International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 63-76
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.07

Mobile-Assisted Anchor Outlier Detection for Localization in Wireless Sensor Networks

Hala Abukhalaf, Jianxin Wang and Shigeng Zhang

School of Information Science and Engineering, Central South University, Changsha, 410083, China
h_hf2005@yahoo.com, jxwang@mail.csu.edu.cn, sgzhang@csu.edu.cn

Abstract

Accurate location information is critical to many applications in wireless sensor networks (WSNs) such as target tracking, environmental monitoring and geographical routing. Localization aims to figure out the locations of unknown nodes based on global locations of anchors and inter-node distance measurements. However, the existence of outlier anchors and outlier distances degrade localization accuracy in many localization algorithms. Most existing outlier detection approaches focus on distance outlier detection; few efforts have been devoted to anchor outlier detection. In this paper, we propose a mobile-assisted approach to detect outlier anchors and mitigate their negative effects in localization to achieve high localization accuracy. The proposed approach, namely Mobile-Assisted Anchor Outlier detection (MAAO),employs a mobile element to traverse the wireless sensor network several times to collect position information from static anchors in the network. For every static anchor, the mobile element computes the average of the anchor's positions acquired from all tours, and compare it with the position acquired from the last mobile tour to detect whether the anchor is an outlier or not. The evaluation results show that MAAO can effectively detect outlier anchors, which consequently results in remarkable improvement in localization accuracy by not using outlier anchors in the localization process.

***Keywords**: Anchor outlier detection, mobile-assisted, localization, wireless sensor network*

1. Introduction

Wireless sensor networks (WSNs) are a collection of spatially distributed autonomous sensors connected by wireless communication links in ad hoc manner. A WSN is usually densely deployed in a region of interest to monitor physical or environmental conditions, such as sound, temperature, pressure. WSNs could be used in many applications including smart environments, search and rescue, target tracking, industrial monitoring, medical care and military. In these applications, it is necessary for the nodes to know their own physical locations. In addition, location information provides essential network operations such as routing protocols, clustering, data centric storage and geographic key distribution[1-3].

The process of finding the locations (coordinates) of the nodes is usually called localization. A straightforward solution for localization is to equip each WSN node with a GPS[4] receiver that can provide each node with its exact location. However, because GPS receivers are high energy consuming and expensive, it is not a practical solution especially when a WSN consists of a massive number of nodes. In the past several years, a number of localization algorithms have been proposed to reduce the dependence on GPS in WSNs [5-12]. Most of these localization algorithms share a common feature: A small portion nodes called anchor nodes or beacon nodes that know their positions (e.g. via

ISSN: 2233-7857 IJFGCN

manual placement or GPS) send beacons containing their coordinates to help the rest nodes which called sensor nodes or unknown nodes to compute their positions. In this paper, the nodes that know their own positions are called anchors while the nodes that do not know their positions are called unknown nodes. The mobile anchor which is used to detect outliers is called mobile beacon to distinguish it from the static anchors of the network.

Location accuracy can be considered as the most important metric from localization algorithm, when WSN is deployed to perform monitoring tasks such as search, rescue, target tracking,disaster relief, etc. Localization algorithm should give exact location of unknown nodes so that regarding that task, proper action can be performed[13]. Location accuracy shows how the calculated location of an unknown node is close to its true location; the location accuracy is the ultimate goal of a localization algorithm.

The source data which are used in the most of localization algorithms to calculate unknown node’s locations, include the global positions of anchor nodes and the distances between neighboring nodes. However, these source data may contain outliers (outlier distances and outlier anchors) that deviate from their true values [14]. The existence of the outliers might make the calculated positions not accurate. Thus, it is important to detect and remove outliers in order to achieve high localization accuracy.

Most of localization algorithms assume all anchors are supposed to provide correct reference locations information. However, when the wireless sensor networks are deployed in a hostile environment, where some anchors can be attacked and become outliers. The survey[15] concludes that the majority of the existing outlier detection techniques are developed specifically to detect outlier distances, a few techniques such as [14,16-17] focus on outlier anchor detection.

Furthermore, besides distance outlier, anchor outlier is another key research issue that must be paid attention on it. In [14] outlier anchors are described as follows: The positions of anchors are defined in a global coordinate frame (GCF), for example, GPS coordinate frame. Their purpose is to guarantee that the positions of unknown nodes are also defined in the GCF, which can be understood by the system users. But it is inevitable to have outlier anchors declaring erroneous positions that deviate from their true locations in GCF. The potential sources of outlier anchors can be misconfigurations when deploying the anchor nodes or malignant attacks, e.g., Sybil attack and replay attack.

Regardless of the reasons of outlier anchors ignoring the existence of them is not good choice in applications. For example, if a WSN is used in battlefield, it contains outlier anchors. The outlier anchors send position references deviate from their true values to unknown nodes, thus the derived positions of unknown nodes may go far away from their true positions; when unknown nodes report that their regions are safe, this wrong information can cause severe consequence .

