A Privacy-preserving Approach to Distributed Set-membership Estimation over Wireless Sensor Networks

Xuefeng Yang[1], Li Liu[1,*], Yinggang Zhang[1], Yihao Li[1], Pan Liu[2], and Shili Ai[2]
[1] School of Information and Electrical Engineering, Ludong University, Yantai, Shandong, China
[2] School of Business Information, Shanghai Business School, Shanghai, China
yangxuefeng1109@163.com, liulildu@163.com, zhangygldu@163.com, yihao.li@ldu.edu.cn, liu@sbs.edu.cn, 2115258607@qq.com
*corresponding author

***Abstract*—This paper focuses on the system on wireless sensor networks. The system is linear and the time of the system is discrete as well as variable, which named discrete-time linear time-varying systems (DLTVS). DLTVS are vulnerable to network attacks when exchanging information between sensors in the network, as well as putting their security at risk. A DLTVS with privacy-preserving is designed for this purpose. A set-membership estimator is designed by adding privacy noise obeying the Laplace distribution to state at the initial moment. Simultaneously, the differential privacy of the system is analyzed. On this basis, the real state of the system and the existence form of the estimator for the desired distribution are analyzed. Finally, simulation examples are given, which prove that the model after adding differential privacy can obtain accurate estimates and ensure the security of the system state.**

Keywords- Set-membership estimator; wireless sensor networks; privacy-preserving; unknown but bounded noise

I. INTRODUCTION

The structure formed by sensor nodes in free-form combination via wireless communication technology is a wireless sensor network(WSN) [1,2], which senses, collects, processes and transmits information about target objects in the network, mainly through a collaborative approach. In recent years it has been widely used in the field of electrical automation[3], aviation[4] and positioning[5].

Due to the limitations of their communication capabilities, sensors can only sense partial information, so achieving effective data collection as well as efficient distributed processing becomes a challenge. In practical WSN, the sensor sensing process will be affected by noise, such as process noise and measurement noise, but users are more interested in processed sensory information, so scholars have done a lot of research on the processing estimation of information, most notably are Kalman filtering estimation and $H\infty$ filtering estimation.

Kalman filtering is a processing technique for removing noise from sensor sensory data to obtain the actual data. It is essentially an estimate of actual data based on observed data. Since the process of estimating the state is the process of removing noise, the optimal estimation process can also be referred to as the filtering process. In [6], an improved Kalman filtering algorithm based on a traceless Kalman filtering and a particle filtering is proposed. In [7], a security estimation method combining a security estimator and a Kalman filtering is used, where the attacked nodes are time-varying. In [8], the communication burdens, computational burdens and their scalability are analyzed to further generalize the characteristics of the non-Kalman filtering case based on the constructed filters. In [9], a distributed Kalman filtering with greater fault tolerance is developed for multi-sensor uncertain systems. Thus Kalman filtering can yield accurate estimation in linear models, but it is unoptimal estimation in non-linear models.

Kalman filtering is somewhat limited when the system model, system structure or noise is uncertain. The $H\infty$ filtering results are more stable, robust and accurate. No assumptions need to be made about uncertainties or perturbations, and in the worst case, the $H\infty$ filtering still minimizes the estimation error. In [10], the distributed $H\infty$ for systems with stochastic delays is investigated. In order to avoid the use of transcendental equations during solution, a filter is designed that keeps the system mean square exponent stable despite the decay of the $H\infty$ filtering disturbances. In [11], an algorithm is designed for the coupled random complex networks. For coupled random complex networks, it can resist random disturbance. Thus $H\infty$ filtering can yield accurate estimates in the presence of uncertainty for the system model with noise. However, in practical applications, it is difficult to satisfy the assumptions when applying Kalman filtering or $H\infty$ filtering for estimation.

In practice, when a model of estimating the parameters, it is assumed the noise of the characteristics to demonstrate the convergence of the system. However if the noise is not random in nature, it is difficult to confirm whether the statistical judgments about the noise are consistent with reality, so the assumptions made about the noise are not satisfied. Using traditional estimation models, e.g. Kalman filtering or $H\infty$ filtering, the accuracy of the estimation is compromised, so parameter estimation can be performed using setter estimates that describe the system model using measured data, model structure and noise bounds. In [12,13], set-membership estimation methods for discrete-time nonlinear systems are discussed. For the minimization problem of estimating ellipsoid trajectories, an optimization algorithm is designed.

