Letter

A Trust Assessment-Based Distributed Localization Algorithm for Sensor Networks Under Deception Attacks

Ya Wang, Xinming Chen, Lei Shi, Yuhua Cheng, and Houjun Wang

Dear Editor,

This letter is concerned with the distributed localization issue for wireless sensor networks subject to deception attacks. It is assumed that malicious nodes randomly launch attacks to tamper the ranging information between sensors. In order to accommodate the effects of deception attacks, a trust assessment-based distributed localization algorithm is proposed. Combined with data fusion of barycentric coordinates, our algorithm can achieve accurate localization. Finally, numerical simulations are given to validate the effectiveness of the proposed localization algorithm.

The localization of sensor networks, which aims at obtaining the locations of sensors to achieve the monitoring of networks, is of great significance in various fields of military and industry [1], [2]. In order to achieve exact localization, numerous algorithms have been developed for wireless sensor networks [3]–[6]. For instance, in the presence of uncertainties, a semi-definite programming algorithm was introduced for node localization [3]. A second-order cone programming relaxation of localization was proposed to achieve faster speed than the semi-definite programming algorithm [4]. A gradient-based target localization algorithm was developed for robotic sensor networks by utilizing statistical techniques to estimate the location [5]. A gradient-based fingerprinting system for indoor localization was introduced [6]. However, it should be pointed out that most of existing localization algorithms have certain shortcomings such that they cannot achieve both accurate localization and global convergence. Thus, it is desirable for sensor networks to design an exquisite algorithm with both of the excellent characteristics. To address this issue, a fully distributed iterative localization (DILOC) algorithm on the basis of barycentric coordinates representation was utilized in [7], [8], which can globally converge to the sensors' accurate locations.

Actually, communication channels in sensor networks are quite vulnerable to cyber attacks due to the nature of wireless communication [9]. Deception attacks, as one of the most typical cyber attacks, may ruin the integrity of data by tampering the information transmitted through communication networks, and eventually lead to undesirable consequences such as malicious manipulation or even system breakdown [10]. To alleviate the negative influence resulted from deception attacks, a number of secure control schemes have been studied [11]–[15]. For example, by designing a pinning strategy-based impulsive controller, the problem of synchronization under deception attacks in multi-agent systems was investigated in [11]. A consensus protocol of multiagent systems under sparse linear injection attacks was designed and the relevant optimization problem was solved efficiently by the means of alternating direction method of multipliers [12]. Moreover, a distributed set-membership filtering algorithm along with two recovery mechanisms for a vehicle platooning system was introduced to identify and resist attacks in [13]. A Lyapunov-based nonlinear control scheme based on a multiagent system was presented in [14] to defend real-time false-data-injection attacks. Based on the notion of network robustness, resilient consensus problem of networked control systems under F-local deception attacks was considered [15]. Although there have been some initial works on secure control under deception attacks, most of them focus on multiagent systems. To the best of the authors' knowledge, there is a paucity of related results on the localization of wireless sensor networks. Therefore, it is interesting yet challenging to develop a localization algorithm for wireless sensor networks subject to deception attacks.

Motivated by the above observers, this letter aims to solve the localization issue of sensor networks in the presence of deception attacks. Its contributions are twofold: 1) A universal model of deception attacks under which the ranging information based on received signal strength indicator (RSSI) is tampered by injecting false data is considered; 2) A distributed iterative localization algorithm combined with the techniques of trust assessment and data fusion is developed, and it can effectively achieve the accurate localization of sensor networks.

Problem formulation: Consider a wireless sensor network with N nodes, where there are m anchors with known locations and $N-m$ non-anchors whose locations need to be localized. The communication interactions among these nodes can be represented as a digraph denoted by $\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$, which is comprised of a node set $\mathcal{V}$ and an arc set $\mathcal{E}$. The node set $\mathcal{V}$ can be separated as an anchor node set $\Phi=\{1,2,\ldots,m\}$ and a non-anchor node set $\Psi=\{m+1,m+2,\ldots,N\}$, i.e., $\mathcal{V}=\Phi\cup\Psi$. An arc with an initial node v_i and a terminal node v_j is denoted by (v_i,v_j). There are no self-loops, namely, no such arcs as (v_i,v_i), $i=1,2,\ldots,N$. $Conv\{\mathcal{Z}\}$ denotes the convex hull of a set $\mathcal{Z}$ of nodes which is the smallest convex set containing $\mathcal{Z}$. $\mathcal{N}_i$ refers to the set of neighbor nodes connected to node i. Let $|\mathcal{N}_i|$ be the cardinality of $\mathcal{N}_i$. For $y\in\mathbb{R}$, $abs(y)$ means the absolute value of y.

