



To Hide Private Position Information in Localization Using Time Difference of Arrival

Xiufang Shi , Member, IEEE, and Junfeng Wu 

Abstract—In most existing localization schemes, location information leakage is inevitable, since both the locations of the target and the anchors will be revealed to the entity that conducts location estimation. A malicious entity may destroy the localization infrastructure or attack the target or anchors based on the revealed locations. Therefore, location privacy preservation in localization is of great significance. This paper investigates the privacy preservation problem in localization using time difference of arrival (TDOA) under the assumptions of safe internode communication and an *honest-but-curious* model. Adopting the privacy-preserving summation method, we propose two privacy-preserving localization protocols for two scenarios, where the TDOA measurements are, respectively, obtained by the target and the anchors. The proposed protocols do not utilize any encryption method, and can hide the locations of both the target and the anchors by limiting the available information to other nodes. The localization performance, sufficient conditions for privacy preservation, and computation and communication complexities of the proposed protocols are theoretically analyzed. Through simulation and numerical results, we show that the proposed protocols can implement location privacy preservation without degrading the localization performance.

Index Terms—Localization, privacy, time difference of arrival.

I. INTRODUCTION

UBIQUITOUS positioning has become one of the key technologies in many applications of Internet of Things (IoT) [1], [2], the fifth generation (5G) network [3], etc. It refers to the localization technologies, which can localize objects or devices that may be located anywhere, e.g., outdoors, indoors or other areas where the Global Positioning System (GPS) signals are unavailable. A general localization scheme includes two steps: location-related information collection and location estimation [4]–[6]. Location-related information includes the locations of the reference nodes, i.e., anchors, and the location-related measurements [6]–[10], e.g., Received Signal Strength (RSS), Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), which can be obtained by

the target, the anchors or a third party. The collected location-related information will be sent to the location estimation entity (the target itself or a third party). In such a process, information leakage is inevitable, since both the locations of the target and the anchors will be revealed to the entity that conducts location estimation.

Location privacy preservation in localization is very important in many applications. For examples, in a military reconnaissance application, through sending localization request and harvesting the anchors' locations, an enemy can attack the anchors and further destroy the whole network [4]; in civilian applications, a target user requests localization yet is unwilling to reveal his location to others, since his personal privacy information, e.g., daily agenda, health condition, might be glimpsed by others via correlating his locations with the places he has visited [11], [12]. Therefore, privacy preservation is desirable for all the entities that take part in localization.

There are already some achievements about privacy preservation in various localization schemes. Li *et al.* [12] proposed a privacy-preserving WiFi fingerprint localization scheme (Pri-WFL) to protect both the client's location privacy and the service provider's data privacy using Paillier cryptosystem. Li *et al.* [13] proposed a privacy-preserving site survey scheme using homomorphic encryption and differential privacy to protect the location privacy of the WiFi signal strength suppliers in the offline site survey phase of WiFi fingerprint-based localization. Wang *et al.* [14] proposed to utilize homomorphic encryption and fuzzy logic to protect the location privacy of the user and Access Points (APs) in channel state information (CSI) fingerprint-based localization. Hussain and Koushanfar [15] designed a privacy-preserving triangle localization protocol for smart automobile systems using Yao's Garbled Circuit (GC). Alanwar *et al.* [16] proposed a privacy-preserving localization method ProLoc, which utilized partial homomorphic encryption and was implemented on least squares localization algorithm and an alternating projection localization algorithm. Shu *et al.* [11], [17] investigated the privacy preservation problem in multi-lateral localization and proposed three privacy-preserving protocols to provide different levels of privacy by combining information-hiding (intermediate obfuscation) and homomorphic encryption. Wang *et al.* [18], [19] further proposed an efficient privacy-preserving algorithm via information-hiding based on an adjacent subtraction based localization (ASL) model without using any encryption method.

In the above achievements, the techniques that are used for privacy preservation mainly include encryption based

Manuscript received December 16, 2017; revised April 30, 2018 and June 25, 2018; accepted June 25, 2018. Date of publication July 23, 2018; date of current version August 23, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Chandra R. Murthy. This work was supported in part by the China Postdoctoral Science Foundation under Grant 2017M621930, and in part by the Natural Science Foundation of China under Grant 61801422, Grant 61429301 and Grant U1401253. (Corresponding author: Junfeng Wu.)

The authors are with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China (e-mail: xfshi.zju@gmail.com; jfwu@zju.edu.cn).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TSP.2018.2858187

techniques, differential privacy techniques, information-hiding techniques, etc. Encryption based techniques can provide strong privacy preservation, while they are computationally expensive. Differential privacy techniques are computationally efficient, while they generally degrade the localization accuracy because of the additional noise. Information-hiding techniques, e.g., privacy preserving summation (PPS), are computationally efficient and also have no effect on the localization accuracy since the added noises are all cancelled out. Therefore, information-hiding techniques are very promising for privacy preservation in localization.

In this paper, we consider to adopt one typical information-hiding technique, i.e., PPS, in designing privacy preserving protocols for TDOA-based localization, which however is challenging. Since localization using TDOA measurements is much more complex than a simple summation operation, we need to exploit the special structure of the location estimation problem and determine the terms which conduct PPS. Moreover, providing the theoretical guarantee for the privacy preservation is insightful for system designers. Whereas, PPS-based method lacks a mathematical criterion to evaluate the level of privacy preservation. Motivated by the above observations, in this paper, we aim to provide some solutions for privacy preservation in TDOA-based localization using PPS, and theoretical results about the level of privacy preservation as well. Specifically, the contributions of this paper are summarized as follows:

- To the best of our knowledge, this is the first work that adopts PPS into TDOA-based localization for privacy preservation. We propose two privacy-preserving localization protocols based on a conventional least squares estimation model respectively for two different scenarios, where the TDOA measurements are respectively obtained by the target and the anchors.
- To evaluate the performance of the privacy preservation, we propose a notion of privacy for the PPS-based protocols. Using this notion, we theoretically analyze the level of privacy preservation of the proposed protocols, and provide the sufficient conditions for each node to keep its location private respectively in the cases of non-collusion and collusion.
- We also prove that the proposed privacy-preserving protocols can provide the same estimate of the target location as the conventional localization that does not consider privacy issue. The computation and communication complexities of the proposed protocols are provided as well.

The remainder of this paper is organized as follows. Sec. II formulates the problem of privacy-preserving TDOA localization. Sec. III provides preliminary analyses about PPS and the considered TDOA localization scheme. Sec. IV and Sec. V respectively introduce the proposed protocols, as well as their performance analysis. The performance evaluation is conducted in Sec. VI. In the end, Sec. VII concludes this paper.

II. PROBLEM FORMULATION

A. Scenario Description

We consider a cooperative localization scheme, where a target has lost its location and sends localization request to its

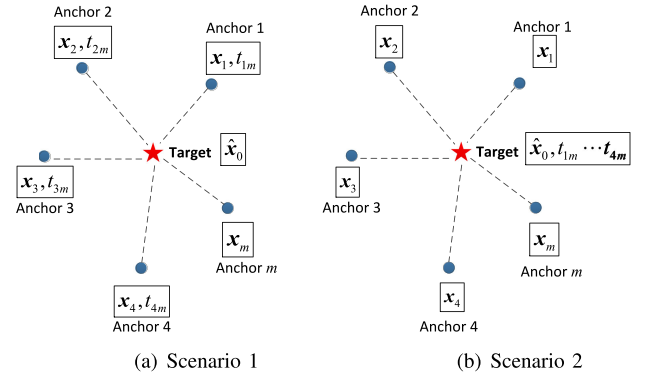


Fig. 1. Overview of TDOA localization scenarios, where the target estimates its location by itself and the available information to each node is shown in the corresponding rectangle.

neighboring nodes, i.e., anchors, within its communication range. The anchors send the location-related information back to the target. Based on the received information, the target conducts location estimation.

The target location is denoted by $\mathbf{x}_0 = [x_{01}, \dots, x_{0n}]^T$, where n stands for the space dimensionality. The anchors' locations are respectively $\mathbf{x}_1, \dots, \mathbf{x}_m$, where m is the number of the anchors and $\mathbf{x}_i = [x_{i1}, \dots, x_{in}]^T, i = 1, \dots, m$. The TDOA measurement between anchor i and j is

$$t_{ij} = t_i - t_j \quad (1)$$

where t_i and t_j are respectively the signal transmission time between anchor i and the target, and the signal transmission time between anchor j and the target. The TDOA measurements can be obtained by various entities, e.g., the target, the anchors or a third party. In this paper, we investigate the localization respectively in two scenarios:

- **Scenario 1:** As shown in Fig. 1(a), by taking one anchor as reference, e.g., anchor m , TDOA measurement t_{im} is obtained by anchor $i, i = 1, \dots, m-1$. In practice, this scenario is like the uplink TDOA (UTDOA) localization in Long Term Evolution (LTE) network [20], where the user equipment (UE) is the target and the base stations (BSs) are the anchors. The UE sends positioning reference signal (PRS) to the BSs and the BSs obtain the TDOA measurements. For simplicity, we call this scenario "UTDOA localization".
- **Scenario 2:** As shown in Fig. 1(b), by taking anchor m as the reference anchor, all the TDOA measurements $t_{im}, i = 1, \dots, m-1$ are obtained by the target. In practice, this scenario is like the observed TDOA (OTDOA) localization in LTE network [21], where the UE is the target and the BSs are the anchors. Different from Scenario 1, the BSs send PRSs to the UE and the UE obtains the TDOA measurements. For simplicity, we call this scenario "OTDOA localization".