2767-6684/22/$31.00 ©2022 IEEE
DOI 10.1109/DSA56465.2022.00137

At the same time, complex networks are being used on a large scale and network security is under threat. The security of data information is gradually becoming a major obstacle to smooth network communication, and the openness of the data interaction channel of sensor nodes makes the network system more vulnerable to attacks [14]. Thus the issue of data privacy in the network has also become a key issue for scholar to study. Privacy protection has gradually become a hot topic in the study of data security. Adding privacy protection can ensure that the real data information of the initial state is not leaked, so that the security of the information is guaranteed. In [15] the differential privacy problem of discrete-time multi-intelligent network systems is studied. A new distributed differential privacy problem is proposed and its convergence, accuracy and privacy are analyzed, where the privacy of state at the initial moment is preserved during the information interaction. In [16], a new fractional order estimation error method is developed based on the consideration of random network attacks, in addition to the design of an expectation non-fragile state estimator. In order to obtain accurate estimation of unknown parameters based on the system security, the distributed filtering method containing privacy protection needs further research.

Intentionally, this paper mainly studies DLTVS containing privacy protection. The main innovations of the method proposed include: firstly, privacy noise obeying Laplace distribution is introduced to state at the initial moment to achieve the purpose of protecting state at the initial moment and to analyze its privacy. Secondly, the set-membership estimator is designed to obtain accurate estimates despite the unknown but bounded (UBB) noise property. Finally the expectation estimates are analyzed by means of a recursive convex optimization algorithm, ensuring that actual values are always included within the estimated range.

Each part of this paper works as follows. Section II models a distributed set-membership estimation method on WSN, which affected by privacy protection noise as well as UBB noise. Section III provides an analysis of the existence form using the expected distribution estimator. Section IV presents simulations of the proposed method. The paper is summarized in section V.

Notation: $\mathbb{R}^N$ represents a n-dimensional vector space, $\|.\|$ denotes the 2-norm of the matrix, $col_N\{.\}$ denotes a column vector with one block, and $diag_N\{.\}$ denotes a diagonal matrix with one block.

II. MAIN TASKS

In a distributed network configuration environment, the network topology used in this paper is a directed graph, which is defined in the following form.

Assume that the node index set is denoted by $V=\{1,2,...,N\}$, set of node edges are denoted by $\varepsilon \in V\times V$, the weighted adjacency matrix is denoted by $A=[a_{ij}]\in\mathbb{R}^{N\times N}$. $D=(V,\varepsilon,A)$ denotes the weighted directed graph of the N-node interaction topology. For any $i,j\in V$, a_{ij} in A denotes the weight of an edge between two neighboring nodes when node i be able to collect message from node j, $a_{ij}>0$, if $a_{ij}=0$, node i cannot collect message from node j. $N_i=\{j\in V:(i,j)\in\varepsilon\}$ represents the neighbor set of node i. All elements in this set are called neighboring nodes of node i.

The bounded noise is treated in this paper as a set of bounded ellipsoids in the model building process.

$Z\triangleq\{a:a=b+Ec,\|c\|\le 1\}$ stands for ellipsoid, the center of the ellipsoid is $b\in\mathbb{R}^N$, $E\in\mathbb{R}^{n\times m}$ is the lower triangular matrix of the ellipsoid, $rank(E)=m\le n$. Suppose E is a lower triangular matrix with all elements positive, and another representation of the ellipsoid can be obtained by cholesky decomposition as $Z\triangleq\{a:(a-b)^T P^{-1}(a-b)\le 1\}$, where $P=EE^T$.

A. System Model

To protect the security of state information, it needs to be protected by differential privacy, and due to the dependence of the Laplace mechanism in differential privacy on the introduced noise characteristics, this paper adds the privacy noise with Laplace distribution to the initial state. And under the influence of process noise and measurement noise, the discrete time-varying linear system model established in this paper is described as follows.

$$\begin{cases}\zeta(t)=x(t)+\eta(t)\\ x(t+1)=C(t)\zeta(t)+F(t)w(t),\ \ x(0)=x_0\end{cases}\tag{1}$$

where $x(t)\in\mathbb{R}^{n_x}$ denotes the state variable at t time, x_0 is a given initial state value, $C(t)$ and $F(t)$ are real-valued matrices, $\zeta(t)\in\mathbb{R}^{n_\zeta}$ repersents the internal state of the system after adding privacy noise, $\eta(t)\in\mathbb{R}^{n_\eta}$ is privacy noise and follows the Laplace distribution

$$\eta(t)\sim Lap(b),b=cq^t\tag{2}$$

where c and q satisfy the following conditions

$$c>0,q\in(0,1)\tag{3}$$

$w(t)\in\mathbb{R}^{n_w}$ is UBB process noise which is within a certain range

$$W_t\triangleq\{w(t):w^T(t)R^{-1}(t)w(t)\le 1\}\tag{4}$$

where $R(t)=R^T(t)>0$ is a time-varying matrix.

