Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 972101, 13 pages
doi:10.1155/2012/972101

Research Article

Robust Multihop Localization for Wireless Sensor Networks with Unreliable Beacons

Renjian Feng, Xiaolei Guo, Ning Yu, and Jiangwen Wan

School of Instrumentation Science and Opto-electronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191, China

Correspondence should be addressed to Xiaolei Guo, xiaoleiguo@aspe.buaa.edu.cn

Received 28 November 2011; Revised 14 February 2012; Accepted 28 February 2012

Academic Editor: Wensheng Zhang

Multihop localization is a popular approach for determining the positions of normal nodes in large-scale wireless sensor networks. However, most existing multihop localization studies assume that the declared positions of beacon nodes are always reliable or even free of errors, which is not a valid assumption in practice. In this paper, we propose a robust multihop localization algorithm (RMLA) based on trust evaluation for diminishing the effect of unreliable beacons on the accuracy of node localization. Firstly, the trust evaluation framework is established on the basis of evidence theory. According to the multihop geometric relationship among nodes, every beacon evaluates the reliability of other beacons' declared positions. Then, the normal nodes integrate the evaluation results to obtain the total trust degrees of their multihop communication beacons, by use of an average method or an enhanced D-S evidence combination rule. Finally, the normal nodes employ the weighted Taylor-series least squares solver to estimate the optimal values of their coordinates. Extensive simulation results in isotropic and anisotropic networks show the robustness and effectiveness of our algorithm.

1. Introduction

Wireless sensor networks (WSNs) which consist of a large number of low-cost, small-size, and multifunctional sensor nodes spark a revolution in the field of information technology (IT). Due to the advantages of easy deployment, self-management, and no requirement for fixed infrastructure, WSNs can be applied to a wide variety of areas, such as environment monitoring, target tracking, traffic management, battlefield spying, healthcare service, and bush fire surveillance [1–6]. In these applications, the sensor nodes need to collaborate with each other in sensing events of interest by exchanging acquired data. To make the data collected from sensor nodes meaningful, the positions of nodes are often required. Being an essential support technology, WSN localization has got more and more attention in recent years [7–12].

WSN localization is to determine the positions of normal nodes based on the knowledge of beacon nodes (beacons for short) and internode distance or bearing measurements. Since the beacons usually obtain their positions through global positioning system (GPS) or manual configuration in fixed places, raising the density of beacons will significantly increase the cost of network deployment. Therefore, the beacons should make up only a small proportion of sensor nodes in large-scale WSNs. In this case, the normal nodes may fail to estimate their positions by directly measuring the distances to beacons due to their short-range measurement abilities. To solve this problem, multihop localization approach is proposed.

In multihop localization, the normal nodes are not necessarily the one-hop neighbors of beacons, and the distances between any pairs of nonneighboring nodes are inferred by approximating the length of the shortest path to the Euclidean distance. A common assumption in most existing multihop localization studies [13–23] is that the beacons' declared positions are always reliable or even free of errors. However, due to several unavoidable factors (e.g., beacon movement, GPS uncertainties, malicious attacks, etc.) in practice, some beacons (called unreliable beacons (UBs)) may broadcast erroneous or inaccurate position information. A representative application scenario is that sensor

nodes are deployed in the wild to monitor the bush fire or wildlife behavior. Some fixed beacons may be moved by animals or strong wind because they are normally quite tiny. But they still send their original coordinates that are far away from their current positions. In a typical underwater sensor network [24], the beacons first localize themselves through communicating with the surface buoys, that are equipped with GPS receivers, and then assist normal nodes in estimating their locations. Affected by GPS error, nonline-of-sight (NLOS) and other factors, the beacon positions are subject to certain uncertainties. What is more, in hostile environments, the WSNs may suffer from various kinds of internal or external attacks [25]. Some malicious or compromised beacon nodes may give fake position information to disturb the localization procedure of normal nodes. In the above circumstances, robustness and resistance against UBs is an important concern of WSN localization.

In this paper, we devise a robust multihop localization algorithm (RMLA) based on trust evaluation for solving the node self-localization problem in the presence of UBs. To the best of our knowledge, this paper is the first one that introduces the idea of trust evaluation into the unreliable beacon-tolerant multihop localization. In RMLA algorithm, the beacons first observe each other to evaluate the credibility of their multihop communication beacons. Specially, the concepts of evidence theory are employed to deal with the uncertainty factors in trust evaluation. Then the normal nodes integrate the evaluation results to obtain a total view about the trust degrees of their multihop communication beacons. Finally, the normal nodes use the total trust degrees of beacons as weights to achieve robust estimation of their positions. As all these above operations are carried out on each sensor node, RMLA is a completely distributed localization approach with less communication and computation cost. Through simulations, we demonstrate that RMLA can efficiently reduce the influence of both UBs and distance estimation errors on node multihop localization. Under various conditions, compared with some existing localization algorithms, RMLA has apparent advantages in accuracy and robustness.

The rest of this paper is organized as follows. In Section 2 we introduce related works on multihop localization and unreliable beacon-tolerant localization. In Section 3 we formulate the multihop localization problem and introduce some necessary definitions. In Section 4 we present the details of our proposed RMLA algorithm. Section 5 evaluates the performance of RMLA algorithm through simulations. Lastly, Section 6 concludes this paper.

2. Related Works

2.1. Multihop Localization Studies. Based on the idea of distance vector (DV) routing and GPS positioning, Niculescu and Nath [13] proposed two low-cost localization solutions, called DV-distance (range-based) and DV-hop (range-free) algorithms. They are the origination of multihop localization schemes for WSNs. In both algorithms, the lengths of shortest paths or minimum hop counts to beacons are estimated through the message flooding that is similar to the distance vector routing. The accuracy of DV-distance and DV-hop is built on the assumption that the shortest path between a pair of nodes is close to a straight line, which may not always be achievable in anisotropic networks. Shang et al. [14] studied the effect of beacon selection on multihop localization of WSNs. The experimental results show that using only the four nearest beacons could get better localization performance in most cases. In this paper, we denote this method as 4-Multihop. Lim and Hou [15] designed a proximity-distance map (PDM) to characterize the anisotropic features of WSNs. Firstly, the beacons derive an optimal linear transformation collaboratively to map the precise Euclidean distances and the proximities between pairwise beacons. Then, the map is sent to normal nodes to assist them in modifying their multihop estimative distances. The intuition of PDM is that the topology character of entire WSN can be well represented by beacons, but it is not the case in beacon-clustered networks. Cheng et al. [16] developed an algorithm called hybrid localization (HyBloc) to provide reliable localization service with a limited number of clustered beacons. It combines two techniques: MDS-MAP and PDM. HyBloc is less susceptible to the adverse effect of beacon placement, but it requires more communication and computation cost than PDM. Wong et al. [17] proposed a density-aware hop-count localization (DHL) algorithm. In DHL, node density is considered, and an empirical range ratio (the ratio of expected hop distance to node's communication range for a given local density) table is constructed to reduce the overestimation of multihop distances. Wang and Xiao [18] presented an improved multihop algorithm called i-Multihop to minimize theeffect of erroneous multihop estimative distances on node localization. First, the upper bound constraints are utilized to filter out the incorrect distance estimations, and the estimated positions of nodes are pinpointed to the intersection constrained by the correct distances. Second, the distance fitting is used to fit the correct distance measurements, which makes the final estimated positions less affected by the layout of beacons. But i-Multihop has higher computation complexity. Severi et al. [19] gave a constrained semidefinite programming localization algorithm (CSDPLA) which is highly robust when inaccurate range information is present. CSDPLA can run in both centralized and distributed ways and reduce communication cost compared with the classic message-passing localization solutions. To tolerate network anisotropy, Xiao et al. [20] introduced a distributed pattern-driven scheme to produce accurate multihop distance estimation. The main idea of the pattern-driven scheme is to exploit the observation that in anisotropic networks the hop count field propagated from a beacon exhibits three patterns, namely, concentric ring (CR), centrifugal gradient (CG), and distorted gradient (DG). For each pattern has its dominating error source in multihop distances, different distance estimation schemes are adopted in node localization. Lee and Kim [21] considered the relationship between node's communication range and localization accuracy of range-free schemes and proposed a selection method of communication range for DV-Hop algorithm. By utilizing

the selection method, DV-Hop can produce more accurate estimations of average hop distances for normal nodes, and therefore obtain better localization results than the algorithms with fixed communication range. Guo et al. [22] designed a backpropagation (BP) neural network-based localization algorithm (BPL) for three-dimensional (3D) WSNs, in which a BP model is constructed to revise the multihop estimative distances among non-neighboring nodes. Actually BPL is a semidistributed localization solution. Wan et al. [23] gave a light-weight multihop localization algorithm based on grid-scanning (MLGS). By computing the intersection of bounding square rings, the candidates of node coordinates are restricted within a small scope. Then, the close-to-optimal values of node coordinates are searched through a grid-scanning procedure. When all beacons are reliable, MLGS has better adaptability to irregular network topology and lower computation complexity for node localization in large-scale WSNs.

