi_t}{\mathrm{d}\varrho_t}\right|_{\varrho_t=0}=-\vec{\theta}_t<0\\ \left.\frac{\mathrm{d}\pi_t}{\mathrm{d}\varrho_t}\right|_{\varrho_t=1}=\vec{\theta}_t>0.\end{cases} \tag{58}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

Thus, it is easy to see that π_t is minimized when

$$\frac{\mathrm{d}\pi_t}{\mathrm{d}\varrho_t} = 0,$$

which means

$$\varrho_t = \frac{1}{1+\sqrt{\lambda_{\max}(\Psi_t)}}.$$

Therefore, the proof is complete. ■

Remark 2: In Theorem 1, within the set-membership estimation framework, the sufficient condition for the validity of the secure state estimation problem has been derived through successfully navigating the challenges posed by the HES and the nonlinear activation function. Leveraging contemporary techniques such as the Minkowski sum technique, the outer-bounding ellipsoid method, and the recursive equation approach, the procedure to compute the recursive solution for the corresponding estimator gains has been deduced. Furthermore, in Theorems 2–4, the parameters have been optimized utilizing the Lagrange multiplier method.

C. Design of the Secure State Estimation Scheme

In this subsection, a secure state estimation scheme is proposed with the aid of the EDM-based homomorphic encryption approach.

Before proceeding further, the following properties (i.e., additive homomorphic properties) of the Paillier encryption technique are necessary for deriving the secure state estimation scheme:

$$[\![x]\!] \odot [\![y]\!] = [\![x+y]\!] \tag{59}$$

$$[\![x]\!]^k = [\![kx]\!] \tag{60}$$

where $\odot$ represents multiplication between ciphertexts and x, y, k are integers.

We strive to design a secure state estimation algorithm that allows the computing device to perform operations on encrypted data. This strategy ensures information security by preserving the data in its encrypted state throughout the computation. Specifically, the sought-after estimated information can be derived from the *encrypted* output $[\![\check{y}_t]\!]$, thereby mitigating potential system information leaks.

Encrypted Estimator: According to Theorems 1–4, the quantized state estimator gain $\vec{F}_{t+1}$ is calculated in the encrypted estimator. Before performing homomorphic operations (with the help of the EDM-based encryption mechanism), it is necessary to convert the estimator gain $\vec{F}_{t+1}$ into the integer matrix:

$$\check{F}_{t+1} = \frac{2^{b-1}}{r}\vec{F}_{t+1}.$$

Then, the encrypted estimator performs the following computation regarding the integer matrix $\check{F}_{t+1}$ and the encrypted data $[\![\check{y}_{t+1}]\!]$:

$$\begin{aligned}&[\![h(\check{y}_{\jmath,t+1})]\!]\\ &\triangleq [\![\check{y}_{1,t+1}]\!]^{\check{F}_{\jmath 1,t+1}} \odot [\![\check{y}_{2,t+1}]\!]^{\check{F}_{\jmath 2,t+1}} \odot \cdots \odot [\![\check{y}_{l,t+1}]\!]^{\check{F}_{\jmath l,t+1}}\end{aligned} \tag{61}$$

for $\jmath = 1,2,\cdots,m$, where $\check{F}_{\jmath\iota,t+1}$ is the $(\jmath,\iota)$-element of the matrix $\check{F}_{t+1}$. Next, the ciphertexts $[\![h(\check{y}_{\jmath,t+1})]\!]$ ($\jmath = 1,2,\cdots,m$) are transmitted to the decryptor in the user side.

Local Decryptor: By utilizing the additive homomorphic properties (59) and (60), one has

$$\begin{aligned}&\mathrm{Dec}\big[[\![h(\check{y}_{\jmath,t+1})]\!]\big]\\ &= \mathrm{Dec}\big[[\![\check{y}_{1,t+1}]\!]^{\check{F}_{\jmath 1,t+1}} \odot [\![\check{y}_{2,t+1}]\!]^{\check{F}_{\jmath 2,t+1}} \odot \cdots\\ &\quad \odot [\![\check{y}_{l,t+1}]\!]^{\check{F}_{\jmath l,t+1}}\big]\\ &= \mathrm{Dec}\big[[\![\check{F}_{\jmath 1,t+1}\check{y}_{1,t+1} + \check{F}_{\jmath 2,t+1}\check{y}_{2,t+1} + \cdots\\ &\quad + \check{F}_{\jmath l,t+1}\check{y}_{l,t+1}]\!]\big]\\ &= \check{F}_{\jmath 1,t+1}\check{y}_{1,t+1} + \check{F}_{\jmath 2,t+1}\check{y}_{2,t+1} + \cdots + \check{F}_{\jmath l,t+1}\check{y}_{l,t+1}.\end{aligned} \tag{62}$$

