Distributed Privacy-Preserving Data Aggregation Against Dishonest Nodes in Network Systems

Jianping He, *Member, IEEE*, Lin Cai, *Senior Member, IEEE*, Peng Cheng, *Member, IEEE*, Jianping Pan, *Senior Member, IEEE*, and Ling Shi, *Senior Member, IEEE*

***Abstract*—Privacy-preserving data aggregation (DA) in network systems, e.g., Internet of Things (IoT), is a challenging problem, considering the dynamic network topology, limited computing capacity, energy supply of IoT devices, etc. The difficulty is exaggerated when there exist dishonest nodes, and how to ensure privacy, accuracy, and robustness of the DA process against dishonest nodes remains an open issue. Different from the widely investigated cryptographic approaches, in this paper, we address this challenging problem by exploiting the distributed consensus technique. To mitigate the pollution from dishonest nodes, we propose an enhanced secure consensus-based DA (E-SCDA) algorithm that allows neighbors to detect dishonest nodes, and derive the error bound when there are undetectable dishonest nodes. We prove the convergence of the E-SCDA and show that the algorithm can preserve the privacy associated to nodes' initial states. Extensive simulations have shown that the proposed algorithm has a high convergence accuracy and low complexity, even when there exist dishonest nodes in the network.**

***Index Terms*—Average consensus, data aggregation (DA), distributed computing, network systems, privacy preservation.**

I. Introduction

DATA aggregation (DA) has many applications in network systems, including Internet of Things (IoT), mobile social networks, crowdsensing, smart metering systems, etc., [1]–[9]. In network systems, DA should be carried out in a distributed way. For instance, in a smart metering system, smart meters collect real-time electricity usages and the aggregated usage in an area that is used by the utility company for various control purposes. In these applications, data are often privacy-sensitive [7]. Achieving accurate DA while preserving privacy is essential but challenging, due to the dynamics in network topology, limited node computing capacity, communication errors, losses, delays, etc.

To achieve privacy-preserving DA in network systems, typical solutions often rely on various cryptographic techniques, which require either secure communication channels, pre-established shared secret/keys, a trusted authority, or the combination of them. The computation complexity of them is high, so applying encryption/decryption for data exchange can be very expensive, not desirable for large-scale IoT networks. Without solely relying on cryptography techniques, distributed privacy-preserving DA can be achieved using privacy-preserving average consensus algorithms.

Several privacy preserving average consensus algorithms have been proposed in [10]–[17]. The basic idea is adding random noises to the traditional average consensus algorithm to preserve the privacy, and then carefully design the noise adding process, such that the average consensus is achieved. For example, Huang *et al.* [14] used independent and exponentially decaying Laplacian noises to the consensus process. The algorithm can ensure differential privacy while cannot guarantee the average consensus (DA may not converge to the average). The algorithm was optimized by Nozari *et al.* [10]. With a linear Laplacian-based consensus algorithm, it guarantees that the average consensus can be achieved almost surely with differential privacy preservation. Manitara and Hadjicostis [11] first added correlated noises to the consensus process, and [15] proved that using exponentially decaying and zero-sum correlated normal noises can ensure the average consensus in the mean-square sense. Recently, [22] proved that an exactly average consensus can be achieved definitely while the privacy is preserved, if the added correlated noises are bounded, decaying, and zero-sum.

However, these existing solutions depend on the assumption that all the nodes will follow the rules designed in the algorithms and there are no selfish/dishonest nodes in network systems. In fact, if some nodes in network systems are selfish or even dishonest, they may manipulate their data to better protect their own privacy and interest, while the aggregation results will be polluted by the manipulation. Considering these selfish and dishonest nodes, the performance of many existing privacy-preserving DA solutions will be degraded and even lose efficiency. This motivates us to investigate the distributed privacy-preserving DA against the dishonest nodes in network systems. The main contributions are summarized as follows.

Manuscript received February 3, 2018; revised April 13, 2018; accepted May 3, 2018. Date of publication May 9, 2018; date of current version May 8, 2019. This work was supported in part by the Natural Science Foundation of China under Grant 61773257, Grant 61761136012, and Grant 61473251 and in part by the Natural Sciences and Engineering Research Council of Canada. The work of L. Shi was supported under the HKUST Caltech Partnership FP009. *(Corresponding author: Lin Cai.)*

J. He is with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China, and also with the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: jphe@sjtu.edu.cn).

L. Cai and J. Pan are with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada (e-mail: cai@ece.uvic.ca; pan@uvic.ca).

P. Cheng is with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 314400, China (e-mail: pcheng@iipc.zju.edu.cn).

L. Shi is with the Department of Electrical and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong (e-mail: eesling@ust.hk).

Digital Object Identifier 10.1109/JIOT.2018.2834544

1) To the best of our knowledge, this is the first work to investigate the distributed privacy-preserving DA for network systems with dishonest nodes.
2) We propose the neighbor nodes monitoring and dimension expansion mechanisms, and use them to design an enhanced secure consensus-based DA (E-SCDA) algorithm to achieve accurate and privacy-preserving DA.
3) We prove the convergence of the proposed E-SCDA algorithm, and derive the error bound between the achieved consensus and the average, and show that the privacy of nodes' initial states can be preserved by the proposed algorithm.

The remainder of this paper is organized as follows. After the related work in Section II, System model and problem formulation are presented in Section III. E-SCDA is proposed and analyzed in Section IV. Simulation is presented in Section V followed by concluding remarks and further research issues in Section VI.

II. Related Work

Great efforts have been devoted to investigating privacy-preserving DA for sensor networks [2]–[5], [24]–[26], smart grid [6]–[9], [29], [30], and cloud computing [31]–[33].

Privacy-preserving DA has been addressed using different cryptographic techniques. For example, secure multiparty computation was used to collaboratively compute the aggregation with privacy preservation in [8]. Considering a dishonest-but-nonintrusive adversary, a modulo addition-based encryption scheme was adopted in [29] to design differential privacy-preserving aggregation for smart metering systems. In [2], two schemes were proposed using the Shamir secret sharing and secret splitting technique for privacy-preserving additive aggregations. Meanwhile, cryptographic schemes can also be combined with differential privacy techniques for sensitive DAs. Dwork *et al.* [27] designed a distributed random noise generation protocol aiming at a distributed implementation of privacy-preserving statistical databases. Shi *et al.* [28] proposed a novel solution where a trusted aggregator can obtain desired statistics over participants' data, without compromising each individual's privacy. These protocols rely on a verifiable secret sharing scheme so secure channels and a fixed topology are required for the key allocation. Moreover, cryptographic techniques often have high computation complexity.

Recently, how to preserve privacy in dynamical systems has been investigated using advanced signal processing and modern control solutions, e.g., using private filters [23], or private consensus [12]–[15]. The idea is to add noise to the data to protect the privacy. For example, [23] designed the private filters for dynamical systems by adding white Gaussian perturbations. An independent and exponentially decaying Laplacian noises are used to the consensus computation such that consensus can be achieved with privacy preserved [14]; however, this algorithm does not guarantee the exact average consensus convergence. PPAC algorithm was proposed in [15], in which an average consensus is achieved in expectation, i.e., the mean square convergence is provable. In [22], we have shown that adding bounded, exponentially decaying and zero-sum noises can guarantee an exactly average consensus, and introduced the consensus-based privacy-preserving DA algorithm followed by the convergence and privacy analysis. Inspired by these works, this paper designs a privacy-preserving average consensus algorithm which guarantees the accurate privacy-preserving DA, and more importantly, we consider more complex but realistic scenarios where dishonest nodes exist in networks.