The objective of this letter is to design a distributed localization algorithm for non-anchors such that they can converge to accurate locations in spite of the existence of deception attacks.

1) Barycentric coordinate representation: In this letter, the location of each non-anchor node can be calculated by barycentric coordinates with respect to their neighbor nodes. The barycentric coordinate is a geometric concept proposed in [16], which represents the relative position of one node in regard to other nodes. In the two-dimensional space, three nodes that are not on one straight line can determine the whole plane. Therefore, without losing generality, we show the barycentric coordinates of one node with respect to three other nodes. The Euclidean coordinates of four nodes, say i, r, s, t in the plane are denoted by p_i, p_r, p_s, p_t, respectively. The barycentric coordinates of node i with respect to r, s, t are a_{ir}, a_{is}, a_{it}, which satisfy

$$p_i = a_{ir}p_r + a_{is}p_s + a_{it}p_t. \tag{1}$$

Particularly when $a_{ir}+a_{is}+a_{it}=1$, the barycentric coordinates can be calculated by the proportion of signed areas between specified triangles. Fig. 1 provides an illustration of node i lying in the convex hull spanned by nodes r, s, t, and the barycentric coordinates of node i can be determined by

$$a_{ir}=\frac{S_{\triangle ist}}{S_{\triangle rst}},\ a_{is}=\frac{S_{\triangle irt}}{S_{\triangle rst}},\ a_{it}=\frac{S_{\triangle irs}}{S_{\triangle rst}} \tag{2}$$

where $S_{\triangle ist}$, $S_{\triangle irt}$, $S_{\triangle irs}$, $S_{\triangle rst}$ indicate the signed areas of the corresponding triangles $\triangle ist$, $\triangle irt$, $\triangle irs$, $\triangle rst$. Furthermore, we can utilize Cayley-Menger determinant [17] to calculate $S_{\triangle ist}$, $S_{\triangle irt}$, $S_{\triangle irs}$, $S_{\triangle rst}$, for instance,

$$S^2_{\triangle ist}=-\frac{1}{16}\det\begin{bmatrix}0&1&1&1\\1&0&d^2_{is}&d^2_{it}\\1&d^2_{si}&0&d^2_{st}\\1&d^2_{ti}&d^2_{ts}&0\end{bmatrix} \tag{3}$$

Corresponding author: Lei Shi.

Citation: Y. Wang, X. M. Chen, L. Shi, Y. H. Cheng, and H. J. Wang, "A trust assessment-based distributed localization algorithm for sensor networks under deception attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 10, pp. 1879–1882, Oct. 2022.

Y. Wang is with the School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, and also with the School of Intelligent Manufacturing, Chengdu Technological University, Chengdu 611730, China (e-mail: ya-wang@outlook.com).

X. M. Chen, L. Shi, Y. H. Cheng, and H. J. Wang are with the School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: chenxinming1997@126.com; shilei 910918@126.com; chengyuhua_auto@uestc.edu.cn; hjwang@uestc.edu.cn).

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

Digital Object Identifier 10.1109/JAS.2022.105881

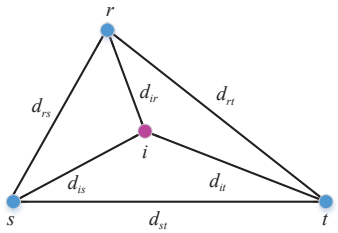

Fig. 1. Illustration of a node lying in the convex hull of its adjacent nodes.

where d_{is} denotes the Euclidean distance between nodes i and s.

Definition 1: $\Delta_i(\delta_i)=\{j\in\mathcal{N}_i: d_{ij}<\delta_i\}$ is denoted as the triangulation set of a node $i\in\Psi$, provided that the following conditions are satisfied:

$$\Delta_i(\delta_i)\subseteq\mathcal{N}_i,\ \ i\in Conv\{\Delta_i(\delta_i)\},|\Delta_i(\delta_i)|=3. \tag{4}$$

Assumption 1: All non-anchors locate in the convex hull of anchors, that is, $Conv\{\Psi\}\subseteq Conv\{\Phi\}$.