Then, by applying the decoding technique (11), we have

$$\begin{aligned}&\hbar\Big(\frac{r^2}{2^{2b-2}}\mathrm{Dec}\big[[\![h(\check{y}_{\jmath,t+1})]\!]\big]\Big)\\ &= \hbar\Big(\frac{r^2}{2^{2b-2}}(\check{F}_{\jmath 1,t+1}\check{y}_{1,t+1} + \check{F}_{\jmath 2,t+1}\check{y}_{2,t+1} + \cdots\\ &\quad + \check{F}_{\jmath l,t+1}\check{y}_{l,t+1})\Big)\\ &= \hbar(\vec{F}_{\jmath 1,t+1}\hat{y}_{1,t+1} + \vec{F}_{\jmath 2,t+1}\hat{y}_{2,t+1} + \cdots + \vec{F}_{\jmath l,t+1}\hat{y}_{l,t+1})\\ &= \alpha_{t+1}(\vec{F}_{\jmath 1,t+1}\acute{y}_{1,t} + \vec{F}_{\jmath 2,t+1}\acute{y}_{2,t} + \cdots + \vec{F}_{\jmath l,t+1}\acute{y}_{l,t})\\ &\quad + \beta_{t+1}(\vec{F}_{\jmath 1,t+1}\hat{y}_{1,t+1} + \vec{F}_{\jmath 2,t+1}\hat{y}_{2,t+1} + \cdots\\ &\quad + \vec{F}_{\jmath l,t+1}\hat{y}_{l,t+1})\\ &= \vec{F}_{\jmath 1,t+1}\acute{y}_{1,t+1} + \vec{F}_{\jmath 2,t+1}\acute{y}_{2,t+1} + \cdots + \vec{F}_{\jmath l,t+1}\acute{y}_{l,t+1}\\ &= [\vec{F}_{t+1}\acute{y}_{t+1}]_\jmath\end{aligned} \tag{63}$$

for $\jmath = 1,2,\cdots,m$, where $[\vec{F}_{t+1}\acute{y}_{t+1}]_\jmath$ is the $\jmath$th-element of $\vec{F}_{t+1}\acute{y}_{t+1}$. Thus, the information $\vec{F}_{t+1}\acute{y}_{t+1}$ can be obtained from the decryptor.

Based on (61)–(63), the estimated state $\hat{x}_{t+1}$ can be obtained by using the encrypted output, that is,

$$\vec{x}_{t+1} = \Phi_t\hat{x}_t + W_t\sigma(\hat{x}_t) \tag{64}$$

$$\begin{aligned}\hat{x}_{t+1} &= G_{t+1}\vec{x}_{t+1} + \begin{bmatrix}\hbar\big(\frac{r^2}{2^{2b-2}}\mathrm{Dec}\big[[\![h(\check{y}_{1,t+1})]\!]\big]\big)\\ \hbar\big(\frac{r^2}{2^{2b-2}}\mathrm{Dec}\big[[\![h(\check{y}_{2,t+1})]\!]\big]\big)\\ \vdots\\ \hbar\big(\frac{r^2}{2^{2b-2}}\mathrm{Dec}\big[[\![h(\check{y}_{m,t+1})]\!]\big]\big)\end{bmatrix}\\ &= G_{t+1}\vec{x}_{t+1} + \vec{F}_{t+1}\acute{y}_{t+1}.\end{aligned} \tag{65}$$

The detailed encrypted state estimation algorithm (i.e., Algorithm 2) is given as follows.

Remark 3: In Theorems 1–4, we have mainly delved into the secure set-membership state estimation for ANNs by leveraging the HES. Specifically, we have devised a robust data security strategy that effortlessly combines both encoding and encrypting functions for data in transit. Then, we have developed an encrypted state estimation method that overcomes the hurdles presented by bandwidth restrictions, the intricacies of the HES, and the influence of unknown-but-bounded disturbances. Finally, we have designed the optimal estimator parameters while ensuring robust security during the state estimation computation.

Remark 4: In this paper, we have embarked on a comprehensive exploration of secure state estimation for ANNs

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

Algorithm 2 Encrypted State Estimation Algorithm

procedure ENCRYPTED ESTIMATOR
  Compute the quantized state estimator gain $\vec{F}_{t+1}$ according to Theorems 1–4 and convert it into the integer matrix $\check{F}_{t+1}$.
  Compute $[\![h(\check{y}_{\jmath,t+1})]\!] \triangleq [\![\check{y}_{1,t+1}]\!]^{\check{F}_{\jmath 1,t+1}} \odot [\![\check{y}_{2,t+1}]\!]^{\check{F}_{\jmath 2,t+1}} \odot \cdots \odot [\![\check{y}_{l,t+1}]\!]^{\check{F}_{\jmath l,t+1}}$ $(\jmath = 1, 2, \cdots, m)$.
  Return $[\![h(\check{y}_{\jmath,t+1})]\!]$ as the encrypted message, and transmit this message to the local decryptor.
end procedure
procedure LOCAL DECRYPTOR
  Compute $\vec{F}_{t+1}\acute{y}_{t+1}$ according to (63).
  Compute $\hat{x}_{t+1}$ according to (64) and (65).
  Return the result as the decrypted state estimate.
end procedure

influenced by open and bandwidth-limited communication networks. The distinct aspects of our findings can be summarized as follows: 1) the tackled secure set-membership state estimation issue is novel, incorporating the HES; 2) the developed EDM-based HES is new, which effectively addresses the challenges posed by bandwidth limitations; and 3) the introduced homomorphic-encryption-based state estimation algorithm is innovative, which ensures both secure data transmission and secure estimate computation.

