International Core Journal of Engineering Volume 7 Issue 3, 2021
ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

Cooperative Security Location of UWSN Nodes Based on Weighted DV-HOP Algorithm

Hao Li

College of Information Engineering, Shanghai Maritime University, Shanghai, 201306, China.

1171973620@qq.com

Abstract

Positioning technology is one of the most important technologies in underwater wireless sensor networks and plays an important role in many applications. Underwater sensor network nodes have the characteristics of sparse distribution and limited energy. In the process of locating, there are problems such as node failure, false locating information issued by captured beacon nodes, malicious nodes falsely accusing benign beacon nodes, etc., which interfere with node locating. In order to solve the above problems, this paper proposes an underwater wireless sensor network node cooperative and secure location algorithm based on weighted DV-HOP. Before the unknown node is located, it is necessary to conduct security detection of beacon node, detect the beacon node releasing false positioning information and malicious node falsely accusing benign beacon node, so as to reduce positioning interference. After the unknown node completes the localization, it acts as a new beacon node to cooperate with the unknown node to locate, which improves the localization coverage rate and reduces the localization error. Simulation results show that the proposed method can effectively propose malicious nodes, reduce positioning errors, and improve positioning coverage.

Keywords

DV-HOP; Safety Detection; Collaborative Localization.

1. Introduction

In recent years, with the development of Marine engineering and underwater communication technology, underwater wireless sensor networks have been widely used in Marine environment monitoring, Marine biological monitoring, disaster prediction, auxiliary navigation, resource exploration and military applications[1, 2]. In the underwater wireless sensor network, the application research of underwater wireless sensor network is based on the node location, so the node location is very important. The particularity of underwater sensor network environment increases the difficulty of node positioning. Firstly, underwater environment can only choose the underwater acoustic communication mode with small bandwidth and large noise. Secondly, underwater wireless sensor network is deployed in three-dimensional environment, and many two-dimensional positioning algorithms are no longer applicable. In addition, the sparse distribution of beacon nodes and the mobility of nodes increase the difficulty of location[3].

DV-HOP algorithm is a node localization algorithm proposed by Niculescu et al[4]. In this algorithm, the average hop distance of each beacon node is first calculated according to the distance and hops between beacon nodes, and then the unknown node estimates the distance between the unknown node and the beacon node by multiplying the average hop distance of beacon node with the hops of unknown node to the beacon node. The algorithm can be divided into three stages:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

Step 1: Calculate the minimum number of hops between nodes. All beacon nodes send data packets, including their own location information and the initial value of 0 hop, to the neighbor nodes in the network by means of flood broadcasting. Every time a node receives a packet, it will increment the hop value by 1 and save the data in its own position information table. Then it will forward the packet with the increment of hop value to its neighbor node and discard the packet with a larger hop value from the same beacon node. The minimum number of hops from each beacon node to that node can be known from this position information table.

Step 2: Calculate the distance between the unknown node and the beacon node. Each beacon node uses the location data of other beacon nodes received and the minimum hops apart, and uses Equation (1) to calculate the average hops of each beacon node in the network:

$$HopSize_i = \frac{\sum_{j\neq i}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2+(z_i-z_j)^2}}{\sum_{j\neq i} hop_{ij}} \tag{1}$$

(x_i, y_i, z_i) and (x_j, y_j, z_j) represent the coordinates of beacon node i and j respectively, hop_{ij} represents the minimum number of hops between beacon node i and beacon node$j$.

Then the beacon node sends its average hop to the network, and the unknown node records the average hop value of each beacon node received, and forwards it to the neighbor node. After receiving the value, the unknown node is multiplied by the minimum jump value recorded in the local information table to the beacon node to estimate the distance from the unknown node to the beacon node. As shown in Equation (2):

$$d_{ui} = HopSize_i \times hop_{ui} \tag{2}$$

Where d_{ui} represents the distance from unknown node u to beacon node i, $HopSize_i$ represents the average hop of beacon node i, hop_{ui} represents the minimum number of hops between unknown node u beacon node i.