III. System Model and Problem Formulation

A. System Model

We consider a network system where nodes are self-organized into several clusters (e.g., using a clustering algorithm [18]). We focus on one connected cluster with n nodes. We need to aggregate the data from the nodes in the cluster, while the data of each node should not be revealed to any other nodes (including the aggregator). The aggregator can poll any node to acquire the aggregated data.

To construct an overlay network, two nodes can select each other as neighbors to exchange data with a logical link (a single-hop or multihop communication path) between them. We then model the overlay network as an undirected graph, $G = (V, E)$, where V is the set of nodes and E is the set of logical links (edges). Define N_i the neighbor set of node i, where $j \in N_i$ iff $(j, i) \in E$. The logic links are negotiated in a distributed way, and thus node i knows its neighbor set N_i, but does not know the full topology of the overlay network. However, we suppose that the whole network topology is available to the aggregator.[1] Let $x_i(0)$ be the initial state of node i, which is privacy-sensitive. $\mathbf{N}^+$ is the set of positive integers. Let $\|\mathbf{x}\|_\infty = \max\{|x_i|\}$.

In network systems, the initial state usually denotes each node's sensitive information (e.g., age, location, income, etc.), which may compromise the privacy. But the aggregated data only reflects the statistics of all nodes' states (e.g., their average, sum, and variance), which will not release the privacy of each individual node directly if the number of the nodes in the network is sufficiently large. Consider the example that the smart meters collect real-time electricity usages and the usage in an area is aggregated by the utility company for various control purposes. In this example, the electricity usage of each user is the privacy information, while the total usage in an area is not. Thus, this paper focuses on the preservation of the privacy of nodes' initial states.

B. Problem Formulation

In this paper, we study how to obtain the additive aggregation, i.e., $\sum_{i=1}^{n} x_i(0)$. The main design objectives are listed below. First, the aggregation goal should be achieved in a fully distributed way. Second, due to the privacy concerns, the initial

[1] It is a reasonable assumption in the targeted application scenario, such as in the smart grid system, that customers are willing to tell their communication topology but keep their realtime power usage secret to the power control center due to the privacy concern.

state of each node should not be known to others (including its neighbors and the aggregator), while the aggregation should be accurate. Third, the computation and communication cost should be minimized. Lastly, there are dishonest nodes in the system, and thus distributed safeguard mechanisms are needed to fast detect the suspicious behaviors and bound the error in the aggregation caused by the undetectable dishonest behaviors. From [22], the sum can be obtained by multiplying the average of the initial states by n, where the number of nodes, n, is known. If dishonest nodes do not exist, a privacy-preserving average consensus algorithm can be used to achieve the first three objectives. Thus, this paper is aiming to solve the problem focusing on the last design objective.

We first introduce the general privacy-preserving average consensus. To preserve privacy, each node will add a noise to its current state for each time of communication, i.e., each node will broadcast

$$x_i^+(k) = x_i(k) + \theta_i(k), i \in V \tag{1}$$

to its neighbor nodes, where $x_i(k)$ is the state of node i at iteration k, and θ_i is the noise to be added for privacy preservation. θ_i is a continuous random variable, and node i can set the distribution independently. The averaging process is updated by

$$x_i(k+1) = w_{ii}x_i^+(k) + \sum_{j \in N_i} w_{ij}x_j^+(k),\ \ i \in V;\ \ i \in V \tag{2}$$

where w_{ij}'s are the Metropolis weights [20]

$$w_{ij} = \begin{cases} 1/\big[1 + \max\{|N_i|,\ |N_j|\}\big], & j \in N_i \\ 1 - \sum_{l \in N_i} w_{il}, & i = j \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

These weights can be obtained in a distributed manner. The matrix form of (2) is given by

$$\mathbf{x}(k+1) = W(\mathbf{x}(k) + \theta(k)) \tag{4}$$

where $\mathbf{x},\ \theta \in R^n$, $W \in R^{n\times n}$, satisfying $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ and $\theta = [\theta_1, \theta_2, \ldots, \theta_n]^T$, and $W = [w_{ij}]_{n\times n}$. Equation (4) is named as the general privacy-preserving average consensus algorithm.

If $\theta(k) = 0$, the exact average consensus is achieved exponentially since W is doubly stochastic [19]–[21], i.e.,

$$\lim_{k\to\infty} x_i(k) = \bar{x}, i \in V \tag{5}$$

exponentially fast, where $\bar{x} = (1/n)\sum_{i\in V} x_i(0)$. However, to preserve privacy, the noise cannot be zero. To achieve the exact average consensus, $\theta(k)$ must be carefully designed. As proved in [22] that adding bounded, exponentially decaying, and zero-sum correlated noises can guarantee an exact average consensus definitely by (4). Unfortunately, dishonest nodes may add the noise freely, and thus can break the convergence and degrade the performance easily if without any safeguard mechanism. For example, a dishonest node can always select a positive noise at each iteration such that the consensus cannot be achieved. How to guarantee the accurate and private average consensus when there are dishonest nodes in network systems is an open issue. To solve it, we design the algorithm with the detailed theoretical analysis in the following section.

IV. DA Against Dishonest Nodes

In this section, we design an E-SCDA algorithm to deal with malfunctioning, selfish, or dishonest nodes whose data may pollute the aggregation.

The challenge is that we need to preserve privacy while monitoring whether or not nodes are misbehaving. We use two key designs to address this difficult problem. First, using the idea of dimension expansion, the initial state of each node can be divided into two parts and they will be sent with added noises to two neighbor sets. This procedure introduces additional noises to the initial state for privacy preservation. Second, we design guidelines for nodes to monitor their neighbors to identify any misconduct. To achieve it, we design a monitoring process as a safeguard mechanism, which constrains the dishonest nodes for ensuring the accuracy of aggregation. The detailed procedure is described below.