B. Output Measurement Models

At time t, build a measurement model for sensor i.

$$y_i(t)=H_i(t)x(t)+D_i(t)\ v_i(t)\tag{5}$$

where $y_i(t) \in \mathbb{R}^{n_y}$ represents the output measurement by sensor node i at time t, $H_i(t)$ and $D_i(t)$ are time-varying real-valued matrices with appropriate dimensionality, $v_i(t) \in \mathbb{R}^{n_{v_i}}$ is UBB measurement noise which is within a certain range

$$V_t^i \triangleq \{v_i(t) : v_i^T(t) Q_i^{-1}(t) v_i(t) \le 1\} \quad (6)$$

where $Q_i(t) = Q_i^T(t) > 0$ is a time-varyingm matrix.

Remark: If $\Pr[Alg(x^{(1)}) \in \Xi] \le e^{\varepsilon\varsigma} \Pr[Alg(x^{(2)}) \in \Xi]$ holds, any pair of neighboring initial states are denoted by $x_i^{(2)}(0)$ and $x_i^{(1)}(0)$, and the algorithm satisfies ϵ-differential privacy performance, where $\epsilon_i = \dfrac{\varsigma q_i}{c_i(q_i - \hat{A}_i)}$. Note that $Alg(.)$ denote running this algorithm and Ξ represent the entire execution state domain of the algorithm [17] .

C. Set-Membership Estimator

The estimated system state at time $t+1$, which obtained from the estimator i execution, is expressed as

$$\hat{x}_i(t+1) = \hat{A}_i(t)\hat{x}_i(t) + \hat{B}_i(t) \sum_{j \in N_i} a_{ij} \tilde{y}_j(t) \quad (7)$$

where $\hat{A}_i(t)$ and $\hat{B}_i(t)$ represent the estimated gain matrices with the appropriate dimensions and $\tilde{y}_i(t) = y_i(t) - H_i(t)\hat{x}_i(t)$ represents the measurement residual at time t. And the estimation at the initial time $\hat{x}_{i,0}$ is confined to an ellipsoid

$$X_0^i \triangleq \{x_0 : (x_0 - \hat{x}_{i,0})^T U_{i,0}^{-1} (x_0 - \hat{x}_{i,0}) \le \beta_i\} \quad (8)$$

where $U_{i,0} = U_{i,0}^T > 0$ is a known real-valued matrix, $\beta_i > 0$ represents a scaling parameter about the ellipsoid.

Typically, when performing distributed estimation on a WSN, each sensor needs to be estimated point by point. Since it is a vector with no fixed boundaries, there is no guarantee that all estimates are within the same confidence interval [18]. However, in practical application, there is a need to estimate the target with 100 per cent confidence, to establish a confidence interval that contains all the true states of the target. Therefore, it is necessary to apply set-membership estimation.

When systems (1) and (5) are subjected to UBB process noise $w(t)$, measurement noise $v(t)$ and privacy noise $\eta(t)$, the state $x(t+1)$ can still lie within the estimation interval of the sensor and therefore a set of estimates containing the true state can be obtained

$$X_{t+1}^i \triangleq \{x(t+1) : e_i^T(t+1) U_i^{-1}(t+1) e_i(t+1) \le \beta_i\} \quad (9)$$

where $e_i(t+1) = x(t+1) - \hat{x}_i(t+1)$, $e_i(t+1)$ represents the estimation error, $U_i(t+1) = U_i^T(t+1) > 0$ is a time-varying matrix.

Based on the above conditions, for the problem of set-membership estimation, the problem now needs to be solved as follows: for prescribed scalars $\beta_i > 0$, and $\eta(t) \in \mathbb{R}^{n_\eta}$, $w(t) \in \mathbb{R}^{n_w}$ and $v_i(t) \in \mathbb{R}^{n_{v_i}}$, $i \in v$, one-step predicted state of the system $x(t+1)$ can be guaranteed to remain within the ellipsoid X_{t+1}^i of the estimated state when time-varying real-valued matrices $U_i(t+1) > 0$, $\hat{A}_i(t)$ and $\hat{B}_i(t)$ exist.