Step 3: Compute the coordinates of the unknown node. The distance equation is shown in (3), which adopts the maximum likelihood estimation method to deal with the coordinates of positioning nodes:

$$\begin{cases} (x_1-x_u)^2+(y_1-y_u)^2+(z_1-z_u)^2 = d_{u1}^2 \\ \vdots \\ (x_n-x_u)^2+(y_n-y_u)^2+(z_n-z_u)^2 = d_{un}^2 \end{cases} \tag{3}$$

where the coordinates of the beacon node are (x_1, y_1, z_1),(x_2, y_2, z_2),…, (x_n, y_n, z_n).(x_u, y_u, z_u) represents the coordinates of the unknown node u.d_{u1}, d_{u2},…, d_{un}respectively represent the distance between unknown node u and each beacon node. (3) can be represented by the linear equation shown in (4).

$$AX = B \tag{4}$$

where

$$A = \begin{pmatrix} 2(x_1-x_n) & 2(y_1-y_n) & 2(z_1-z_n) \\ \vdots & \vdots & \vdots \\ 2(x_{n-1}-x_n) & 2(y_{n-1}-y_n) & 2(z_{n-1}-z_n) \end{pmatrix}$$

$$X = \begin{pmatrix} x_u \\ y_u \\ z_u \end{pmatrix}$$

$$B = \begin{pmatrix} x_1^2-x_n^2+y_1^2-y_n^2+z_1^2-z_n^2+d_{un}^2-d_{u1}^2 \\ \vdots \\ x_{n-1}^2-x_n^2+y_{n-1}^2-y_n^2+z_{n-1}^2-z_n^2+d_{un}^2-d_{u(n-1)}^2 \end{pmatrix}$$

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

The coordinates of unknown node$u$are:

$$X = (A^T A)^{-1} A^T B \tag{5}$$

2. Beacon node security detection algorithm

At present, most of the node localization algorithms do not pay enough attention to the security problem, and these algorithms all assume that the wireless sensor network is secure and reliable. However, during the positioning process, beacon nodes are vulnerable to attack and capture, and captured beacon nodes issue false positioning information and interfere with the positioning of unknown nodes. In some localization algorithms that contain the security detection of beacon nodes, the problem of malicious nodes falsely accusing benign beacon nodes exists. Aiming at the security problem in node localization process, Literature [7] proposed a secure positioning algorithm DGFSL-3D (Dynamic Group Filtering Security Localization algorithm) based on dynamic packet screening in 3D space. The algorithm grouped the beacon nodes according to their distance, voted the beacon node group according to the error size, and judged the malicious nodes by the votes. At the same time, in order to prevent malicious nodes from conducting malicious voting, the voting filtering strategy is adopted to ensure the effective screening of malicious nodes.

In DV-HOP positioning algorithm, the farther the distance is, the greater the positioning error will be, resulting in more votes for the beacon node group with a longer distance, which cannot effectively screen out the malicious nodes. To solve this problem, this section proposes a beacon node security detection algorithm, the specific steps are as follows:

1) Each beacon node sends data packets, including node ID, coordinate, hop number and other information, to the network by means of flood broadcasting. The packet$M_i$is shown as follows:

$$M_i = \{ID_i, (x_i, y_i, z_i), hop_i, NT_i\} \tag{6}$$

Where, ID_i represents the ID of beacon node i,(x_i, y_i, z_i) represents the coordinate position of beacon node$i$, and hop_i represents the number of hops between nodes, which is initialized to 0. After receiving the packet, the receiving node will increment the hop value by 1 and save the data in its own position information table. Then, the packet with the increment of hop value will be forwarded to its neighbor node, and the packet with larger hop value from the same beacon node will be discarded. The minimum number of hops from each beacon node to that node can be known from this position information table.NT_i is the untrust of the beacon node, initialized to 0.

2) After receiving broadcast messages from other beacon nodes, beacon node$i$calculates the actual distance to other beacon nodes and generates a list of local beacon node information. According to the ID of beacon node, it is grouped from small to large with 4 beacon nodes in each group.

