# A Secure Localization Algorithm in Wireless Sensor Networks with Mobile Anchor Nodes

Jifeng Cui [1,a] , Feng Xu[1,b] , Wei Zhou [1,c]

[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing P.R.China 210016

[a]cuijfeng2010@163.com, [b]nuaaos@gmail.com, [c]hi_zhouwei@163.com

**Keywords:**wireless sensor networks, secure localization, mobile anchor node, identity authentication

**Abstract.** In process of localization in wireless sensor networks (WSNs)， to improve localization precision, lower network cost and reduce network consumption, mobile anchor node-based localization algorithms for WSNs are ceaselessly put forward and improved. In WSNs localization algorithm with a few mobile anchor nodes, the whole network is utterly dependent on the few mobile anchor nodes, which causes serious security hidden dangers. In this case, we study existing methods and propose a secure localization algorithm based on anchor node identity authentication and communication encryption security policy. Comparing to the conventional methods, the algorithm is able to effectively isolate impersonation attacks from hostile nodes. We simulate with the method and the result shows that our method can effectively restrain impersonation attacks.

## Introduction

In process of the localization in wireless sensor networks (WSNs)[1], more anchor nodes are used to achieve high precision, but it increases network overhead which is inconsistent with the features of low power consumption, low cost of WSN. With bringing mobile anchor nodes [2-6] in WSN, both localization efficiency and localization effect are improved. Therefore, mobile anchor node is gaining popularity and many scholars are researching it for localization.

Karim and Nasser propose Range-free Energy efficient, Localization technique using Mobile Anchor (RELMA) [7] for large scale WSNs. The proposed technique not only reduces power consumption by reducing the number of anchor nodes, but also improves localization accuracy. Ou proposes a range-free localization algorithm [8] for wireless sensor networks (WSNs) with mobile anchor nodes, which is equipped with four directional antennas. In the proposed scheme, each mobile anchor node is localized by GPS, and then each coordinate would be broadcasted with mobile anchor nodes moving through the WSN. The unknown sensor nodes accept these beacon messages and determine their own coordinates based on those of the anchors by utilizing a simple processing scheme. Jiang and Han propose a Localization algorithm with a Mobile Anchor node based on Trilateration (LMAT) [9]. The proposed algorithm uses a mobile anchor node to move according to the equilateral triangle trajectory in deployment area. The unknown sensor nodes detect beacon messages from the mobile anchor and utilize trilateration to determine their own coordinates based on that of the anchor.

One of the best advantages based on mobile anchor node is that it can locate precisely in WSNs with a few mobile anchor nodes. As the mobile anchor node is captured and the malicious node disguises as the anchor node, the localization of whole WSN will stop working, for the whole localization process relies heavily on the few mobile anchor nodes.

Based on anchor node identity authentication and communication encryption security policy, we propose a secure localization algorithm with existing algorithm [10]. Moreover, the security policy can be applied in many other mobile anchor node-based algorithms as well.

## Localization algorithm based on mobile anchor nodes

When choose trilateration to locate, unknown nodes gain the location of neighboring anchor nodes and the distance to these anchor nodes firstly. Obviously, for Range-free localization algorithm, the unknown nodes are closer to the anchor nodes, the higher in localization accuracy. On the contrary, the localization error is larger. SHI proposes an accurate localization algorithm based on three mobile anchor nodes [10]. First of all, the moving strategy of mobile anchor nodes and the topological structure formed by park positions of mobile anchor nodes would be shown. The algorithm mainly utilizes three mobile anchor nodes to traversal the whole network according to moving strategy what mentioned above. When the anchor nodes sent messages according to topological structure, any network unknown nodes can receive messages from at least three different position and nearer anchor nodes. This can ensure that all the unknown nodes can accurately determine their coordinates.

Assume that all nodes are randomly distributed over a circular region, the radius of the circle is R. As shown in Fig.1, we first place anchor node $N_1$ in the circle center O. Then the anchor node $N_2$ and $N_3$ are placed on A and B respectively, and constitute an equilateral triangle whose side is r with the anchor node $N_1$.