III. Analysis of Expected Distribution Estimators

This section provides a unified description of the N subsystems in the distributed system, and to facilitate the analysis of this model, the main parameters are described as following.

$$\tilde{e}(t) = col_N\{e_i(t)\}, \tilde{x}(t) = col_N\{x(t)\}$$
$$\hat{x}(t) = col_N\{\hat{x}_i(t)\}, \tilde{\eta}(t) = col_N\{\eta(t)\}$$
$$\tilde{M}(t) = diag_N\{M(t)\}, M(t) = 2b(t)^2$$
$$\tilde{w}(t) = col_N\{w(t)\}, \tilde{v}(t) = col_N\{v_i(t)\}$$
$$\tilde{\alpha} = col_N\{\alpha_i\}, \tilde{\beta} = diag_N\left\{\beta_i^{\frac{1}{2}}\right\}$$
$$\tilde{U}(t) = diag_N\{U_i(t)\}, \tilde{L}(t) = diag_N\{L_i(t)\}$$
$$\tilde{R}(t) = diag_N\{R(t)\}, \tilde{Q}(t) = diag_N\{Q_i(t)\}$$
$$\tilde{C}(t) = diag_N\{C(t)\}, \tilde{F}(t) = diag_N\{F(t)\}$$
$$\tilde{H}(t) = diag_N\{H_i(t)\}, \tilde{D}(t) = diag_N\{D_i(t)\}$$
$$\hat{A}(t) = diag_N\{\hat{A}_i(t)\}, \hat{B}(t) = diag_N\{\hat{B}_i(t)\}$$

Next, Theorem 1 analyses the existence of forms for estimators with the expected distribution.

Theorem 1: For a prescribed scalar $\beta_i > 0$, $\eta(t) \in \mathbb{R}^{n_\eta}$, $w(t) \in \mathbb{R}^{n_w}$ and $v_i(t) \in \mathbb{R}^{n_{v_i}}$, $i \in v$, if exists a sequence of real-valued matrices $U_i(t+1) > 0$, $\hat{A}_i(t)$, $\hat{B}_i(t)$ and a sequence of scalars $\epsilon_m(t) > 0$, $m = 1,2,3,4$ so that

$$\begin{pmatrix} -\tilde{U}(t+1) & \Phi(t) \\ * & \Lambda(t) \end{pmatrix} \le 0, \forall t \in N \quad (10)$$

where

$$\Phi(t)=[(\tilde{C}(t)-\hat{A}(t))\hat{x}(t),\tilde{\beta}(\tilde{C}(t)-\hat{B}(t)A\tilde{H}(t))L(t),\tilde{F}(t),\tilde{C}(t),-\hat{B}(t)A\tilde{D}(t)]$$

and $\Lambda(t)=[\Lambda_{p,q}(t)]_{5\times5}$ is a matrix (since $\Phi(t)$ is a 1×5 matrix, it follows that the matrix is a 5×5 matrix) and the non-zero terms in the matrix are represented as folloing:

$$\Lambda_{1,1}(t)=-\sum_{i=1}^{N}\beta_i+\epsilon_1(t)N+\epsilon_3(t)N+\epsilon_4(t)N$$

$$\Lambda_{2,2}(t)=-\epsilon_4(t)I$$

$$\Lambda_{3,3}(t)=-\epsilon_1(t)\tilde{R}^{-1}(t)$$

$$\Lambda_{4,4}(t)=\epsilon_2(t)\tilde{M}^{-1}(t)$$

$$\Lambda_{5,5}(t)=-\epsilon_3(t)\tilde{Q}^{-1}(t)$$

Then, based on the implementation of state estimation, it is guaranteed that the one-step predicted state $x(t+1)$ of the system always lies within the state estimation ellipsoid X_{t+1}^{i}.

Proof: For this proof the method of mathematical induction is used. First, $e_{i,0}^{T}U_{i,0}^{-1}e_{i,0}\le\beta_i$ is obtained from(8). At time t, assuming $x(t)\in X_t^i$, which satisfies $e_i^T(t)U_i^{-1}(t)e_i(t)\le\beta_i$. Then, just prove that $e_i^T(t+1)U_i^{-1}(t+1)e_i(t+1)\le\beta_i$ holds.

Redefine the ellipsoid satisfied by the estimation error at moment t as $(x(t)-\hat{x}_i(t))^TU_i^{-1}(t)(x(t)-\hat{x}_i(t))\le\beta_i$. The Schur complement is then used to redefine $\beta_i^{-1}e_i(t)e_i^T(t)\le U_i(t)$. $U_i(t)$ is decomposed by a cholesky factorization, such that $U_i(t)=L_i(t)L_i^T(t)$, where $L_i(k)$ is a lower triangular matrix with elements greater than zero. That is, the above equation can be rewritten as $\beta_i^{-1}e_i(t)e_i^T(t)\le L_i(t)L_i^T(t)$.