Although it is important to detect outlier anchors in order to high localization accuracy, the related work is rare in the literature. In this study, we propose a novel technique, called Mobile-Assisted Anchor Outlier detection (MAAO), for detecting and rejecting outlier anchors before using their location information in the localization process. In our proposed approach the mobile beacon moves in the whole network several times using predefined trajectories to obtain the location values of all anchors. For each anchor the average of its location values which obtained from all mobile tours is calculated, then the average is compared with the last obtained anchor location reading. If the average is far from the last anchor location the anchor is considered as outlier, otherwise it is considered as normal. Also the mobile can detect if any anchor sends every time the same wrong location by using method called SWPC which employs some mathematical calculation and comparison to discover if any anchor always send the same not correct position.

Extensive simulations are conducted by using MATLAB to examine the effectiveness of the proposed MAAO approach. The simulation results show that even there are large number of outliers reach to half of all anchors in the network, the proposed MAAO approach succeed in identifying more than 83.6 % of outlier anchors. In addition, the results show that MAAO approach improves the localization accuracy by rejecting outlier anchors.

The rest of this paper is organized as follows. Section 2 introduces the related work. Problem statement is presented in Section 3. Our MAAO technique in Section 4. Section 5 provides simulation results. Finally, Section 6 concludes the paper.

2. Related Work

Localization can be considered as one of the most basic and important technologies in wireless sensor networks. In recent years, a number of localization methods [5- 12] have been proposed. In most of these methods, the nodes in WSNs can be classified into two types: anchor nodes and unknown nodes. Anchor nodes have a priori information about their coordinates. The unknown nodes do not know their location information and need to be localized. The localization methods can be roughly classified into two types: range-based localization and range-free localization. Range-based localization methods apply range (angle or distance) information to calculate the location; the ranging measurement techniques include Angle of Arrival (AOA)[5], Received Signal Strength (RSS)[18], Time of Arrival (TOA)[19] and Time Difference of Arrival (TDOA) [20]. Range-free localization methods apply network connections information (connectivity or hop count) to calculate the location, APIT[6] and DV-Hop[7] are examples about these methods. Range-based methods are generally more accurate but they need additional hardware cost.

The process of estimating the positions of unknown nodes can be called as localization process, which can be divided into the following two steps:

(1) Source data acquisition: The source data for localization is collected, which may include distance measurements between neighboring nodes and the position knowledge of anchors. To measure distances between neighboring nodes, the distance ranging techniques such as RSS [18], TOA [19] and TDOA [20] are adopted. The position information of anchor can be obtained by GPS[4] or manual placement.

(2) Position computation: Once the source data is collected, position is computed. Several methods can be used to compute the location of an unknown node such as triangulation [5], multilateration [8], and trilateration [21]. The choice of which methods to use depends on ranging technique used in step (1).

From the above description localization we can notice that this process relies on the source data. But the existence of the outliers (outlier distances and outlier anchors) among source data is a fact that cannot be neglected [13]. The outliers can severely degrade the localization accuracy. Therefore, we need outlier detection techniques that can detects and handle these outliers.

In general, most of the existing outlier detection techniques consider outlier distances more than outlier anchors [15]. The works such as [22-25] consider distance measurement outliers, the study in [22] showed that triangle inequality had some limitations and then designed and to identify outlier distance measurements beyond triangle inequality. The proposed bilateration generic cycles algorithm improves the location accuracy by wisely removing distance outliers during the localization process. By applying graph rigidity theory Yang et al. [23] defined verifiable edges and derived the conditions for an edge to be verifiable. On this basis, they designed a localization approach with outlier detection, which explicitly eliminated distance measurement outliers before location computation and thus improved location accuracy. Noise-tolerant localization algorithm called NLIRM was presented in [24]. NLIRM can recover the missing range measurements and explicitly sift Gaussian noise and outlier distance measurements simultaneously. In addition, NLIRM provided an accurate prediction of outlier positions, which is the prerequisite for malfunction diagnosis in WSN. In [25] Ash and Moses proposed a robust self-localization algorithm that effectively mitigated the effects of outlier measurements. They employed the EM algorithm[26] to iteratively detected outlier measurements.

As far as we know, a little work such as [14,16-17] has considered outlier anchors. Xiao et al. [14] focus on the problem of localizing a wireless sensor network robustly against outlier distances and outlier anchors, so they proposed RobustLoc algorithm. RobustLoc iteratively invokes patch merging operation that can reject outlier distances for both multilateration and patch merging. In addition, the authors proposed an enhancement to RobustLoc to tolerate multiple outlier anchors that can collude due to malicious attacks; the simulations showed that it can reject colluding outlier anchors reliably in both convex and concave networks. To the best of our knowledge, RobustLoc is the first algorithm that rejects both outlier distances and outlier anchors. LAD [16] was proposed to detect and identify the outliers and perform compromise resistant localization without remove the malicious anchors from the wireless sensor network. LAD takes advantage of the deployment knowledge that is available in many WSN applications. In [16] the outlier or anomaly problem was formulated as an anomaly intrusion detection problem and several ways to detect localization outliers were proposed. Malicious anchors transmitting outliers and erroneous estimates was dealt with by Li et al. [17] instead of removing them. The basic idea in [17] was to live with bad nodes rather than eliminate all possible bad nodes, so robust statistical methods are develop to make localization attack-tolerant.