IV. Illustrative Example

In this section, simulation examples are provided to illustrate the efficacy of the proposed encrypted state estimation algorithm for ANNs.

A. Example 1

The parameters for system (3) are specified as follows:

$$\Phi_t = \mathrm{diag}\{0.65, 0.5, 0.3 + 0.15\sin(0.1t)\}$$
$$W_t = \begin{bmatrix} 0.2 & 0.3 & 0.3 \\ 0.1 + 0.1e^{-t} & 0.15 & 0.2 \\ 0.3 & 0.25 & 0.1 \end{bmatrix},$$
$$C_t = \begin{bmatrix} 1 & 4 & 0 \\ 5 & 0.1\cos(0.2t) & 2 \end{bmatrix}$$

and the neuron activation function is

$$\sigma(x_t) = \begin{bmatrix} \tanh(x_{1,t}) & \tanh(x_{2,t}) & \tanh(x_{3,t}) \end{bmatrix}^{\mathrm{T}}.$$

Moreover, the process noise w_t and the measurement noise v_t are selected as

$$w_t = \begin{bmatrix} \phi(0.2)\sin(0.2t) & \phi(0.3)\sin(0.3t) & 0.2\cos(0.2t) \end{bmatrix}$$
$$v_t = \begin{bmatrix} \phi(0.1)\cos(0.25t) & \phi(0.1)\cos(0.1t) \end{bmatrix}$$

where $\phi(a)$ obeys the uniform distribution $\mathscr{U}(-a, a)$ with a being a positive scalar. The positive matrices Q_t and R_t are selected as

$$Q_t = \mathrm{diag}\{0.16\sin^2(0.2t), 0.28\sin^2(0.3t), 0.15\}$$
$$R_t = \mathrm{diag}\{0.1\cos^2(0.25t), 0.1\}.$$

TABLE I
PARAMETER SELECTION

Parameter	Value	Parameter	Value
α_t	$1 + 0.6e^{-0.5t}$	β_t	$1.2 + e^{-0.3t}$
r	15	b	8
p	41	q	13
x_0	$[0.5\ 1\ 0.2]^{\mathrm{T}}$	$\hat{x}_0$	$[0.7\ 0.8\ 0.3]^{\mathrm{T}}$

The other parameters used in the simulation are specified in Table I. Then, by utilizing the parameters in Table I and the Algorithm 1, the public key and the secret key of the EDM-based HES are, respectively, generated as $(533, 5291)$ and $(120, 0.0022)$.

Figs. 2 and 3, respectively, show the amplitude changes of the measured output y_t, decoded data $\acute{y}_t$, and encoded data $\hat{y}_t$. It is clear that the amplitude of the encoded data is smaller than the measurement output, which indicates that the proposed EDM is capable of compressing the data effectively. In addition, the decoding error is shown in Fig. 4, from which we can see that the decoding errors are all smaller than the decoding error upper bound 0.1406. Accordingly, it means that the measurement output can be recoverable from the encoded data, which shows the effective of the proposed method.

Fig. 5 illustrates the variation of the encrypted output $[\![\check{y}_{\iota,t}]\!]$. It can be seen that the encrypted output is totally different from the measurement output, which means that it is difficult to obtain system information from encrypted data. Then, the dynamic trajectories of system states and their estimates are depicted in Figs. 6–8. It is obvious that the designed recursive state estimation algorithm achieves a satisfactory level of performance under the encryption mechanism. Fig. 9 illustrates the estimation error from the eavesdropper. We can see that the eavesdropper obtains an estimation error on the order of 10^4 magnitudes, making it unable to effectively compute the state estimate, which shows that the proposed secure state estimation algorithm can present a desired performance.

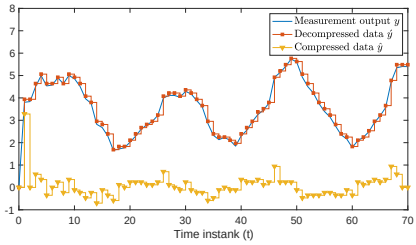


Fig. 2. Measurement output, decoded data and encoded data.