3) Beacon node$i$calculates the average hop distance with each beacon node group, and calculates the estimated distance to each beacon node in the beacon node group by multiplying the average hop distance by the hops. By using the maximum likelihood estimation method, beacon node i can calculate the estimated coordinates relative to the beacon node group.

4) i beacon node will have to calculate several estimate coordinates, comparing with the actual coordinates, if the error exceeds a certain threshold, then the estimate the coordinate of the beacon node group, there could be a malicious beacon node calibration for suspected group to the group, the group suspected of ID radio beacon node, a vote for beacon node selection, don't trust plus 1. In order to prevent repeated voting by malicious nodes, the principle of "secret ballot" was adopted, that is, after beacon node i initiated voting on beacon node j, the voting logo $Tag(i,j) = 1$ was updated. When beacon node i repeatedly votes on beacon node j, other beacon nodes check the voting flag $Tag(i,j)$. If it is 1, it is a repeated vote. Then, the beacon node i is directly marked as a malicious node and the beacon node list is updated.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

5) The other beacon nodes repeat step 4 and broadcast the vote to the group of beacon nodes that may have malicious nodes.

6) When the vote is over, the beacon node is judged as a malicious node and the beacon node list is updated when the vote is not trusted beyond a certain threshold.

3. Weighted DV-HOP algorithm

3.1 Error analysis of DV-HOP algorithm

In practical applications, wireless sensor network nodes are randomly deployed underwater, and the distribution of underwater nodes is very random, and the distribution of nodes is not uniform. Therefore, there will be a large error when calculating the direct distance between unknown nodes and beacon nodes by using the average jump distance. As shown in Figure 1, the number of hops from unknown nodes B and C to beacon node is two hops, which can be obtained from Equation (2):

$$d_{AB} = 2HopSize_A$$
$$d_{AC} = 2HopSize_A$$

As you can see, $d_{AB} = d_{AC}$ is a big deviation from the actual distance.

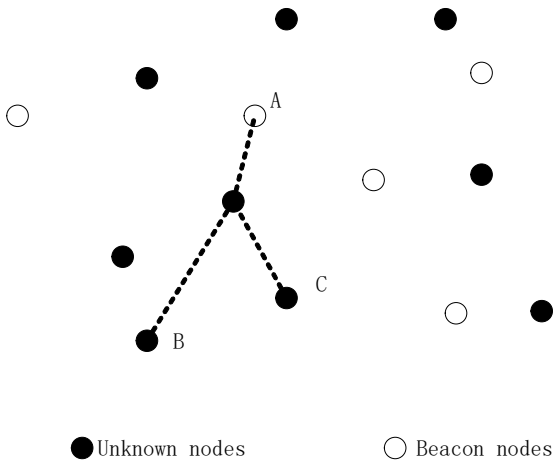

Figure 1. Error analysis diagram

Aiming at the error of DV-HOP algorithm in localization process, some researchers put forward some improvement measures. In literature [5], Abdelali Hadir and Khalid Zine-dine scholars proposed a DV-HOP algorithm (HWDV-HOP) based on weighted average hop based on the difference value of average hop. This algorithm used the reciprocal of the absolute value of average hop difference of each beacon node to weight the average hop, which improved the accuracy of DV-HOP algorithm to a certain extent. In literature [6], a TWDV-HOP algorithm is proposed. According to the global and local characteristics of the network, the weighted average of the average hops is corrected twice, the effective distance between the unknown node and the beacon node is estimated, and the positioning accuracy of the unknown node is improved.

3.2 Principle of weighted DV-HOP algorithm

As mentioned above, due to the irregular distribution of nodes deployed in the wireless sensor network, only using the average hop distance of the beacon node closest to the unknown node to estimate the distance between the unknown node and the beacon node will lead to the problem of unsatisfactory positioning accuracy. To solve this problem, literature [8] defines the concept of the average hop length of the entire network:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

$$HopSize_{ave} = \frac{\sum_{i=1}^{n} HopSize_i}{n} \quad (7)$$

$HopSize_i$ is the average hop distance of each beacon node calculated according to formula (1), and n is the total number of beacon nodes.