2.2. Unreliable Beacon-Tolerant Localization Studies. In the literature, Kuo et al. [26] defined the beacon movement detection (BMD) problem and proposed four BMD schemes to reduce the effect of beacon movement on node localization. Through mutual observations among beacons, the BMD engine automatically monitors the unnoticed location changes of beacons. After identifying such UBs, the WSNs remove them from the localization engine. Fan et al. [27] presented a two-step localization algorithm to deal with the case, where both inaccurately positioned beacons and ranging error accumulation exist. First, a ranging error-tolerable topology reconstruction method is utilized to estimate the relative positions of sensor nodes. Then, the inaccurately positioned beacons are detected according to the pairs of connected beacons. Both steps need to be performed in a central controller. Based on the fusion of GPS measurements and beacon-to-beacon distance or angle-of-arrival (AOA) estimates, Yu and Guo [28] devised an effective approach to improve the accuracy of beacon positions for both line-of-sight (LOS) and NLOS scenarios. But this method is only suitable to the beacons equipped with GPS receivers. Srirangarajan et al. [29] developed a distributed localization algorithm based on second-order cone programming (SOCP) relaxation. In the presence of beacon position errors, the beacons refine their positions by using the relative distance information communicated with their neighbors. Due to frequent information exchange, this algorithm is energy-inefficient. Vemula et al. [30] formulated node localization from a probabilistic point of view. They proposed four iterative and Monte Carlo sampling-based methods that incorporate beacon position uncertainties to estimate the position distribution (mean and covariance) of normal nodes. These methods have relatively good performance in inhibiting the accumulation of localization errors. Lui et al. [31] brought forward a novel semi-definite programming algorithm for WSN localization with uncertainties in both beacon position and signal propagation speed and presented its simplified form assuming that beacon position errors are independently and identically distributed. Srinivasan et al. [32] introduced the concept of reputation to WSN localization and proposed an approach called distributed reputation-based beacon trust system (DRBTS) for excluding malicious beacons that provide false location information. In DRBTS, each beacon monitors its one-hop neighborhood for misbehaving beacons and updates the reputations of the corresponding beacons. When estimating their coordinates, the normal nodes adopt a simple majority voting scheme to determine whether or not to use a given beacon's location information. Park and Shin [33] gave an attack-tolerant localization protocol, named verification for iterative localization (VeIL). By exploiting the high spatiotemporal correlation existing among neighboring nodes, VeIL can prevent most of the UBs from localization system. Zhu et al. [34] proposed an innovative modular solution featuring two light-weight-modules that are for dedicated functionalities, respectively, but can also be closely integrated. First, some simple geometric triangular rules and an efficient voting technique are harnessed to enable the attack detection module which identifies and filters out unreliable location references. Then, a secure localization module is constructed to compute and cluster certain reference points and estimate the position of normal node with the centroid of the most valuable reference points identified. Jadliwala et al. [35] theoretically analyzed the necessary and sufficient conditions to guarantee a bounded localization error during a two-dimensional (2D) distance-based location estimation in the presence of UBs. On this basis, they outlined three distance-based localization algorithms that can guarantee the localization accuracy, when UB number is below a given threshold. These studies above mainly concentrate on the one-hop or centralized WSN localization. Most of them require densely deployed beacons and higher communication cost, which limit their widespread application in large-scale WSNs.

3. Preliminaries

3.1. Problem Formulation. We consider a network consisting of P beacon nodes and Q normal nodes. All nodes are randomly distributed in a 3D spatial region. The identities (IDs) of beacon nodes are from 1 to P, and those of normal nodes are from $P + 1$ to $P + Q$. Every node is capable of measuring the distance to any of its immediate neighbors. The ranging error ε follows the zero-mean Gaussian distribution, that is, $\varepsilon \sim N(0, \lambda^2)$, where λ is the standard deviation of ranging errors. Every node's communication and ranging radius is R. In multihop localization, each beacon first broadcasts a message that carries its declared position to its one-hop neighbors. Then, the message is propagated in the network in a controlled flooding manner. Through hop-by-hop dissemination of the estimated distances to beacons, every node could estimate the lengths of shortest paths (i.e., multihop estimative distances) to beacons.

As shown in Figure 1, when the normal node N_u gets enough estimated distances d_{ui} to beacons N_i ($i = 1, 2, \ldots, K$), $K \geq 4$, a system of Euclidean equations can be set up:

$$\sqrt{(x_u - x_1)^2 + (y_u - y_1)^2 + (z_u - z_1)^2} = d_{u1},$$

$$\sqrt{(x_u - x_2)^2 + (y_u - y_2)^2 + (z_u - z_2)^2} = d_{u2},$$
$$\vdots$$
$$\sqrt{(x_u - x_K)^2 + (y_u - y_K)^2 + (z_u - z_K)^2} = d_{uK}, \quad (1)$$

where $\mathbf{X}_u = [x_u, y_u, z_u]^T$ is N_u's coordinates that need to be estimated, $\mathbf{X}_i = [x_i, y_i, z_i]^T$ is beacon N_i's declared position.

Generally, $\mathbf{X}_u$ should be located in the intersection of K spheres of which the centers and radiuses are $\mathbf{X}_i$ and d_{ui}, respectively. The smaller the intersection is, the more accurately $\mathbf{X}_u$ can be pinpointed. When both $\mathbf{X}_i$ and d_{ui} are accurate, the $\mathbf{X}_u$ can be well estimated by solving (1). However, if an UB exists (e.g., N_2 is a malicious beacon, its declared position is far from its real location), the system would incorrectly estimate the $\mathbf{X}_u$ to a location that is close to the UB's declared position. It will be even worse and complex, when more beacons are unreliable. In practice, the UBs may seriously affect the localization accuracy of normal nodes and further endanger the applications of WSNs. How to mitigate the influence of UBs and improve the accuracy and robustness of WSN multihop localization is the main topic of our study.

3.2. Related Definitions. Before describing our proposed algorithm, we first introduce some necessary definitions:

(1) multihop communication range: the largest range that a node's propagation packet can reach through multihop forwarding. In dense networks, the radius of a node's multihop communication range is approximately TTL (time to live, i.e., the maximum times that a node's propagation packet can be forwarded) times of its communication radius R;

(2) multihop communication beacon: If a node N_p can communicate with a beacon N_i in one-hop or multihop manner, that is, the beacon N_i is in the TTL field of N_p's propagation packet, the beacon N_i is called N_p's multihop communication beacon. The set of N_p's all multihop communication beacons is denoted by $\mathbf{C}_p$;

(3) multihop count: the number of line segments in the shortest path between a pair of sensor nodes. If the shortest path V_{pq} between nodes N_p and N_q passes L nodes (including N_p and N_q), V_{pq}'s multihop count is $H_{pq} = L - 1$;

(4) calculated distance: the Euclidean distance between the declared positions of pairwise beacons. If the declared coordinates of beacons N_i and N_j are respectively $\mathbf{X}_i$ and $\mathbf{X}_j$, the calculated distance between N_i and N_j is denoted by,

$$D_{ij} = \left\|\mathbf{X}_i - \mathbf{X}_j\right\|_2 = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2 + \left(z_i - z_j\right)^2}. \quad (2)$$

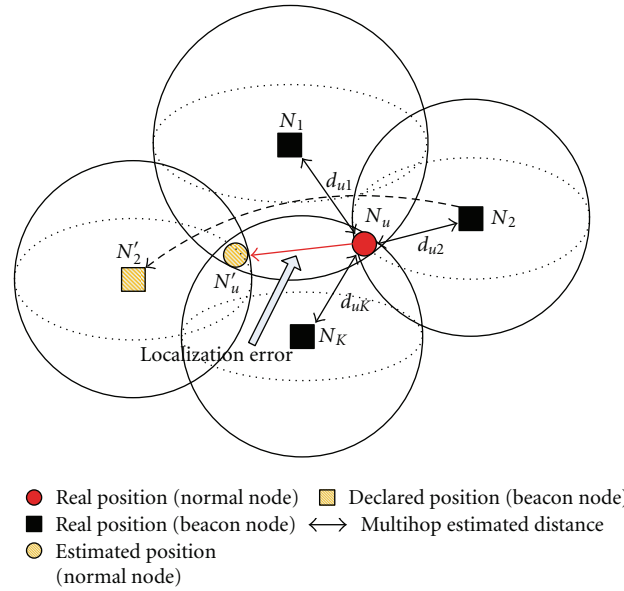

Figure 1: Node localization with an unreliable beacon.

4. Robust Multihop Localization Algorithm

In RMLA algorithm, each beacon evaluates the reliability of other beacons according to the multihop geometric relationship among them, which helps the normal nodes obtain the total trust degrees of their multihop communication beacons and further lays a foundation for robust localization of WSNs. In general, the RMLA algorithm includes three main phases: trust evaluation among beacons, calculation of integrated trust values and weighted estimation of node coordinates. The details of RMLA algorithm are given in the following.