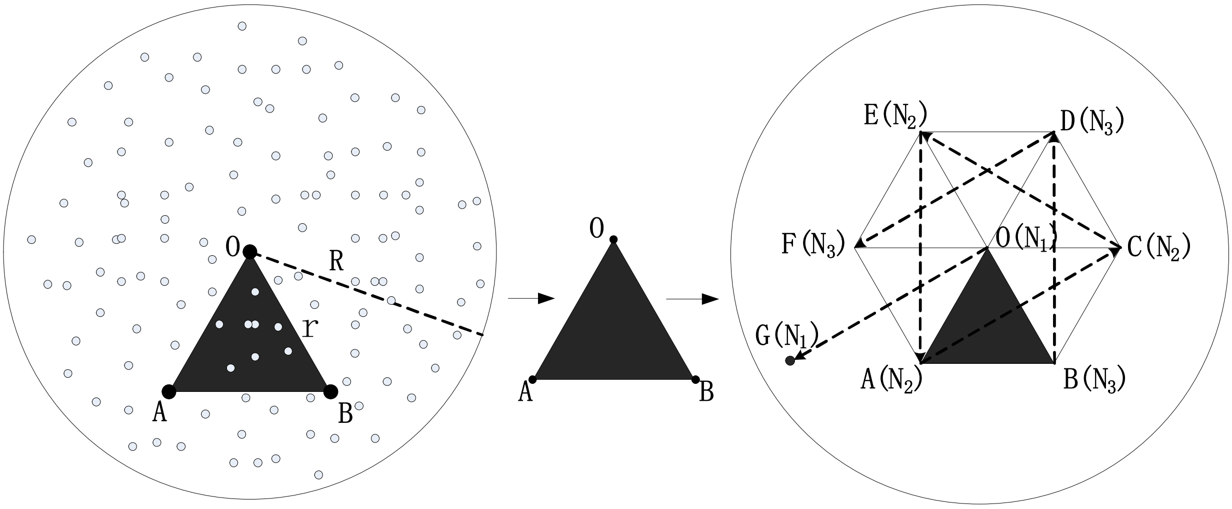
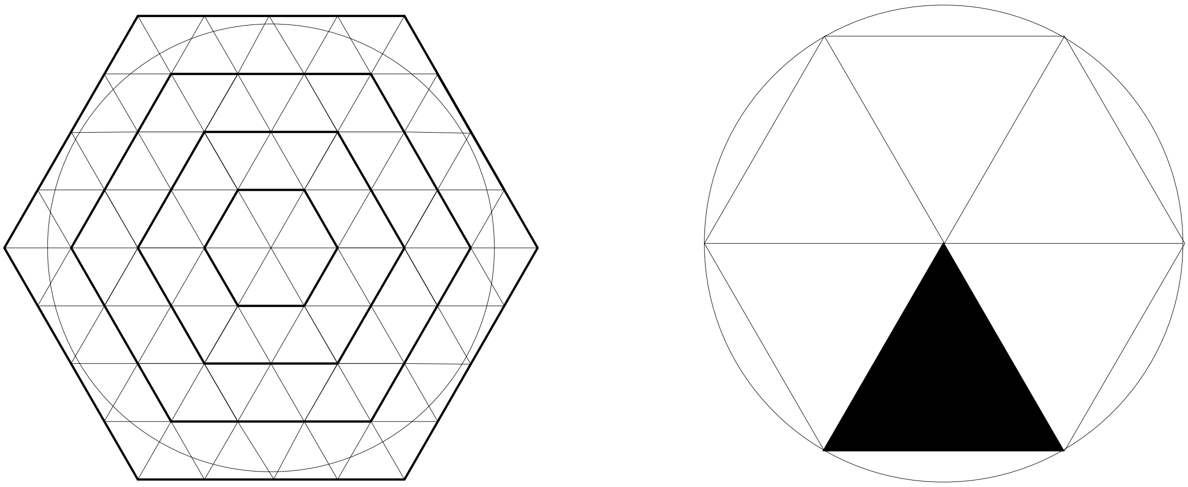


Fig.1 From initial location of anchor nodes to the first layer movement

The three anchor nodes will move successively at the same rate according to the moving strate gy in Fig.1 after their placement. The first movement: the anchor nodes $N_1$ and $N_3$ at O and B do not move, the anchor node $N_2$ at A moves to C along the perpendicular bisector of OB, and constitutes another equilateral triangle whose side is r with $N_1$ and $N_3$. The second movement: the anchor nodes $N_1$ and $N_2$ do not move, $N_3$ moves to D along the perpendicular bisector of OC, and constitutes another equilateral triangle whose side is r with $N_1$ and $N_2$. With this analogize, the anchor node $N_2$ return to A after fifth movement, and it constitutes the last equilateral triangle of the first layer movement. Then, the anchor nodes $N_2$ and $N_3$ at A and B do not move, the anchor node $N_1$ at O moves to G along the perpendicular bisector of AF, and it constitutes the first equilateral triangle whose side is r of the second layer movement. Then, the three anchor nodes complete the second layer movement according to the moving strategy of first layer movement.