Obviously, if you take all of the beacon node data and you substitute $HopSize_{ave}$ for $HopSize_i$. This method is more comprehensive and objective. However, although the algorithm takes into account the average hop distance of all beacon nodes, the weights of different beacon nodes are not taken into account in the calculation. In order to estimate the average hop distance of the whole network, the same weight will inevitably bring some errors to the positioning. Therefore, on the basis of previous theoretical research, this paper puts forward the following improvement measures:

Since the coordinates of all beacon nodes and the minimum number of hops between them are known, the actual distance between any two beacon nodes i and j can be calculated first. The actual distance can be calculated by the following formula:

$$D_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2} \quad (8)$$

(x_i, y_i, z_i) and (x_j, y_j, z_j) respectively represent the coordinates of beacon node i and j. Then, formula (8) is used to calculate the theoretical distance between the beacon node i and j:

$$d_{ij} = hop_{ij} \times HopSize_i \quad (9)$$

hop_{ij} is the number of hops between the beacon nodes i and j.

Finally, the error of the average hop distance of each beacon node can be obtained:

$$\varepsilon_i = \frac{\sum_{j \neq i}^{n} (|D_{ij} - d_{ij}| / hop_{ij})}{n-1} \quad (10)$$

In the form of flooding, the beacon node broadcasts the calculated average hop distance $HopSize_i$ and its average hop distance error ε_i in the network. The unknown node will take the following two steps to process the information it receives:

Step 1: The weight value of anchor point is calculated according to the error of average hop distance of each beacon node.

Step 2: Use the weight value correction formula obtained in Step 1 (6):

$$HopSize'_{ave} = \sum_{i=1}^{n} \omega_i HopSize_i \quad (12)$$

4. Cooperative weighted DV-HOP algorithm

In underwater wireless sensor networks, beacon nodes are relatively few. At the same time, beacon nodes fail due to energy exhaustion and capture and destruction, which increases the positioning error of unknown nodes in the network and reduces the positioning coverage. In this regard, literature [9] proposed that unknown nodes that have been located should be taken as beacon nodes to participate in positioning, so as to realize collaborative and rapid positioning of the whole network. In order to improve the positioning coverage, this paper will adopt the cooperative method for positioning. The whole positioning process is as follows:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

(1) The weighted DV-HOP algorithm is used to locate the unknown nodes directly.

(2) The located unknown node is marked as beacon node, and the unknown node and beacon node set are updated.

(3) The newly labeled beacon node calculates its average jump distance and broadcasts its ID, coordinates and average jump distance information through flood.

(4) Repeat the above steps until the number of unknown nodes is no longer reduced, the positioning process is completed, and the remaining nodes are marked as unlocatable nodes.

In general, the coordinates of unknown nodes obtained through positioning have certain errors. When these nodes participate in the positioning of other unknown nodes as cooperative nodes, the positioning errors of other unknown nodes will be increased. In this way, in the positioning process, error accumulation, greatly reduce the positioning accuracy. Therefore, in the process of collaborative positioning, the priority selection error is small, the smaller the error, the higher the priority level. Among them, the priority level of the original beacon node is the highest, and the priority level of the newly added beacon node after the first round of positioning is lowered, and so on, the priority level is lower. At the same time, when new beacon nodes cooperate to locate unknown nodes, the fewer the number of new beacon nodes, the smaller the positioning error. Generally, in 3D underwater environment, this algorithm only needs four beacon nodes to complete the localization of unknown nodes. Therefore, the four beacon nodes with the highest priority can be selected.

5. GFCWDV-HOP algorithm

On the basis of the cooperative weighted DV-HOP algorithm and the comprehensive consideration of the beacon node security detection algorithm, this paper proposes an underwater WSN node cooperative security location algorithm based on the weighted DV-HOP algorithm -- GFCWDV-Hop algorithm. The algorithm is described as follows:

(1) Each beacon node sends data packets, including node ID, coordinate, hop number and other information, to the network by means of flood broadcasting.

(2) Beacon node i groups other beacon nodes according to ID in groups of four. To calculate the estimated coordinates of the beacon node i relative to each beacon node group, the beacon node group with an error over a certain threshold was demarcated as the suspect group. The beacon node i initiates a vote on the beacon node in the suspect group, adding 1 to the distrust. In order to prevent malicious nodes from repeating voting, the "secret ballot" mechanism is adopted.