Let define $\alpha_i=\beta_i^{-1/2}L_i^{-1}(t)(x(t)-\hat{x}_i(t))$, then

$$\alpha_i^T\alpha_i=\beta_i^{-1}(x(t)-\hat{x}_i(t))U_i^{-1}(t)(x(t)-\hat{x}_i(t))\le1 \quad (11)$$

Which satisfies $\|\alpha_i\|\le1$.

From the above equation, it follows that

$$x(t)=\beta_i^{1/2}L_i(t)\alpha_i+\hat{x}_i(t) \quad (12)$$

From(1), (7) and (12), the estimation error $e_i(t+1)$ is regained, i.e.

$$\begin{aligned}e_i(t+1)&=C(t)(x(t)+\eta(t))+F(t)w(t)-(\hat{A}_i(t)\hat{x}_i(t)\\&\quad+\hat{B}_i(t)\sum_{j\in N_i}a_{ij}\tilde{y}_j(t))\\&=(C(t)-\hat{A}_i(t))\hat{x}_i(t)+\beta_i^{1/2}C(t)L_i(t)\alpha_i\\&\quad+F(t)w(t)+C(t)\eta(t)\\&\quad-\hat{B}_i(t)\sum_{j\in N_i}a_{ij}\beta_j^{1/2}H_j(t)L_j(t)\alpha_j\\&\quad-\hat{B}_i(t)\sum_{j\in N_i}a_{ij}(D_j(t)v_j(t))\end{aligned} \quad (13)$$

Let $\psi(t)=[1,\tilde{\alpha},\tilde{w}(t),\tilde{\eta}(t),\tilde{v}(t)]^T$, then (13) can be rewritten as: $\tilde{e}(t+1)=\Phi(t)\psi(t)$, where $\Phi(t)=[(\tilde{C}(t)-\hat{A}(t))\hat{x}(t),\tilde{\beta}(\tilde{C}(t)-\hat{B}(t)A\tilde{H}(t))L(t),\tilde{F}(t),\tilde{C}(t),-\hat{B}(t)A\tilde{D}(t)]$, so the one-step prediction state error $e_i^T(t+1)U_i^{-1}(t+1)e_i(t+1)\le\beta_i$ be able to redifined as

$$\psi^T(t)(\Phi^T(t)U^{-1}(t+1)\Phi(t)+\Theta)\psi(t)\le0 \quad (14)$$

where $\Theta=diag\{-\sum_{i=1}^{N}\beta_i,0,0,0,0\}$.

From (2), (4), (6) and $\|\alpha_i\|\le1$, we have $\psi^T(t)\Gamma_1(t)\psi(t)\ge0$, $\psi^T(t)\Gamma_2(t)\psi(t)\ge0$, $\psi^T(t)\Gamma_3(t)\psi(t)\ge0$ and $\psi^T(t)\Gamma_4(t)\psi(t)\ge0$. Note that $\Gamma_1(t)=diag\{N,0,-\tilde{R}^{-1}(t),0,0\}$, $\Gamma_2(t)=diag\{0,0,0,\tilde{M}^{-1}(t),0\}$, $\Gamma_3(t)=diag\{N,0,0,0,-\tilde{Q}^{-1}(t)\}$, $\Gamma_4(t)=diag\{N,-I,0,0,0\}$.

By the *S*-procedure, there exists a scalar sequences $\epsilon_m(t)$, $m=1,2,3,4$, which is greater than zero. And then, (14) is able to redfined as

$$\begin{aligned}&\Phi^T(t)\tilde{U}^{-1}(t+1)\Phi(t)+\Theta+\epsilon_1(t)\Gamma_1(t)+\epsilon_2(t)\Gamma_2(t)\\&+\epsilon_3(t)\Gamma_3(t)+\epsilon_4(t)\Gamma_4(t)\le0\end{aligned} \quad (15)$$

According to the Schur complement, (10) can be obtained from (15). To the end the proof is complete.

IV. SIMULATION

The ship transportation process is in a vast space, the speed is affected by the external environment, for instance currents and winds that can generate a certain amount of noise, and the ship's resistance is also changed accordingly. In order to avoid that the initial speed and resistance are not leaked during the ship sailing, the initial transmitted state needs to be protected, and the differential privacy method is introduced.