Subsequently, the three mobile anchor nodes moves layer by layer according to the moving strategy mentioned above, until the topological structure can cover the entire region monitored by the network. After the whole moving process, all unknown nodes in the monitoring area can use at least three anchor nodes localization and the distance to these nodes and ensure their own localization by trilateration. After the moving, the topological structure would be formed by park positions of mobile anchor nodes which shown in Fig.2.



(a) r<R (b) r=R

Fig.2 Topology structure of the location of anchor nodes

## The secure localization algorithm based on mobile anchor nodes

The WSN localization algorithm proposed above can use three mobile anchor nodes to localize precisely with low power consumption and low cost. This is the strength of the algorithm, but it is also the most serious security hidden danger of the method. For the whole network node localization is utterly dependent on the three mobile anchor nodes, when the hijacked node disguises as the anchor node, it will cause algorithm failure and make the whole WSN stop working.

Therefore, we bring anchor node identity authentication and communication encryption in the method and make the localization algorithm safer.

## Communication Encryption

In order to prevent localization information is intercepted maliciously by the device from the outside network, packets issued by the anchor node have to be encrypted. Symmetric encryption is utilized, for the computing capacity limitation of the sensor node and the low power requirements. All the unknown nodes and anchor nodes are pre-set with the shared key K0 before placed.

## Anchor node identity authentication

With the shared key $K_0$, unknown nodes and anchor nodes cannot be used to identify whether the localization packet is sent by anchor node or the hostile node. One-way Hash chain is adopted to authenticate the location message sender's identity. Each mobile anchor node $N_i$ has a unique password $PW_i$ , meanwhile other anchor nodes and unknown nodes will not be informed in advance. $PW_i$ is hidden in the Hash functions such as $MD_5$. For operating only one-way, Hash function guarantees attacker will not find $PW_j$, making $PW_i \neq PW_j$ and $H(PW_i) = H(PW_j)$, where $H$ stands for the Hash function. Hash chain generation algorithm is as follows: $H_0=PW_i,H_i=H(H_{i-1}),i=1,\cdots\cdots,n$. $n$ is a big enough number, $H_0$ is own by the anchor node. Each node is preloaded with three anchor node ID number and the corresponding $H_n(PW_i)$. Each mobile anchor node moves to reach the designated position to send packets, in accordance with positioning strategic. Packet contains $(H_{n-j}(PW_i), j)$ , $j$ represents the serial number of the locate packet. The first packet $j=1$, unknown node needs simply to determine $H(H_{n-1}(PW_i))= H_n(PW_i)$ to verify the identity of anchor nodes, and $(H_{n-1}(PW_i)$ is saved to memory. It can be determined that the locate packet is sent by the anchor if the equation is true. Otherwise, a malicious node can be determined to camouflage as the anchor node sending messages, then alert will be sent immediately and malicious nodes will be excluded. Second packet contains $(H_{n-j}(PW_i), j),j=2$, unknown node only needs to verify whether the equation $H(H_{n-2}(PW_i))= H_{n-1}(PW_i)$ is ture,to determine if the packet is sent by the anchor node $N_i$.

## The realization of secure localization

Suppose the unknown nodes in the network are uniformly distributed. Before the localization, we must estimate the average hop distance. As follows: place anchor node $N_1$ and $N_2$ at the WSNs randomly. After the placement, $N_1$ send message which contain the location coordinates of $N_1$ and the hops to $N_2$. Accept the message, $N_2$ figure up the actual distance to $N_1$ according to the location coordinates. Base on the actual distance and the hops, the average hop distance would be obtain simply. Change the location of $N_1$ and $N_2$, large number of experiments would be carried out as above. Figure out the average of all the average hop distances, we get the value of $hop_{avg}$.