The work in [14] was reliably reject multiple outlier anchors which may collude but our proposed MAAO technique focus on outlier anchor which deviated from the ground truth position and whose position has abnormally large error, MAAO does not consider multiple colluding outlier anchors. MAAO detect the outliers before using in localization process different from LAD [16] in which the outlier detection was employed after localization process finished. Also MAAO different from all related techniques that it uses mobile beacon to detect outliers. To the best of our knowledge, this is the first work that uses mobile beacon node to detect outlier anchors.

3. Problem Statement

In this section, we present the network model, assumptions and outlier anchor problem.

3.1. Network Model

In this work, we assume two-dimensional network, denoted by *NT*, consists of n wireless sensor nodes, among them a small portion na ($na \ll n$) nodes know their own positions, these nodes are called anchors. The rest nodes called unknown nodes which they do not know their positions. The network NT is modelled as distance graph G=< Ac, Un, D> where $Ac = \{aci\ ,\ i = 1\ldots\ldots na\}$ is set of anchors, $Un = \{ui,\ i=1\ldots\ldots\ldots(n-na)\}$ is set of unknown nodes. $D = \{di,\ i = 1\ldots\ldots nd\}$ is set of distances between two neighboring nodes where nd is number of these distances.

3.2. Assumptions

- The anchor nodes and the unknown nodes are static, so they should not move after deployment.
- The deployment area is regular and the density of the nodes is uniform.
- Two nodes can communicate with each other only if they are within the communication range defined by the radius R.
- An anchor node is assumed to know its own location through GPS.
- The mobile beacon is denoted by M and assumed to know its own location correctly via GPS.
- The reception range of the mobile beacon is denoted by mr.

- An outlier anchor is an anchor node attacked by adversary to make it out of its original position.
- The set of predefined trajectories is denoted by *Tr*, *Tr*=$\{t_i\ ,\ i = 1\ldots\ldots nt\}$ where *nt* is number of trajectories or paths.

3.3. Outlier Anchor Problem

Denote the ground truth position of an anchor *Pgtr*. Let *Pas* be the sent anchor position which it is measured by GPS and then the anchor sends it to its neighboring nodes. When WSN is deployed in not benign environment the anchor node is susceptible to adversary attack that make it deviated from the ground truth position and becomes an outlier. An anchor outlier can be understood as anchor whose position or location measurement error (i.e., the difference between the ground truth anchor position and the sent anchor position) is abnormally large. Let *Errp* is the position measurement error, which can be calculated by using the following equation

$$Errp = |Pgtr - Pas| \tag{1}$$

We define the two kinds of anchor as normal anchor and outlier anchor, respectively as in the following definition:

Definition 1: Given a distance graph G=< Ac, Un, D>, an anchor $ac \in Ac$ is a normal anchor if $|Errp| \le \varepsilon$; otherwise, ac is an outlier anchor, where the error tolerance ε is a dynamically adjusted parameter according to application requirements.

Since outlier anchors degrade localization accuracy it is essential to detect and reject outlier anchors positions before using them in localization process to achieve high localization accuracy. We formulate the problem of anchor outlier detection as follows:

Problem 1 (Anchor Outlier Detection): Given a distance grounded graph G =< Ac, Un, D> consisting of normal anchors and outlier anchors, detect and identify those outlier anchors in G.

.

4. Mobile-Assisted Anchor Outlier Detection (MAAO) Technique

The basic idea of MAAO technique is that the mobile beacon (M) travels through the WSN several time collecting position values from each anchor, then average of these position values is computed and compared with anchor's position value which obtained when mobile beacon moves in the final trajectory. If final anchor position is far from the average it will be considered as an outlier. Also M can discover if anchor always sends the same wrong position value by using method called SWPC. The details of the anchor outlier detection technique and SWPC method are described in the following subsections.

4.1. Outlier Anchor Detection

In MAAO the mobile beacon M moves several times in the network *NT* collecting position values (location coordinates) from each anchor $ac \in \{ac_i\ ,\ \ i = 1\ldots\ldots na\}$,where na is the number of anchors in the *NT*.

The mobile beacon in its travels uses the following predefined trajectories: SCAN, DOUBLE SCAN, HILBERT, CIRCLE and S-CURVES [27-28]. We denote the predefined trajectory by *ti* , $i = 1\ldots\ldots nt$, where *nt* is the number of trajectories. The mobile M moves every time by using predefined trajectory different from the previous time. For example if M in the first tour used SCAN trajectory (*t1* = SCAN), so in the second tour M using HILBERT trajectory (*t2* = HILBERT). This keeps M itself safe from attack because the external adversary cannot predict the trajectory or path of Mwhen M in every tour through *NT* uses different trajectory from the previous tour.