B. Example 2

To validate that the estimation algorithm proposed in this paper is also applicable to unstable systems, we present an example with system parameters having eigenvalues greater than 1. The system parameter is

$$\Phi_t = \mathrm{diag}\{1.1, 0.3 + 0.75\cos(0.3t), 0.35 + 0.2\sin(0.2t)\}$$

and the other parameters are the same as in Example 1.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

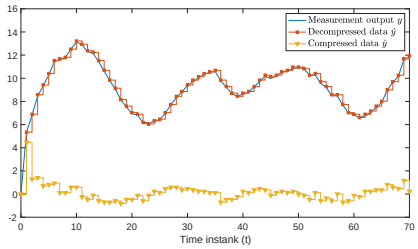


Fig. 3. Measurement output, decoded data and encoded data.

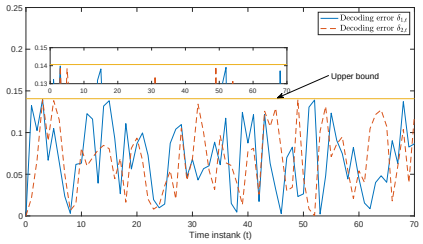


Fig. 4. Decoding error of the EDM.

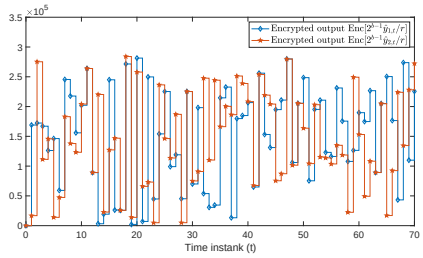


Fig. 5. Encrypted output data under the EDM-based HES.

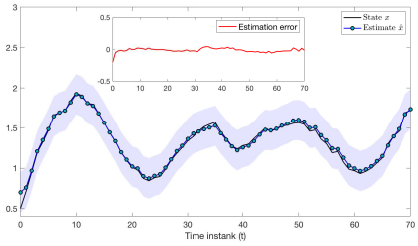


Fig. 6. System state x, estimate $\hat{x}$ and estimation error $x - \hat{x}$.

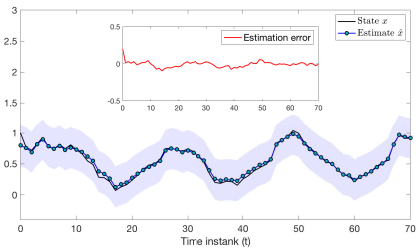


Fig. 7. System state x, estimate $\hat{x}$ and estimation error $x - \hat{x}$.

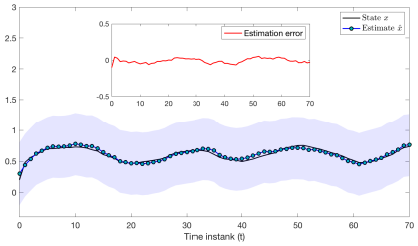


Fig. 8. System state x, estimate $\hat{x}$ and estimation error $x - \hat{x}$.

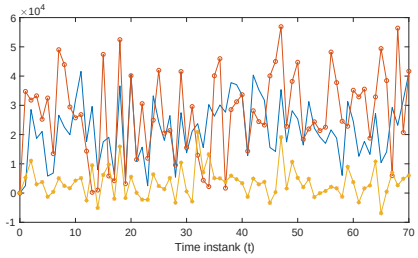


Fig. 9. Estimation error from eavesdropper.

Figs. 10–12 shows the dynamic trajectories of system states and their estimates. In particular, Fig. 10 illustrates the estimation of unstable system states, showing that the designed estimation algorithm still achieves the expected estimation performance. Fig. 13 shows the dynamic trajectory of the estimation error, which indicates that the designed estimation algorithm is effective for unstable systems. The decoding error is shown in Fig. 14, from which we can see that the decoding errors are all smaller than the decoding error upper bound 0.1406. Accordingly, it means that the measurement output can be recoverable from the encoded data, which shows the effective of the proposed method for unstable systems. In summary, Fig. 10–14 shows the effectiveness of the proposed secure state estimation algorithm.

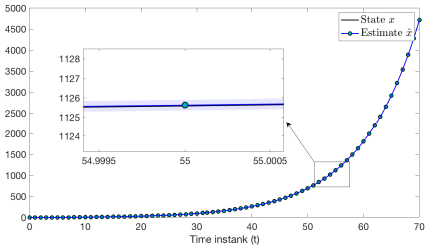


Fig. 10. System state x and estimate $\hat{x}$.

V. Conclusion

In this investigation, the secure set-membership state estimation issue has been addressed for a certain class of ANNs influenced by unknown-but-bounded noises and bandwidth-limited communication networks. A novel EDM-based HES has been introduced, which ensures the security of both data transmission and estimate computation processes. Leveraging this encryption mechanism, a secure state estimation algorithm for ANNs has been devised to confine the estimation error

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

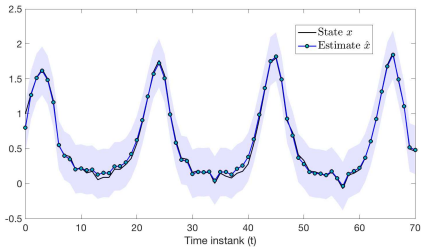


Fig. 11. System state x and estimate $\hat{x}$.