A. Dimension Expansion

First, the initial state of each node i is divided into two parts, given by

$$x_i^1(0) = \frac{1}{2}x_i(0) + \vartheta_i \tag{6}$$

and

$$x_i^2(0) = \frac{1}{2}x_i(0) - \vartheta_i \tag{7}$$

respectively, where ϑ_i is a random variable selected from $[-(\alpha/2)\rho, (\alpha/2)\rho]$, and $0 < \rho < 1$. Clearly, we have $x_i(0) = x_i^1(0) + x_i^2(0)$. The aggregator divides the graph $G = (V, E)$ into two undirected and connected subgraphs, denoted by $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, respectively, where $E_1, E_2 \subset E$ ($E_1 \cap E_2 = \emptyset$ and $E_1 \cup E_2 = E$ cannot be true). Define the neighbor node set N_i^ν of node i, where $j \in N_i^\nu$ iff $(j, i) \in E_\nu$ and $\nu = 1, 2$. For $\nu = 1, 2$, the aggregator will let each node know the information of N_i^ν, and then nodes will calculate the corresponding weights $w_{ij}^\nu, j \in N_i^\nu$, using (3). Then, each node will transmit $x_i^{1+}(k)$ and $x_i^{2+}(k)$ to its neighbor nodes who are in N_i^1 and N_i^2, respectively, for iteratively average updating, where

$$x_i^{\nu+}(k) = x_i^\nu(k) + \theta_i^\nu(k), \nu = 1, 2 \tag{8}$$

for $i \in V$. Let $\hat{x}_i(0)$ be the estimation of $x_i(0)$ by the aggregator for $i \in V$. It is assumed that $|\hat{x}_i(0) - x_i(0)| \le E_x$, where E_x is the estimation or prediction error bound of the initial state and is assumed to be only known by the neighbors or the aggregator. Define two information sets, $I_i^\nu(k)$, of every node i for $\nu = 1, 2$ as

$$I_i^\nu(k) = \Big\{\nu, d_i^\nu, d_j^\nu, \hat{x}_i(0), E_x, x_i^{\nu+}(k), x_j^{\nu+}(k) : j \in N_i^\nu\Big\}$$

for $k = 0$ or $k \in \mathbf{N}^+$, where d_i^ν (d_j^ν) is the number of neighbor nodes in N_i^ν (N_j^ν), which is used in the information monitoring process described below.

The monitoring process is to detect and constrain the dishonest nodes. Assume that the aggregator can randomly select some nodes, namely selected nodes, in each cluster to monitor their neighbor nodes, where the selected nodes are assumed to

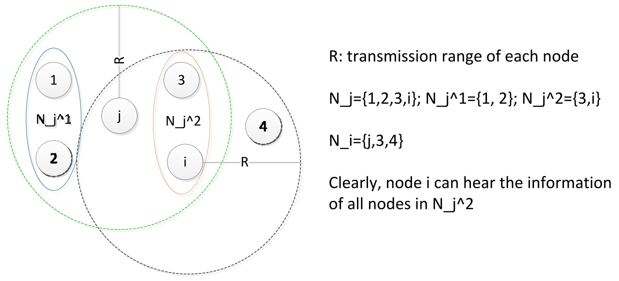

R
1
2
N_j^1
j
3
N_j^2
i
4
R
R: transmission range of each node
N_j={1,2,3,i}; N_j^1={1, 2}; N_j^2={3,i}
N_i={j,3,4}
Clearly, node i can hear the information of all nodes in N_j^2

Fig. 1. Example for illustration, where node i is the selected node.

overhear the information transmitted to the nodes they monitor [which guarantees that the information $x_l^{\nu+}(k), x_j^{\nu+}(k) : l \in N_j^\nu$ can be listened by the selected node i]. So long as $N_i \supseteq N_j^\nu$ for $\nu = 1$ or $\nu = 2$, node i can hear all the broadcast information of node in N_j^ν. This is easy to be realized in real networks, and an example is given in Fig. 1. As shown in the figure, for the wireless network with the transmission range of R, node i can receive the information of nodes in N_j^2, and it cannot overhear the communications from nodes in N_j^1 (e.g., nodes 1 and 2). Furthermore, even if node i can hear all the communications between j and its neighbor nodes, so long as node i does not have $I_j^1(k)$, it cannot derive $x_j^1(0)$. Therefore, we do not require any cryptography when nodes send their messages to their neighbors to protect privacy, which is indeed an important advantage of our solution.

Then, the aggregator just needs to send the information of ν, d_l^ν, d_j^ν, and N_j^ν (the topology information only) to the selected node only, and it can guarantee that the selected nodes have the knowledge of $I_j^\nu(k)$ for $\nu = 1$ or $\nu = 2$. We thus assume that one of the information sets $I_j^\nu(k)$ (it should be noticed that not both here) is available to one selected node i for $\nu = 1$ or $\nu = 2$. That is, node i can have the full knowledge of the information used for one part of state update of node j, and how node j updates this part at each iteration, i.e., the $x_j^\nu(k)$ is available to node i for $k \in \mathbf{N}^+$, where $\nu = 1$ or $\nu = 2$. The details of the monitoring checking process are given as follows.

B. Neighbor Monitoring

The aggregator can request a neighbor node to monitor a node at a random time instant. Once receiving such a request, a neighbor node i of node j checks the following three conditions based on the available information set, $I_j^\nu(k)$, for $\nu = 1$ or $\nu = 2$ and $k = 0$ or $k \in \mathbf{N}^+$.

c_1: $|\theta_j^\nu(k)| \le (1/2)\alpha\rho^k$, where $\theta_j^\nu(k)$ is calculated by

$$\theta_j^\nu(k) = x_j^{\nu+}(k) - \left[w_{jj}^\nu x_j^\nu + (k-1) + \sum_{l \in N_j^\nu} w_{jl}^\nu x_l^{\nu+}(k-1) \right] \tag{9}$$

and w_{jl}^ν is calculated from (3) for $k \in \mathbf{N}^+$.

c_2: $|x_j^+(0) - \hat{x}_j(0)| \le E_x + (1/2)\alpha\rho$.

c_3: $|(x_j^+(0)/2) - x_j^{\nu+}(0)| \le (5/4)\alpha\rho$.

If conditions c_1, c_2, and c_3 hold, then node j is credible. Otherwise, node j will be viewed as a dishonest node which will be reported to the aggregator, and then node j will be isolated so that its data will not pollute the aggregation.

In the above process, c_1 is used to guarantee that the update in each iteration is an averaging process and the added noise is exponentially decaying, c_2 ensures that the initial states of dishonest nodes are bounded by the estimation error, which constrains the initial state selection of each dishonest node, and c_3 is utilized to ensure that two parts dividing the initial states of nodes follow the rules of (6) and (7). Note that based on (6) and (7), one node has

$$\begin{aligned}\left|\frac{x_j^+(0)}{2} - x_j^{\nu+}(0)\right| &\le \left|\frac{x_j(0)}{2} + \frac{\theta_j(0)}{2} - \frac{x_j(0)}{2} \pm \vartheta_j - \theta_j^\nu(0)\Big)\right| \\ &\le \left|\frac{\theta_j(0)}{2} \pm \vartheta_j - \theta_j^\nu(0)\Big)\right| \le \frac{5}{4}\alpha\rho\end{aligned}$$

i.e., they can satisfy c_3. The aggregator only knows the global topology information but does not know the states of nodes, which can preserve the state privacy to the aggregator. If the aggregator checks c_1–c_3 himself, the communication costs will be high as the aggregator needs to collect much more additional information from nodes through longer routing paths of these data.

C. E-SCDA Algorithm

Given the monitoring process, we need to ensure that the dishonest node who arbitrarily selects the values of its noise process can be detectable. We then have the E-SCDA algorithm as in Algorithm 1.

In the above algorithm, the Max_Iteration_Number in step 7 is given initially. We can simply let Max_Iteration _Number equal n^2, which is sufficiently large to guarantee an accurate aggregation. Also, we can set $|x_i(k) - x_j(k)| \le \varepsilon$ for $\forall j \in N_i$, where ε is a small positive constant, as the condition to terminate the iteration. For E-SCDA, the two neighbor sets of each node are the input, and the output is the nodes updated states. Clearly, if a node follows steps 9–12, c_1–c_3 can be satisfied obviously, and thus the honest nodes can pass the monitoring process.