4.1. Trust Evaluation Framework. Trust is an evaluation behavior of a subject to an object. It specifies, evaluates, and sets up trust relationship among entities. Due to the subjectivity of trust evaluation, the evaluation results usually suffer from certain uncertainties. In order to bring the uncertainty factor into the trust evaluation among nodes and make it more reasonable, we employ the concepts of evidence theory [36] to construct the trust evaluation framework in RMLA.

Firstly, we define the identification frame $\Theta = [T, U]$, where T and U represent two exclusive trust states of beacons, namely, "trust" and "distrust." The power set of Θ is $2^\Theta = \{\emptyset, \{T\}, \{T, U\}, \{U\}\}$, in which $\emptyset$ represents the empty set (impossible event), and $\{T, U\}$ represents the "uncertainty" trust state. Then, we construct the basic probability assignment (BPA) function $m : 2^\Theta \to [0, 1]$, in which the BPA values $m(T)$, $m(T, U)$, and $m(U)$ represent the basic confidence level of the following propositions: the beacon is credible, the beacon's trust state is uncertain, and the beacon is incredible. Thus, we can transfer the proposition inference into the set calculation. In this paper,

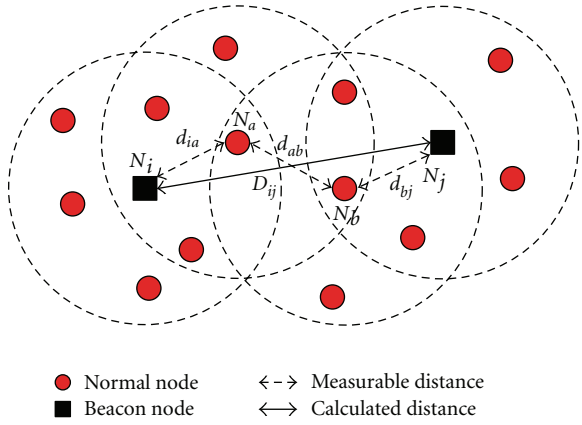

Figure 2: Multihop geometric relationship among beacons.

the trust degree B_i of beacon N_i is defined as the total reliability of proposition T:

$$B_i = \mathrm{Bel}(T) = \sum_{X \subseteq T} m(X) = m(T). \tag{3}$$

In evidence theory, as the rationality and objectivity of BPA function directly influence the accuracy and effectiveness of the evidence fusion, how to determine the BPA function is a key issue. Overall, the BPA values of trust evaluation among beacons should follow the two basic principles:

(1) the sum of all BPA values is equal to 1, that is, $m(T) + m(T,\ U) + m(U) = 1$. This is derived from the definition of BPA function;

(2) the BPA values are dependent on the multihop geometric relationship among beacons. In general, the smaller the difference between the multihop estimative distance (approximation of the Euclidean distance) and the calculated distance is, the larger $m(T)$ is, and the smaller $m(T,\ U)$ and $m(U)$ are. Otherwise, the smaller $m(T)$ is, and the larger $m(T,\ U)$ and $m(U)$ are.

4.2. Trust Evaluation among Beacons. Figure 2 shows the multihop geometric relationship among beacons, in which N_i; N_j represent beacon nodes, and N_a; N_b represent normal nodes. We first consider the ideal condition, where the declared positions of beacons are accurate. According to the declared coordinates of N_j, the beacon N_i can compute the calculated distance to N_j, denoted by D_{ij}. The multihop estimative distance and multihop count between N_i and N_j are $d_{ij} = d_{ia} + d_{ab} + d_{bj}$ and $H_{ij} = 3$, respectively. For N_i and N_j are not adjacent (i.e., N_j is out of N_i's one-hop communication range), the Euclidean distance (equal to the calculated distance under the ideal condition) between them is bigger than their communication radius R, that is, $D_{ij} > R$. According to $(d_{ia}, d_{ab}, d_{bj}) \le R$, we can infer that $d_{ij} \le 3R$. Based on the idea of beeline distance, we can further infer that $D_{ij} \le d_{ij}$. Therefore, the ideal multihop geometric relationship between N_i and N_j should satisfy $R < D_{ij} \le d_{ij} \le H_{ij}R$.

We then extend our consideration to the general case, where the declared positions of beacons may be unreliable. Taking R and $H_{ij}R$ as the boundary points, we divide the trust evaluation of N_i to N_j (i.e., how N_i determine the trust evaluation values $M_{ij} = \{m_{ij}(T),\ m_{ij}(T,\ U),\ m_{ij}(U)\}$ of N_j's declared coordinates $\mathbf{X}_j$) into the following three cases.

(1) if the calculated distance between N_i and N_j exceeds H_{ij} times of nodes' communication radius, that is, $D_{ij} > H_{ij}R$, N_i should consider that the declared position of N_j is incredible. Then N_i should set the trust evaluation values M_{ij} as follows:

$$\begin{aligned} m_{ij}(T) &= 0, \\ m_{ij}(T, U) &= \tau_1, \\ m_{ij}(U) &= 1 - \tau_1. \end{aligned} \tag{4}$$

In practice, due to the influence of environment noise, the measurable distances among neighboring nodes are not exactly accurate. This may lead to the case that a few measurements among neighboring beacons are a little bigger than R (or a few multihop estimative distances between pairwise nonadjacent beacons slightly exceed $H_{ij}R$). In order to prevent the event that beacon N_i incorrectly considers the reliable beacon N_j completely unreliable from appearance in this occasional case, the BPA value $m_{ij}(T,\ U)$ of "uncertainty" in (4) is set to a very small positive decimal τ_1 (such as 0.01). The value of τ_1 mainly depends on the ranging abilities of sensor nodes. If sensor nodes have higher ranging accuracy (i.e., λ is smaller, where λ is the standard deviation of ranging errors), τ_1 should be set to a smaller value. Otherwise, a bigger value should be given to τ_1.

(2) If the calculated distance $D_{ij} \le H_{ij}R$, but the difference between D_{ij} and the multihop estimative distance d_{ij} is larger than nodes' communication radius R (i.e., $|D_{ij} - d_{ij}| > R$), N_i should still consider that the credibility of N_j's declared position is not very high. In this case, we have

$$\begin{aligned} m_{ij}(T) &= 1 - \tau_2 - \omega_2, \\ m_{ij}(T, U) &= \tau_2\ , \\ m_{ij}(U) &= \omega_2, \end{aligned} \tag{5}$$

where τ_2 and ω_2 are positive decimals between 0 and 1. Their values should be determined based on multihop count H_{ij}, local network topology and some other factors. Concretely speaking, τ_2 should be proportional to multihop count H_{ij} (i.e., $\tau_2 \propto H_{ij}$) and be in inverse proportion to N_i's local density I_i (an important parameter that reflects the feature of local network topology) (i.e., $\tau_2 \propto 1/I_i$). This is because larger multihop count and lower local density would make multihop estimative distances

far away from Euclidean distances, which raises the uncertainty of trust evaluation. In contrast to τ_2, ω_2 should be in inverse proportion to H_{ij} (i.e., $\omega_2 \propto 1/H_{ij}$) and be proportional to I_i (i.e., $\omega_2 \propto I_i$). In general, τ_2 is close to 0 (such as 0.1) and ω_2 is close to 1 (such as 0.8).

(3) If $D_{ij} \le H_{ij}R$, and the difference between D_{ij} and d_{ij} is no more than R (i.e., $|D_{ij} - d_{ij}| \le R$), the trust evaluation value M_{ij} of N_i to N_j should be ascertained according to the difference ε_{ij} between D_{ij} and d_{ij}. Thus,

$$\begin{aligned} m_{ij}(T) &= 1 - \frac{\varepsilon_{ij}}{R} = 1 - \frac{\left|D_{ij} - d_{ij}\right|}{R}, \\ m_{ij}(T, U) &= 1 - m_{ij}(T), \\ m_{ij}(U) &= 0. \end{aligned} \tag{6}$$

In multihop scenario, most of trust evaluations among beacons belong to this case. For large-scale or sparse WSNs, we can set a smaller TTL value to reduce the impact of detoured paths on multihop distance estimation. Then the trust evaluation is only confined to the local range (i.e., node's multihop communication range) of WSNs, which prevents the appearance of bigger ε_{ij} between pairwise reliable beacons. In (6), we simplify the mapping between $m_{ij}(T)$ and ε_{ij} to a linear relationship. Actually, their mapping relationship is more complex. If we need to further improve the accuracy of trust evaluation, the determination of $m_{ij}(T)$ should also be combined with the specific network parameters, such as node's ranging ability, multihop count, node's local density, and so forth. For instance, $m_{ij}(T)$ may be in inverse proportion to λ and H_{ij} (i.e., $m_{ij}(T) \propto 1/\lambda$, $m_{ij}(T) \propto 1/H_{ij}$), and be proportional to I_i (i.e., $m_{ij}(T) \propto I_i$). Thus, an accurate expression of $m_{ij}(T)$ can be written as $m_{ij}(T) = f(\varepsilon_{ij}, \lambda, H_{ij}, I_i)$. In order to simplify the computation complexity of trust evaluation, this paper employs the simple linearity in (6) by default.