We take this security policy, which broadcasts the hops and location coordinates separately, to prevent the malicious node changes the receiving information and makes the spoofing broadcast. After the anchor node moving to the specified location according to the moving strategy, it will firstly broadcast a message *MSG1* as described below with the radius r. $MSG1{:}\{ID_i||hop_i||(H^{n-j}(PW_i),j)\}_{K0}$, $j=1$;The $ID_i$ representatives the anchor node's identifier, the hopi representatives the hops with the anchor node $N_i$ , the $(H^{n-j}(PW_i),j)$ representatives the anchor node's authentication information, and the $\{m\}_k$ means encrypting the message m with secret key k. The unknown nodes receive the *MSG1*, decrypte the message with key $K_0$ to verify the anchor node, and store the hop between itself and the anchor node to the memory. Some unknown node will stop broadcasting when its receiving message's $hop_i$ equals to $r/hop_{avg}$ , which ensures every unknown node locates by the anchor node who's distance with it is less than r. And after the broadcast of *MSG1* accomplished, the anchor node will broadcast another message *MSG2* as described below in the same policy.$MSG2{:}\{ID_i||(x_i,y_i)||(H^{n-j}(PW_i),j\}_{K0},j=2,(x_i,y_i)$;The unknown node will calculate its location coordinates by the measurement of three edges after its receiving, decryption, and verification of *MSG2.*

## Performance analysis and comparison

We will perform simulation experiment for the proposed algorithm, the purpose is to compare the system average localization error between the mobile anchor nodes localization algorithm without secure strategy and the anchor nodes localization algorithm with secure strategy when meet the spoofing attack by hostile nodes. We assume that unknown nodes deployed in the monitoring area uniformly, all the simulation experiments in this section use the experiment parameter in Tabel 1.

Table 1 The experiment parameter

| parameter | value |
|---|---|
| monitoring area radius (R) | 100 units |
| unknown nodes density (ρ) | 10 |
| the moving vate of anchor nodes (v) | 100 units/min |
| the standing time of anchor nodes (t) | 1 min |

## The positioning performance comparison under the spoofing attack by hostile nodes

Fig.3 shows the original localization algorithm under spoofing attack by hostile nodes, the relationship between the percentage of location failure nodes and the percentage of hostile nodes. As shown, the higher nodes density and the more hostile nodes, the large percentage of localization failure nodes in WSNs. This is due to the hostile node can interfere with the unknown nodes in the circle with radius r.

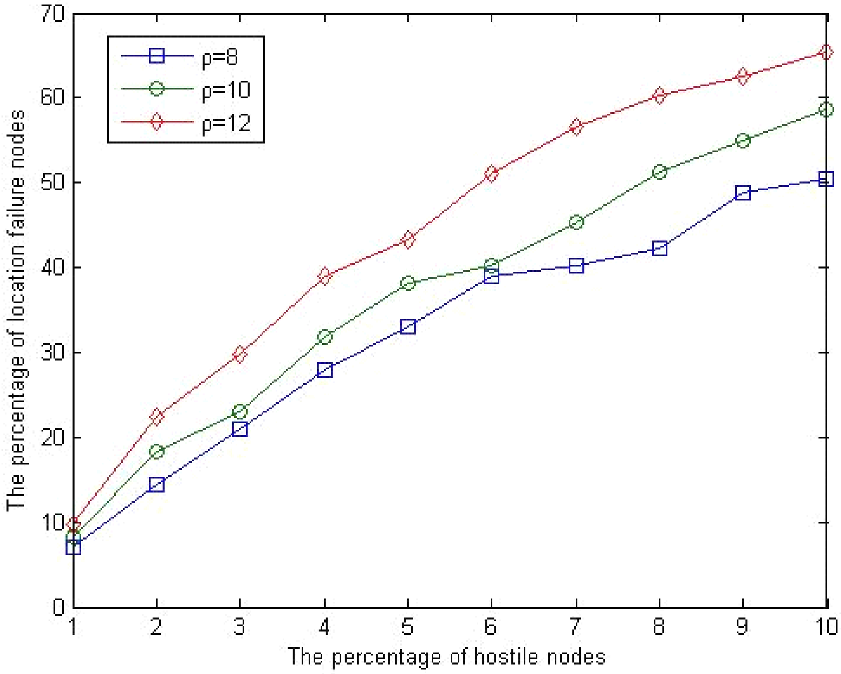


Fig.3 The positioning performance comparison under the spoofing attack by hostile nodes

The secure mobile anchor nodes localization algorithm adopts the anchor node identity authentication mechanism, it can ensure the effective localization messages received by unknown nodes all come from anchor nodes $N_1$, $N_2$ and $N_3$. Therefore, it is immune to the spoofing attack by hostile nodes.