Let *Pti* is the position value of the static anchor ac which M collects it during moving in *NT* by using trajectory *ti*, let the average of position values of ac anchor is denoted by *avgPt*, *avgPt* is calculated as

$$avgPt = \sum_{i=1}^{nt} \frac{Pt_i}{nt} \tag{2}$$

Let Pt_f be the position value of ac at which mobile M obtains by using final predefined trajectory t_f . Notice that Pt_f is equal to Pt_{nt} . The *avgPt* of ac anchor will be compared with Pt_f to determine whether ac is an outlier as follows :

If $avgPt \neq Pt_f$ the ac anchor is detected and identified as an outlier anchor, otherwise it is consider as a normal anchor.

The average is compared with anchor position reading which was obtained by using last predefined trajectory because it was included of all the probabilities that the anchor is vulnerable to attack, which makes it become an outlier in the all the pervious mobile tours.

We assumed that the anchor is static so its position must not change. Therefore, if the anchor broadcasts different positions, there is something wrong and we can considered this anchor as an outlier. However, the following question may be raised: How if an anchor always sends the same location value but this value is not correct. If this happened it can be caused that MAAO fails in detecting outlier anchors. Nevertheless, MAAO also deal with this situation by using a method called SWPC to check if the anchor always sends the same wrong position value. The details of SWPC are given in the next subsection (Section 4.2).

4.2. SWPC Method

For simplicity, in this paper we denote the anchor that sends every time the same wrong position by SWP and the check process to detect it by SWPC. The basic idea of SWPC method is as follows: In every tour of mobile beacon M requests the position information from each static anchor. Also M can calculate the static anchor position, it needs to move around static anchor and placed in three different positions at least, then by applying some mathematical equations the anchor position can be obtained or calculated . After this M compares the calculated anchor position with the position reading which is sent by static anchor. If they are different this means the anchor is sent a wrong position.

The detail of SWPC method is as follows: the mobile beacon knows its correct location via GPS, which is denoted by P_M. Let the distance between mobile beacon and static anchor is denoted by *d*, *d* is known by using the measurement techniques such as TDoA, TOA and RSS. Denote the anchor position by *Pa*. The relation between d, P_M and *Pa* as the following equation

$$d = \left\| P_M - Pa \right\| \tag{3}$$

Assume the coordinate of M is (x_M , y_M) and the coordinate of anchor is (x_a, y_a). The equation (3) is equivalent to the following equation:

$$d = \sqrt{(x_M - x_a)^2 + (y_M - y_a)^2} \tag{4}$$

As an example in Figure1, the mobile beacon M (the gray box) moves in *NT* using SCAN trajectory. At least three non-collinear positions of M are needed in order to calculate *Pa* which is the position of the anchor *ac* (the white circle).

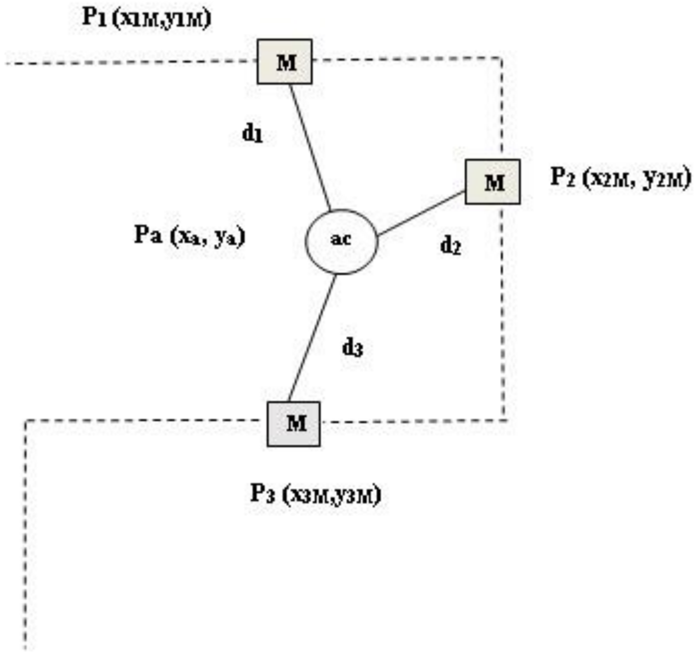

Figure 1. The Principle of SWPC Method

Assume that when M is at position P_1 with the coordinate (x_{1M} ,y_{1M}), at P_2 with the coordinate (x_{2M},, y_{2M}) and at P_3 with the coordinate (x_{3M} ,y_{3M}). The three distances between M and the anchor can be denoted by d_1, d_2 and d_3 . Let (x_a , y_a) be the coordinate of the anchor ac which to be estimated. Now we have the following equation:

$$\begin{aligned} \sqrt{(x_{1M}-x_a)^2+(y_{1M}-y_a)^2} &= d_1 \\ \sqrt{(x_{2M}-x_a)^2+(y_{2M}-y_a)^2} &= d_2 \\ \sqrt{(x_{3M}-x_a)^2+(y_{3M}-y_a)^2} &= d_3 \end{aligned} \tag{5}$$

Square both sides of (5),

$$\begin{aligned} (x_{1M}-x_a)^2+(y_{1M}-y_a)^2 &= d^2{}_1 \\ (x_{2M}-x_a)^2+(y_{2M}-y_a)^2 &= d^2{}_2 \\ (x_{3M}-x_a)^2+(y_{3M}-y_a)^2 &= d^2{}_3 \end{aligned} \tag{6}$$