D. Convergence, Accuracy, and Privacy Analysis

We first analyze the constraint on dishonest nodes using E-SCDA. Then, we reveal the maximum pollution from the dishonest nodes under the constraints. Last, we provide the privacy analysis of E-SCDA.

Let $x_i(0)$ be the true initial state of a dishonest node i. Assume that the dishonest node i uses $\tilde{x}_i(0)$ instead of $x_i(0)$ in the calculation of $x_i^+(0)$ and $x_i^{\nu+}(0)$, i.e., $\tilde{x}_i(0)$ is the false initial state satisfying $|\tilde{x}_i(0) - x_i^+(0)| \le (1/2)\alpha\rho$, and $\tilde{x}_i^\nu(0)$ is one part of the false initial state, satisfying $|\tilde{x}_i^\nu(0) - x_i^{\nu+}(0)| \le (1/2)\alpha\rho$ for $\nu = 1, 2$. We have the following theorem.

Theorem 1: Given the monitoring process using c_1–c_3, for each dishonest node i to be undetectable, it should have

$$|\tilde{x}_i(0) - x_i(0)| \ \le 2E_x + \alpha\rho \tag{12}$$

and

$$\left|\tilde{x}_i^\nu(0) - \frac{\tilde{x}_i(0)}{2}\right| \le 2\alpha\rho, \ \ \nu = 1, 2. \tag{13}$$

The proof of Theorem 1 is given in Appendix A. This theorem implies that the dishonest nodes cannot arbitrarily select false initial states since they are bounded by (12) and (13).

Algorithm 1 E-SCDA Algorithm

```
Generate random vectors $\theta_i(0), \vartheta_i, \theta_i^1(0)$ and $\theta_i^2(0)$ where all the elements are randomly selected from $[-\frac{\alpha}{2}\rho, \frac{\alpha}{2}\rho]$.
Set $x_i^1(0)$ and $x_i^2(0)$ using (6) and (7), respectively.
Set $x_i^+(0)$ and $x_i^{\nu+}(0)$ using (1) and (8), respectively, and transmit them to the corresponding neighbors, while $x_i^+(0)$ is transmitted to nodes in $N_i^1 \cup N_i^2$.
If node $i$ is selected by the aggregator to monitor neighbor node $j$, it will obtain the information $\nu, d_l^\nu, d_j^\nu, N_j^\nu$ from the aggregator for $\nu = 1$ or $\nu = 2$ and $l \in N_j^\nu$.
Set $\delta_i^\nu(0) = \theta_i^\nu(0)$.
Set k=1.
while $k <$ Max_Iteration_Number do
    When node $i$ is a selected node, it uses the received $x_j^\nu(k-1)$ and the information set $I_j^\nu(k-1)$ to monitor whether node $j$'s behavior satisfies $c_1$–$c_3$. If not, report to the aggregator to isolate node $j$ from the cluster.
    Update $x_i^\nu(k)$ by using the following equation,
        $x_i^\nu(k) = w_{ii}^\nu x_i^\nu + (k-1) + \sum_{l \in N_i^\nu} w_{il}^\nu x_l^{\nu+}(k-1).$
    Set $x_i(k) = x_i^1(k) + x_i^2(k)$.
    Select $\delta_i^\nu(k)$ randomly according to
        $|\delta_i^\nu(k)| \leq \frac{\alpha}{2}\rho^{k+1}$    (10)
    for $k \geq 1$ and $\nu = 1, 2$.
    Set $\theta_i^\nu(k)$ by
        $\theta_i^\nu(k) = \delta_i^\nu(k) - \delta_i^\nu(k-1)$    (11)
    Set $x_i^{\nu+}(k)$ using (8) and transmit $x_i^{\nu+}(k)$ and $\nu$ to the corresponding neighbors.
    Set k=k+1.
end while
```

Then, the following theorem proves the convergence of E-SCDA and the accuracy of the aggregation.

Theorem 2: Suppose that the number of the dishonest nodes in a cluster is d. With the E-SCDA algorithm

$$\lim_{k \to \infty} x_i(k) = C, i \in V \tag{14}$$

and

$$|C - \bar{x}| \leq \frac{d\left[5\alpha\rho + 2E_x + \frac{\alpha\rho}{(1-\rho)}\right]}{n} \tag{15}$$

where C is a constant.

The proof of Theorem 2 is given in Appendix B. From this theorem, we have that E-SCDA achieves consensus, and the error between the consensus and the average is bounded by (15). Clearly, if the number of the dishonest nodes is larger, the error may become larger. Specifically, if there is no dishonest node, i.e., $d = 0$, from (15) the error bound is 0. This implies that an average consensus is achieved by E-SCDA. When the number of dishonest nodes is fixed, the accuracy of the aggregation depends on the parameters, α, ρ and E_x. Setting a small $\alpha\rho$ can enhance the accuracy of the aggregation, while reducing the privacy of $x_i(0)$. Increasing the accuracy of E_x can also enhance the aggregation accuracy.

With E-SCDA, dishonest nodes cannot know who are monitoring them and when, since the selected nodes for monitoring are chosen by the aggregator randomly. Hence, to be undetectable, the noise process used for the dishonest nodes should satisfies c_1–c_3, and thus the error due to their pollution can be bounded.

Then, for the node who is monitoring node i, since it has the full information used for partial state update [i.e., $x_i^\nu(k)$, where $\nu = 1$ or $\nu = 2$], it may infer the corresponding initial state [i.e., $x_i^1(0)$ or $x_i^2(0)$ only]. However, since there is a random noise ϑ_i^ν in each part of the initial state, the monitoring node still cannot infer the exact value of $x_i(0)$.

Before given the detailed privacy analysis, we define the optimal estimation as follows.

Definition 1: Let $\mathcal{X}_j$ be the set of the possible values of $x_j(0)$ and $\mathcal{I}_i^{\text{out}}$ be the information outputs of node j. Then, the optimal estimation of $x_j(0)$ is defined by

$$\hat{x}_j^* = \arg\max_{\hat{x}_j \in \mathcal{X}_j} f\left(\mathcal{I}_j^{\text{out}} \mid \hat{x}_j\right), i \in V$$

where $f(\cdot)$ is the PDF of the information outputs.

In the above definition, since the $\mathcal{I}_j^{\text{out}}$ is random, $\hat{x}_j^*$ is a random variable. We use the disclosure probability that the initial state $x_j(0)$ can be successfully estimated by its neighbor nodes using the optimal estimation in a given estimation accuracy ϵ (a small positive constant), to denote the degree of the privacy protection. When a node makes the inference, it usually sets a conservative $\mathcal{X}_j$ to ensure that the real state $x_j(0)$ is in the set of $\mathcal{X}_j$ [i.e., $x_j(0) \in \mathcal{X}_j$]. We then assume that $||x_j(0) - \mathcal{X}_j||_\infty \geq \alpha\rho$. If this is not true, the attack node estimates $x_j(0)$ directly without using the information outputs so that the noise adding process is useless for privacy protection. Especially, when there is no previous knowledge of $\mathcal{X}_j$, we set $\mathcal{X}_j = \mathcal{R}$. We assume each privacy attacker cannot collude with other nodes to attack. Then, we have the following theorem.