(3) The other beacon nodes repeat step 2 until the voting is complete. The beacon nodes whose untrust value exceeds a certain threshold are labeled as malicious nodes and removed, and the beacon node list is updated.

(4) The unknown node estimated the distance from the beacon node by multiplying the hop number by the average hop distance of the beacon node, and estimated its own coordinate by formula (5).

(5) The located unknown node is marked as beacon node, and the unknown node and beacon node set are updated.

(6) The newly labeled beacon node calculates its average jump distance and broadcasts its ID, coordinates and average jump distance information through flood.

(7) Repeat the above steps until the number of unknown nodes is no longer reduced, the positioning process is completed, and the remaining nodes are marked as unlocatable nodes.

6. Simulation experiment and analysis

In this paper, MATLAB2018b will be used to carry out two related simulation experiments, one is the beacon node security detection screening test, the other is the GFCWDV-HOP algorithm positioning evaluation experiment. Specific parameter Settings are shown in Table 1:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

Table 1. Simulation parameter setting

Node deployment scope	1000m*1000m*1000m
Number of beacon nodes	21
Unknown number of nodes	100
Beacon node communication radius	600m
Unknown node communication radius	200m

6.1 The security detection and screening experiment of beacon node

In the localization process of underwater wireless sensor network (WSN), the beacon node is captured externally as a malicious node, and the malicious node broadcasts the wrong coordinate position to other nodes, resulting in the greatly increased positioning error of unknown nodes. In this experiment, we assume that the malicious nodes are randomly deployed in the experimental area and the externally broadcast coordinates are also in the experimental area.

According to the security detection algorithm of beacon nodes, the positioning error of malicious nodes is greater than that of benign beacon nodes, and the number of votes obtained is higher, that is, the degree of mistrust is higher. When the untrust exceeds a certain threshold, the node is labeled as a malicious node. In order to verify the effectiveness of the beacon node security detection algorithm, two indexes defined in literature [7] are adopted:

Recall rate: the proportion of correctly screened malicious nodes in all nodes.

Precision rate: the proportion of malicious nodes screened correctly.