After some arrangement equation (6) could be expressed by the following linear equation

$$AX = B \tag{7}$$

$$A = \begin{bmatrix} 2(x_{1M}-x_{3M}) & 2(y_{1M}-y_{3M}) \\ 2(x_{2M}-x_{3M}) & 2(y_{2M}-y_{3M}) \end{bmatrix}$$

$$B = \begin{bmatrix} x_{1M}^2 - x_{3M}^2 + y_{1M}^2 - y_{3M}^2 + d_3^2 - d_1^2 \\ x_{2M}^2 - x_{3M}^2 + y_{2M}^2 - y_{3M}^2 + d_3^2 - d_2^2 \end{bmatrix} \ , \ X = \begin{bmatrix} x_a \\ y_a \end{bmatrix}$$

Equation (7) can be solved by the minimum mean square estimation (MMSE), so the estimation of the position anchor coordinate (x_a ,y_a) is obtained by the following equation

$$X = \hat{X} = \left(A^T A\right)^{-1} A^T B \tag{8}$$

Let Pas be the position of anchor ac at which it is sent to the mobile beacon, the mobile beacon can detect that the anchor sent wrong position if Pas different from Pa. Therefore, If $Pa \neq Pas$ so ac anchor is considered as SWP, otherwise it is not SWP.

5. Evaluation

The proposed MAAO outlier detection technique is evaluated through simulations by using MATLAB (version 2014b) on a computer with Intel(R) core (TM) i3-2310M CPU (2.10 GHz). The simulation region was assumed to the square area of 100m ×100 m. The WSN nodes are uniform-randomly distributed in the region with communication range equal to R.

5.1. Outlier Detection Accuracy

The outlier detection ratio is used as metric to evaluate the performance of MAAO outlier detection technique. The outlier detection ratio is defined as the ratio of the number of detected outliers to the number of the existed outliers in the network. The outlier detection ratio is denoted by R_{DO} and it is calculated as

$$R_{DO} = \frac{N_{OD}}{N_O} \tag{9}$$

where N_{OD} is the number of detected outliers and N_O is the number of outlier anchors in the network.

We generate networks of 100 nodes; each network contains 22 anchors and 78 unknown nodes. The communication range R is set to 20 m. In these sets of experiments two scenarios are considered. In the first scenario, the mobile reception range mr is set to 20 m. In the second scenario, the mobile reception range mr is set to 30 m.

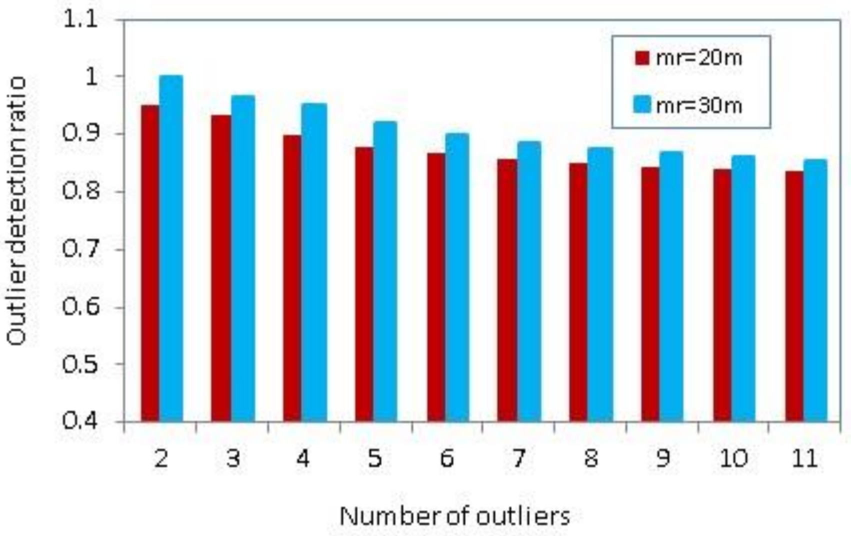

Figure 2. Outlier Detection Ratio versus Number of Outliers

Figure 2 presents the results, which are integrated from 110 network instances. As shown in Figure 2, when the number of outliers N_O increases the outlier ratio R_{DO} slightly decreases for both scenarios. Actually it is natural when there are more outliers the probabilities of occurrence of cases that MAAO fails in the detection of outlier anchors is also more. From Figure 2, the outlier detection ratio mostly more than 83%, which shows that MAAO has relatively good outlier detection ratio. However, R_{DO} with mr =30 is always higher than it with mr =20. Our explanation of this result is that when reception range of the mobile beacon is larger, M can collect more position values from anchors during its tours in *NT* and thus the math operations in MAAO become more accurate.

From Figure 2 we can see that the outlier detection ratio R_{DO} achieves nearly 85.4% when N_O =11 and mr =30, also R_{DO} achieves 83.6 % when N_O =11 and mr =20. This means even if half of anchors are outliers MAAO can effectively detect many of them.