In the above localization scenarios, both the target and the anchors have privacy concern on their locations. The target takes \mathbf{x}_0 as its private information and anchor $i \in \{1, \dots, m\}$ takes \mathbf{x}_i as its private information. This paper aims to design privacy-preserving localization protocols for the above scenarios. The

proposed protocols will achieve accurate location estimation for the target and keep each entity's location private. We will investigate the privacy preservation of each entity (the target or an anchor) in different cases including: (a) there exists no collusion among all the entities, where one entity will not share its location with other entities; (b) a number of entities involve in collusion, where one non-colluding entity will not share its location with other entities and one colluding entity will only share its location with the other colluding entities.

In the following subsections, we will first introduce a conventional TDOA localization algorithm, which provides the fundamental location estimate for the protocol design, then we will provide the specific goals for the protocol design.

B. Conventional TDOA Localization

One of the conventional and widely used TDOA localization method is to formulate the localization problem as least squares (LS) estimation for an over-determined linear system [22].

From TDOA measurement t_{im} , we can get the following range difference measurement

$$d_{im} = t_{im}c = d_i - d_m + e_{im} \quad (2)$$

where c is the signal transmission speed, $d_i = \|\mathbf{x}_i - \mathbf{x}_0\|$, $d_m = \|\mathbf{x}_m - \mathbf{x}_0\|$, $\|\cdot\|$ represents l_2 norm, and e_{im} is the measurement error of the range difference. The LS estimation problem is formulated as

$$\min_{\mathbf{x}} \sum_{i=1}^{m-1} \left((d_{im} + d_m)^2 - d_i^2 \right)^2 \quad (3)$$

It can be transformed into the following linear LS problem

$$\min_{\mathbf{x}} \|\mathbf{A}\mathbf{x} - \mathbf{b}\|^2 \quad (4)$$

where $\mathbf{x} = [\mathbf{x}_0^T, d_m]^T$,

$$\mathbf{A} = \begin{bmatrix} (\mathbf{x}_1 - \mathbf{x}_m)^T & d_{1m} \\ \vdots & \vdots \\ (\mathbf{x}_{m-1} - \mathbf{x}_m)^T & d_{m-1m} \end{bmatrix} \quad (5)$$

and

$$\mathbf{b} = \begin{bmatrix} \mathbf{x}_1^T \mathbf{x}_1 - \mathbf{x}_m^T \mathbf{x}_m - d_{1m}^2 \\ \vdots \\ \mathbf{x}_{m-1}^T \mathbf{x}_{m-1} - \mathbf{x}_m^T \mathbf{x}_m - d_{m-1m}^2 \end{bmatrix} \quad (6)$$

The closed-form estimate of \mathbf{x} is

$$\hat{\mathbf{x}} = \frac{1}{2}(\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \mathbf{b} \quad (7)$$

where $\hat{\mathbf{x}} = [\hat{\mathbf{x}}_0^T, \hat{d}_m]^T$.

The above estimation in (7) does not rely on the statistical distribution of the measurement errors. Its estimation error in the presence of measurements errors has been theoretically analyzed in [23]. In this paper, we will not devote our work to improving the location estimation accuracy but achieving the same estimation result as (7).

C. Privacy-Preserving Localization

In this paper, we adopt an *honest-but-curious* model, where all the entities participating in the localization honestly follow the designed protocols and each entity is curious about other entities' private information. This model is consistent with most studies in this area [11], [13], [15], [17]–[19]. Also, we assume the inter-node communication is safe such that the private information will not be eavesdropped via communication link. This assumption has been adopted in many existing studies and can be realized through encryption techniques [11], [17]–[19]. We consider the case that the target only sends one localization request to the anchors and the anchors will not respond to the same request twice.

Regarding the privacy-preserving localization protocols to be designed in this paper, we aim to achieve the following goals:

- Location estimation: the target can get a location estimate, which is equivalent to the one in (7).
- Privacy preservation: for any node i , $i = 0, \dots, m$, its location cannot be *uniquely estimated* by others.

We will show the designed privacy-preserving localization protocols after preliminary analysis. The location estimation and privacy preservation in both non-collusion and collusion cases will be theoretically analyzed. Moreover, the computation and communication complexities will also be analyzed.

III. PRELIMINARY ANALYSIS

A. Privacy-Preserving Summation

PPS is a computationally efficient method to achieve summation while protecting each entity's private information. Suppose node i holds its private information matrix $\mathbf{X}_i \in \mathbb{R}^{n \times p^1}$, node 0 wants to calculate the sum of \mathbf{X}_i , $i = 1, \dots, m$. To protect the private information, instead of directly sending \mathbf{X}_i , node i sends node 0 an obfuscated matrix by adding a random matrix into \mathbf{X}_i . The PPS method is described as follows.

PPS: For every node i , it randomly generates m matrices, denoted by $\mathbf{W}_{ik} \in \mathbb{R}^{n \times p}$, $k = 1, \dots, m$, such that $\sum_{k=1}^m \mathbf{W}_{ik} = \mathbf{0}$. Then node i keeps one such matrix, e.g., \mathbf{W}_{ii} , and sends the rest to the other $m - 1$ nodes. By adding up all the received random matrices from the other $m - 1$ nodes with the one it keeps, node i can get a random matrix $\mathbf{W}_i \in \mathbb{R}^{n \times p}$. Let $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \mathbf{W}_i$. Node i sends $\tilde{\mathbf{X}}_i$ to node 0. Then node 0 can get the sum of \mathbf{X}_i by adding up $\tilde{\mathbf{X}}_i$, $i = 1, \dots, m$. Fig. 2 shows the flowchart of PPS in an example, where $m = 3$.

Regarding the summation result of PPS, it is straightforward and has been shown in [18], [19]. We summarize it into the following lemma.

Lemma 1: PPS can obtain accurate summation result, i.e., $\sum_{i=1}^m \tilde{\mathbf{X}}_i = \sum_{i=1}^m \mathbf{X}_i$.

Regarding the privacy preservation of PPS, the private information of each node is protected by limiting the available information to the curious nodes. However, PPS lacks a criterion to evaluate the level of privacy preservation. In the following, we will define a notion of privacy, then analyze the level of

¹In PPS, $n \times p$ denotes the size of the private information matrix. In the localization problem, the private information of each node is its location, where n is the space dimensionality and $p = 1$.

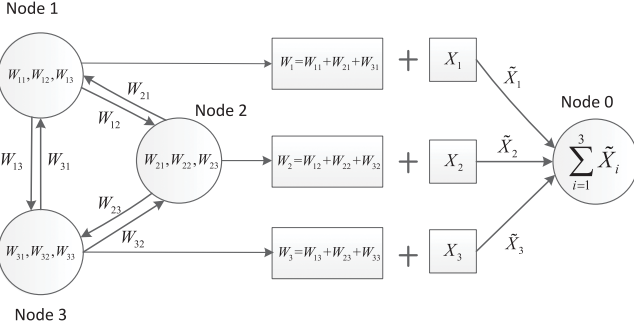


Fig. 2. Flowchart of PPS in a simple example, where node 0 calculates the summation of three nodes' private information.

privacy preservation in PPS. Mathematically, PPS can protect the nodes' privacy information when the curious node/nodes cannot construct enough independent equations for the private information. Based on this observation, we give the following notion of privacy:

$\{N_p\}$ -Privacy: For a set of nodes, denoted by S_c , besides the available information, they need extra information to construct at least N_p independent equations such that they can estimate the private information of another set of nodes, denoted by S_p . We say S_p can preserve $\{N_p\}$ -Privacy to S_c .

In the above, $N_p = N_{scal} - N_{eq}$, where N_{scal} is the number of unknown scalar variables in the private information of S_p and N_{eq} is maximum number of independent equations that S_c can construct based on the available information.

For a conventional summation without adopting PPS, node $i \in \{1, \dots, m\}$ simply sends \mathbf{X}_i to node 0 and can preserve $\{0\}$ -Privacy to node 0, while it can preserve $\{np\}$ -Privacy to node $j \in \{1, \dots, m\}, \forall j \neq i$ since nodes $1 \sim m$ do not have information exchange with each other. If PPS is adopted, nodes $1 \sim m$ only exchange the generated random matrices, they can still preserve $\{np\}$ -Privacy to each other, but can preserve higher privacy level to node 0, since they are not sending the true values of their private information. Specifically, we have the following lemma.

Lemma 2: PPS can realize the following privacy preservation:

- For independent nodes, nodes $1 \sim m$ can preserve $\{(m-1)np\}$ -Privacy to node 0.
- For n_c colluding nodes, if node 0 does not involve in collusion, the non-colluding nodes can preserve $\{(m-n_c)np\}$ -Privacy to the colluding nodes; if node 0 involves in collusion, when $m \geq 3$ and $n_c < m$, the non-colluding nodes can preserve $\{(m-n_c)np\}$ -Privacy to the colluding nodes.