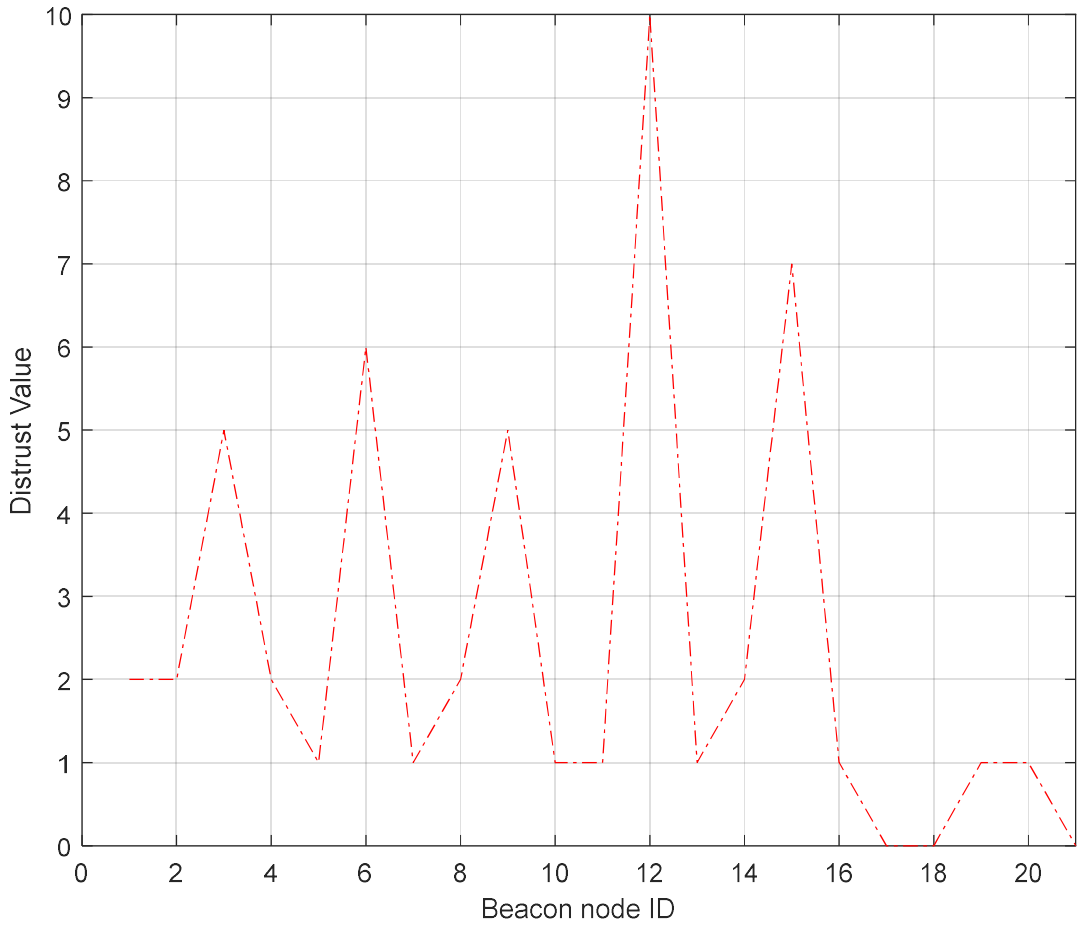

Figure 2. The result diagram of beacon node filtering

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

In the security detection and screening experiment of beacon nodes, 5 beacon nodes with IDS of 3, 6, 9, 12 and 15 were selected as malicious nodes. It can be seen from the figure that the distrust of these 5 beacon nodes is high. When the threshold value of 4 is selected, both the recall and precision of the experiment are 100%. From the experimental results, we can see that under the condition of setting an appropriate threshold, the security detection and screening algorithm for beacon nodes can effectively screen out and eliminate malicious nodes, and reduce the interference of malicious nodes to the unknown node location.

6.2 Experiment of location evaluation of GFCWDV-HOP algorithm

In DV-HOP algorithm, the connectivity of wireless sensor network is related to the number of beacon nodes, and the number of beacon nodes directly affects the positioning results. In a 1000m×1000m×1000m area, the communication radius of beacon nodes and unknown nodes is 600m and 200m respectively, and the number of beacon nodes is set as 5, 10, 15, 20 and 25 in turn. Random experiments are conducted to observe the average positioning error of unknown nodes. The simulation results are shown in Figure 3. According to this result, we can draw the following conclusion: no matter which algorithm is used, the average positioning error always decreases with the increase of the number of beacon nodes, and finally stabilizes at a certain value. If the number of beacon nodes of wireless sensor is small, the positioning error of the three algorithms is relatively high, but the GFCWDV-HOP algorithm is obviously due to the other two algorithms. When the number of beacon nodes reaches a certain number, the positioning errors of the three algorithms are significantly reduced, and the GFCWDV-HOP algorithm is still superior to the other two algorithms. With the increase of the number of beacon nodes, the positioning error tends to be stable. In a word, GFCWDV-HOP algorithm has high positioning accuracy no matter the number of beacon nodes is large or small.