4.3. Calculation of Integrated Trust Values. After the beacon N_i obtains the trust evaluation values $\mathbf{M}_i = \{M_{ij} \mid N_j \in \mathbf{C}_i\}$ of its all multihop communication beacons ($\mathbf{C}_i$), it broadcasts $\mathbf{M}_i$ to the network in a multihop flooding manner. The normal nodes store the trust evaluation values they received, based on which they could calculate the integrated trust values of their multihop communication beacons. Additionally, during this phase, every beacon or normal node could optionally update its trust evaluation results according to other nodes' broadcast information.

Figure 3 shows how the normal node N_u integrates the trust evaluation values of its multihop communication beacon N_k. The circles represent nodes' multihop communication ranges. In the phase of trust evaluation among beacons, all beacons ($\mathbf{C}_k$) in N_k's multihop communication

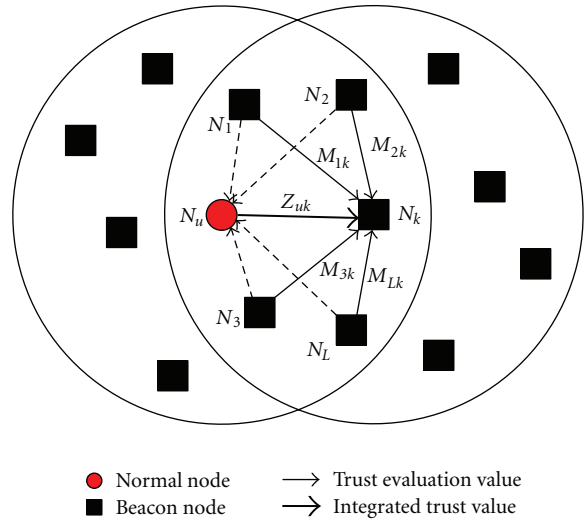

Figure 3: Integration of trust evaluation values.

range evaluate the credibility of N_k's declared position. Through the multihop propagation of beacons' evaluation results, the normal node N_u can receive the trust evaluation values of N_k from some of its multihop communication beacons ($\mathbf{C}_u$). When N_u receives J trust evaluation values M_{jk} ($j = 1, 2, \ldots, J$) of N_k from beacons N_j ($N_j \in \mathbf{C}_u \cap \mathbf{C}_k$), N_u could combine all M_{jk} to obtain an integrated trust value $Z_{uk} = \{m_{uk}(T), m_{uk}(T, U), m_{uk}(U)\}$ of N_k. In this paper, we give two combination methods for calculating the integrated trust values of beacons.

(1) average method: assuming the weights of trust evaluation values M_{jk} ($j = 1, 2, \ldots, J$) obtained from the beacons $N_j \in \mathbf{C}_u \cap \mathbf{C}_k$ are equivalent. From the perspective of traditional probability theory, we take the average value of all M_{jk} as the integrated trust value Z_{uk} of the normal node N_u to the beacon N_k:

$$\begin{aligned} Z_{uk} &= \frac{1}{J}\sum_{j=1}^{J} M_{jk} \\ &= \left\{ \frac{1}{J}\sum_{j=1}^{J} m_{jk}(T),\ \frac{1}{J}\sum_{j=1}^{J} m_{jk}(T, U),\ \frac{1}{J}\sum_{j=1}^{J} m_{jk}(U) \right\}. \end{aligned} \tag{7}$$

This average method is simple and requires less computation cost. But it only balances the beacons' viewpoints, while does not make full use of the uncertainty information in trust evaluation values. Its integration performance needs to be further improved.

(2) enhanced D-S combination method: in evidence theory, the Dempster-Shafer (abbreviated D-S) combination method [36] is a basic rule to evaluate the joint effect of evidences. It can integrate the fuzzy and uncertain information arising from multiple aspects. If the conflict among evidences is weak, the D-S method has preferable integration performance.

However, in the trust evaluation among beacons, some beacons (especially the UBs) may produce evaluation results that are far from most beacons' viewpoints. In this case, there would be strong conflict among evidences, which results in the reduction of combination performance of D-S method. In order to diminish the influence of evidence conflict on trust value integration, we adopt the enhanced D-S combination method in the following.

Firstly, we define the deviation degree of evidence:

$$\delta_{jk} = \left\| M_{jk} - \frac{1}{J}\sum_{j=1}^{J} M_{jk} \right\|_2. \tag{8}$$

When δ_{jk} is large, that is, M_{jk} is far from the average viewpoint of J beacons, we consider that there is strong conflict between M_{jk} and other evidences. Otherwise, M_{jk} was relatively consistent with other evidences. We set a threshold Δ to judge whether M_{jk} should be accepted to participate in the evidence combination:

$$\begin{cases} \delta_{jk} \le \Delta, & M_{jk} \text{ is accepted,} \\ \delta_{jk} > \Delta, & M_{jk} \text{ is refused.} \end{cases} \tag{9}$$

Here, we briefly discuss how to set the value of threshold Δ. As δ_{jk} is essentially the distance of two trust evaluation values, its maximum is $\sqrt{2}$. In order to make (9) meaningful, Δ should be no more than 1.414 (i.e., $\Delta \le 1.414$). In general, Δ is mainly affected by the UB number. When there are more UBs in WSNs, we should set Δ a smaller value to refuse conflicting evidences as many as possible. In contrast, if the UB number is smaller, Δ should be set to a bigger value. In our experience, when $0.6 \le \Delta \le 1.1$, the majority of conflicting evidences caused by UBs can be filtered out.

According to (9), the normal node N_u could select an evidence set $\{M_{1k}, M_{2k}, \ldots, M_{Sk}\}$ with smaller conflict, where $S \le J$. Then, the integrated trust value Z_{uk} of the beacon N_k is calculated by using the traditional D-S combination method:

$$\begin{aligned} & m_{uk}(\varnothing) = 0, \\ & m_{uk}(A) = (m_{1k} \oplus m_{2k} \oplus \cdots \oplus m_{Sk})(A) \\ & \quad = \frac{1}{1-G} \\ & \qquad \times \sum_{\bigcap_{j=1}^{S} A_{jk} = A} m_{1k}(A_{1k}) \times m_{2k}(A_{2k}) \times \cdots \times m_{Sk}(A_{Sk}), \\ & \{A \ne \varnothing,\ A \subseteq \boldsymbol{\Theta},\ (A_{1k}, A_{2k}, \ldots, A_{Sk}) \subseteq \boldsymbol{\Theta}\}, \end{aligned} \tag{10}$$

where $G = \sum_{\bigcap_{j=1}^{S} A_{jk} = \varnothing} m_{1k}(A_{1k}) \times m_{2k}(A_{2k}) \times \cdots \times m_{Sk}(A_{Sk}) < 1$.

Finally, the normal node N_u gets the total trust degree $B_{uk} = m_{uk}(T)$ of the beacon N_k. Generally, through trust evaluation among nodes, the reliable beacons could be endowed with higher total trust degrees, while the UBs are given lower ones. For both average and enhanced D-S combination methods, we can also set a threshold ξ and compare B_{uk} with ξ. If $B_{uk} \ge \xi$, B_{uk} is set to 1, otherwise it is set to 0. In practice, this is an optional operation.

4.4. Weighted Estimation of Node Coordinates. In Section 3.1, the essence of solving (1) is to find an optimal $\mathbf{X}_u$ to minimum the sum of squares of differences between Euclidean distances and multihop estimative distances (EM differences for short), that is, least squares estimation. When an UB exists, its erroneous position information would raise the corresponding EM difference and disturb the least squares estimation. To resolve this problem, two schemes can be used, eliminating the unreliable equation and reducing the weight of the unreliable equation on node coordinate estimation. Considering the former scheme may inevitably lead to a certain loss of valid information, we adopt the latter one. Through multiplying a smaller weight on both sides of the unreliable equation, we can reduce its EM difference in least squares estimation, and therefore diminish the effect of this equation on coordinate estimation.