## The network traffic comparison

The comparison of network traffic between original localization algorithm and secure localization algorithm is shown in Fig.4. Secure localization algorithm increases 128bit identity authentication information than original localization algorithm, so the traffic is bigger than the original localization algorithm. Although the higher power consumption, the whole network become securer in exchange.

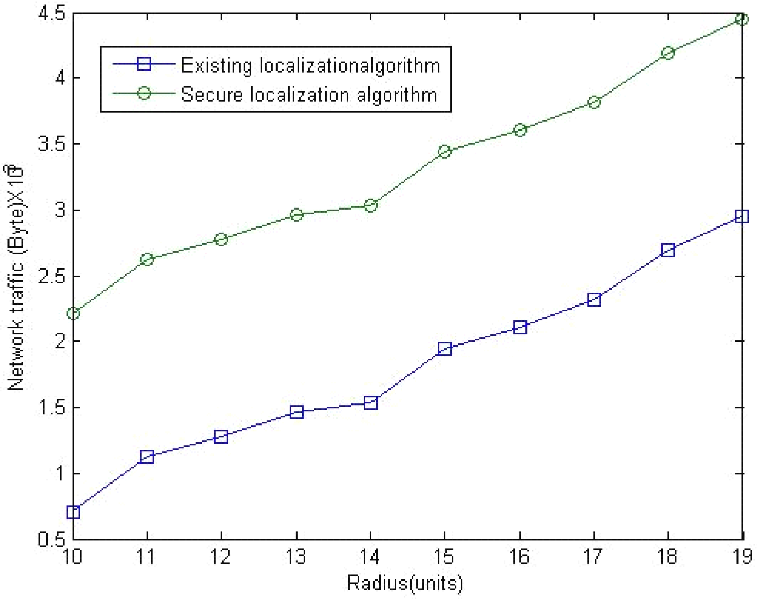


Fig.4 The network traffic comparison

## Conclusions

In order to improve the safety performance of localization algorithm based on mobile anchor nodes, we have studied existing methods and propose a secure localization algorithm propose a secure localization algorithm added to identity authentication and communication encryption security policy. Compared to the primary localization algorithm, the secure localization algorithm can locate unknown nodes in accuracy with the impersonation attack from hostile nodes. Moreover, the security policy can be applied in many other mobile anchor node-based algorithms as well.

## References

[1] Akyildiz IF, Su W, Sankarasubramainam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine, 2002,(8): 102−114.

[2] K. Ssu, C. Ou, and H. Jiau, Localization with Mobile Anchor Points in Wireless Sensor Networks. IEEE Trans. Vehicular Technology. 2005; 54(3): 1187-1197.

[3] K. Liu and J. Xiong, A Fine-grained Localization Scheme Using a Mobile Beacon Node for Wireless Sensor Networks. Journal of Information Processing Systems. 2010; 6(2): 147-162.

[4] D. Koutsonikolas, S. Das and Y.Hu, Path Planning of Mobile Landmarks for Localization in Wireless Sensor Networks. Computer Communication.2007; 30(13): 2577-2592.

[5] Sun GL, Guo W. Comparison of distributed localization algorithms for sensor network with a mobile beacon. In: Proc. of the IEEE Int'l Conf. on Networking, Sensing and Control. 2004. 536−540.

[6] H. Zhen, D. Gu and Z. Song, Localization in Wireless Sensor Networks Using a Mobile Anchor Node. In: Proc. of IEEE/ASME on Advanced Intelligent Mechatronics. 2008; 602-607.

[7] Karim L., Nasser N. and Salti T.E, "RELMA: A Range free Localization Approach using Mobile Anchor Node for Wireless Sensor Networks", IEEE Globecom 2010, Miami, Floria, Dec 6-10, 2010

[8] Chia-Ho Ou;, "A Localization Scheme for Wireless Sensor Networks Using Mobile Anchors With Directional Antennas," Sensors Journal, IEEE, vol.11, no.7, pp.1607-1616, July 2011.

[9] Jinfang Jiang; Guangjie Han; Huihui Xu; Lei Shu; Guizani, M. "LMAT: Localization with a Mobile Anchor Node Based on Trilateration in Wireless Sensor Networks", Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, On page(s): 1 – 6

[10] SHI Ting-Jun; SANG Xia; XU Li-Jie; YIN Xin-Chun. " A Localization Algorithm in Wireless Sensor Networks with Mobile Anchor Nodes", Journal of Software, Vol.20, Supplement, December 2009, pp.278−285