Differential privacy mainly protects the real state from leaking through random noise. When the system state information is stolen, the stealer will get the system state after adding the privacy noise and cannot infer the real state of the system without the privacy noise, so the real state can

be protected. The sensor needs to perceive the speed and resistance information, so it is arranged as a wireless sensor network. In order to verify the effectiveness of the method, this section constructs the system model of ship transportation.

$$\begin{bmatrix} x^1(t+1) \\ x^2(t+1) \end{bmatrix} = \begin{bmatrix} 0.9746 & -0.0013 \\ -0.045 & 0.7528 \end{bmatrix} \begin{bmatrix} x^1(t)+\eta^1(t) \\ x^2(t)+\eta^2(t) \end{bmatrix}$$

Where $x^1(t)$ represents the speed of the ship and $x^2(t)$ represents the resistance to the ship while underway. In practical applications life, process noise is mainly derived from the effects of unpredictable environmental changes, while privacy noise $\eta(t)$ is mainly Laplace-distributed noise added to protect the safety of the initial state. The time-varying parameter matrix in the model is

$$C(t) = \begin{bmatrix} 0.9746 & -0.0013 \\ -0.045 & 0.7528+0.2*\sin(t) \end{bmatrix}$$

$$F(t) = \begin{bmatrix} 0.2+0.2*\sin(i) \\ 0.2 \end{bmatrix}$$

To make the estimator more reliable and accurate, the system deploys a network of five sensors, each of which can only transmit local measurements and estimates to its neighboring sensors, with the topology shown in Figure 1. The adjacency matrix of this network consists of two elements, 0 and 1, i.e. 1 represents the sensor can transmit data to the sensor, conversely, the value is 0. The transmitted measurements in this model are influenced by the measurement noise $v_i(t)$, where the time-varying parameter matrix is $H_i(t) = \begin{bmatrix} 0 & 1+0.1*(i+1)-0.1*\sin(i) \end{bmatrix}$ and $D_i(t) = 1/(i+1)$.

Set the ship's initial operating speed be 1.6m/s and the initial drag be 3.6kgf. For the five estimators the initial estimates at time 0 are set to $\hat{x}_1^0 = \begin{bmatrix} 1.7 & 3.7 \end{bmatrix}$, $\hat{x}_2^0 = \begin{bmatrix} 1.5 & 3.8 \end{bmatrix}$, $\hat{x}_3^0 = \begin{bmatrix} 1.8 & 3.5 \end{bmatrix}$, $\hat{x}_4^0 = \begin{bmatrix} 1.3 & 3.4 \end{bmatrix}$, $\hat{x}_5^0 = \begin{bmatrix} 1.4 & 3.9 \end{bmatrix}$. Set $U_0 = diag_2\{40 \quad 40\}$, $\beta_i = 1$, $R(t) = 0.3$, $Q_i(t) = 0.1$, $b(t) = 1$.