After the normal node N_u gets the total trust degrees $B_{ui}(i = 1, 2, \ldots, K)$ of its all multihop communication beacons, we add different weights to the equations in (1) according to B_{ui}:

$$\begin{aligned} & B_{u1}\sqrt{(x_u - x_1)^2 + (y_u - y_1)^2 + (z_u - z_1)^2} = B_{u1} d_{u1}, \\ & B_{u2}\sqrt{(x_u - x_2)^2 + (y_u - y_2)^2 + (z_u - z_2)^2} = B_{u2} d_{u2}, \\ & \qquad \vdots \\ & B_{uK}\sqrt{(x_u - x_K)^2 + (y_u - y_K)^2 + (z_u - z_K)^2} = B_{uK} d_{uK}. \end{aligned} \tag{11}$$

By weighting, the beacons with lower trust degrees (or UBs) will have smaller influence on the coordinate estimation of node N_u. Then we utilize the weighted Taylor-series least squares solver [37, 38] to calculate the position coordinates of N_u:

(1) calculate the centroid coordinates $\mathbf{X}_0 = [x_0, y_0, z_0]^T$ of K beacons, that is, $\mathbf{X}_0 = 1/K \sum_{i=1}^{K} \mathbf{X}_i$;

(2) expand the function $f(\mathbf{X}_u) = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2}$ in Taylor series at $\mathbf{X}_0$ and ignore the high order terms. Equation (11) is transformed into the following form:

$$\begin{aligned} & B_{u1}\left(\frac{x_0 - x_1}{r_1}\Delta x_u + \frac{y_0 - y_1}{r_1}\Delta y_u + \frac{z_0 - z_1}{r_1}\Delta z_u\right) \\ & \quad = B_{u1}(d_{u1} - r_1), \\ & B_{u2}\left(\frac{x_0 - x_2}{r_2}\Delta x_u + \frac{y_0 - y_2}{r_2}\Delta y_u + \frac{z_0 - z_2}{r_2}\Delta z_u\right) \\ & \quad = B_{u2}(d_{u2} - r_2), \\ & \qquad \vdots \\ & B_{uK}\left(\frac{x_0 - x_K}{r_K}\Delta x_u + \frac{y_0 - y_K}{r_K}\Delta y_u + \frac{z_0 - z_K}{r_K}\Delta z_u\right) \\ & \quad = B_{uK}(d_{uK} - r_K), \end{aligned} \tag{12}$$

where $r_i = \|\mathbf{X}_0 - \mathbf{X}_i\|_2$ represents the Euclidean distance between $\mathbf{X}_0$ and $\mathbf{X}_i$;

(3) set

$$\mathbf{W} = \begin{bmatrix} B_{u1} & 0 & 0 \\ 0 & B_{u2} & 0 \\ & \ddots & \\ 0 & 0 & B_{uK} \end{bmatrix},$$

$$\mathbf{A} = \begin{bmatrix} \frac{x_0 - x_1}{r_1} & \frac{y_0 - y_1}{r_1} & \frac{z_0 - z_1}{r_1} \\ \frac{x_0 - x_2}{r_2} & \frac{y_0 - y_2}{r_2} & \frac{z_0 - z_2}{r_2} \\ & \vdots & \\ \frac{x_0 - x_K}{r_K} & \frac{y_0 - y_K}{r_K} & \frac{z_0 - z_K}{r_K} \end{bmatrix}, \quad (13)$$

$$\Delta\mathbf{X}_u = \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} d_{u1} - r_1 \\ d_{u2} - r_2 \\ \vdots \\ d_{uK} - r_K \end{bmatrix},$$

thus (12) can be reformulated as

$$\mathbf{WA}\Delta\mathbf{X}_u = \mathbf{WB}; \quad (14)$$

(4) solve (14) by using the least squares method, and we get $\Delta\mathbf{X}_u = (\mathbf{A}^T\mathbf{W}^T\mathbf{WA})^{-1}\mathbf{A}^T\mathbf{W}^T\mathbf{WB}$;

(5) judge whether the iteration termination condition $\|\Delta\mathbf{X}_u\|_2 \le \gamma$ is satisfied, where γ is a prior-defined and flexible threshold based on the accuracy requirement. If $\|\Delta\mathbf{X}_u\|_2 \le \gamma$ is satisfied, we stop the iteration process. Otherwise, we set $\mathbf{X}_0 = \mathbf{X}_0 + \Delta\mathbf{X}_u$ and go to step (2);

(6) repeat steps (2) to (5) until the iteration termination condition is satisfied or the maximum iteration number is reached, whichever comes earlier. The final output $\mathbf{X}_0$ is the estimated coordinates of N_u.

4.5. Discussion of RMLA Algorithm. As all the localization procedures in RMLA are carried out on every sensor node, RMLA is essentially a distributed multihop localization algorithm. Relative to centralized algorithms, RMLA has the advantages that distributed algorithms possess, such as low computation complexity, less communication cost, and high network scalability. As mentioned above, RMLA is comprised of three steps, namely, trust evaluation, trust value integration, and position estimation. Their computation complexities are $O(P)$, $O(Q)$, and $O(Q)$, respectively, where P is the number of beacons, and Q is the number of normal nodes. For large-scale networks, P is usually much smaller than Q. Thus the total computation complexity of RMLA is $O(Q)$, while that of MDS-MAP (a typical centralized algorithm proposed by Shang et al. [12], in which the matrix

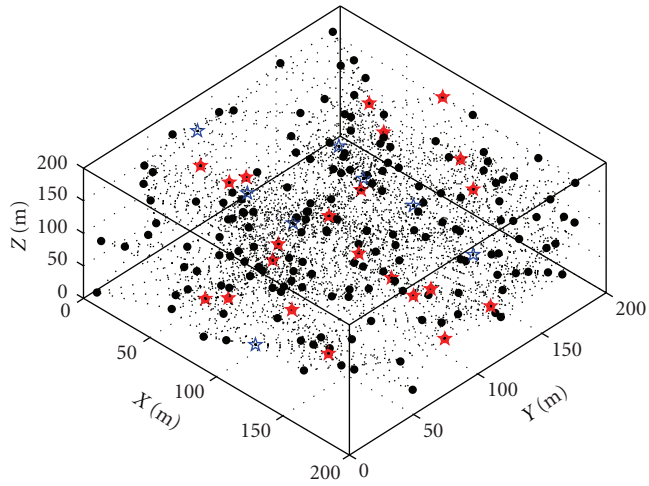

Figure 4: Network topology (isotropic network).

comprised by the multihop estimative distances between all pairs of nodes are required) is $O((P+Q)^3)$. In localization, RMLA requires only the local information to be sent to the corresponding nodes, while the centralized algorithms need to collect all internode measurements to a central processor. Therefore, RMLA is more energy-efficient than centralized algorithms, especially in large-size WSNs. The detailed discussion about the performance comparison of centralized and distributed algorithms can be found in [8].

For normal nodes, the computation and communication cost required in RMLA is comparable to most existing multihop localization solutions. The additional cost is in the phase of trust value integration in which the normal nodes need to receive the trust evaluation values from beacons (resulting in communication cost) and compute the integrated trust values of their multihop communication beacons (resulting in computation cost). However, relative to the entire process of multihop localization, the cost of trust value integration is lower. It is nearly equivalent to (or even smaller than) the cost required for distance modification in some improved multihop localization solutions, such as PDM [15], Hybloc [16], and BPL [22]. As described in Section 4.4, the weighted calculation of node coordinates includes iteration operations, and the computation cost of normal nodes is related to the iteration number. If requesting higher localization accuracy, we should set the threshold γ a smaller value, which will increase the iteration number and further raise the computation cost. Otherwise, we can set γ a bigger value. Empirically, we could get a better tradeoff between computation cost and localization accuracy of RMLA when $\gamma = (0.001 \sim 1)$.

5. Performance Evaluation

In this section, we conduct extensive simulations to study the performance of the proposed RMLA algorithm. All simulations are run in MatLab. Figure 4 shows a typical realization of 3D WSN with a number of UBs. The solid pentagrams "★", hollow pentagrams "☆", and solid dots "•" represent reliable

Table 1: Default network configuration parameters.

Parameters	Values
Network size (in meters)	$200 \times 200 \times 200$
Deployment strategy	Random
Number of nodes $(P + Q)$	200
Number of beacon nodes (P)	30
UB Number	8
TTL	5
Ranging radius R (in meters)	$50 \sim 70$
Network connectivity	15
Standard deviation of ranging errors (λ)	1

beacons, unreliable beacons, and normal nodes, respectively. The default network configuration parameters are shown in Table 1. Unless specified, we use the default parameters in simulations.

We first compare the average localization errors (ALEs) of the traditional multihop localization method without trust evaluation (abbrevd. t-Multihop) in which Taylor-series least squares solver is also used to compute nodes' coordinates, the proposed algorithm with average method (abbrevd. RMLA1) and the proposed algorithm with enhanced D-S combination rule (abbrevd. RMLA2). Then, we present the accuracy comparison results of our RMLA methods and other typical localization algorithms (PDM, 4-Multihop, i-Multihop, and MDS-MAP). To reduce the influence of outliers, we run each simulation 100 times and take the average results as the final data points. The ALE is normalized by the nodes' communication (or ranging) radius R:

$$\text{ALE} = \frac{1}{QR} \sum_{u=P+1}^{P+Q} \left|\left|\mathbf{X}_u - \mathbf{X}_u^r\right|\right|_2 \times 100\%, \tag{15}$$

where $\mathbf{X}_u^r$ is the real coordinates of normal node N_u.