5.2. SWPC Efficiency

We use the average discovered SWP metric to measure the efficiency of SWPC method which is employed by MAAO to discover the anchor outlier that sends every time same wrong position (SWP). The Average discovered SWP is defined as the ratio of the number of discovered SWPs to the number of SWPs in network. It is denoted by $Avgd_{SWP}$ and calculated as follows:

$$Avgd_{SWP} = \frac{Nd_{SWP}}{N_{SWP}} \tag{10}$$

Where Nd_{SWP} is the number of discovered SWPs and N_{SWP} is the number of SWPs.

We generate network instances of 100 nodes, 32% of them which are anchors, half of anchors are outliers, this means NO=16. The communication range is set as R = 30 m while the mobile reception range is also set as mr =30 m. In these experiments, we consider three scenarios; *Npm* equals 3 in the first scenario, *Npm* equals 4 in the second scenario and in the third scenario *Npm* equals 5, where *Npm* is the number of mobile positions which M used to calculate the estimated anchor position Pa.

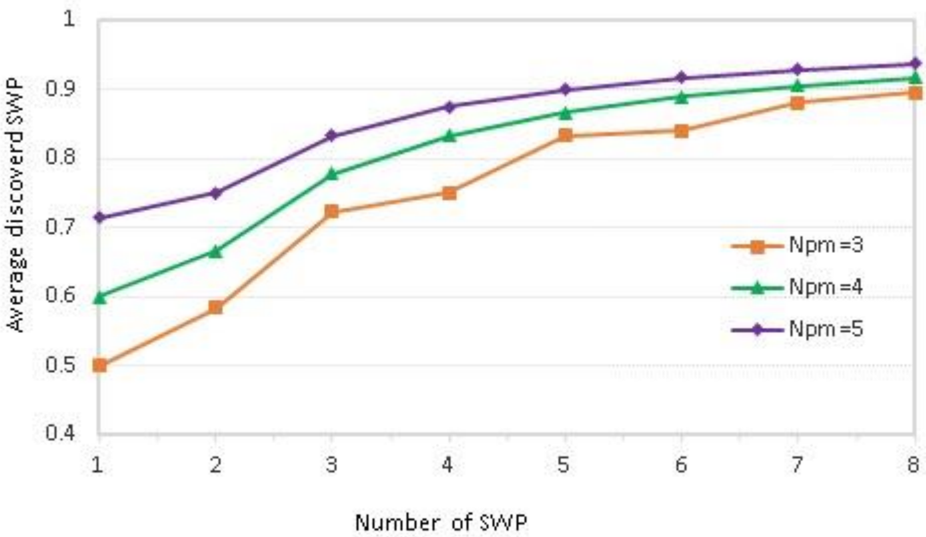

Figure 3. Average discovered SWP versus Number of SWP

The results in Figure 3 are obtained by averaging over 140 simulation runs. As shownin Figure 3, $Avgd_{SWP}$ in scenario3 (*Npm*=5) always higher than in scenario 2 (*Npm*=4) and in scenario1(*Npm*=3), also $Avgd_{SWP}$ in scenario 2 always higher than in scenario1, it is clear that as *Npm* increases the $Avgd_{SWP}$ also increases. This means when

M used more number of its positions around the anchor to calculate *Pa* the SWPC method become more accurate and can caught more SWP.

As shown in Figure 3 when N_{SWP} is equal to 8. The SWPC method discovers approximately 93.7% of SWPs when *Npm*=5, approximately 91.6% of SWPs when *Npm*=4, and approximately 89.5% of SWPs when *Npm*=3. These results indicate that the SWPC method can effectively discovered SWPs.

5.3. Localization Accuracy

To investigate the effect of using the proposed MAAO technique on the localization accuracy, we randomly generate 144 networks of 100 nodes, in each network 20% of nodes are anchors. The communication range is set as R=25 m while the mobile reception range is set as mr=25 m. The multilateration [8] is used as the basic localization algorithm and its localization accuracy is evaluated in two cases. The first case ignores the existence of outlier anchors and uses multilateration alone without outlier detection and this case is denoted by (without MAAO). The second case use multilateration after employing MAAO to detect outliers, this case is denoted by (with MAAO). Note that the MAAO approach works well with any arbitrary localization algorithms, but we employ multilateration because it is widely used. We use the metric location error to measure localization accuracy. The location error can be defined as difference between estimated location and true location. The average location error is denoted by *Lerr* and it is calculated as

$$Lerr = \sum_{i=1}^{n} \frac{|Le_i - Lt_i|}{n} \tag{11}$$

where *n* is the number of network nodes, Le_i is the estimated location that the unknown node *i* (ui) derived by a certain localization algorithm (in this study multilateration is the localization algorithm), and Lt_i is the true location of node *i*.