Proof: In the absence of collusion, node 0 only knows value of $\sum_{i=1}^m \mathbf{X}_i$, which constructs np independent equations about $\mathbf{X}_i, i = 1, \dots, m$, where the number of the unknown scalars to node 0 is mnp . Since $mnp > np$ always holds, node 0 cannot uniquely estimate \mathbf{X}_i and nodes $1 \sim m$ can preserve $\{(m-1)np\}$ -Privacy to node 0.

In the occurrence of collusion, the set of colluding nodes is S_c and the set of non-colluding nodes is S_p . If node 0 does not involve in collusion, S_c can only learn the value

of $\sum_{i=1, i \notin S_c}^m \mathbf{W}_i$, from which, S_c cannot know S_p 's private information. In this case, S_p can preserve $\{(m-n_c)np\}$ -Privacy to S_c . If node 0 involves in collusion, S_c can learn the value of $\sum_{i=1, i \notin S_c}^m \mathbf{X}_i$, where the number of unknown scalar variables is at most np . When $m \geq 3$ and $n_c < m$, then $(m-n_c+1)np > np$, which makes S_c unable to learn S_p 's private information and S_p can preserve $\{(m-n_c)np\}$ -Privacy to S_c . ■

In PPS, the computation complexity for each node is $\mathcal{O}(mnp)$, which comes from matrix summation operation. Regarding the communication complexity, node $i, i = 1, \dots, m$ transmits mnp scalars and receives $(m-1)np$ scalars, while node 0 receives mnp scalars but does not transmit any scalar.

PPS can be applied in an environment where the communication resource is sufficient and is favourable for distributed computation because of its low computational complexity. If there exists a trusted central node, we can use this central node to generate random numbers and distribute to other nodes, which will reduce the communication overhead.

B. Location Estimate Analysis

To realize privacy-preserving localization, we preliminarily analyze the estimate in (7). We rewrite \mathbf{A} as follows

$$\mathbf{A} = \sum_{i=1}^m \mathbf{M}_i + \mathbf{H} \quad (8)$$

where $\mathbf{M}_i \in \mathbb{R}^{(m-1) \times (n+1)}$ is defined as

$$\mathbf{M}_i = \begin{bmatrix} 0 & 0 \\ \vdots & \vdots \\ \mathbf{x}_i^T & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix}, \quad i = 1, \dots, m-1$$

Except for the i th row, all the other rows of \mathbf{M}_i are zeros. And $\mathbf{M}_m \in \mathbb{R}^{(m-1) \times (n+1)}$ and $\mathbf{H} \in \mathbb{R}^{(m-1) \times (n+1)}$ are respectively defined as

$$\mathbf{M}_m = \begin{bmatrix} -\mathbf{x}_m^T & 0 \\ \vdots & \vdots \\ -\mathbf{x}_m^T & 0 \end{bmatrix}, \quad \mathbf{H} = \begin{bmatrix} 0 & \cdots & 0 & d_{1m} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & d_{m-1m} \end{bmatrix}$$

Similarly, \mathbf{b} can be rewritten as

$$\mathbf{b} = \sum_{i=1}^m \mathbf{h}_i + \mathbf{d} \quad (9)$$

where $\mathbf{h}_i \in \mathbb{R}^{(m-1) \times 1}, i = 1, \dots, m-1$ is defined as $\mathbf{h}_i = [0, \dots, \mathbf{x}_i^T \mathbf{x}_i, \dots, 0]^T$. Except for the i th element, all the other elements of \mathbf{h}_i are zeros. And $\mathbf{h}_m \in \mathbb{R}^{(m-1) \times 1}$ and $\mathbf{d} \in \mathbb{R}^{(m-1) \times 1}$ are respectively defined as $\mathbf{h}_m = [-\mathbf{x}_m^T \mathbf{x}_m, \dots, -\mathbf{x}_m^T \mathbf{x}_m]^T$ and $\mathbf{d} = [-d_{1m}^2, \dots, -d_{m-1m}^2]^T$.

According to (8), we can easily obtain that

$$\begin{aligned} \mathbf{A}^T \mathbf{A} &= \sum_{i=1}^m \sum_{j=1}^m \mathbf{M}_i^T \mathbf{M}_j + \sum_{j=1}^m \mathbf{M}_i^T \mathbf{H} \\ &\quad + \mathbf{H}^T \sum_{i=1}^m \mathbf{M}_i + \mathbf{H}^T \mathbf{H} \\ &= \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \end{aligned} \quad (10)$$

where

$$\begin{aligned} A_{11} &= (m-1)\mathbf{x}_m \mathbf{x}_m^T + \sum_{i=1}^{m-1} \mathbf{x}_i \mathbf{x}_i^T \\ &\quad - \left(\sum_{i=1}^{m-1} \mathbf{x}_i \right) \mathbf{x}_m^T - \mathbf{x}_m \left(\sum_{i=1}^{m-1} \mathbf{x}_i^T \right) \end{aligned} \quad (11)$$

$$A_{12} = \sum_{i=1}^{m-1} \mathbf{x}_i d_{im} - \mathbf{x}_m \sum_{i=1}^{m-1} d_{im} \quad (12)$$

$$A_{21} = \sum_{i=1}^{m-1} \mathbf{x}_i^T d_{im} - \mathbf{x}_m^T \sum_{i=1}^{m-1} d_{im} \quad (13)$$

$$A_{22} = \sum_{i=1}^{m-1} d_{im}^2 \quad (14)$$

And A_{11} , A_{12} , A_{21} and A_{22} are respectively calculated from $\sum_{i=1}^m \sum_{j=1}^m \mathbf{M}_i^T \mathbf{M}_j$, $\sum_{j=1}^m \mathbf{M}_i^T \mathbf{H}$, $\mathbf{H}^T \sum_{i=1}^m \mathbf{M}_i$ and $\mathbf{H}^T \mathbf{H}$. Accordingly, from (8) and (9), we have

$$\begin{aligned} \mathbf{A}^T \mathbf{b} &= \sum_{i=1}^m \sum_{j=1}^m \mathbf{M}_i^T \mathbf{h}_j + \sum_{j=1}^m \mathbf{M}_i^T \mathbf{d} + \mathbf{H}^T \sum_{i=1}^m \mathbf{h}_i + \mathbf{H}^T \mathbf{d} \\ &= \begin{bmatrix} B_{11} + B_{12} \\ B_{21} + B_{22} \end{bmatrix} \end{aligned} \quad (15)$$

where

$$\begin{aligned} B_{11} &= (m-1)\mathbf{x}_m \mathbf{x}_m^T \mathbf{x}_m + \sum_{i=1}^{m-1} \mathbf{x}_i \mathbf{x}_i^T \mathbf{x}_i \\ &\quad - \left(\sum_{i=1}^{m-1} \mathbf{x}_i \right) \mathbf{x}_m^T \mathbf{x}_m - \mathbf{x}_m \left(\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i \right) \end{aligned} \quad (16)$$

$$B_{12} = - \sum_{i=1}^{m-1} \mathbf{x}_i d_{im}^2 + \mathbf{x}_m \sum_{i=1}^{m-1} d_{im}^2 \quad (17)$$

$$B_{21} = \sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i d_{im} - \mathbf{x}_m^T \mathbf{x}_m \sum_{i=1}^{m-1} d_{im} \quad (18)$$

$$B_{22} = - \sum_{i=1}^{m-1} d_{im}^3 \quad (19)$$

Straightforwardly, the estimate $\hat{\mathbf{x}}$ in (7) can be rewritten as

$$\hat{\mathbf{x}} = \frac{1}{2} \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}^{-1} \begin{bmatrix} B_{11} + B_{12} \\ B_{21} + B_{22} \end{bmatrix} \quad (20)$$

To achieve the above estimation, the target needs to calculate A_{11} , A_{12} , A_{21} , A_{22} , B_{11} , B_{12} , B_{21} , and B_{22} , which are formed by a number of summation terms. The overall idea for the design of privacy-preserving localization protocols is to calculate these summation terms via PPS and obtain the location estimate without revealing each entity's location. In different scenarios, each entity holds different information and the summation terms which need PPS are different. In the following, we will introduce the privacy-preserving localization protocols respectively for Scenario 1 and Scenario 2 conducting PPS on different summation terms.

IV. PRIVACY-PRESERVING PROTOCOL FOR SCENARIO 1

A. Protocol Design

In Scenario 1, the information about the anchors' locations and TDOA measurements is on the anchor side. In order to complete the location calculation, the target needs the help from the anchors to obtain A_{11} , A_{12} , A_{21} , A_{22} , B_{11} , B_{12} , B_{21} , and B_{22} . By taking advantage of PPS, we propose the following privacy-preserving protocol for Scenario 1.