5.1. Distribution of Node Localization Errors. Firstly, we analyze the distribution of node localization errors in the default environments. Figure 5 with log-scale y-axis presents the distribution boxplots of node localization errors. It can be seen that the localization performance of t-Multihop method is much affected by UBs. t-Multihop gives an average error of 50.24% and a median error of 44.37%, and its maximum outlier even reaches 254.92%. Compared with t-Multihop, both RMLA1 and RMLA2 have significant improvement in localization accuracy. Among them, RMLA2 performs better. Its average, median, and maximum errors are respectively 28.54%, 27.64%, and 68.18% (compared with 35.35%, 32.17%, and 103.72% of RMLA1). As RMLA1 employs the simple average method to calculate the integrated trust values of beacons, its evaluation results are worse than those of RMLA2, which further leads to the reduction of its localization accuracy. However, the performance of RMLA1 is much better than that of t-Multihop.

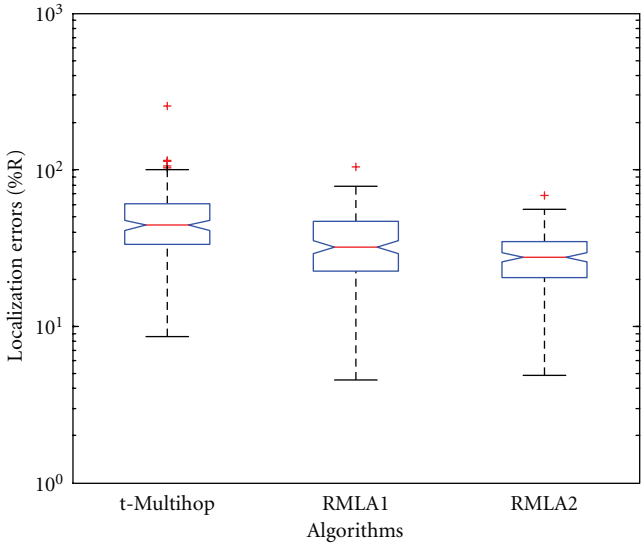

Figure 5: Distribution boxplots of node localization errors.

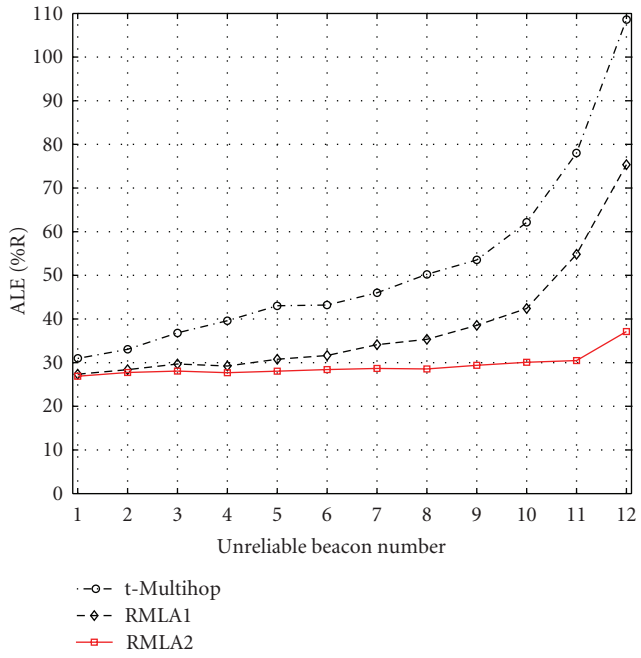

Figure 6: ALE versus UB number.

5.2. Impact of UB Number. In this part, we investigate the effects of UB number on localization accuracies of t-Multihop, RMLA1, and RMLA2. The statistics for ALEs of three methods is shown in Figure 6. With the increase of UB number, the ALEs of t-Multihop and RMLA1 rise obviously, while that of RMLA1 remains stable (nearly a horizontal line when the UB number is no more than 11). When there are 5 UBs, the ALE of t-Multihop is more than 40% (compared with about 30% of both RMLA methods). The performance of RMLA1 is almost the same as that of RMLA2 when UBs are less (no more than 5). However, the ALE of RMLA1 exceeds 40% when UB number reaches 10, while that of RMLA2 is

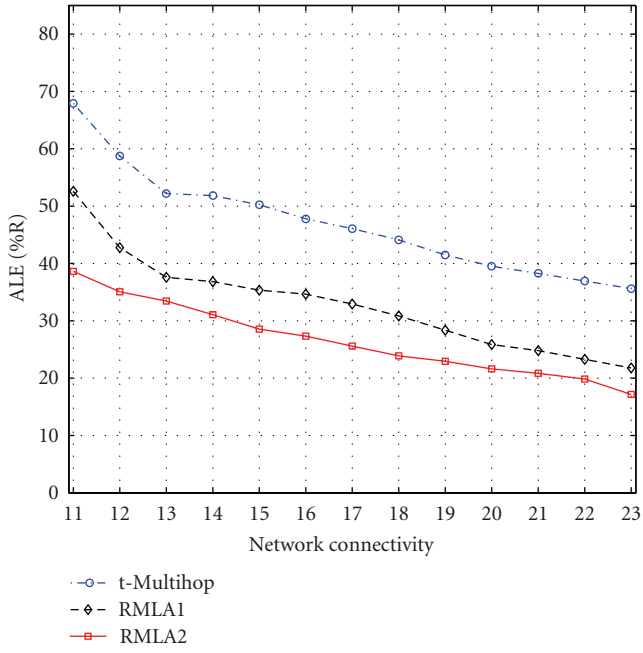

Figure 7: ALE versus network connectivity.

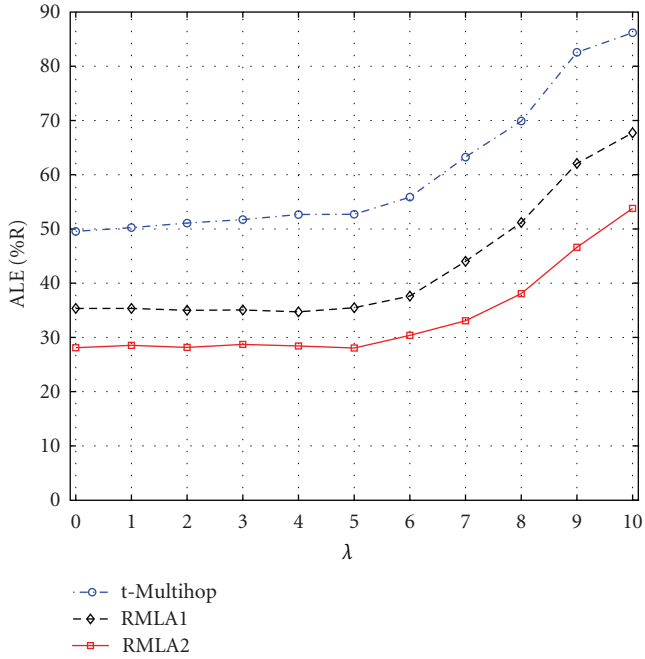

Figure 8: ALE versus ranging error.

still about 30%. Therefore, RMLA2 is more robust to UBs for WSN multihop localization, especially there are more UBs. When UB number is 12 (i.e., 40% of beacons are unreliable), the ALE of RMLA2 is still less than 40% of nodes' communication radius.

5.3. Impact of Network Connectivity. We vary nodes' communication radius and get the accuracy comparisons of three methods under different network connectivity, ranging from 11 to 23 (see Figure 7). Generally, the probability that a shortest path between a pair of nodes is close to a straight line grows as the node densities increase, which directly results in the improvement of localization accuracy. So the ALEs of three methods decline with the network connectivity increasing. But both RMLA methods always produce more accurate results. Compared with t-Multihop, RMLA1 and RMLA2 improve the localization accuracy by at least 13% and 17%, respectively. When the network connectivity is 11, the accuracy improvement of RMLA2 even reaches more than 25%. In RMLA, through trust evaluation among nodes, the beacons (reliable or unreliable) with low local densities to which the shortest paths are generally winding lines would be given lower trust degrees, which further lowers the influence of multihop distance estimation errors on node localization. Therefore, the RMLA algorithm also has positive effects on dealing with the uncertainties in multihop estimative distances.

5.4. Impact of Ranging Error. Figure 8 shows the comparison results of ALEs under different standard derivations λ of ranging errors. It can be seen that both RMLA methods always perform much better than t-Multihop. The accuracy improvements of RMLA1 and RMLA2 are respectively about 15% and more than 20%. When $\lambda \leq 5$, the variation trend of ALEs of three methods are not very distinct. That is because the multihop distance estimation errors mainly arise from the approximations between the lengths of the shortest paths and the Euclidean distances when the ranging errors are small. Constant network connectivity makes the multihop distance estimation errors relatively stable. When λ increases to 6, the direct ranging errors begin to play a leading role in the distance estimation uncertainties. From this point ($\lambda = 6$), all ALEs of three methods rise gradually with λ increasing. Among them, RMLA2 has better inhibition effect on ranging errors. When $\lambda \geq 7$, compared with t-Multihop, RMLA2 can improve the localization accuracy by more than 30%.