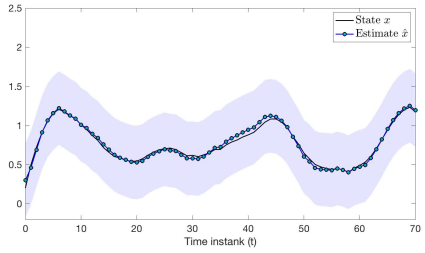


Fig. 12. System state x and estimate $\hat{x}$.

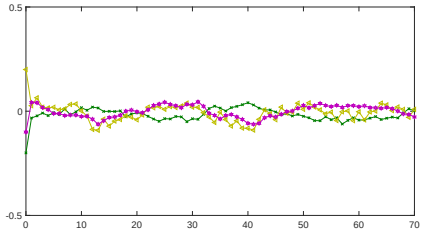


Fig. 13. Estimation error.

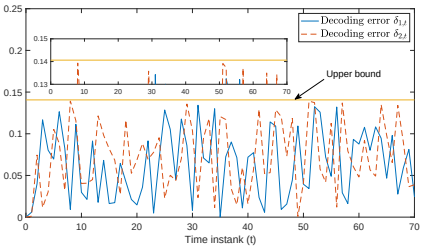


Fig. 14. Decoding error of the EDM.

within an optimal ellipsoidal set and assure the estimation performance. The pertinent parameters have been determined through optimization problems, and the sought-after state estimator gains have been derived from recursive equations. A simulation example has been showcased to validate the efficacy of the proposed secure state estimation approach.

In practical engineering, there remain several complex and significant challenges, such as distributed sensor networks, that have yet to be explored within a unified framework of ANNs. Furthermore, additional estimation approaches, such as the proportional-integral-observer technique, warrant further investigation.

REFERENCES

[1] A. Alessandri and L. Zaccarian, Stubborn state observers for linear time-invariant systems, *Automatica*, vol. 88, pp. 1–9, 2018.
[2] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Boston: Birkhäuser, 2008.
[3] S. Boyd, L. E. Ghaoui, E. Feron and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA, USA: SIAM, 1994.
[4] R. Caballero-Águila, A. Hermoso-Carazo and J. Linares-Pérez, Networked fusion estimation with multiple uncertainties and time-correlated channel noise, *Information Fusion*, vol. 54, pp. 161–171, 2020.
[5] J. Cao, Y. Wang, J. He, W. Liang, H. Tao and G. Zhu, Predicting grain losses and waste rate along the entire chain: a multitask multigated recurrent unit autoencoder based method, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4390–4400, 2021.
[6] J. Cao, Y. Wang, H. Tao and X. Guo, Sensor-based human activity recognition using graph LSTM and multi-task classification model, *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 18, no. 3s, art. no. 139, 2022.
[7] Z. Cao, Z. Wang, Y. Niu, J. Song and H. Liu, Sliding mode control for sampled-data systems subject to deception attacks: handling randomly perturbed sampling periods, *IEEE Transactions on Cybernetics*, vol. 53, no. 11, pp. 7034–7047, 2023.
[8] Y. Chen, N. Zhang and J. Yang, A survey of recent advances on stability analysis, state estimation and synchronization control for neural networks, *Neurocomputing*, vol. 515, pp. 26–36, 2023.
[9] J. Cheng, A. Lin, J. Cao, J. Qiu and W. Qi, Protocol-based fault detection for discrete-time memristive neural networks with effect, *Information Sciences*, vol. 615, pp. 118–135, 2022.
[10] J. Cheng, L. Liang, H. Yan, J. Cao, S. Tang and K. Shi, Proportional-integral observer-based state estimation for markov memristive neural networks with sensor saturations, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 405–416, 2024.
[11] M. S. Darup, A. B. Alexandru, D. E. Quevedo and G. J. Pappas, Encrypted control for networked systems: An illustrative introduction and current challenges, *IEEE Control Systems Magazine*, vol. 41, no. 3, pp. 58–78, 2021.
[12] S. Ding, Z. Wang and X. Xie, Periodic event-triggered synchronization for discrete-time complex dynamical networks, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 8, pp. 3622–3633, 2022.
[13] S. Ding and Z. Wang, Synchronization of coupled neural networks via an event-dependent intermittent pinning control, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 3, pp. 1928–1934, 2022.
[14] A. Dong, A. Starr and Y. Zhao, Neural network-based parametric system identification: A review, *International Journal of Systems Science*, vol. 54, no. 13, pp. 2676–2688, 2023.
[15] C. Durieu, B. T. Polyak and E. Walter, Trace versus determinant in ellipsoidal outer-bounding with application to state estimation, in: *IFAC Proceedings Volumes*, vol. 29, no. 1, pp. 3975–3980, 1996.
[16] S. Feng, X. Li, S. Zhang, Z. Jian, H. Duan and Z. Wang, A review: State estimation based on hybrid models of Kalman filter and neural network, *Systems Science & Control Engineering*, vol. 11, no. 1, 2023, Art. no. 2173682.
[17] H. Gao, Y. Li, L. Yu and H. Yu, Collaborative-prediction-based recursive filtering for nonlinear systems with sensor saturation under duty cycle scheduling, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2247007, 2023.
[18] Y. Gao, J. Hu, H. Yu and J. Du, Robust resilient H_∞ state estimation for time-varying recurrent neural networks subject to probabilistic quantization under variance constraint, *International Journal of Control Automation and Systems*, vol. 21, no. 2, pp. 684–695, 2023.
[19] H. Geng, Z. Wang, J. Hu, H. Dong and Y. Cheng, Distributed recursive filtering over sensor networks under random access protocol: When state saturation meets censored measurement, *IEEE Transactions on Cybernetics*, vol. 53, no. 12, pp. 7760–7772, 2023.
[20] F. Han, J. Liu, J. Li, J. Song, M. Wang and Y. Zhang, Consensus control for multi-rate multi-agent systems with fading measurements: the dynamic event-triggered case, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2158959, 2023.
[21] J. Huang, D. W. C. Ho, F. Li, W. Yang and Y. Tang, Secure remote state estimation against linear man-in-the-middle attacks using watermarking, *Automatica*, vol. 121, 2020, Art. no. 109182.