UTDOA Privacy-Preserving Localization (UTDOA-PPL) :

- 1) Anchor m calculates $\sum_{i=1}^{m-1} \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$, $\sum_{i=1}^{m-1} d_{im}$ and $\sum_{i=1}^{m-1} d_{im}^2$ respectively via PPS;
- 2) Let $\Omega_i = \mathbf{x}_i \mathbf{x}_i^T$ for $i = 1, \dots, m-1$, and $\Omega_m = (m-1)\mathbf{x}_m \mathbf{x}_m^T - (\sum_{i=1}^{m-1} \mathbf{x}_i) \mathbf{x}_m^T - \mathbf{x}_m (\sum_{i=1}^{m-1} \mathbf{x}_i^T)$. The target calculates $A_{11} = \sum_{i=1}^m \Omega_i$ via PPS;
- 3) Let $\Upsilon_i = \mathbf{x}_i d_{im}$ for $i = 1, \dots, m-1$, and $\Upsilon_m = -\mathbf{x}_m \sum_{i=1}^{m-1} d_{im}$. The target calculates $A_{12} = \sum_{i=1}^m \Upsilon_i$ via PPS, and $A_{21} = A_{12}^T$;
- 4) The target calculates $A_{22} = \sum_{i=1}^{m-1} d_{im}^2$ and $B_{22} = -\sum_{i=1}^{m-1} d_{im}^3$ respectively via PPS;
- 5) Let $\psi_i = \mathbf{x}_i \mathbf{x}_i^T \mathbf{x}_i$ for $i = 1, \dots, m-1$, and $\psi_m = (m-1)\mathbf{x}_m \mathbf{x}_m^T \mathbf{x}_m - \sum_{i=1}^{m-1} \mathbf{x}_i \mathbf{x}_i^T \mathbf{x}_m - \mathbf{x}_m \sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$. The target calculates $B_{11} = \sum_{i=1}^m \psi_i$ via PPS;
- 6) Let $\Theta_i = -\mathbf{x}_i d_{im}^2$ for $i = 1, \dots, m-1$, and $\Theta_m = \mathbf{x}_m \sum_{i=1}^{m-1} d_{im}^2$. The target calculates $B_{12} = \sum_{i=1}^m \Theta_i$ via PPS;
- 7) Let $\Gamma_i = \mathbf{x}_i^T \mathbf{x}_i d_{im}$ for $i = 1, \dots, m-1$, and $\Gamma_m = -\mathbf{x}_m^T \mathbf{x}_m \sum_{i=1}^{m-1} d_{im}$. The target calculates $B_{21} = \sum_{i=1}^m \Gamma_i$ via PPS;
- 8) The target calculates the estimate of \mathbf{x} through (20), and gets the location estimate $\hat{\mathbf{x}}_0$.

The flowchart of the proposed UTDOA-PPL protocol is shown in Fig. 3

B. Protocol Analysis

1) *Localization Result Analysis:* About the location estimate obtained by UTDOA-PPL, we have the following theorem.

Theorem 1: Through UTDOA-PPL, the target can get a location estimate, which is equivalent to the one in (7).

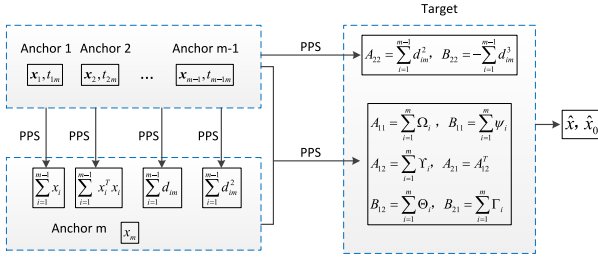


Fig. 3. Flowchart of UTDOA-PPL.

Proof: The proof is straightforward. Eq. (20) is an equivalent transformation of (17) no matter if there exist noises in the measurements. Because of the adoption of PPS in computing the summation terms in A_{11} , A_{12} , A_{21} , A_{21} , B_{11} , B_{12} , B_{21} , and B_{22} , from Lemma 1, the target can correctly calculate the above terms. Therefore, the target can obtain the same estimate \hat{x} as (20), where the location estimate is equivalent to the one in (17). This equivalence is invariant to the measurements. ■

2) *Privacy Preservation Analysis:* We discuss the location privacy preservation of UTDOA-PPL in two cases: (a) there exists no collusion among the nodes; (b) a certain number of nodes collude with each other. In each case, we analyze the information that each node has obtained, and see if the available information is sufficient for one node or the colluding nodes to estimate other nodes' locations. The overall idea for our analysis is to compare the number of the unknown scalars with the number of the available independent equations, and determine if the location privacy can be preserved along with the corresponding privacy levels.

In the absence of collusion, we have the following theorem, whose proof is shown in Appendix A.

Theorem 2: In the absence of collusion, UTDOA-PPL can guarantee the following privacy preservation:

- To every anchor $i \in \{1, \dots, m-1\}$, any anchor $j \in \{1, \dots, m-1\}$ and $j \neq i$ can preserve $\{n\}$ -Privacy; the target together with anchor m can preserve $\{2n-1\}$ -Privacy.
- To anchor m , the target together with other anchors can preserve $\{mn-n-3\}$ -Privacy.
- To the target, if $m > \frac{n}{2} + \frac{3}{n} + 3\frac{1}{2}$, the anchors can preserve $\{mn - (\frac{n^2+n}{2} + 3n + 3)\}$ -Privacy.

In the case of collusion, we have the following theorem, whose proof is shown in Appendix B.

Theorem 3: Suppose the set of colluding nodes is S_c and the number of colluding nodes is n_c , UTDOA-PPL can realize the following privacy preservations:

- When node $0 \notin S_c$ and $m \notin S_c$, anchor m can preserve $\{n-1\}$ -Privacy to S_c ; each non-colluding anchor among $1, \dots, m-1$ can preserve $\{n\}$ -Privacy to S_c ; if $n_c < n+1$, the target can preserve $\{n-n_c+1\}$ -Privacy to S_c .
- When node $0 \in S_c$ and $m \notin S_c$, if $n_c < m - \frac{n}{2} - \frac{4}{n} - 2\frac{1}{2}$, the non-colluding nodes can preserve $\{(m-n_c-2)n - \frac{n^2+n}{2} - 4\}$ -Privacy to S_c .
- When node $0 \notin S_c$ and $m \in S_c$, if $n_c < n+1$, the target can preserve $\{n-n_c+1\}$ -Privacy to S_c ; if $n_c < m - \frac{3}{n} - 1$, the non-colluding anchors can preserve $\{(m-n_c-1)n-3\}$ -Privacy to S_c .

- When node $0 \in S_c$ and $m \in S_c$, if $n_c < m - \frac{n}{2} - \frac{5}{n} - 3\frac{1}{2}$, the non-colluding nodes can preserve $\{(m-n_c-3)n - \frac{n^2+n}{2} - 5\}$ -Privacy to S_c .

3) *Computation Complexity:* Regarding the computation complexity of UTDOA-PPL, we only keep the leading terms in each step [24]. The computation complexities for each anchor in step 1–8) are respectively $\mathcal{O}(mn)$, $\mathcal{O}(mn^2)$, $\mathcal{O}(mn)$, $\mathcal{O}(m)$, $\mathcal{O}(mn)$, $\mathcal{O}(mn)$, $\mathcal{O}(m+n)$, and 0. The computation complexities for the target in step 1–8) are respectively 0, $\mathcal{O}(mn^2)$, $\mathcal{O}(mn)$, $\mathcal{O}(m)$, $\mathcal{O}(mn)$, $\mathcal{O}(mn)$, $\mathcal{O}(m+n)$, and $\mathcal{O}((n+1)^3)$. Therefore, by keeping the leading terms, the computation complexity of UTDOA-PPL is $\mathcal{O}(mn^2)$ for each anchor and $\mathcal{O}(\max\{mn^2, (n+1)^3\})$ for the target.

4) *Communication Complexity:* The communication complexity is analyzed by counting the transmitted and received scalars by each node. The communication occurs in step 1–7). For each anchor i , $i = 1, \dots, m-1$, the numbers of transmitted scalars in step 1–7) are respectively $(m-1)(n+3)$, mn^2 , mn , $2m-2$, mn , mn , and m ; the numbers of received scalars in step 1–7) are respectively $(m-2)(n+3)$, $(m-1)n^2$, $(m-1)n$, $2m-4$, $(m-1)n$, $(m-1)n$, and $m-1$. For anchor m , the numbers of transmitted scalars in step 1–7) are respectively 0, mn^2 , mn , 0, mn , mn , and m ; the numbers of received scalars in step 1–7) are respectively $(m-1)(n+3)$, $(m-1)n^2$, $(m-1)n$, 0, $(m-1)n$, $(m-1)n$, and $m-1$. For the target, the numbers of transmitted scalars in step 1–7) are all 0; the numbers of received scalars in step 1–7) are respectively 0, mn^2 , mn , $2m-2$, mn , mn , and m . In total, each anchor i , $i = 1, \dots, m-1$, transmits $mn^2 + (4m-1)n + 6m - 5$ scalars and receives $(m-1)n^2 + (4m-5)n + 6m - 11$ scalars; anchor m transmits $mn^2 + 3mn + m$ scalars and receives $(m-1)n^2 + (4m-4)n + 4m - 4$ scalars; the target does not transmit scalars and receives $mn^2 + 3mn + 3m - 2$ scalars.