Theorem 3: With the E-SCDA algorithm, the disclosure probability under a given estimation accuracy ϵ, denoted by $\Pr\{|\hat{x}_j^* - x_j(0)| \leq \epsilon\}$, satisfies

$$\Pr\left\{\left|\hat{x}_j^* - x_j(0)\right| \leq \epsilon\right\} \leq \max_{\ell=0}^{3} \max_{z \in [-2\alpha\rho, 2\alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_\ell(y) \, \mathrm{d}y$$

where $f_1^\nu(y)$ ($\nu = 1$ or 2), $f_2(y)$ and $f_3(y)$ are the PDFs of $2(\theta_j^\nu(0) \pm \vartheta_j)$, $\theta_j^1(0) + \theta_j^2(0)$ and $2\vartheta_j$, respectively, $f_0(y) = f_1^1(y)$ and $f_1(y) = f_1^2(y)$.

The proof of Theorem 3 is given in Appendix C. Therefore, E-SCDA can preserve privacy while enabling the capability of detecting dishonest nodes, and further bound the error due to the undetectable dishonest behavior.

V. Performance Evaluation

In this section, simulations are conducted to evaluate the performance of the proposed algorithm E-SCDA.

A. Simulation Setup

In the simulation, there are 100 nodes randomly deployed over a 1000 × 1000 m^2 square area, where the communication range of each node is 300 m. We set $\alpha = 5$ and $\rho = 0.4$. Define the maximum difference between nodes' states by

$$V(\mathbf{x}(k)) = \max_{i,j \in \mathcal{V}} \left|x_i(k) - x_j(k)\right|.$$

Clearly, a consensus is achieved if $V(\mathbf{x}) = 0$.

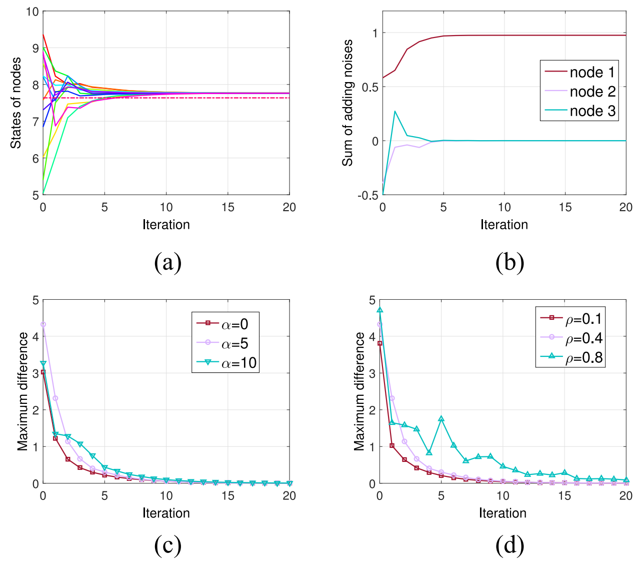


Fig. 2. Performance of E-SCDA. (a) Average consensus. (b) Sum of noises. (c) Different α. (d) Different ρ.

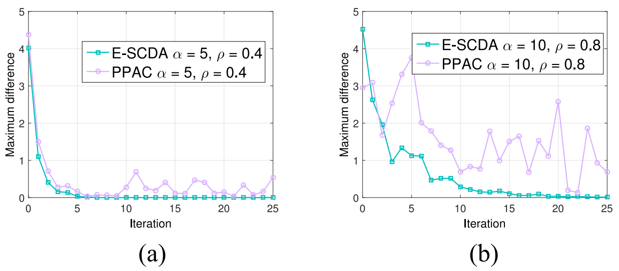


Fig. 3. Comparisons between algorithms. (a) and (b) E-SCDA and PPAC.

B. Evaluation of E-SCDA

We evaluate the performance of the E-SCDA algorithm. There are 5% dishonest nodes, and the elements in $\theta_i(k)$ used for dishonest node i are randomly selected from $[0, \alpha\rho^k]$, and $E_x = 2$. It is observed from Fig. 2(a) that all states exponentially converge to a constant state, i.e., a consensus is achieved, while it may not be equal to the true average due to the pollution introduced by the dishonest nodes.

As shown in Fig. 2(b), the sum of $\theta(k)$ used for the dishonest nodes does not converge to 0, where node 1 is dishonest. This is the main reason why the consensus is not fully accurate. The gap between the consensus achieved by E-SCDA and the average consensus is small, which is bounded by (15), e.g., the gap is lower than 0.1 in Fig. 2(b).

We also vary the values of α and ρ to study the convergence of E-SCDA. The results are shown in Fig. 2(c) and (d), respectively. It is observed that the convergence rate is affected slightly when α changes as the maximum difference is still less than 10^{-4} within 20 iterations. With a larger ρ, e.g., $\rho = 0.8$ in Fig. 2(d), the convergence rate may decrease, as the dishonest nodes have a higher freedom to introduce undetectable pollution. Since the privacy and accuracy depend on $\alpha\rho$, we can set a large α and a small ρ to ensure a fast convergence rate while guaranteeing the accuracy.

Second, we compare our algorithm with PPAC [15]. The mean and variance of the normal distribution noises used in PPAC are set to 0 and $\alpha\rho$, respectively, and the decaying factor $\varphi = \rho$. For a fair comparison, we use the same noise distribution for honest nodes in E-SCDA, and the noises will be regenerated when they exceed the decaying bound. The comparison is shown in Fig. 3. It is observed that E-SCDA and PPAC have similar convergence speed while PPAC cannot fully converge, especially when α and ρ are large. This is because unlike E-SCDA, the dishonest nodes use the normal distribution random variables as the added noises and set $\varphi = 1$ for PPAC, i.e., PPAC is more vulnerable. We also compare our algorithm with that proposed in [22]. A very similar result as shown in Fig. 3 was obtained. The main reason is that both of the existing algorithms add decaying and zero-sum noises to the traditional average consensus process but do not consider the presents of the dishonest nodes.

VI. Conclusion

In this paper, we have investigated the distributed privacy-preserving DA against dishonest nodes in network systems using the average consensus technique. Considering the scenario that dishonest nodes may pollute the aggregation, we designed the E-SCDA algorithm that adopts a neighbor monitoring process to detect misbehaving nodes, and derived the error bounds due to undetectable dishonest behaviors. Simulation results have shown that the proposed algorithm has a fast convergence rate and high accuracy, and they are robust against network dynamics and dishonest nodes. To the best of our knowledge, this is the first privacy-preserving DA solution to have such robustness and ensure bounded error with the presence of dishonest nodes.

There are still many open issues worth further investigation. First, the overlay network should be a connected, undirected graph. Second, in E-SCDA, the aggregator should have the knowledge of the topology of the overlay network, and how to relax these requirements requires further investigation. A possible direction is to design an incentive mechanism such that all nodes are willing to be honest so as to achieve an accurate privacy-preserving aggregation at a lower cost.