[22] M. I. Khedher, H. Jmila and M. A. El-Yacoubi, On the formal evaluation of the robustness of neural networks and its pivotal relevance for AI-based safety-critical domains, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 4, art. no. 100018, Dec. 2023.

[23] J. Le Ny and G. J. Pappas, Differentially private filtering, *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[24] B. Li, F. Liu, Q. Song, D. Zhang and H. Qiu, State estimation of complex-valued neural networks with leakage delay: A dynamic event-triggered approach, *Neurocomputing*, vol. 520, pp. 230–239, 2023.

[25] W. Li and F. Yang, Information fusion over network dynamics with unknown correlations: An overview, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, 2023, Art. no. 100003.

[26] X. Li and D. Ye, Dynamic event-triggered distributed filtering design for interval type-2 fuzzy systems over sensor networks under deception attacks, *International Journal of Systems Science*, vol. 54, no. 15, pp. 2875–2890, 2023.

[27] C. Liu, H. Rao, X. Yu, Y. Xu and C.-Y. Su, State estimation for recurrent neural networks with intermittent transmission, *IEEE Transactions on Cybernetics*, in press, doi: 10.1109/TCYB.2023.3239368.

[28] J. Liu, Y. Wang, J. Cao, D. Yue and X. Xie, Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack, *IEEE Transactions on Cybernetics*, vol. 51, no. 8, pp. 4000–4010, 2021.

[29] J. Liu, J. Xia, J. Cao and E. Tian, Quantized state estimation for neural networks with cyber attacks and hybrid triggered communication scheme, *Neurocomputing*, vol. 291, pp. 35–49, 2018.

[30] Y. Liu, B. Shen and P. Zhang, Synchronization and state estimation for discrete-time coupled delayed complex-valued neural networks with random system parameters, *Neural Networks*, vol. 150, pp. 181–193, 2022.

[31] X. Luo, H. Wu and Z. Li, NeuLFT: A novel approach to nonlinear canonical polyadic decomposition on high-dimensional incomplete tensors, *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 6, pp. 6148–6166, 2023.

[32] M. R. G. Meireles, P. E. M. Almeida and M. G. Simões, A comprehensive review for industrial application of artificial neural networks, *IEEE Transactions on Industrial Electronics*, vol. 50, no. 3, pp. 585–601, 2003.

[33] P. Paillier, *Public-key cryptosystems based on composite degree residuosity classes*. Berlin, Germany: Springer, 1999.

[34] Z.-H. Pang, L.-Z. Fan, Z. Dong, Q.-L. Han and G.-P. Liu, False data injection attacks against partial sensor measurements of networked control systems, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 1, pp. 149–153, 2022.

[35] P. Y. Reddy and L. C. Saikia, Hybrid AC/DC control techniques with improved harmonic conditions using DBN based fuzzy controller and compensator modules, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2188406, 2023.

[36] X. Tan, C. Xiang, J. Cao, W. Xu, G. Wen and L. Rutkowski, Synchronization of neural networks via periodic self-triggered impulsive control and its application in image encryption, *IEEE Transactions on Cybernetics*, vol. 52, no. 8, pp. 8246–8257, 2022.

[37] X. Wang, J. H. Park, H. Yang and S. Zhong, A new settling-time estimation protocol to finite-time synchronization of impulsive memristor-based neural networks, *IEEE Transactions on Cybernetics*, vol. 52, no. 6, pp. 4312–4322, 2022.

[38] Y.-A. Wang, B. Shen, L. Zou and Q.-L. Han, A survey on recent advances in distributed filtering over sensor networks subject to communication constraints, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, 2023, Art. no. 100007.