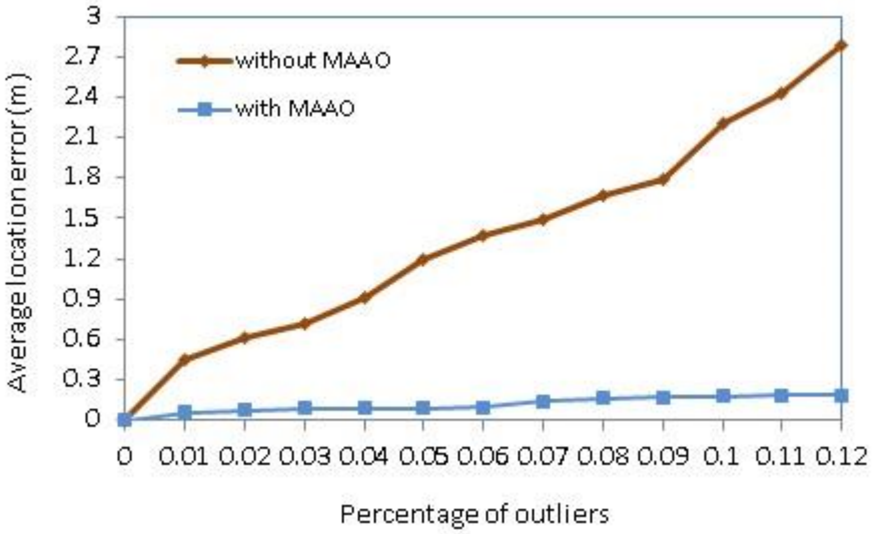

Figure 4. Average Location Error versus Percentage of Outliers

As shown in Figure 4, in without MAAO case the average location error sharply linearly increases along with the increase of percentage outliers in the network. However, in with MAAO case, it is slightly increases because the influence of anchor outliers is small as most of them are deleted when they detected. The average location errors with MAAO case, are much less than those without MAAO case, because the same reason that the identified outlier anchors are deleted by MAAO before using them in computing the unknown nodes' positions via multilateration. When the percentage of outliers is 0.12 the gap between these two cases reaches to 2.59 m. From these results, it is clear that using MAAO technique helps achieve high localization accuracy.

6. Conclusions

Outlier detection is necessary for localization in WSNs because the existence of outliers degrade the localization accuracy. In this article, we have discussed the problem of outlier anchors and proposed a new anchor outlier detection approach called Mobile-Assisted Anchor Outlier detection (MAAO). The proposed MAAO technique is based on mobile beacon to detect and identify outlier anchors. In MAAO a mobile beacon travels during the WSN several times in order to collect the positions of anchors and make mathematical calculations and comparisons to detect outlier anchors. In addition, MAAO used method named SWPC to discover if any anchor sends every time the same wrong location. The simulation results have shown that MAAO is efficient to detect outlier anchors. Furthermore, our experiments have shown that even the number of outliers nearly half of anchors the proposed MAAO can still effectively detect more than 83.6 % of them. Our results also have shown that MAAO improves the localization accuracy by eliminating the information that transmitted from outlier anchors before using them in the localization process.

Acknowledgments

This paper is partially supported by the National Science Foundation of China under Grant Nos. 61402056, and 61420106009. We appreciate the reviewers' comments on improving the quality of this paper.

References

[1] X. Li, N. Mitton, I. S. Ryl, and D. S. Ryl, "Dynamic beacon mobility scheduling for sensor localization", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, **(2012)**, pp. 1439-1452.
[2] U. Singh and M. Jha, "Performance evaluation of localization technique in wireless sensor network", International Journal of Engineering and Computer Science, vol. 2, no. 4, **(2013)**, pp. 1381-1384.
[3] X. Wang, D. Bi, L. Ding and S. Wang, "Agent collaborative target localization and classification in wireless sensor networks", Sensors, vol. 7, no. 8, **(2007)**, pp. 1359-1386.
[4] B. H. Wellenhof, H. Lichtenegger and J. Collins, "Global Positioning System Theory and Practice", 4th edn, Springer, New York, **(1997)**.
[5] D. Niculescu and B. Nath, "Ad doc positioning system (APS) using AOA", Proceedings of IEEE INFOCOM, San Francisco, CA, **(2003**, pp. 1734-1743.
[6] T. He, C. Huang, B. M. Blum, J. A. Stankovic and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks", Proceedings of ACM MobiCom, **(2003)**, pp. 81-95.
[7] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks", Telecommunication Systems, vol. 22, no. 1, **(2003)**, pp. 267-280.
[8] A. Savvides, C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in Ad-hoc networks of sensors", Proceedings of ACM MobiCom, **(2001)**.
[9] N. Bulusu, J. Heidemann and D. Estrin, "GPS-less low cost outdoor localization for very small devices", IEEE Personal Communications Magazine, **(2000)**, pp.28–34.
[10] L. Doherty, K. S. Pister and L. E. Ghaoui, "Convex optimization methods for sensor node position estimation", Proceedings of INFOCOM'01, **(2001)**.
[11] R. Nagpal, H. Shrobe and J. Bachrach, "Organizing a global coordinate system from local information on an ad hoc sensor network", IPSN'03, **(2003)**.
[12] A. Nasipuri, K. Li, "A directionality based location discovery scheme for wireless sensor networks", Proceedings of ACM WSNA'02, **(2002)**.
[13] U. Nazir, M. A. Arshad, N. Shahid, S. H Raza "Classification of localization algorithms for wireless sensor network: A survey," IEEE International Conference on Open Source Systems and echnologies (ICOSST), Lahore, **(2012)**, pp1–5.
[14] Q. Xiao, K. Bu, Z. Wang and B. Xiao, "Robust localization against outliers in wireless sensor networks", ACM Transactions on Sensor Networks, vol. 9, no. 2, **(2013)**.