Assumption 2: For each non-anchor node $i\in\Psi$, there exist multiple triangulation sets denoted by $\Delta_i^{(k)}(\delta_i)\in\{\Delta_i^{(1)}(\delta_i),\Delta_i^{(2)}(\delta_i),\ldots,\Delta_i^{(K_i)}(\delta_i)\}$, such that any two nodes from the set $\{i\}\cup\Delta_i^{(k)}(\delta_i)$ can communicate with each other.

Remark 1: The assumptions mentioned above are feasible for wireless sensor networks in practice. The locations of anchors are often determined by GPS or fixed manually. On the other hand, by appropriately increasing the communication radius δ_i, the number of triangulation sets that satisfy the conditions can be obtained.

2) Deception attack model: In this letter, it is assumed that malicious nodes are randomly distributed throughout the wireless sensor network which occasionally launch deception attacks on the nearest node, leading to the disintegrity of data transmitted among some of neighbor nodes. As depicted in Fig. 2, the nodes in green refer to sensors in the network, whereas the nodes in red stand for deception attack launchers, and the circles of red dotted line indicate the attack range of malicious nodes. Deception attacks aim to reduce the positioning accuracy or even make the whole sensor network unstable by modifying the data transmitted in the communication channels. In the scenario of this letter, the distances between sensors are measured based on RSSI. Therefore, the packet sent by a node, say r not only includes the location information $p_r(t)$ at the current iteration time t but also contains its transmitted signal power. With the same radio signal transmitting power, the distance between one node and its adjacent node is inversely proportional to the received signal power from the neighbor node, which as follows:

$$PR_{ir}(t)=c\frac{PT_{ir}(t)}{d_{ir}^{\mu}(t)}\Leftrightarrow d_{ir}(t)=\sqrt[\mu]{\frac{cPT_{ir}(t)}{PR_{ir}(t)}} \tag{5}$$

where c and μ are constants related to communication channel model, $PR_{ir}(t)$ denotes the signal power received by node i, and $PT_{ir}(t)$ is the signal power transmitted by neighbor node r, and $d_{ir}(t)$ refers to the distance between node i and node r. It is assumed that attacker can achieve the purpose of deception by tampering $PT_{ir}(t)$ in the packets.

Based on above assumptions, the distance measurements between the node and its triangulation neighbor node may be modified. Deception attacks mainly include data tampering, false data injection and replay attacks. Compared with other attacks, false data injection attacks which can bypass the surveillance of attack detection mechanism silently, are more destructive to the system. Furthermore, in this letter, the tampering of distance measurement can be well modeled through the false data injection model. Therefore, we set up the model that the distance values $d_{ir}(t)$ are tampered by injecting false data

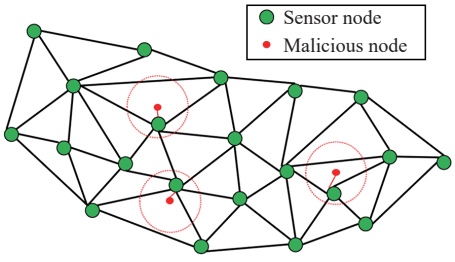

Fig. 2. Illustration of deception attack model.

$$\widetilde{d}_{ir}(t)=d_{ir}(t)+(1-\alpha_{ir}(t))\delta_{ir}(t)+\varsigma_{ir}(t) \tag{6}$$

where $\varsigma_{ir}(t)\sim N(0,\sigma_{ir}^2(t))$, $\sigma_{ir}(t)=\lambda d_{ir}(t)$, and λ is a constant noise parameter, ensuring that distance noise changes proportionally to the scale of network. $\delta_{ir}(t)$ denotes attack signal injected by malicious attackers, and attack signal strength is much greater than measurement noise. Hence, attack signals can make distance measurements deviate from $d_{ir}(t)$ to $\widetilde{d}_{ir}(t)$. $\alpha_{ir}(t)$ follows Bernoulli distribution with probability ϕ and has the value of 0 or 1 where $\alpha_{ir}(t)=0$ means that the adversary has launched false data injection attack, and $\alpha_{ir}(t)=1$ means that the transmitted data is normal.

Assumption 3: For each non-anchor i, there is at least one credible triangulation set in which each node is immune to deception attacks during the entire process of localization.