V. PRIVACY-PRESERVING PROTOCOL FOR SCENARIO 2

A. Protocol Design

In Scenario 2, the target has all the TDOA measurements and it can easily calculate A_{22} and B_{22} . To complete the location calculation, the target also needs the help from the anchors to calculate A_{11} , A_{12} , A_{21} , B_{11} , B_{12} , and B_{21} . By observing A_{11} and B_{11} in (11) and (16), we find that they are only related to the anchors' locations. Thus, they can be calculated in the same way as that in UTDOA-PPL. Regarding A_{12} , A_{21} , B_{12} , and B_{21} , they are related to the anchors' locations, which are on the anchor side, and the TDOA measurements, which are on the target side. This observation makes UTDOA-PPL inapplicable to Scenario 2. We design the following privacy-preserving protocol for Scenario 2.

OTDOA Privacy-Preserving Localization (OTDOA-PPL) :

- The target calculates A_{22} and B_{22} based on the TDOA measurements;
- The target calculates A_{11} and B_{11} in the same way as that in UTDOA-PPL;
- The target sends the range difference ratios $r_i = \frac{d_{im}}{\sum_{i=1}^{m-1} d_{im}}$ and $r_{2i} = \frac{d_{im}^2}{\sum_{i=1}^{m-1} d_{im}^2}$ to anchor $i \in \{1, \dots, m-1\}$;

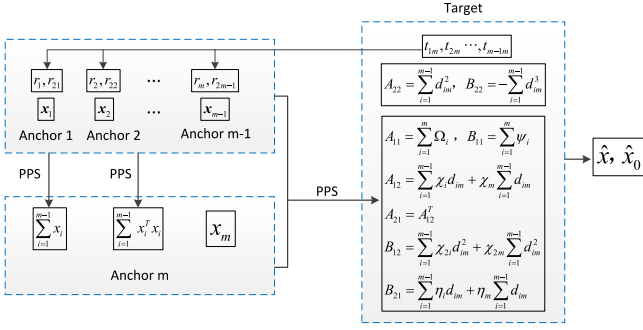


Fig. 4. Flowchart of OTDOA-PPL.

- 4) In the same way of generating random matrices as that in PPS, anchor $i \in \{1, \dots, m\}$ generates $\delta_i \in \mathbb{R}^{n \times 1}$, $\delta_{2i} \in \mathbb{R}^{n \times 1}$ and $\rho_i \in \mathbb{R}^{1 \times 1}$, such that $\sum_{i=1}^m \delta_i = 0$, $\sum_{i=1}^m \delta_{2i} = 0$ and $\sum_{i=1}^m \rho_i = 0$;
- 5) For every anchor $i \in \{1, \dots, m-1\}$, it calculates $\chi_i = \mathbf{x}_i + \frac{\delta_i}{r_i}$, $\chi_{2i} = -\mathbf{x}_i + \frac{\delta_{2i}}{r_{2i}}$, and $\eta_i = \mathbf{x}_i^T \mathbf{x}_i + \frac{\rho_i}{r_i}$, then sends them to the target.
- 6) For anchor m , it calculates $\chi_m = -\mathbf{x}_m + \delta_m$, $\chi_{2m} = \mathbf{x}_m + \delta_{2m}$ and $\eta_m = -\mathbf{x}_m^T \mathbf{x}_m + \rho_m$, then sends them to the target.
- 7) The target calculates A_{12} , A_{21} , B_{12} , and B_{21} as follows

$$A_{12} = \sum_{i=1}^{m-1} \chi_i d_{im} + \chi_m \sum_{i=1}^{m-1} d_{im} \quad (21)$$

$$A_{21} = A_{12}^T \quad (22)$$

$$B_{12} = \sum_{i=1}^{m-1} \chi_{2i} d_{im}^2 + \chi_{2m} \sum_{i=1}^{m-1} d_{im}^2 \quad (23)$$

$$B_{21} = \sum_{i=1}^{m-1} \eta_i d_{im} + \eta_m \sum_{i=1}^{m-1} d_{im} \quad (24)$$

- 8) The target calculates the estimate of \mathbf{x} through (20), and gets the location estimate $\hat{\mathbf{x}}_0$.

The flowchart of the proposed OTDOA-PPL protocol is shown in Fig. 4.

B. Protocol Analysis

1) *Localization Result Analysis*: Regarding the target location estimate obtained by OTDOA-PPL, we have the following theorem.

Theorem 4: Through OTDOA-PPL, the target can get a location estimate, which is equivalent to the one in (7).

Proof: Straightforwardly, A_{22} , B_{22} , A_{11} and B_{11} are correctly calculated by the target in step 1) and step 2). In step 7),

$$\begin{aligned} & \sum_{i=1}^{m-1} \chi_i d_{im} + \chi_m \sum_{i=1}^{m-1} d_{im} \\ &= \sum_{i=1}^{m-1} \mathbf{x}_i d_{im} - \mathbf{x}_m \sum_{i=1}^{m-1} d_{im} + \sum_{i=1}^{m-1} \frac{\delta_i}{r_i} d_{im} + \delta_m \sum_{i=1}^{m-1} d_{im} \end{aligned}$$

and

$$\sum_{i=1}^{m-1} \frac{\delta_i}{r_i} d_{im} + \delta_m \sum_{i=1}^{m-1} d_{im} = \sum_{i=1}^m \delta_i \sum_{i=1}^{m-1} d_{im} = 0$$

Therefore, (21) is equivalent to (12). That is to say, A_{12} is correctly calculated.

Similarly, we can prove that (22)-(24) are equivalent to (13), (17), and (18), respectively. Thus the target can correctly calculate A_{21} , B_{12} and B_{21} . Then the target can obtain the same estimate $\hat{\mathbf{x}}$ as (20). And the location estimate in (20) is equivalent to the one in (7), because of the equivalence between (20) and (7). The proof is completed. ■

2) *Privacy Preservation Analysis*: We also analyze the location privacy preservation of OTDOA-PPL using the similar way as that in UTDOA-PPL respectively in the absence of collusion and in the occurrence of collusion.

In the absence of collusion, we have the following theorem, whose proof is shown in Appendix C.

Theorem 5: In the absence of collusion, OTDOA-PPL can guarantee the following privacy preservation:

- a) To every anchor $i \in \{1, \dots, m-1\}$, the other nodes (including both the target and the anchors) can preserve $\{mn-2\}$ -Privacy.
- b) To anchor m , the target can preserve $\{n\}$ -Privacy and other anchors can preserve $\{mn-2n-1\}$ -Privacy.
- c) To the target, if $m > \frac{n}{2} + \frac{3}{n} + 3\frac{1}{2}$, the anchors can preserve $\{mn - (\frac{n^2+n}{2} + 3n + m)\}$ -Privacy.

In the occurrence of collusion, we have the following theorem, whose proof is shown in Appendix D.

Theorem 6: Suppose the set of colluding nodes is S_c and the number of colluding nodes is n_c , OTDOA-PPL can realize the following privacy preservations:

- a) When node $0 \notin S_c$ and $m \notin S_c$, if $n_c < n+2$, the target can preserve $\{n-n_c+2\}$ -Privacy to S_c ; if $n_c < m-1$, the non-colluding anchors can preserve $\{(m-n_c)n-3\}$ -Privacy to S_c ; if $n_c = m-1$, the non-colluding anchors can preserve $\{n-1\}$ -Privacy to S_c .
- b) When node $0 \in S_c$ and $m \notin S_c$, if $n_c < m - \frac{n}{2} - \frac{5}{n-1} - 3$, the non-colluding nodes can preserve $\{(m-n_c-2)n - \frac{n^2+n}{2} - m - n_c + 2\}$ -Privacy to S_c .
- c) When node $0 \notin S_c$ and $m \in S_c$, if $n_c < n+1$, the target can preserve $\{n-n_c+1\}$ -Privacy to S_c ; if $n_c < m - \frac{n}{2} - 1$, the non-colluding anchors can preserve $\{(m-n_c-1)n-2\}$ -Privacy to S_c .
- d) When node $0 \in S_c$ and $m \in S_c$, if $n_c < m - \frac{n}{2} - \frac{7}{n-1} - 4$, the non-colluding nodes preserve $\{(m-n_c-3)n - \frac{n^2+n}{2} - m + n_c - 3\}$ -Privacy to S_c .