5.5. Impact of Network Topology. In this part, we analyze the impact of irregular network topology on the performance of three methods. Figure 9 shows a typical anisotropic network in which sensor nodes are randomly distributed in a C-shape spatial area. We still use the default parameters in Table 1. The only difference is that the value of TTL is set to 4 for longer shortest paths are more susceptible to concave shapes. Figure 10 presents the result of accuracy comparisons. Since the shortest path between pairwise distant nodes in irregular networks is generally more winding than that in uniform networks, the ALEs of three methods in Figure 10 are bigger than those in Figure 6. However, RMLA still performs consistently much better than t-Multihop. Compared with RMLA2, the irregular network topology has more significant influence on the performance of RMLA1 and t-Multihop of which the ALEs rise sharply with UB number increasing. When the UB number is no more than 10, the ALE curve of RMLA2 approaches to a horizontal line (always less than 40%). When the UB number reaches 11, the accuracy of

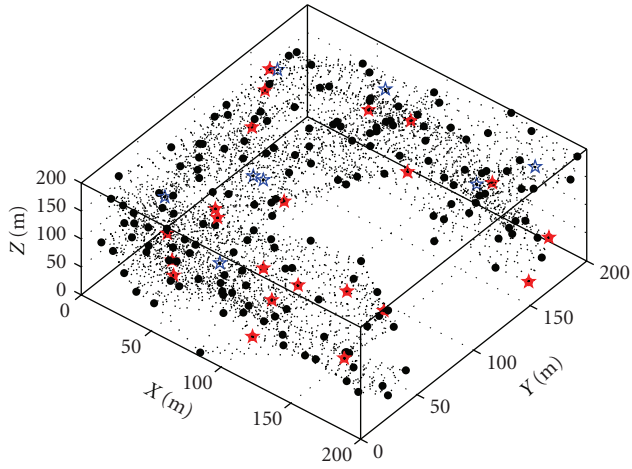

Figure 9: Network topology (anisotropic network).

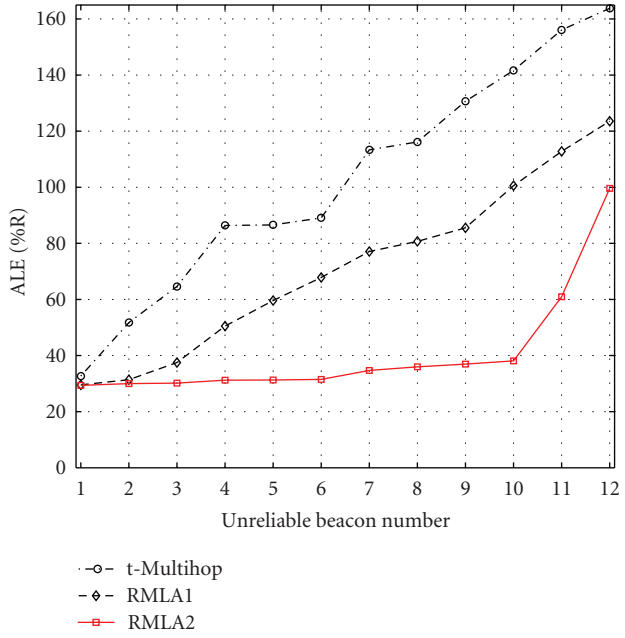

Figure 10: ALE versus UB number (anisotropic network).

RMLA2 begins to decrease markedly, but it is still superior to those of RMLA1 and t-Multihop.

5.6. Comparison of RMLA and Other Typical Algorithms. Finally, we evaluate the localization performance of RMLA by comparing it with three typical multihop algorithms (1) the 4-Multihop algorithm [14], (2) the PDM algorithm [15], (3) the i-Multihop algorithm [18], and one representative centralized algorithm, MDS-MAP [12], in the isotropic network shown in Figure 4 and the anisotropic network shown in Figure 9. Figures 11–13 present the comparison results when the UB ratios are 0%, 10%, and 20%, respectively (i.e., the UB numbers are 0, 3, and 6). As can be seen from Figure 11, when there is no UB, i-Multihop gives the best accuracy, PDM comes second, and MDS-MAP performs

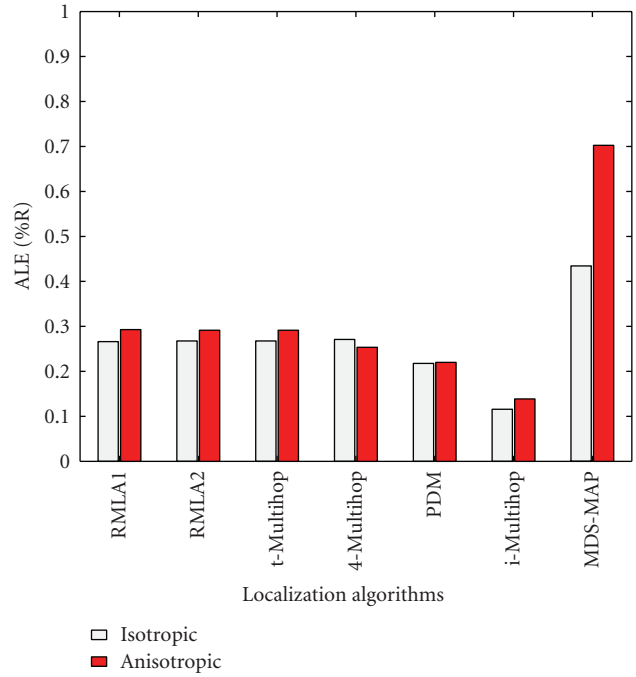

Figure 11: Performance comparison of various algorithms (no UB).

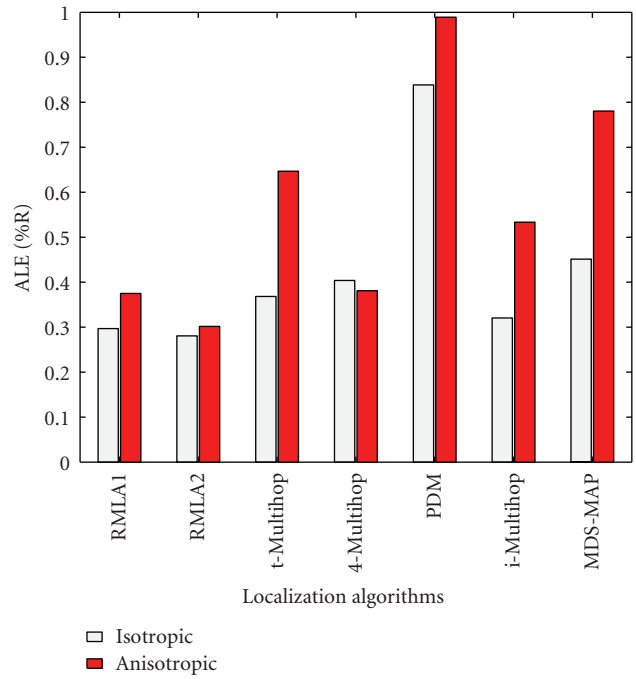

Figure 12: Performance comparison of various algorithms (10% UBs).

the worst. In isotropic networks, the ALEs of RMLA1, RMLA2, t-Multihop, and 4-Multihop are nearly equivalent (about 27%), while in anisotropic networks the ALE of 4-Multihop is about 4% lower than those (about 29%) of the other three algorithms. When 10% UBs exist in WSNs (see Figure 12), the performance of PDM declines most

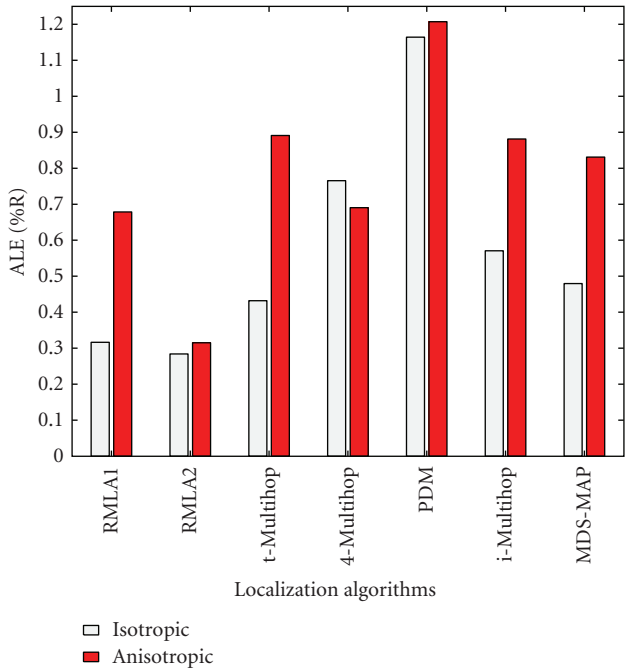

Figure 13: Performance comparison of various algorithms (20% UBs).

significantly (its ALEs in both networks are more than 60%). This is because the erroneous information provided by UBs severely affects the feature extraction of PDM, which further leads to the failure of multihop localization. 4-Multihop and i-Multihop also have a marked decrease in accuracy, especially in anisotropic networks. In Figure 12, RMLA2 performs the best, and its accuracy is comparable with that in Figure 11. MDS-MAP is less affected by UBs, but its ALE is still much higher than those of the other algorithms except PDM. With the increase of UB number, the advantage of RMLA2 becomes more obvious (see Figure 13). In isotropic networks, compared with 4-Multihop, PDM, i-Multihop, and MDS-MAP, it can improve localization accuracy by 48%, 88%, 29%, and 20%, respectively. In anisotropic networks, the gaps can reach 38%, 89%, 57%, and 52%. From Figures 11–13, we can conclude that the RMLA algorithms have better performance in resistance against UBs than the other five solutions. It is worth noting that RMLA2 is more efficient in anisotropic networks.