Remark 2: Due to the randomness of deception attacks launched and limited resources for stealth of malicious nodes, as well as the diversity of the triangulation sets of non-anchors, Assumption 3 is reasonable.

Algorithm design: In this section, a trust assessment based distributed iterative localization algorithm is proposed to eliminate the influence of deception attacks. Here we first introduce an evaluation scheme based on statistical characteristics to assess the trustworthiness of triangulation sets of non-anchors, and then in the process of distributed iterative localization, the weights of the triangulation sets those are evaluated as untrustworthy are reduced.

1) Trust assessment model: The statistical characteristics of non-anchors' distance measurements are analyzed to realize the monitoring of the system. When the transmitted signal power is not tampered by deception attack, the distance measurements ought to follow Gaussian distribution, that is, $\widetilde{d}_{ir}(t)\sim N(d_{ir}(t),\sigma_{ir}^2(t))$. Therefore, we set a threshold for the statistical characteristics of standard deviation as a criterion for judging whether it is subject to deception attacks.

Define trust assessment function of $\Delta_i^{(k)}(\delta_i)$ as follows:

$$\varepsilon_i^{(k)}(t)=\max_{j,r\in\{i\}\cup\Delta_i^{(k)}(\delta_i)}(abs(\widetilde{d}_{jr}(t)-\widetilde{d}_{jr}(t-1))-2n\widetilde{\sigma}_{jr}(t-1)) \tag{7}$$

where $\Delta_i^{(k)}(\delta_i)$ refers to the kth triangulation set of node i, n is a constant which can be modified to adjust the discriminating threshold, $\widetilde{\sigma}_{jr}(t)=\lambda\widetilde{d}_{ir}(t)$. If $\varepsilon_i^{(k)}(t)\le 0$, the ranging information among the nodes in $\{i\}\cup\Delta_i^{(k)}(\delta_i)$ is considered to have not been tampered by deception attacks. Furthermore, using the mean value to update the distance measurement at time t among non-anchors in $\{i\}\cup\Delta_i^{(k)}(\delta_i)$

$$\widetilde{d}_{jr}(t)=\frac{1}{t}\sum_{m=1}^{t}\widetilde{d}_{jr}(m)=\frac{t-1}{t}\widetilde{d}_{jr}(t-1)+\frac{1}{t}\widetilde{d}_{jr}(t) \tag{8}$$

where $j,\ r\in\{i\}\cup\Delta_i^{(k)}(\delta_i)$ and $j\ne r$. On the contrary, if $\varepsilon_i^{(k)}(t)>0$, it is deduced that triangulation set $\Delta_i^{(k)}(\delta_i)$ is not credible for non-anchor i at iteration time t, and then the distance measurement is remained as the value at time $t-h$

$$\widetilde{d}_{jr}(t)=\widetilde{d}_{jr}(t-h) \tag{9}$$

where $t-h$ is the latest moment such that $\varepsilon_i^{(k)}(t-h)\le 0$. If such preceding moment does not exist, the distance measurement is not updated at current time.

Consequently, in the following stage of distributed iterative localization, the degree of unreliable triangulation sets to influence the positioning process will be decreased to alleviate the negative impacts of deception attacks on the wireless sensor networks.

2) Distributed iterative localization: In this letter, we adopt a data fusion method of barycentric coordinates combined with trust assessment, on the basis of the DILOC algorithm [7] to resist deception

attacks.

According to Assumption 2, the position of non-anchor i can be determined by its triangulation sets, thus the location of node i can be represented in the following iterative form:

$$p_i(t+1)=(1-\gamma)p_i(t)+\gamma\sum_{k=1}^{K_i}\sum_{r\in\Delta_i^{(k)}(\delta_i)}\eta_i^k(t)a_{ir}^k(t)p_r^k(t) \tag{10}$$

where γ is a constant gain parameter, K_i denotes the number of triangulation sets; $\eta_i^k(t)$ refers to the trust weight of $\Delta_i^{(k)}(\delta_i)$ which satisfies $\sum_{k=1}^{K_i}\eta_i^k(t)=1$ and starts with equal weights $\eta_i^k(0)=1/K_i$; $a_{ir}^k(t)$ stands for the barycentric coordinate of node i with respect to node r in the kth triangulation set at time t. If $\varepsilon_i^{(k)}(t)\le 0$, we have $\eta_i^k(t)=\eta_i^k(t-1)$. Otherwise, in order to mitigate the adverse effects caused by deception attacks, the proposed strategy is to reduce the weights of untrustworthy triangulation sets $\Delta_i^{(k)}(\delta_i)$ that determine the positions of non-anchors