Appendix A
Proof of Theorem 1

We first prove (12). Note that

$$\begin{aligned}|\tilde{x}_i(0) - x_i(0)| &= \big|\tilde{x}_i(0) - x_i^+(0) + x_i^+(0) - \hat{x}_i(0) \\ &\quad + \hat{x}_i(0) - x_i(0)\big| \\ &\le \big|\tilde{x}_i(0) - x_i^+(0)\big| + \big|x_i^+(0) - \hat{x}_i(0)\big| \\ &\quad + \big|\hat{x}_i(0) - x_i(0)\big| \\ &\le 2E_x + \alpha\rho \qquad (16)\end{aligned}$$

where we have used the conditions c_2, $|\tilde{x}_i(0) - x_i^+(0)| \le \alpha\rho$, and $|\hat{x}_i(0) - x_i(0)| \le E_x$.

Next, we prove (13). Note that

$$\begin{aligned}
&\left|\tilde{x}_i^\nu(0) - \frac{\tilde{x}_i(0)}{2}\right| \\
&= \left|\tilde{x}_i^\nu(0) - x_i^{\nu+}(0) + x_i^{\nu+}(0) - \frac{x_i^+(0)}{2} + \frac{x_i^+(0)}{2} - \frac{\tilde{x}_i(0)}{2}\right| \\
&\le \left|\tilde{x}_i^\nu(0) - x_i^{\nu+}(0)\right| + \left|x_i^{\nu+}(0) - \frac{x_i^+(0)}{2}\right| \\
&\quad + \left|\frac{x_i^+(0)}{2} - \frac{\tilde{x}_i(0)}{2}\right| \\
&\le \frac{3}{4}\alpha\rho + \left|x_i^{\nu+}(0) - \frac{x_i^+(0)}{2}\right|
\end{aligned} \tag{17}$$

for $\nu = 1, 2$ where we have used the conditions $|\tilde{x}_i^\nu(0) - x_i^{\nu+}(0)| \le [(\alpha\rho)/2]$ and $|\tilde{x}_i(0) - x_i^+(0)| \le \alpha[(\alpha\rho)/2]$. Then, from condition c_3, we have

$$\left|\tilde{x}_i^\nu(0) - \frac{\tilde{x}_i(0)}{2}\right| \le \frac{3}{4}\alpha\rho + \frac{5}{4}\alpha\rho \le 2\alpha\rho$$

for $\nu = 1, 2$. ■

Appendix B
Proof of Theorem 2

According to c_1 in the checking process, one infers that $\theta_i^\nu(k)$ used by dishonest node i should satisfy

$$\left|\theta_i^\nu(k)\right| \le \frac{1}{2}\alpha\rho^k, \quad k \in \mathbf{N}^+, \quad \nu = 1, 2$$

which means that the added noises are exponentially decaying. Then, one infers that there exists

$$\lim_{k\to\infty} x_i^\nu(k) = C^\nu, \quad i \in V; \quad \nu = 1, 2$$

where C^ν is a constant vector. Then, from step 10, we have

$$\lim_{k\to\infty} x_i(k) = \lim_{k\to\infty}\left(x_i^1(k) + x_i^2(k)\right) = C^1 + C^2 = C, \quad i \in V$$

which means that (14) holds.

Since W is still a doubly stochastic matrix, we have $\sum(W\mathbf{x}) = \sum(\mathbf{x})$ for any a vector $\mathbf{x}$. Then, we have

$$\begin{aligned}
\sum\left(\mathbf{x}^\nu(k)\right) &= \sum\left[W\left(\mathbf{x}^\nu(k-1) + \theta^\nu(k-1)\right)\right] \\
&= \sum\left(\mathbf{x}^\nu(k-1) + \theta^\nu(k-1)\right) \\
&= \sum\left(\mathbf{x}^\nu(0) + \sum_{\ell=0}^{k-1}\theta^\nu(\ell)\right)
\end{aligned} \tag{18}$$

for $\nu = 1, 2$. Note that for each cluster c, the initial state vector used for each honest node, say i, is $x_i^\nu(0)$, and for each dishonest node, say j, is $\tilde{x}_j^\nu(0)$, for $\nu = 1, 2$. And, the added noise process for each honest node i satisfies $\sum_{\ell=0}^{\infty}\theta_i^\nu(\ell) = 0$. Let V^s be the set of honest nodes and V^a be the set of dishonest nodes in each cluster. Then, taking limiting of both sides of (18), we have

$$\begin{aligned}
\lim_{k\to\infty}\sum\left(\mathbf{x}^\nu(k)\right) &= \sum\left(\mathbf{x}^\nu(0) + \sum_{\ell=0}^{\infty}\theta^\nu(\ell)\right) \\
&= \sum_{i\in V^s} x_i^\nu(0) + \sum_{j\in V^a}\tilde{x}_j^\nu(0) + \sum_{j\in V^a}\sum_{\ell=0}^{\infty}\theta_j^\nu(\ell).
\end{aligned} \tag{19}$$

Clearly, we have $\lim_{k\to\infty}\sum(\mathbf{x}^\nu(k)) = nC^\nu$ and $x_i(0) = x_i^1(0) + x_i^2(0)$ for honest nodes. Since the added noise process of every dishonest node is exponentially decaying, one infers that $|\sum_{\ell=0}^{\infty}\theta_j^\nu(\ell))| \le ([\alpha\rho]/[2(1-\rho)])$. Then, from (12) and (13), one follows that:

$$\begin{aligned}
&\left|\sum_{\nu=1}^{2}\sum_{j\in V^a}\tilde{x}_j^\nu(0) - \sum_{j\in V^a} x_j(0)\right| \\
&\le \sum_{j\in V^a}\left|\tilde{x}_j^1(0) + \tilde{x}_j^2(0) - x_j(0)\right| \\
&\le \sum_{j\in V^a}\left(\left|\tilde{x}_j^1(0) - \frac{\tilde{x}_j(0)}{2}\right| + \left|\tilde{x}_j^2(0) - \frac{\tilde{x}_j(0)}{2}\right|\right. \\
&\qquad\qquad \left. + \left|\tilde{x}_j(0) - x_j(0)\right|\right) \\
&\le \sum_{j\in V^a}\left(2\alpha\rho + 2\alpha\rho + 2E_x^j + \alpha\rho\right) \\
&\le d(5\alpha\rho + 2E_x)
\end{aligned} \tag{20}$$

and from (19), one further infers that

$$\begin{aligned}
n\sum_{\nu=1}^{2} C^\nu &= \sum_{\nu=1}^{2}\left[\sum_{i\in V^s} x_i^\nu(0) + \sum_{j\in V^a}\tilde{x}_j^\nu(0) + \sum_{j\in V^a}\sum_{\ell=0}^{\infty}\theta_j^\nu(\ell)\right] \\
&= \sum_{i\in V} x_i(0) + \sum_{j\in V^a}\left[\sum_{\nu=1}^{2}\left(\tilde{x}_j^\nu(0) - x_j^\nu(0)\right) + \sum_{\ell=0}^{\infty}\theta_j^\nu(\ell)\right].
\end{aligned}$$