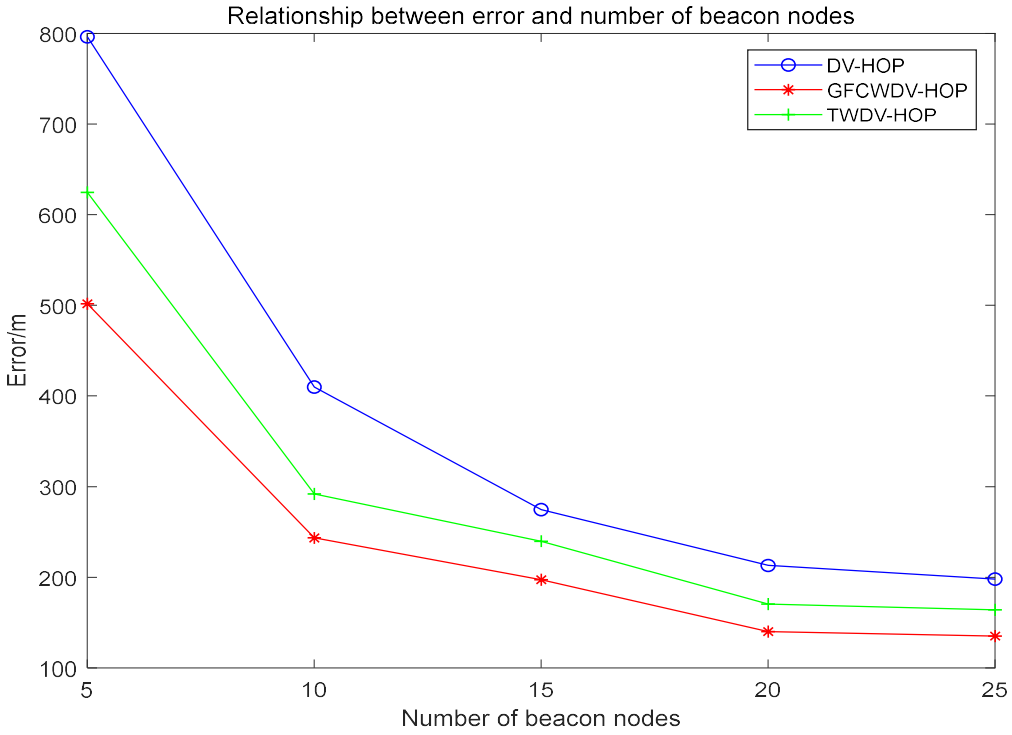

Figure 3. The relationship between error and the number of beacon nodes

In the localization algorithm of wireless sensor network, the localization coverage is also an index to evaluate the advantages and disadvantages of the localization algorithm. Similarly, we kept the communication radius of beacon nodes and unknown nodes unchanged, which were 600m and 200m respectively, and set the number of beacon nodes in turn as 5, 10, 15, 20 and 25. Experiments were

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

carried out randomly. The positioning coverage of different algorithms was simulated, and the simulation results were shown in Figure 4. With the increase of the number of beacon nodes, the coverage of the three algorithms will increase. The coverage of DV-HOP algorithm is significantly lower than that of the other two algorithms. Compared with TWDV-Hop algorithm, the coverage of GFCWDV-Hop algorithm is relatively higher. When the number of beacon nodes is 25, the coverage of GFCWDV-HOP algorithm reaches more than 90%.