3) *Computation Complexity*: We utilized the same way to analyze the complexities of OTDOA-PPL as the analysis of UTDOA-PPL. In OTDOA-PPL, the computation complexities for anchor i , $i = 1, \dots, m-1$ come from step 2), step 4) and step 5), which are respectively $\mathcal{O}(mn^2)$, $\mathcal{O}(mn)$ and $\mathcal{O}(n)$; the computation complexities for anchor m come from step 2), step 4) and step 6), which are respectively $\mathcal{O}(mn^2)$, $\mathcal{O}(mn)$ and $\mathcal{O}(n)$; the computation complexities for the target come from step 1-4) and step 7-8), which are respectively $\mathcal{O}(m)$, $\mathcal{O}(mn^2)$, $\mathcal{O}(m)$, $\mathcal{O}(mn)$, $\mathcal{O}(mn)$, and $\mathcal{O}((n+1)^3)$. Therefore, by

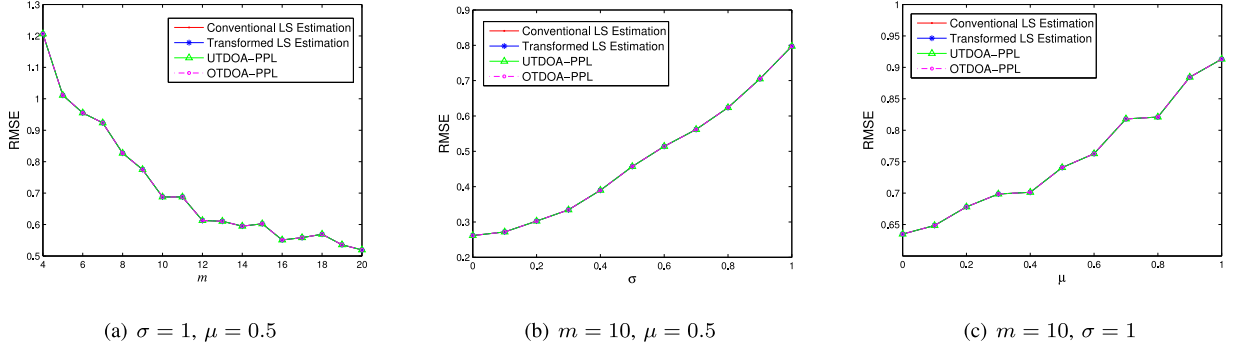


Fig. 5. Localization accuracy comparison.

keeping the leading terms, the computation complexity of OTDOA-PPL is $\mathcal{O}(mn^2)$ for each anchor and $\mathcal{O}(\max\{mn^2, (n+1)^3\})$ for the target.

4) *Communication Complexity*: The communication complexity is also analyzed by counting the transmitted and received scalars by each node. The communication occurs in step 1-6). For each anchor i , $i = 1, \dots, m-1$, the numbers of transmitted scalars in step 1-6) are respectively 0, $mn^2 + (2m-1)n + m - 1$, 0, $(m-1)(2n+1)$, $2n+1$, and 0; the numbers of received scalars in step 1-6) are respectively 0, $(m-1)n^2 + (2m-3)n + m - 2$, 2, $(m-1)(2n+1)$, 0, and 0. For anchor m , the numbers of transmitted scalars in step 1-6) are respectively 0, $mn^2 + mn$, 0, $(m-1)(2n+1)$, 0 and $2n+1$; the numbers of received scalars in step 1-6) are respectively 0, $(m-1)(n+1)^2$, 0, $(m-1)(2n+1)$, 0 and 0. For the target, it only transmits $2(m-1)$ scalars in step 3); the numbers of received scalars in step 1-6) are respectively 0, $mn^2 + mn$, 0, 0, $(m-1)(2n+1)$, and $2n+1$. In total, each anchor i , $i = 1, \dots, m-1$, transmits $mn^2 + (4m-1)n + 2m - 1$ scalars and receives $(m-1)n^2 + (4m-5)n + 2m - 1$ scalars; anchor m transmits $mn^2 + 3mn + m$ scalars and receives $(m-1)n^2 + (4m-4)n + 2m - 2$ scalars; the target transmits $2m - 2$ scalars and receives $mn^2 + 3mn + m$ scalars.

VI. PERFORMANCE EVALUATION

In this section, the performances of the proposed privacy-preserving localization protocols will be evaluated via simulation and numerical results. Specifically, we will evaluate the localization performance, execution time, and the privacy preservation level of each protocol.

A. Localization Accuracy

In the simulations, we consider a $50 \text{ m} \times 50 \text{ m}$ square area in 2 dimensional space. The anchors are uniformly distributed in this area and the target is located at $[0, 0]^T$. Considering that the noise on the range difference is often assumed to follow a Gaussian distribution [5], [25]–[27], we also generate the noise using Gaussian distribution with mean being μ and standard deviation being σ . We run the simulations using MATLAB R2013a on a Thinkpad laptop PC with Intel(R) Core (TM) i7-6500U CPU and 8G RAM. For each simulation, we conduct 500 Monte

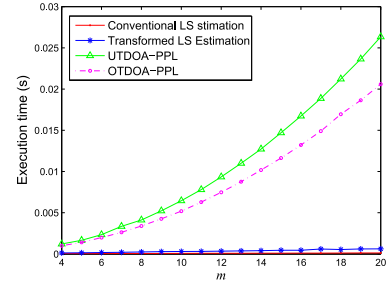


Fig. 6. Execution time comparison.

Carlo trials and show the average results. The localization performance is evaluated by root mean square error (RMSE), i.e. $\sqrt{\frac{\sum_{t=1}^N \|\hat{\mathbf{x}}_0(t) - \mathbf{x}_0\|^2}{N}}$, where N is the number of Monte Carlo trials and $\hat{\mathbf{x}}_0(t)$ is the target location estimate in the t th trial.

We conduct three sets of simulations: (a) let $\sigma = 1$ and $\mu = 0.5$, while m changes; (b) let $m = 10$ and $\mu = 0.5$, while σ changes; (c) let $m = 10$ and $\sigma = 1$, while μ changes. Fig. 5 shows the RMSEs of the localization results obtained respectively in case (a), (b), (c). In this figure, conventional LS estimation refers to the estimation in (7) and transformed LS estimation refers to the estimation in (20). From Fig. 5, we can see the RMSEs obtained by conventional LS estimation, transformed LS estimation, UTDOA-PPL and OTDOA-PPL are completely the same. That is to say, UTDOA-PPL and OTDOA-PPL will not degrade the localization performance. In addition, Fig. 5(a) shows that RMSEs decrease with the increase of m , Fig. 5(b) and Fig. 5(c) respectively shows that RMSEs increase with the increase of σ and μ .

B. Execution Time

Fig. 6 shows the execution time of each protocol. We can find that the execution time of the transformed LS estimation is slightly higher than that of the conventional LS estimation, while UTDOA-PPL and OTDOA-PPL need much more execution time than the conventional LS estimation and the transformed LS estimation since additional computation complexities are introduced in the privacy-preserving protocols. Moreover, the execution time of UTDOA-PPL and OTDOA-PPL quickly increases with the increase of m . We observe that the execution time of UTDOA-PPL and OTDOA-PPL is much less than 1s even when $m = 20$. In many practical applications, execution

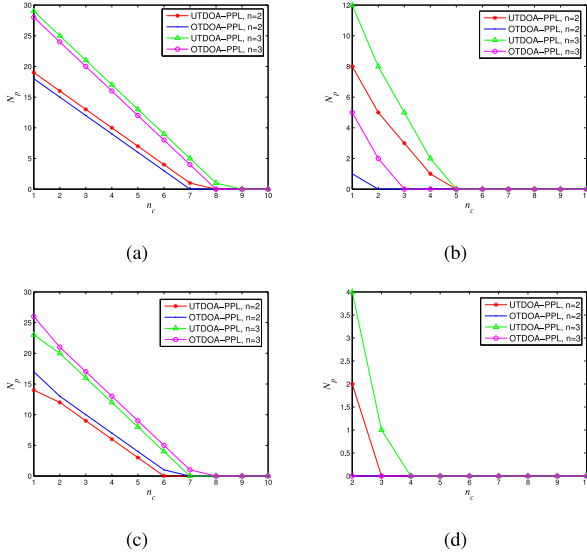


Fig. 7. Privacy preservation level: (a) node $0 \notin S_c$ and $m \notin S_c$; (b) node $0 \in S_c$ and $m \notin S_c$; (c) node $0 \notin S_c$ and $m \in S_c$; (d) node $0 \in S_c$ and $m \in S_c$.

time within 1s is acceptable. Thus, we say that the execution time of the proposed privacy-preserving protocols can meet the practical application requirements.

C. Privacy Preservation

In this subsection, we evaluate the location privacy preservation levels of UTDOA-PPL and OTDOA-PPL respectively in 2 dimensional and 3 dimensional spaces. Specifically, let $m = 10$ and suppose there are n_c colluding nodes, we investigate the privacy preservation levels of the non-colluding nodes in four cases of collusion: (a) node $0 \notin S_c$ and $m \notin S_c$; (b) node $0 \in S_c$ and $m \notin S_c$; (c) node $0 \notin S_c$ and $m \in S_c$; (d) node $0 \in S_c$ and $m \in S_c$. It should be noted that when $n_c = 1$, there is no collusion and we can get the corresponding privacy levels from Theorem 2 and Theorem 4 for cases (a), (b), (c). Since both the target and anchor m involve in collusion in case (d), $n_c = 1$ is not applicable for this case. Fig. 7 shows the location privacy preservation levels of the non-colluding nodes to the colluding nodes. From this figure, we can see that, if the number of colluding nodes is given, UTDOA-PPL and OTDOA-PPL can achieve higher location privacy preservation levels when $n = 3$ than those when $n = 2$. In cases (a)(b)(d), UTDOA-PPL can achieve higher privacy preservation levels than OTDOA-PPL, while in case (c), the privacy preservation level of UTDOA-PPL is lower than that of OTDOA-PPL. By comparing the values of N_p in all the cases, we can find, the location privacy preservation levels will be degraded if anchor m or the target involves in collusion. The degradation induced by the target's involvement in collusion is much greater than that induced by anchor m 's involvement. When both the target and anchor m involve in collusion, the location privacy preservation levels are the lowest.