Since $\sum_{i\in V} x_i(0) = n\bar{x}$ and $\sum_{\nu=1}^{2} C^\nu = C$, from the above equation, it follows that:

$$\begin{aligned}
|n(C-\bar{x})| &= \left|\sum_{j\in V^a}\sum_{\nu=1}^{2}\left[\tilde{x}_j^\nu(0) - x_j^\nu(0) + \sum_{\ell=0}^{\infty}\theta_j^\nu(\ell)\right]\right| \\
&\le \left|\sum_{j\in V^a}\sum_{\nu=1}^{2}\left(\tilde{x}_j^\nu(0) - x_j^\nu(0)\right)\right| + \left|\sum_{j\in V^a}\sum_{\nu=1}^{2}\sum_{\ell=0}^{\infty}\theta_j^\nu(\ell)\right| \\
&\le d(5\alpha\rho + 2E_x) + \sum_{j\in V^a}\sum_{\nu=1}^{2}\sum_{\ell=0}^{\infty}\left|\theta_j^\nu(\ell)\right| \\
&\le d(5\alpha\rho + 2E_x) + d\frac{\alpha\rho}{(1-\rho)} \\
&\le d\left[5\alpha\rho + 2E_x + \frac{\alpha\rho}{(1-\rho)}\right].
\end{aligned} \tag{21}$$

Hence, it follows that:

$$\|C - \bar{x}\|_\infty \le \frac{d\left[5\alpha\rho + 2E_x + \frac{\alpha\rho}{(1-\rho)}\right]}{n}.$$

Therefore, we have completed the proof. ■

Appendix C
Proof of Theorem 3

Based on the different available information set, we analyze the disclosure probability considering the following three cases, respectively.

Case 1: The information set $\mathcal{I}_{ij}^{\nu}(k) = \{x_j^{\nu+}(0), \dots, x_j^{\nu+}(k)\}$, where $\nu = 1$ or $\nu = 2$, is available to node i for estimation, i.e., node i belongs to one of the neighbor set N_j^{ν} (not both). In this case, it holds that

$$x_j(0) = 2\left(x_j^{\nu}(0) \pm \vartheta_j\right). \tag{22}$$

Then, by referring to [22, Th. 3.8], it is observed that the best estimation is made from using the initial information output only, as the later information output embeds more and larger uncertainty to the initial state. Thus, based on the information output $x_j^{\nu+}(0)$ and (22), we obtain

$$\begin{aligned}\hat{x}_j^* &= \arg\max_{\hat{x}_j \in \mathcal{X}_j} f\left(x_j^{\nu+}(0) \mid \hat{x}_j\right) \\ &= 2x_j^{\nu+}(0) - \arg\max f_1^{\nu}(y).\end{aligned}$$

Then we have

$$\Pr\left\{|\hat{x}_j^* - x_j(0)| \le \epsilon\right\} = \max_{z \in [-2\alpha\rho, 2\alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_1^{\nu}(y)\mathrm{d}y. \tag{23}$$

Case 2: Both $\mathcal{I}_{ij}^{1}(k)$ and $\mathcal{I}_{ij}^{2}(k)$ are available to node i for estimation, i.e., node i belongs to both of the neighbor set N_j^{ν} for $\nu = 1, 2$. In this case, except the similar estimation as in case 1, we can still use the following fact for estimation:

$$x_j(0) = x_j^{1+}(0) + x_j^{2+}(0) - \left(\theta_j^1(0) + \theta_j^2(0)\right). \tag{24}$$

Based on the above fact, it infers that

$$\Pr\left\{|\hat{x}_j^* - x_j(0)| \le \epsilon\right\} \le \max_{z \in [-\alpha\rho, \alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_2(y)\mathrm{d}y \tag{25}$$

where $f_2(y)$ is the PDF of $\theta_j^1(0) + \theta_j^2(0)$. Therefore, in this case, we have

$$\Pr\left\{|\hat{x}_j^* - x_j(0)| \le \epsilon\right\} \le \max_{\ell=0}^{2} \max_{z \in [-2\alpha\rho, 2\alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_\ell(y)\mathrm{d}y. \tag{26}$$

Case 3: The information set $I_i^{\nu}(k)$, where $\nu = 1$ or $\nu = 2$, is available to node i for estimation, i.e., node i is one of the selected nodes. In this case, based on $I_i^{\nu}(k)$, we can use (9) to obtain $\theta_j^{\nu}(k)$ for $k \in \mathbf{N}^+$, and then infer $\theta_j^{\nu}(0)$ using the fact that $\sum_{k=0}^{\infty} \theta_j^{\nu}(k) = 0$. It means that $x_j^{\nu}(0)$ is known and available for estimation. Then, with (22), we obtain

$$\Pr\left\{|\hat{x}_j^* - x_j(0)| \le \epsilon\right\} \le \max_{z \in [-\alpha\rho, \alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_3(y)\mathrm{d}y. \tag{27}$$

Also, (26) could hold in this case since both $\mathcal{I}_{ij}^{1}(k)$ and $\mathcal{I}_{ij}^{2}(k)$ may be available to a selected node.

Combine the above three cases, we conclude that

$$\Pr\left\{|\hat{x}_j^* - x_j(0)| \le \epsilon\right\} \le \max_{\ell=0}^{3} \max_{z \in [-2\alpha\rho, 2\alpha\rho]} \int_{z-\epsilon}^{z+\epsilon} f_\ell(y)\mathrm{d}y \tag{28}$$

which completes the proof. ■

Acknowledgment

The authors would like to thank the editor and the anonymous reviewers for their helpful and constructive comments, which have helped us improve this paper significantly.

References

[1] T. Jung *et al.*, "Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2634–2642.

[2] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, 2007, pp. 2045–2053.

[3] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.*, vol. 53, no. 12, pp. 2022–2037, 2009.

[4] J. Shi, R. Zhang, Y. Zhang, and Y. Liu, "PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–6.

[5] M. M. Groat, W. Hey, and S. Forrest, "KIPDA: K-indistinguishable privacy-preserving data aggregation in wireless sensor networks," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 2024–2032.

[6] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, 2014, pp. 504–512.

[7] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 75–86, Mar. 2013.

[8] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1342–1354, Jul. 2013.

[9] H. Li, X. Liang, R. Lu, X. Lin, and X. Shen, "EDR: An efficient demand response scheme for achieving forward secrecy in smart grid," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, 2012, pp. 929–934.

[10] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.

[11] N. E. Manitara and C. N. Hadjicostis, "Privacy-preserving asymptotic average consensus," in *Proc. IEEE ECC*, Zürich, Switzerland, 2013, pp. 760–765.

[12] J. He, L. Cai, and X. Guan, "Optimal state estimation for distributed algorithm with noise adding mechanism," in *Proc. IEEE CDC*, Melbourne, VIC, Australia, 2017, pp. 4135–4140.

[13] X. Wang, J. He, P. Cheng, and J. Chen, "Privacy preserving average consensus with different privacy guarantee," in *Proc. IEEE ACC*, 2018.

[14] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proc. ACM Workshop Privacy Electron. Soc.*, Raleigh, NC, USA, 2012, pp. 81–90.