[39] Z. Xiao, Y. Guo, C. Liu and Y. Zhou, Anti-synchronization for Markovian neural networks via asynchronous intermittent control, *Neurocomputing*, vol. 528, pp. 217–225, 2023.

[40] Y. Xu, W. Lv, W. Lin, R. Lu and D. E. Quevedo, On extended state estimation for nonlinear uncertain systems with round-robin protocol, *Automatica*, vol. 138, Article 110154, 2022.

[41] J. Yang, L. Ma, Y. Chen and X. Yi, ℓ_2-ℓ_∞ state estimation for continuous stochastic delayed neural networks via memory event-triggering strategy, *International Journal of Systems Science*, vol. 53, no. 13, pp. 2742–2757, 2022.

[42] Z. Yang, L. Yu, Y. Liu, N. D. Alotaibi and F. E. Alsaadi, Event-triggered privacy-preserving bipartite consensus for multi-agent systems based on encryption, *Neurocomputing*, vol. 503, pp. 162–172, 2022.

[43] X. Yi, H. Yu, Z. Fang and L. Ma, Probability-guaranteed state estimation for nonlinear delayed systems under mixed attacks, *International Journal of Systems Science*, vol. 54, no. 9, pp. 2059–2071, 2023.

[44] H. Yin, P. Seiler and M. Arcak, Stability analysis using quadratic constraints for systems with neural network controllers, *IEEE Transactions on Automatic Control*, vol. 67, no. 4, pp. 1980–1987, 2021.

[45] Y. Yuan, X. Tang, W. Zhou, W. Pan, X. Li, H.-T. Zhang, H. Ding and J. Goncalves, Data driven discovery of cyber physical systems, *Nature Communications*, vol. 10, no. 1, pp. 1–9, 2019.

[46] F. M. M. Zegers, R. Sun, G. Chowdhary and W. E. E. Dixon, Distributed state estimation with deep neural networks for uncertain nonlinear systems under event-triggered communication, *IEEE Transactions on Automatic Control*, vol. 68, no. 5, pp. 3107–3114, 2023.

[47] B.-L. Zhang, E.-Z. Cao, Z. Cai, H. Su and G.-Y. Tang, Event-triggered H_∞ control for networked spar-type floating production platforms with active tuned heave plate mechanisms and deception attacks, *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 3554–3584, 2021.

[48] H. Zhang, D. Yue, C. Dou, X. Xie and G. P. Hancke, Two-stage optimal operation strategy of isolated micro-grid with TSK fuzzy identification of supply security, *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3731–3743, 2020.

[49] Y. Zhang, Z. Wang, L. Zou, H. Dong and X. Yi, Neural-network-based secure state estimation under energy-constrained denial-of-service attacks: An encoding-decoding scheme, *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 4, pp. 2002–2015, 2023.

[50] Z. Zhang, S. Yang, W. Xu and K. Di, Privacy-preserving distributed ADMM with event-triggered communication, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 2, pp. 2835–2847, 2024.

[51] D. Zhao, Z. Wang, L. Wang and G. Wei, Proportional-integral observer design for multirate-networked systems under constrained bit rate: An encoding-decoding mechanism, *IEEE Transactions on Cybernetics*, vol. 53, no. 7, pp. 4280–4291, 2023.

[52] T. Zheng, Y. Zhou, M. Hu and J. Zhang, Dynamic scheduling for large-scale flexible job shop based on noisy DDQN, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 4, art. no. 100015, Dec. 2023.

[53] Y. Zhou, Y. Guo, C. Liu, H. Peng and H. Rao, Synchronization for Markovian master-slave neural networks: An event-triggered impulsive approach, *International Journal of Systems Science*, vol. 54, no. 12, pp. 2551–2565, 2023.

[54] K. Zhu, Z. Wang, Y. Chen and G. Wei, Event-triggered cost-guaranteed control for linear repetitive processes under probabilistic constraints, *IEEE Transactions on Automatic Control*, vol. 68, no. 1, pp. 424–431, 2023.

[55] K. Zhu, Z. Wang, Y. Chen and G. Wei, Neural-network-based set-membership fault estimation for 2-D systems under encoding-decoding mechanism, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 2, pp. 786–798, 2023.

[56] Y. Zou, J. Zhu, X. Wang and L. Hanzo, A survey on wireless security: Technical challenges, recent advances and future trends, *Proceeding of the IEEE*, vol. 104, no. 9, pp. 1727–175, 2016.

Kaiqun Zhu received the Ph.D. degree in control science and engineering from University of Shanghai for Science and Technology, Shanghai, China, in 2022.