[15] H. Abukhalaf, J. Wang and S. Zhang, "Outlier Detection Techniques for Localization in Wireless Sensor Networks: A Survey", International Journal of Future Generation Communication and Networking, vol. 8, no. 6, **(2015)**, pp. 99-114.

[16] W. Du, L. Fang and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks", Journal of Parallel and Distributed Computing, vol. 66, no.7, **(2006)**, pp. 874-886.

[17] Z. Li, W. Trappe, Y. Zhang and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks", Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, **(2005)**.

[18] A. Hatami, K. Pahlavan, M. Heidari and F. Akgul, "On RSS and TOA based indoor Geolocation - A comparative performance evaluation", Proceedings of IEEE Wireless Communications and Networking Conference, Las Vegas, NV, **(2006)**, pp. 2267- 2272X.

[19] I. Guvenc and Z. Sahinoglu, "Threshold-based TOA estimation for impulse radio UWB systems", Proceedings of IEEE International Conference on Ultra-Wideband, Zurich, Switzerland, **(2005)** September, pp. 420-425.

[20] X. Wei, L. Wang and J. Wan, "A new localization technique based on network TDOA information", Proceedings of IEEE International Conference on ITS Telecommunications, **(2006)**, pp. 127-130.

[21] D. Niculescu, B. Nath, "Ad hoc positioning system (APS)", Proceedings of the 2001 IEEE Global Telecommunications Conference of the IEEE Communications Society, vol. 5, **(2001)**, pp. 2926–2931**.**

[22] Z. Yang, L. Jian, C. Wu and Y. Liu, "Beyond triangle inequality: Sifting noisy and outlier distance measurements for localization", ACM Transactions on Sensor Networks (TOSN), vol. 9, no. 2, **(2013)**.

[23] Z. Yang, C. Wu, T. Chen, Y. Zhao, W. Gong, and Y. Liu, "Detecting outlier measurements based on graph rigidity for wireless sensor network localization", Vehicular Technology, vol. 62, no. 1, **(2013)**, pp. 374-383.

[24] F. Xiao, C. Sha, L. Chen, L. Sun and R. Wang. "Noise-tolerant localization from incomplete range measurements for wireless sensor networks", Proceedings of INFOCOM 2015, **(2015)**, pp. 2794-2802.

[25] J.N. Ash and R.L. Moses, "Outlier compensation in sensor network self_localization via the EM algorithm", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'05), **(2005)**, pp. 749–752.

[26] A. P. Dempster, N. M. Laird and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm", Journal of the Royal Statistical Society, vol. 39, no. 1, **(1977)**, pp. 1- 38

[27] D. Koutsonikolas, S. M. Das and Y. C. Hu, "Path planning of mobile landmarks for localization in wireless sensor networks",Computer Communications, vol. 30, no. 13, **(2007)**, pp. 2577–2592.

[28] R. Huang and G. V. Zaruba, "Static Path Planning for Mobile Beacons to Localize Sensor Network", Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW), White Plains, NY, USA, **(2007)**, pp. 323-330.

Authors

Hala Abukhalaf, she received her BSc in Computer Systems Engineering from Palestine Polytechnic University. She received her MSc in Computer Science from Al-Quds University, Jerusalem, in 2008. She worked as a part time lecturer in Al-Quds Open University from 2010 to 2011. She is currently studying towards her PhD degree at the School of Information Science and Engineering, Central South University, Changsha, China. Her research interests include wireless sensor networks and mobile ad hoc networks.

Jianxin Wang, he received his BSc and MSc degrees in Computer Science from Central South University of Technology, China, and his PhD degree in Computer Science from Central South University. Currently, he is the vice dean and a professor in the School of Information Science and Engineering, Central South University, Changsha, Hunan, China. He has served as a program committee member for many international conferences. He was a program committee co-chair for the International Symposium on Bioinformatics Research and Applications (ISBRA) in 2011, 2012 and 2014, and a program committee co-chair for the 8th International Frontiers of Algorithmics Workshop (FAW2014). His current research interests include algorithm analysis and optimization, parameterized algorithm, bioinformatics and computer networks. He has published more than 200 papers in various international journals and refereed conferences. He is a senior member of the IEEE.

Shigeng Zhang, he received the BSc, MSc, and DEng degrees, all in Computer Science, from Nanjing University, China, in 2004, 2007, and 2010, respectively. He is currently an assistant professor in School of Information Science and Engineering at Central South University, China. His research interests include cloud computing, Internet of Things, wireless sensor networks, and RFID systems. He has published more than 40 technique papers in international journals and conferences. He is a member of IEEE, a member of ACM, and a member of CCF.