[15] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[16] P. Braca, R. Lazzeretti, S. Marano, and V. Matta, "Learning with privacy in consensus + obfuscation," *IEEE Signal Process. Lett.*, vol. 23, no. 9, pp. 1174–1178, Sep. 2016.

[17] C. Zhao, J. He, P. Cheng, and J. Chen, "Privacy-preserving consensus-based energy management in smart grid," in *Proc. IEEE PESGM*, Chicago, IL, USA, 2017, pp. 1–5.

[18] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 14–15, pp. 2826–2841, 2007.

[19] J. He, P. Cheng, L. Shi, J. Chen, and Y. Sun, "Time synchronization in WSNs: A maximum-value-based consensus approach," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 660–675, Mar. 2014.

[20] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. IPSN*, Boise, ID, USA, 2005, pp. 63–70.

[21] A. Olshevsky and J. N. Tsitsiklis, "Convergence speed in distributed consensus and averaging," *SIAM Rev.*, vol. 53, no. 4, pp. 747–772, 2011.

[22] J. He, L. Cai, P. Cheng, J. Pan, and L. Shi, *Consensus-Based Privacy-Preserving Data Aggregation*, Dept. Elect. Comput. Eng., Univ. Victoria, Victoria, BC, Canada, 2017. [Online]. Available: http://www.ece.uvic.ca/∼cai/tech1709.pdf

[23] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[24] Q. Li and G. Cao, "Efficient and privacy-preserving data aggregation in mobile sensing," in *Proc. IEEE ICNP*, Austin, TX, USA, 2012, pp. 1–10.

[25] J. A. M. Naranjo, L. G. Casado, and M. Jelasity, "Asynchronous privacy-preserving iterative computation on peer-to-peer networks," *Computing*, vol. 94, nos. 8–10, pp. 763–782, 2012.

[26] M. Xue, P. Papadimitriou, C. Raïssi, P. Kalnis, and H. K. Pung, "Distributed privacy preserving data collection," in *Proc. DASFAA*, Hong Kong, 2011, pp. 93–107.

[27] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Eurocrypt*, 2006, pp. 486–503.

[28] E. Shi, T.-H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. NDSS*, San Diego, CA, USA, 2011, pp. 489–505.

[29] G. Ács and C. Castelluccia, "I have a DREAM! (DiffeRentially privatE smArt Metering)," in *Proc. Int. Workshop Inf. Hiding*, 2011, pp. 118–132.

[30] I. Rouf *et al.*, "Neighborhood watch: Security and privacy analysis of automatic meter reading systems," in *Proc. ACM CCS*, Raleigh, NC, USA, 2012, pp. 462–473.

[31] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[32] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, 2014, pp. 2112–2120.

[33] L. Xiong, S. Chitti, and L. Liu, "Preserving data privacy in outsourcing data aggregation services," *ACM Trans. Internet Technol.*, vol. 7, no. 3, pp. 1–17, 2007.

Jianping He (M'15) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013.

He is currently an Associate Professor with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China, and was a Research Fellow with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada, from 2013 to 2017. His current research interests include the smart sensing and control, security and privacy theory and applications, distributed learning and big data.

Dr. He was a recipient of the Best Paper Award of IEEE WCSP'17 and the Finalist Best Student Paper Award of IEEE ICCA'17. He serves as an Associate Editor for the *KSII Transactions on Internet and Information Systems*. He was also a Guest Editor for the *International Journal of Robust and Nonlinear Control* and *Neurocomputing*.

Lin Cai (S'00–M'06–SM'10) received the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2002 and 2005, respectively.

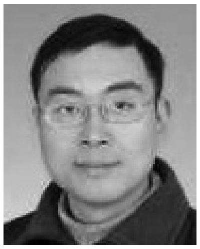
Since 2005, she has been with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada, where she is currently a Professor. Her current research interests include communications and networking with a focus on network protocol and architecture design supporting emerging multimedia traffic over wireless, mobile, ad hoc, and sensor networks.

Dr. Cai was a recipient of the NSERC Discovery Accelerator Supplement Grant in 2010 and 2015, and the Best Paper Awards of IEEE ICC 2008 and IEEE WCNC 2011. She has served as a TPC Symposium Co-Chair for IEEE Globecom'10 and Globecom'13. She has served as a member of the Steering Committee of the IEEE TRANSACTIONS ON BIG DATA, an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the *EURASIP Journal on Wireless Communications and Networking*, the *International Journal of Sensor Networks*, and the *Journal of Communications and Networks*, and the Distinguished Lecturer of the IEEE VTS Society. She has founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She is a Registered Professional Engineer in the Province of British Columbia, Canada.

Peng Cheng (M'10) received the B.E. degree in automation and Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively.

He is currently a Professor with the College of Control Science and Engineering, Zhejiang University. His current research interests include networked sensing and control, cyber-physical systems, and control system security.

Dr. Cheng serves as an Associate Editor for the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, *Wireless Networks*, and the *International Journal of Communication Systems*. He also serves/served as a Guest Editor for the IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS and the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He served as the TPC Co-Chair of IEEE IOV 2016, the Local Arrangement Co-Chair for ACM MobiHoc 2015, and the Publicity Co-Chair for IEEE MASS 2013.



Jianping Pan (S'96–M'98–SM'08) received the bachelor's and Ph.D. degrees in computer science from Southeast University, Nanjing, China.

He is currently a Professor of computer science with the University of Victoria, Victoria, BC, Canada. He was a Post-Doctoral Researcher with the University of Waterloo, Waterloo, ON, Canada. He was also with the Fujitsu Laboratories of America, Sunnyvale, CA, USA, and NTT Laboratories. His current research interests include computer networks, distributed systems, protocols for advanced networking, performance analysis of networked systems, and applied network security.

Dr. Pan was a recipient of the IEICE Best Paper Award in 2009, the Telecommunications Advancement Foundation's Telesys Award in 2010, the WCSP 2011 Best Paper Award, the IEEE Globecom 2011 Best Paper Award, the JSPS Invitation Fellowship in 2012, the IEEE ICC 2013 Best Paper Award, and the NSERC DAS Award in 2016. He has been serving on the Technical Program Committees of major computer communications and networking conferences, including IEEE INFOCOM, ICC, Globecom, WCNC, and CCNC. He was the Ad Hoc and Sensor Networking Symposium Co-Chair of IEEE Globecom 2012 and an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is a Senior Member of the ACM.

Ling Shi (M'08–SM'17) received the B.S. degree in electrical and electronic engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2002, and the Ph.D. degree in control and dynamical systems from the California Institute of Technology, Pasadena, CA, USA, in 2008.

He is currently an Associate Professor with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology. His current research interests include cyber-physical systems security, networked control systems, sensor scheduling, and event-based state estimation.

Dr. Shi served as an Editorial Board member of the European Control Conference from 2013 to 2016. He has been serving as a Subject Editor for the *International Journal of Robust and Nonlinear Control* since 2015, an Associate Editor for the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS since 2016, and the IEEE CONTROL SYSTEMS LETTERS since 2017. He also served as an Associate Editor for the "Special Issue on Secure Control of Cyber Physical Systems" in the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS from 2015 to 2017. He serves as the General Chair of the 23rd International Symposium on Mathematical Theory of Networks and Systems in 2018.