VII. CONCLUSION

In this paper, we address the privacy preservation problem in TDOA localization. By adopting PPS based technique, we

propose two privacy-preserving localization protocols UTDOA-PPL and OTDOA-PPL to hide private location information for two scenarios, where the TDOA measurements are respectively obtained by the target and the anchors. To evaluate the level of privacy preservation, we define a notion of privacy for the PPS based technique. Using this notion, we theoretically analyze sufficient conditions for the privacy preservation of different nodes in the proposed protocols and also provide the corresponding privacy preservation levels. Moreover, we show that, compared with the conventional LS estimation which does not consider privacy preservation, the proposed protocols can achieve location privacy preservation without degrading the localization performance. The computation and communication complexities of the proposed protocols are also provided. Our future work can be the privacy preservation problem in more TDOA localization scenarios, for instance, the entity that conducts location estimation is a third party.

APPENDIX A

PROOF OF THEOREM 2

For every anchor $i \in \{1, \dots, m-1\}$, it only has the range difference d_{im} , which can form an equation about the locations of the target and anchor m , which includes $2n$ unknown scalar variables. From d_{im} , anchor i can estimate neither the target location nor anchor m 's location. Thus the target and anchor m can preserve $\{2n-1\}$ -Privacy. Anchor i does not receive any information about the location of anchor $j \in \{1, \dots, m-1\}, j \neq i$ and it needs to construct at least n independent equations to estimate anchor j 's location. Thus anchor j can preserve $\{n\}$ -Privacy to anchor i .

For anchor m , it can obtain the values of $\sum_{i=1}^{m-1} \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$, $\sum_{i=1}^{m-1} d_{im}$ and $\sum_{i=1}^{m-1} d_{im}^2$, which can form at most $n+3$ independent linear equations. The number of unknown scalar variables to anchor m is mn , which comes from the locations of the target and anchor $1, \dots, m-1$. Since $m \geq 3$ must hold, $mn > n+3$ always holds. Thus, anchor m cannot know the locations of the target and anchors $1 \sim m-1$. The target together with anchors $1 \sim m-1$ can preserve $\{mn-n-3\}$ -Privacy.

For the target, the number of unknown scalar variables about the anchors' locations is mn . The target knows the values of $A_{11}, A_{12}, A_{21}, A_{22}, B_{11}, B_{12}, B_{21}$, and B_{22} . Since A_{11} is a symmetric matrix, from which, the target can construct at most $\frac{n^2+n}{2}$ independent linear equations. From $A_{12}, A_{22}, B_{11}, B_{12}, B_{21}$ and B_{22} , the numbers of constructed equations are respectively $n, 1, n, n, 1$ and 1 . Therefore, the total number of independent linear equations is at most $\frac{n^2+n}{2} + 3n + 3$. If $m > \frac{n}{2} + \frac{3}{n} + 3\frac{1}{2}$, the number of independent linear equations is less than the number of unknown scalar variables. In this case, the target cannot know the anchors' locations and the anchors can preserve $\{mn - (\frac{n^2+n}{2} + 3n + 3)\}$ -Privacy.

APPENDIX B

PROOF OF THEOREM 3

When node $0 \notin S_c$ and $m \notin S_c$, even though anchor m does not involve in collusion, the colluding anchors can take one

of them as reference and obtain $n_c - 1$ TDOA measurements, which can construct at most $n_c - 1$ independent linear equations about the target location like (2), where the number of unknown scalar variables is n . If $n_c < n + 1$, the number of unknown scalars is larger than the number of independent linear equations, then the target location cannot be estimated and can preserve $\{n - n_c + 1\}$ -Privacy. Even if the target location is estimated, the non-colluding anchors can only derive d_m , which is insufficient to estimate anchor m 's location. Thus anchor m can preserve $\{n - 1\}$ -Privacy to S_c . Except for the received random matrices, the colluding nodes do not have additional information about the locations of the non-colluding anchors among $1, \dots, m - 1$. Thus, each non-colluding anchor among $1, \dots, m - 1$ can preserve $\{n\}$ -Privacy to S_c .

When node $0 \in S_c$ and $m \notin S_c$, the target and other $n_c - 1$ colluding anchors can estimate d_m via their locations and TDOA measurements. To S_c , the number of unknown scalars in the anchors' locations is $(m - n_c + 1)n$. The number of independent linear equations is at most $1 + \frac{n^2+n}{2} + 3n + 3$, which comes from $d_m, A_{11}, A_{12}, A_{22}, B_{11}, B_{12}, B_{21}$, and B_{22} . If $n_c < m - \frac{n}{2} - \frac{4}{n} - 2\frac{1}{2}$, the number of unknown scalars is larger than the number of independent linear equations. Thus, the locations of the non-colluding nodes cannot be estimated and the non-colluding nodes can preserve $\{(m - n_c - 2)n - \frac{n^2+n}{2} - 4\}$ -Privacy to S_c .

When node $0 \notin S_c$ and $m \in S_c$, similarly with case a), if $n_c < n + 1$, the target can preserve $\{n - n_c + 1\}$ -Privacy to S_c when all the colluding nodes are anchors. Regarding the location information about the non-colluding anchors, anchor m can obtain the values of $\sum_{i=1}^{m-1} \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$, $\sum_{i=1}^{m-1} d_{im}$, and $\sum_{i=1}^{m-1} d_{im}^2$, which can construct at most $n + 3$ independent linear equations. The non-colluding anchors' locations consist of $(m - n_c)n$ unknown scalars. If $n_c < m - \frac{3}{n} - 1$, the locations of the non-colluding anchors cannot be estimated and can preserve $\{(m - n_c - 1)n - 3\}$ -Privacy to S_c .

When node $0 \in S_c$ and $m \in S_c$, the colluding nodes know the values of $A_{11}, A_{12}, A_{21}, A_{22}, B_{11}, B_{12}, B_{21}, B_{22}$, $\sum_{i=1}^{m-1} \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$ and $\sum_{i=1}^{m-1} d_{im}$. The number of unknown scalars to S_c is $(m - n_c + 1)n$. The number of independent linear equations is at most $\frac{n^2+n}{2} + 4n + 5$. If $n_c < m - \frac{n}{2} - \frac{5}{n} - 3\frac{1}{2}$, then $\frac{n^2+n}{2} + 4n + 5 < (m - n_c + 1)n$. Thus, the locations of the non-colluding nodes cannot be estimated and can preserve $\{(m - n_c - 3)n - \frac{n^2+n}{2} - 5\}$ -Privacy to S_c .

APPENDIX C PROOF OF THEOREM 5

For every anchor $i \in \{1, \dots, m - 1\}$, it only has the range difference ratios r_i and r_{2i} , which can construct at most 2 independent linear equations about other nodes' locations. The number of unknown scalar variables to anchor i is mn . Since $mn > 2$ always holds, the locations of the target and other anchors can be protected. Therefore, statement a) holds.

For anchor m , it knows the values of $\sum_{i=1}^{m-1} \mathbf{x}_i$ and $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$, where the number of independent linear equations

is at most $n + 1$ and the number of unknown scalar variables is $(m - 1)n$. Either in 2 dimensional space or 3 dimensional space, $(m - 1)n > n + 1$ always holds, which makes anchor m unable to know other anchors' locations. Moreover, anchor m has no information about the target location. Therefore, statement b) holds.

For the target, the available information includes: the range difference d_{im} , $i = 1, \dots, m - 1$, $A_{11}, A_{12}, A_{21}, B_{11}, B_{12}$, and B_{21} , from which, the target can get at most $\frac{n^2+n}{2} + 3n + m$ independent linear equations. If $m > \frac{n}{2} + \frac{4}{n-1} + 4$, the target will not know the anchors' locations. Therefore, statement c) holds.

APPENDIX D PROOF OF THEOREM 6

When node $0 \notin S_c$ and $m \notin S_c$, the colluding nodes can construct $n_c + 1$ independent equations including $d_{jm} = r_j \sum_{i=1}^{m-1} d_{im}$, $(r_j \sum_{i=1}^{m-1} d_{im})^2 = r_{2j} \sum_{i=1}^{m-1} d_{im}^2$, $\forall j \in S_c$. From these equations, the colluding anchors can derive $n_c - 2$ independent equations about the target location, i.e. $\frac{d_{ij}}{d_{ik}} = \frac{r_i - r_j}{r_i - r_k}$, $\forall i, j, k \in S_c$. If $n_c < n + 2$, the target location cannot be estimated and can preserve $\{n - n_c + 2\}$ -Privacy to S_c . Even if the target location is estimated, the colluding anchors can derive the values of $d_m, \sum_{i=1}^{m-1} d_{im}, \sum_{i=1}^{m-1} d_{im}^2$. If $n_c = m - 1$, only anchor m ' location is unknown and cannot be estimated from the above information; if $n_c < m - 1$, the above information can construct at most 3 independent linear equations, which is insufficient to estimate the non-colluding anchors' locations. Thus, statement a) holds.