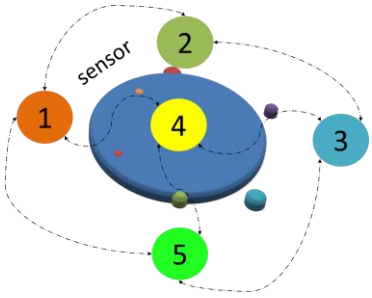

Fig. 1. Sensor relationship diagram

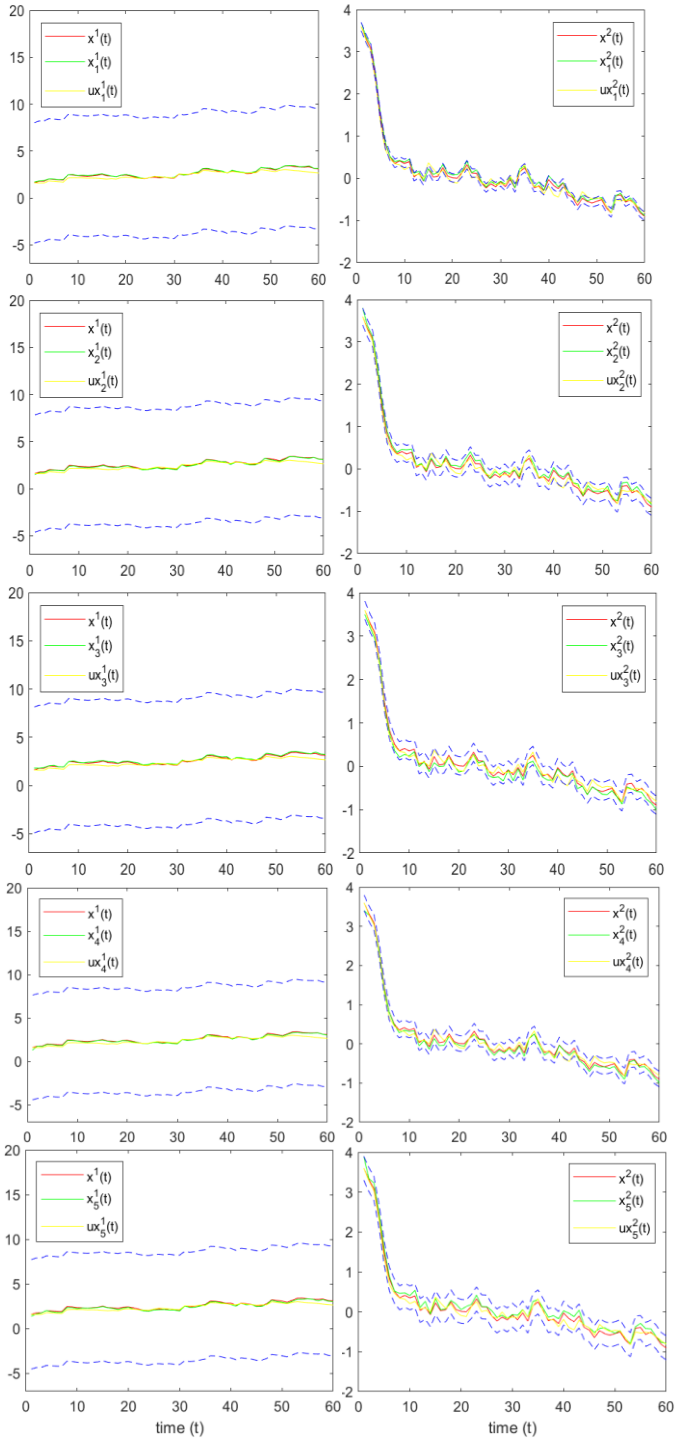

Fig. 2. Actual and estimated values of the system state, and state estimation intervals

In Figure 2, $x^1(t)$ and $x^2(t)$ represent the first and second parameters in the state vector. $x_i^1(t)$ and $x_i^2(t)$ represent the first and second parameters of the estimated values of the estimator i. $ux_i^1(t)$ and $ux_i^2(t)$ represent the state estimates obtained without adding UBB noise. That is, the yellow solid line in Figure. 2 represents the state

estimation value without UBB noise, and the green solid line represents the state estimation value with UBB noise and privacy noise. From Figure 2, even when UBB noise and privacy noise are added, the state values of the system and the corresponding estimates of each estimator are within the estimation interval. The accurate estimated value can be obtained that the model can be successfully applied to the ship sailing system.

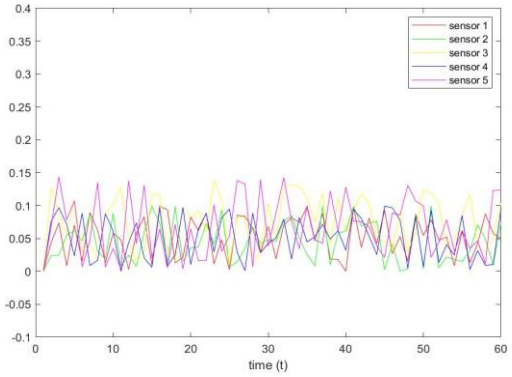

Fig. 3. Estimation error

The estimation errors corresponding to each estimator are depicted in Figure 3, and all estimation errors are before 0-0.15. A good application can be obtained for the proposed model in the estimation of the state, with the estimates at each moment converging to the state value of the system at that moment.

V. CONCLUSION

This study addresses the security of DLTVS over WSN. The purpose of protecting state at the initial moment is achieved by incorporating privacy noise. It is then verified that the one-step predicted state is always ensured to be within the estimated ellipsoid and the differential privacy of the system is analyzed. Finally, it is verified using simulations that the designed estimator yields accurate estimates. The future work will be focus on the issue of the differential privacy for DLTVS with time delays.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (61903172).

REFERENCES

[1] B. Chaudhari, "Role of Swarm Intelligence Algorithms on Secured Wireless Network Sensor Environment-A Comprehensive Review," International Journal of Performability Engineering, vol. 18, no. 2, pp. 92-100, February 2022.

[2] A. C. Savitha, M. N. Jayaramb, and S. S. Mallikarjuna, "Development of Energy Efficient and Secure Routing Protocol for M2M Communication," International Journal of Performability Engineering, vol. 18, no. 6, pp. 426-433, June 2022.

[3] J.M. Liu, Z.Y. Zhao, J. Ji and M.L. Hu," Research and Application of Wireless Sensor Network Technology in Power Transmission and Distribution System," Intelligent and Converged Networks, vol.1, Sept. 2020, pp. 199-220, doi:10.23919/icn.2020.0016.