6. Conclusions

In this paper, we address the problem of node multihop localization in large-scale wireless sensor networks with unreliable beacons. Based on trust evaluation and evidence theory, we present a robust multihop localization algorithm, called RMLA, which is shown to be able to effectively mitigate the influence of UBs on the position estimation of normal nodes and improve WSN localization accuracy. In the phase of evidence combination, both the average method and the enhanced D-S combination method can be utilized to calculate the integrated trust values of beacons. The average method is simple and requires less computation cost, it is very suitable to sensor nodes with low computing power. As the D-S method makes full use of the uncertainty information in trust evaluation values, it produces more accurate results than the average method, especially there are more UBs in WSNs. In practice, we should make a reasonable tradeoff between localization accuracy and computation cost to determine which method to be adopted. Through simulations, we demonstrate that RMLA performs much better than some existing localization solutions. In isotropic networks, RMLA could achieve robust multihop localization even if 40% of beacons are unreliable. In anisotropic networks, the ratio can also reach more than 30%. Additionally, RMLA has the advantages in resistance against uncertainties in both multihop estimative distances and direct ranging results. In our future work, we will construct a more accurate BPA function related to specific network environment and implement the RMLA algorithm on experimental WSN prototypes to verify its practicability.

Acknowledgments

The authors would like to thank the anonymous reviewers for their comments. This paper is supported by the National Natural Science Foundation of China (NSFC) under Grants no. 60974121 and no. 61001138.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[3] I. Bekmezci and F. Alagöz, "Energy efficient, delay sensitive, fault tolerant wireless sensor network for military monitoring," *International Journal of Distributed Sensor Networks*, vol. 5, pp. 729–747, 2009.

[4] D. Hamel, M. Chwastek, S. Garcia, B. Farouk, M. Kam, and K. R. Dandekar, "Sensor placement for urban homeland security applications," *International Journal of Distributed Sensor Networks*, vol. 2010, Article ID 859263, 15 pages, 2010.

[5] H. Alemdar, Y. Durmus, and C. Ersoy, "Wireless healthcare monitoring with RFID-enhanced video sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2010, Article ID 473037, 10 pages, 2010.

[6] N. Trigoni and B. Krishnamachari, "Sensor network algorithms and applications introduction," *Philosophical Transactions of the Royal Society A*, vol. 370, no. 1958, pp. 5–10, 2012.

[7] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization systems for wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 6–12, 2007.

[8] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *Computer Networks*, vol. 51, no. 10, pp. 2529–2553, 2007.

[9] M. Erol-Kantarci, H. T. Mouftah, and S. Oktug, "A survey of architectures and localization techniques for underwater acoustic sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 3, pp. 487–502, 2011.

[10] S. Čapkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[11] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 96–101, 2008.

[12] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz, "Localization from mere connectivity," in *Proceedings of the 4th International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pp. 201–212, Annapolis, Md, USA, June 2003.

[13] D. Niculescu and B. Nath, "DV based positioning in Ad Hoc networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 267–280, 2003.

[14] Y. Shang, H. Shi, and A. A. Ahmed, "Performance study of localization methods for ad-hoc sensor networks," in *Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 184–193, Fort Lauderdale, Fla, USA, October 2004.

[15] H. Lim and J. C. Hou, "Localization for anisotropic sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, pp. 138–149, Miami, Fla, USA, March 2005.

[16] K. Y. Cheng, K. S. Lui, and V. Tam, "HyBloc: localization in sensor networks with adverse anchor placement," *Sensors*, vol. 9, no. 1, pp. 253–280, 2009.

[17] S. Y. Wong, J. G. Lim, S. V. Rao, and W. K. G. Seah, "Multihop localization with density and path length awareness in non-uniform wireless sensor networkss," in *Proceedings of IEEE Vehicular Technology Conference (VTC '05)*, pp. 2551–2555, Stockholm, Sweden, May 2005.

[18] C. Wang and L. Xiao, "Sensor localization in concave environments," *ACM Transactions on Sensor Networks*, vol. 4, no. 1, article 3, pp. 1–31, 2008.

[19] S. Severi, G. Abreu, and D. Dardari, "A quantitative comparison of multihop localization algorithms," in *Proceedings of the 7th Workshop on Positioning, Navigation and Communication (WPNC '10)*, pp. 200–205, Dresden, Germany, March 2010.

[20] Q. J. Xiao, B. Xiao, J. N. Cao, and J. P. Wang, "Multihop range-free localization in anisotropic wireless sensor networks: a pattern-driven scheme," *IEEE Transactions on Mobile Computing*, vol. 9, no. 11, pp. 1592–1607, 2010.

[21] S. Lee and K. Kim, "Determination of communication range for range-free multi-hop localization in wireless sensor networks," in *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN '11)*, pp. 1–4, Maui, Hawaii, USA, July 2011.

[22] X. L. Guo, N. Yu, Y. F. Wu, and J. W. Wan, "Application of BP neural network to 3D localization in wireless sensor networks," *Chinese High Technology Letters*, vol. 21, no. 5, pp. 471–477, 2011.

[23] J. W. Wan, X. L. Guo, N. Yu, Y. F. Wu, and R. J. Feng, "Multihop localization algorithm based on grid-scanning for wireless sensor networks," *Sensors*, vol. 11, no. 4, pp. 3908–3938, 2011.

[24] Z. Zhou, J. H. Cui, and S. Zhou, "Localization for large-scale underwater sensor networks," *Lecture Notes in Computer Science*, vol. 4479, Article ID 0644190, pp. 108–119, 2007.

[25] S. Hong, S. Lim, and J. Song, "Unified modeling language based analysis of security attacks in wireless sensor networks: a survey," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 4, pp. 805–821, 2011.

[26] S. P. Kuo, H. J. Kuo, and Y. C. Tweng, "The beacon movement detection problem in wireless sensor networks for localization applications," *IEEE Transactions on Mobile Computing*, vol. 8, no. 10, pp. 1326–1338, 2009.

[27] R. F. Fan, H. Jiang, S. H. Wu, and N. T. Zhang, "Ranging error-tolerable localization in wireless sensor networks with inaccurately positioned anchor nodes," *Wireless Communications and Mobile Computing*, vol. 9, no. 5, pp. 705–717, 2009.

[28] K. Yu and Y. J. Guo, "Anchor global position accuracy enhancement based on data fusion," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1616–1623, 2009.

[29] S. Srirangarajan, A. H. Tewfik, and Z. Q. Luo, "Distributed sensor network localization using SOCP relaxation," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4886–4895, 2008.

[30] M. Vemula, M. E. Bugallo, and P. M. Djurić, "Sensor self-localization with beacon position uncertainty," *Signal Processing*, vol. 89, no. 6, pp. 1144–1154, 2009.

[31] K. W. K. Lui, W. K. Ma, H. C. So, and F. K. W. Chan, "Semi-definite programming algorithms for sensor network node localization with uncertainties in anchor positions and/or propagation speed," *IEEE Transactions on Signal Processing*, vol. 57, no. 2, pp. 752–763, 2009.

[32] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: distributed reputation-based beacon trust system," in *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06)*, pp. 277–283, Indianapolis, Ind, USA, September 2006.

[33] T. Park and K. G. Shin, "Attack-tolerant localization via iterative verification of locations in sensor networks," *Transactions on Embedded Computing Systems*, vol. 8, no. 1, article 2, 2008.

[34] W. T. Zhu, Y. Xiang, J. Y. Zhou, R. H. Deng, and F. Bao, "Secure localization with attack detection in wireless sensor networks," *International Journal of Information Security*, vol. 10, no. 3, pp. 155–171, 2011.

[35] M. Jadliwala, S. Zhong, S. Upadhyaya, C. M. Qiao, and J. P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 6, pp. 810–823, 2010.

[36] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, NJ, USA, 1976.

[37] W. H. Foy, "Position-location solutions by Taylor-series estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 12, no. 2, pp. 187–194, 1976.

[38] J. W. Wan, N. Yu, R. J. Feng, Y. F. Wu, and C. M. Su, "Localization refinement for wireless sensor networks," *Computer Communications*, vol. 32, no. 13-14, pp. 1515–1524, 2009.