When node $0 \in S_c$ and $m \notin S_c$, the colluding nodes have their own locations, the TDOA measurements and the values of $A_{11}, A_{12}, A_{21}, B_{11}, B_{12}$, and B_{21} . Using the known locations and TDOA measurements, the colluding nodes can firstly obtain the distances between the target and anchor m , then obtain the distances between the target and the other non-colluding anchors. These distances construct $m - n_c + 1$ independent equations. Moreover, $A_{11}, A_{12}, A_{21}, B_{11}, B_{12}$ and B_{21} construct at most $\frac{n^2+n}{2} + 3n + 1$ independent linear equations. The number of independent linear equations is at most $\frac{n^2+n}{2} + 3n + m - n_c + 2$. The number of unknown scalar variables is $(m - n_c + 1)n$. If $n_c < m - \frac{n}{2} - \frac{5}{n-1} - 3$, the colluding nodes cannot estimate the non-colluding nodes' locations. Thus, statement b) holds.

When node $0 \notin S_c$ and $m \in S_c$, the colluding nodes have their own locations, the received range difference ratios and the values of $\sum_{i=1}^{m-1} \mathbf{x}_i$ and $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$, where the number of independent linear equations is at most $n_c + n + 1$. From these equations, the colluding anchors can derive $n_c - 1$ independent equations only about the target location, i.e. $\frac{d_{im}}{d_{jm}} = \frac{r_i}{r_j}$, $\forall i, j \in S_c$. If $n_c < n + 1$, the target location cannot be estimated and can preserve $\{n - n_c + 1\}$ -Privacy. Even if the target location is accurately estimated, the colluding anchors can derive the values of $\sum_{i=1}^{m-1} d_{im}, \sum_{i=1}^{m-1} d_{im}^2, \sum_{i=1}^{m-1} \mathbf{x}_i$ and $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$. The above information can construct at most $n + 2$ independent linear equations and the number of unknown scalar variables

is $(m - n_c)n$. If $n_c < m - \frac{2}{n} - 1$, then $n + 2 < (m - n_c)n$ and the colluding nodes cannot estimate the locations of non-colluding anchors. Thus, statement c) holds.

When node $0 \in S_c$ and $m \in S_c$, the colluding nodes have their own locations, all the TDOA measurements, the values of $A_{11}, A_{12}, A_{21}, B_{11}, B_{12}, B_{21}, \sum_{i=1}^{m-1} \mathbf{x}_i$ and $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$. From the above information, the colluding nodes can derive the values of $\sum_{i=1}^{m-1} \mathbf{x}_i \mathbf{x}_i^T$, $\sum_{i=1}^{m-1} \mathbf{x}_i d_{im}$, $\sum_{i=1}^{m-1} \mathbf{x}_i \mathbf{x}_i^T \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i d_{im}^2$ and $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i d_{im}$, from which, along with $\sum_{i=1}^{m-1} \mathbf{x}_i$, $\sum_{i=1}^{m-1} \mathbf{x}_i^T \mathbf{x}_i$ and the TDOA measurements, the colluding nodes can construct at most $\frac{n^2+n}{2} + 4n - n_c + m + 3$ independent linear equations. The number of unknown scalar variables to the colluding nodes is $(m - n_c + 1)n$. If $n_c < m - \frac{n}{2} - \frac{7}{n-1} - 4$, then $\frac{n^2+n}{2} + 4n - n_c + m + 3 < (m - n_c + 1)n$ and the colluding nodes cannot estimate the locations of the non-colluding nodes. Thus, statement d) holds.

REFERENCES

- [1] SRI Consulting Bus. Intell., Menlo Park, CA, USA, "Disruptive civil technologies, appendix F: The internet of things (background)," Conf. Rep. CR 2008-07, 2008.
- [2] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband internet of things: Implementations and applications," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2309–2314, Dec. 2017.
- [3] K. Witrals et al., "High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend," *IEEE Signal Process. Mag.*, vol. 33, no. 2, pp. 59–70, Mar. 2016.
- [4] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 56–62, Nov. 2015.
- [5] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 41–53, Jul. 2005.
- [6] G. Mao, B. Fidan, and B. D. Anderson, "Wireless sensor network localization techniques," *Comput. Netw.*, vol. 51, no. 10, pp. 2529–2553, 2007.
- [7] C. Gentile, N. Alsindi, R. Raulefs, and C. Teolis, *Geolocation Techniques: Principles and Applications*. New York, NY, USA: Springer, 2012.
- [8] M. R. Gholami, R. M. Vaghefi, and E. G. Ström, "RSS-based sensor localization in the presence of unknown channel parameters," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3752–3759, Aug. 2013.
- [9] X. Shi, B. D. Anderson, G. Mao, Z. Yang, J. Chen, and Z. Lin, "Robust localization using time difference of arrivals," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1320–1324, Oct. 2016.
- [10] X. Shi, G. Mao, B. D. Anderson, Z. Yang, and J. Chen, "Robust localization using range measurements with unknown and bounded errors," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 4065–4078, Jun. 2017.
- [11] T. Shu, Y. Chen, and J. Yang, "Protecting multi-lateral localization privacy in pervasive environments," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1688–1701, Oct. 2015.
- [12] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in wifi fingerprint-based localization," in *Proc. IEEE INFOCOM*, 2014, pp. 2337–2345.
- [13] S. Li, H. Li, and L. Sun, "Privacy-preserving crowdsourced site survey in wifi fingerprint-based localization," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, 2016, Art. no. 123.
- [14] X. Wang, Y. Liu, Z. Shi, X. Lu, and L. Sun, "A privacy-preserving fuzzy localization scheme with csi fingerprint," in *Proc. IEEE GLOBECOM*, 2015, pp. 1–6.
- [15] S. U. Hussain and F. Koushanfar, "Privacy preserving localization for smart automotive systems," in *Proc. ACM Annu. Des. Automat. Conf.*, 2016, Art. no. 26.
- [16] A. Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. B. Srivastava, "Proloc: Resilient localization with private observers using partial homomorphic encryption," in *Proc. 16th Int. Conf. Inf. Process. Sensor Netw.*, 2017, pp. 41–52.
- [17] T. Shu, Y. Chen, J. Yang, and A. Williams, "Multi-lateral privacy-preserving localization in pervasive environments," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 2319–2327.
- [18] G. Wang, J. Pan, J. He, and S. Shen, "An efficient privacy-preserving localization algorithm for pervasive computing," in *Proc. 26th Int. Conf. Comput. Commun. Netw.*, 2017, pp. 1–9.
- [19] G. Wang, J. He, X. Shi, J. Pan, and S. Shen, "Analyzing and evaluating efficient privacy-preserving localization for pervasive computing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2993–3007, Aug. 2018.
- [20] "Stage 2 functional specification of user equipment (UE) positioning in UTRAN," 3rd Gener. Partnership Project, Sophia Antipolis Cedex, France, Tech. Spec. 25.305, v11.0.0, 2012.
- [21] S. Fischer, "Observed time difference of arrival (OTDOA) positioning in 3GPP LTE," White Paper, Qualcomm, San Diego, CA, USA, 2014.
- [22] M. D. Gillette and H. F. Silverman, "A linear closed-form algorithm for source localization from time-differences of arrival," *IEEE Signal Process. Lett.*, vol. 15, pp. 1–4, 2008.
- [23] Y. Weng, W. Xiao, and L. Xie, "Total least squares method for robust source localization in sensor networks using TDOA measurements," *Int. J. Distrib. Sens. Netw.*, vol. 7, no. 1, 2011, Art. no. 172902.
- [24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [25] K. Yang, G. Wang, and Z.-Q. Luo, "Efficient convex relaxation methods for robust target localization by a sensor network using time differences of arrivals," *IEEE Trans. Signal Process.*, vol. 57, no. 7, pp. 2775–2784, Jul. 2009.
- [26] A. N. Bishop, B. Fidan, K. Doğançay, B. D. Anderson, and P. N. Pathirana, "Exploiting geometry for improved hybrid AOA/TDOA-based localization," *Signal Process.*, vol. 88, no. 7, pp. 1775–1791, 2008.
- [27] E. Xu, Z. Ding, and S. Dasgupta, "Reduced complexity semidefinite relaxation algorithms for source localization based on time difference of arrival," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1276–1282, Sep. 2011.



Xiufang Shi (M'17) received the B.Sc. degree in automation from the East China University of Science and Technology, Shanghai, China, in 2011, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2016. She was a joint Ph. D. student with The University of Sydney in 2015. She is currently a Postdoctoral Researcher with the College of Control Science and Engineering, Zhejiang University. Her major research interests include wireless localization, target tracking, wireless sensor network, and statistical signal processing.



Junfeng Wu received the B.Eng. degree from the Department of Automatic Control, Zhejiang University, Hangzhou, China, in 2009, and the Ph.D. degree in electrical and computer engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2013. From September to December 2013, he was a Research Associate with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology. He is currently a Postdoctoral Researcher with the Automatic Complex Communication Networks, Signals and Systems Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden. His research interests include networked control systems, state estimation, and wireless sensor networks, multi-agent systems. He received the Guan Zhao-Zhi Best Paper Award at the 34th Chinese Control Conference in 2015.