[4] S. Chakraborty, N.K. Goyal and S. Soh," On Area Coverage Reliability of Mobile Wireless Sensor Networks With Multistate Nodes," IEEE Sensors Journal, vol.20, May. 2020, pp. 4992-5003, doi:10.1109/jsen.2020.2965592.

[5] Y.T. Ma, K.Z. Liu, M.Z. Chen, J. Ma, X.M. Zeng, K.H. Wang, et al.," ANT: Deadline-Aware Adaptive Emergency Navigation Strategy for Dynamic Hazardous Ship Evacuation With Wireless Sensor Networks," IEEE Access, vol.8, Aug. 2020, pp. 135758-135769, doi:10.1109/access.2020.3011545.

[6] I. Ullah, Y. Shen, X. Su, C. Esposito and C. Choi," A Localization Based on Unscented Kalman Filter and Particle Filter Localization Algorithms," IEEE Access, vol.8, Dec. 2020, pp. 2233-2246, doi:10.1109/access.2019.2961740.

[7] Y.H. Chang, Q. Hu and C.J. Tomlin," Secure Estimation Based Kalman Filter for Cyber–Physical Systems Against Aensor Attacks," Automatica, vol.95, Jun. 2018, pp. 399-412, doi:10.1016/j.automatica.2018.06.010.

[8] D. Ding, Q.-L. Han, Z. Wang and X. Ge," A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Informatics, vol.15, May. 2019, pp. 2483-2499, doi:10.1109/tii.2019.2905295.

[9] J.X. Feng, Z.D. Wang and M. Zeng," Distributed Weighted Robust Kalman Filter Fusion for Uncertain Systems with Autocorrelated and Cross-Correlated noises," Information Fusion, vol.14, Dec. 2013, pp. 78-86, doi:10.1016/j.inffus.2011.09.004.

[10] Y. Chen, Z. Wang, Y. Yuan and P. Date," Distributed Hinfinity Filtering for Switched Stochastic Delayed Systems Over Sensor Networks With Fading Measurements," IEEE Trans Cybern, vol.50, Jun. 2020, pp. 2-14, doi:10.1109/TCYB.2018.2852290.

[11] Y.Q. Luo, Z.D. Wang, Y. Chen and X.J. Yi," Hinfinity State Estimation for Coupled Stochastic Complex Networks With Periodical Communication Protocol and Intermittent Nonlinearity Switching," IEEE Transactions on Network Science and Engineering, vol.8, Jun. 2021, pp. 1414-1425, doi:10.1109/tnse.2021.3058220.

[12] D.R. Ding, Z.D. Wang and Q.L. Han," A Set-Membership Approach to Event-Triggered Filtering for General Nonlinear Systems Over Sensor Networks," IEEE Transactions on Automatic Control, vol.65, Apr. 2020, pp. 1792-1799, doi:10.1109/tac.2019.2934389.

[13] L. Gao, S.J. Deng and W. Ren," Differentially Private Consensus With an Event-Triggered Mechanism," IEEE Transactions on Control of Network Systems, vol.6, Mar. 2019, pp. 60-71, doi:10.1109/tcns.2018.2795703.

[14] L.N. Jerome and M. Meisam," Differentially Private MIMO Filtering for Event Streams," IEEE Transactions on Automatic Control, vol.63, Jan. 2018, pp. 145-157, doi:10.1109/tac.2017.2713643.

[15] A.J. Wang, X.F. Liao and H.B. He," Event-Triggered Differentially Private Average Consensus for Multi-Agent Network," IEEE/CAA Journal of Automatica Sinica, vol.6, Jan. 2019, pp. 75-83, doi:10.1109/jas.2019.1911327.

[16] Y.S. Tan, M.H. Xiong, B.Y. Zhang and S.M. Fei," Adaptive Event-Triggered Nonfragile State Estimation for Fractional-Order Complex Networked Systems With Cyber Attacks," IEEE Transactions on Systems, Man, and Cybernetics: Systems, May. 2021, pp. 1-13, doi:10.1109/tsmc.2021.3049231.

[17] Z. Huang, S. Mitra and G. Dullerud," Differentially Private Iterative Synchronous Consensus," Proceedings of the 2012 ACM workshop on Privacy in the electronic society, vol.12, Oct. 2012, pp. 81-90, doi:10.11452381966.2381978.

[18] L. Zou, Z.D. Wang, H. Geng and X.H. Liu," Set-Membership Filtering Subject to Impulsive Measurement Outliers: A Recursive Algorithm," IEEE/CAA Journal of Automatica Sinica, vol.8, Feb. 2021, pp. 377-388, doi:10.1109/jas.2021.1003826.