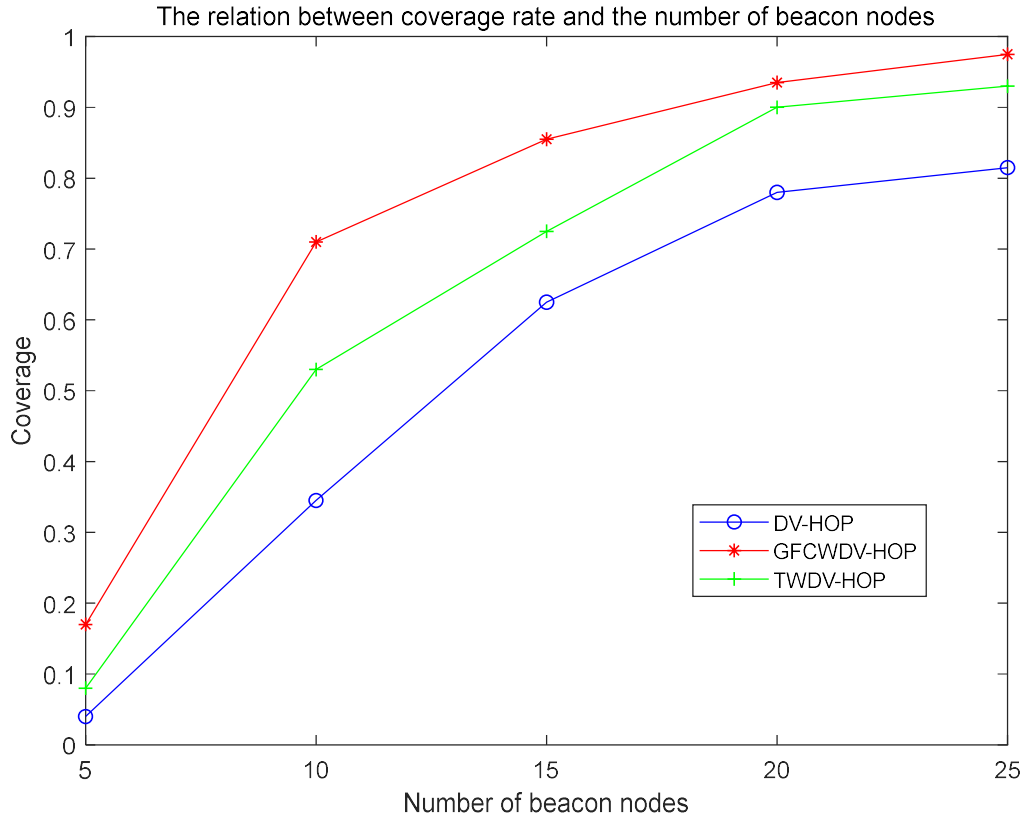

Figure 4. The relation between coverage rate and the number of beacon nodes

7. Conclusion

Based on DV-HOP localization algorithm, this paper proposes an underwater WSN node cooperative safety localization algorithm based on weighted DV-HOP algorithm. Aiming at the problem that beacon nodes are easy to be captured and release wrong location information during the localization process of underwater wireless sensor network, the malicious nodes can be effectively proposed and the interference can be reduced through the security detection and screening of beacon nodes. At the same time, the cooperative localization method can effectively solve the problem of low localization coverage caused by node failure and the sparse distribution of beacon nodes. Simulation results show that the localization error of the proposed algorithm is significantly less than that of DV-HOP and TWDV-HOP algorithms, and the localization coverage is improved.

References

[1] Nuo W, Ming-Lei S, Ming Y, et al. A localization algorithm for underwater wireless sensor networks with the surface deployed mobile anchor node[C]//2015 Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA). IEEE, 2015: 30-32.

[2] Wang X, Qin D, Zhao M, et al. UWSNs positioning technology based on iterative optimization and data position correction[J]. EURASIP Journal on Wireless Communications and Networking, 2020, 2020(1): 1-19.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202103_7(3).0008

[3] Akyildiz, Ian F., D. Pompili, and T. Melodia. "Challenges for efficient communication in underwater acoustic sensor networks." Acm Sigbed Review 1.2(2004):3-8.

[4] W. Fang, H. Xu and G. Yang. Improved DV-Hop Algorithm Based on Minimum Hops Correction and Reevaluate Hop Distance. 2019 5th International Conference on Information Management (ICIM), Cambridge, United Kingdom, 2019:102-107.

[5] Hadir A, Zine-Dine K, Bakhouya M, et al. An optimized DV-hop localization algorithm using average hop weighted mean in WSNs[C]//2014 5th Workshop on Codes, Cryptography and Communication Systems (WCCCS). IEEE, 2014: 25-29.

[6] Zhipeng X, Chunwen L, Huanyu L. An improved hop size estimation for DV-hop localization algorithm in wireless sensor networks[C]//The 27th Chinese Control and Decision Conference (2015 CCDC). IEEE, 2015: 1431-1434.

[7] Yongbo M. Research on accurate dynamic location and its Security of Wireless Sensor Networks[D]. Jilin university, 2010.

[8] S. Y. LU, J. Y. Xie and L. L. Pang.An Improved WSN Localization Algorithm.2018 IEEE 2nd International Electrical and Energy Conference (CIEEC), Beijing, China, 2018:392-396.

[9] Ying Z , Ji-Xing L, Sheng-Ming J, et al. Cooperative Nodes Localization for Three-Dimensional Underwater Wireless Sensor Network Based on Weighted Centroid Localization Algorithm[J]. Journal of Donghua University, 2016, 33(3).