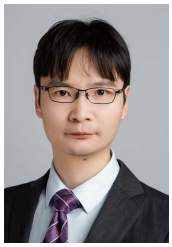
From 2020 to 2022, he was a visiting Ph.D. student with the Department of Computer Science, Brunel University London, Uxbridge, U.K. He is currently a Postdoctoral Fellow with the University of Macau. His research interests include set-membership filtering, model predictive control, neural networks, privacy preserving and their applications in autonomous vehicles.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TNNLS.2024.3389873, IEEE Transactions on Neural Networks and Learning Systems

Zidong Wang (Fellow, IEEE) received the B.Sc. degree in mathematics from Suzhou University, Suzhou, China, in 1986, and the M.Sc. degree in applied mathematics and the Ph.D. degree in electrical engineering from Nanjing University of Science and Technology, Nanjing, China, in 1990 and 1994, respectively.

From 1990 to 2002, he held teaching and research appointments in universities in China, Germany, and the U.K. He is currently a Professor of Dynamical Systems and Computing with the Department of Computer Science, Brunel University London, Uxbridge, U.K. He has authored a number of papers in international journals. His research interests include dynamical systems, signal processing, bioinformatics, and control theory and applications.

Prof. Wang is a member of the Academia Europaea and the European Academy of Sciences and Arts, an Academician of the International Academy for Systems and Cybernetic Sciences, a fellow of the Royal Statistical Society, and a member of program committee for many international conferences. He holds of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong. He serves (or has served) as the Editor-in-Chief for *International Journal of Systems Science*, *Neurocomputing*, *Systems Science & Control Engineering*, and an Associate Editor for 12 international journals including *IEEE Transactions on Automatic Control*, *IEEE Transactions on Control Systems Technology*, *IEEE Transactions on Neural Networks*, *IEEE Transactions on Signal Processing*, *and IEEE Transactions on Systems, Man, and Cybernetics–Part C: Applications and Reviews*.



Derui Ding (Senior Member, IEEE) received both the B.Sc. degree in Industry Engineering in 2004 and the M.Sc. degree in Detection Technology and Automation Equipment in 2007 from Anhui Polytechnic University, Wuhu, China, and the Ph.D. degree in Control Theory and Control Engineering in 2014 from Donghua University, Shanghai, China. He is currently a Senior Research Fellow with the School of Science, Computing and Engineering Technologies, Swinburne University of Technology, Melbourne, VIC, Australia. His research interests include nonlinear stochastic control and filtering, as well as distributed control, filtering and optimization.

He was the recipient of the 2021 Nobert Wiener Review Award from IEEE/CAA Journal of Automatica Sinica, and the 2020 and 2022 Andrew P. Sage Best Transactions Paper Awards from the IEEE Systems, Man, and Cybernetics (SMC) Society. He is a *Senior Member* of the Chinese Association of Automation (CAA). He is serving as an Associate Editor for *IEEE Transactions on Industrial Informatics*, *IEEE/CAA Journal of Automatica Sinica*, *Neurocomputing* and *IET Control Theory & Applications*.

Hongli Dong (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from the Harbin Institute of Technology, Harbin, China, in 2012.

From 2009 to 2010, she was a Research Assistant with the Department of Applied Mathematics, City University of Hong Kong, Hong Kong. From 2010 to 2011, she was a Research Assistant with the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong. From 2011 to 2012, she was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, London, U.K. From 2012 to 2014, she was an Alexander von Humboldt Research Fellow with the University of Duisburg–Essen, Duisburg, Germany. She is currently a Professor with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing, China. She is also the Director of the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Daqing, China. Her current research interests include robust control and networked control systems.

Dr. Dong is a very active reviewer for many international journals.

Cheng-Zhong Xu (Fellow, IEEE) received the B.Sc. and M.Sc. degrees from Nanjing University, in 1986 and 1989 respectively, and the Ph.D. degree from the University of Hong Kong in 1993, all in Computer Science and Engineering.

He is currently the Dean of Faculty of Science and Technology and the Interim Director of Institute of Collaborative Innovation, University of Macau (UM), and a Chair Professor of Computer and Information Science. He was a professor of Wayne State University and the Director of Institute of Advanced Computing of Shenzhen Institutes of Advanced Technologies, Chinese Academy of Sciences before he joined UM in 2019. His research interests lie in parallel and distributed computing and cloud computing, in particular, with an emphasis on resource management for system's performance, reliability, availability, power efficiency, and security, and in big data and data-driven intelligence applications in smart city and self-driving vehicles.

Dr. Xu is a Chief Scientist of Key Project on Smart City of the Ministry of Science and Technology, China. He was a Best Paper Nominee or Awardee of the 2021 ACM Symposium on Cloud Computing, 2013 IEEE High Performance Computer Architecture, the 2013 ACM High Performance Distributed Computing, IEEE Cluster'2016, ICPP'2005, GPC'2018, UIC'2018, AIMS'2019, and IEEE Edge'2020. He serves or served on a number of journal editorial boards, including *IEEE Transactions on Computers*, *IEEE Transactions on Cloud Computing*, *IEEE Transactions on Parallel and Distributed Systems*, *Journal of Parallel and Distributed Computing*, *Science China: Information Science*. He was the Chair of IEEE Technical Committee on Distributed Processing from 2015 to 2020.