$$\eta_i^k(t)=\beta\eta_i^k(t-1) \tag{11}$$

where $\beta\in(0,1)$ is an attenuation factor. After that, for each triangulation set of non-anchor i, we conduct normalization process

$$\eta_i^k(t)=\frac{\eta_i^k(t)}{\sum_{e=1}^{K_i}\eta_i^e(t)}. \tag{12}$$

Next, we integrate the trust evaluation scheme into the process of distributed iterative localization. The detailed realization is given in Algorithm 1.

Remark 3: Note that when there are not any untrusted nodes and the number of trigulation sets for every non-anchor is only one, Algorithm 1 is reduced to the case of the DILOC algorithm in [7].

Algorithm 1 Distributed Localization Based on Trust Assessment

1: Set the Bernoulli distribution parameter ϕ, gain coefficient γ, noise parameter λ, threshold parameter n, attenuation factor β and the initiate estimations $\check{p}_i(0)$, for $i\in\Psi$;

2: At each iteration step t, non-anchor $i\in\Psi$ estimates its coordinates according to the following rules:

3: Evaluate the confidence of each triangulation set $\Delta_i^{(k)}(\delta_i)$ according to (7);

4: **if** $\varepsilon_i^{(k)}(t)\le 0$ **then**

5: Update $\widetilde{d}_{jr}(t)$ using (8) and calculate $a_{ir}^k(t)$;

6: $\eta_i^k(t)=\eta_i^k(t-1)$.

7: **else**

8: **if** $\varepsilon_i^{(k)}(t-h)\le 0$ exists **then**

9: Update $\widetilde{d}_{jr}(t)$ using (9) and calculate $a_{ir}^k(t)$;

10: **else**

11: $\widetilde{d}_{jr}(t)=\widetilde{d}_{jr}(t)$ and calculate $a_{ir}^k(t)$;

12: **end**

13: Reduce $\eta_i^k(t)$ according to (11).

14: **end**

15: Normalize the modified weights using (12);

16: Update the coordinates of i based on the parameters obtained above according to (10).

Numerical example: A network with 3 anchors and 7 non-anchors are taken into account. The position of anchors are fixed as $p_1=(50,50\sqrt{3})$, $p_2=(0,0)$, $p_3=(100,0)$, and the accurate coordinates of non-anchors are set as

$$p_4=\left(\frac{200}{3},\frac{200\sqrt{3}}{9}\right),\ p_5=\left(50,\frac{250\sqrt{3}}{9}\right)$$

$$p_6=\left(\frac{100}{3},\frac{200\sqrt{3}}{9}\right),\ p_7=\left(\frac{100}{3},\frac{100\sqrt{3}}{9}\right)$$

$$p_8=\left(50,\frac{50\sqrt{3}}{9}\right),\ p_9=\left(\frac{200}{3},\frac{100\sqrt{3}}{9}\right),\ p_{10}=\left(50,\frac{50\sqrt{3}}{3}\right).$$

The triangulation sets of non-anchors are given as

$$\Delta_4^{(1)}(\delta_4)=\{1,3,10\},\ \Delta_4^{(2)}(\delta_4)=\{1,3,5\},\ \Delta_4^{(3)}(\delta_4)=\{1,3,9\}$$

$$\Delta_5^{(1)}(\delta_5)=\{1,4,10\},\ \Delta_5^{(2)}(\delta_5)=\{1,4,6\},\ \Delta_5^{(3)}(\delta_5)=\{1,6,10\}$$

$$\Delta_6^{(1)}(\delta_6)=\{1,2,10\},\ \Delta_6^{(2)}(\delta_6)=\{1,2,5\},\ \Delta_6^{(3)}(\delta_6)=\{1,2,7\}$$

$$\Delta_7^{(1)}(\delta_7)=\{2,6,8\},\ \Delta_7^{(2)}(\delta_7)=\{2,8,10\},\ \Delta_7^{(3)}(\delta_7)=\{2,6,10\}$$

$$\Delta_8^{(1)}(\delta_8)=\{2,3,10\},\ \Delta_8^{(2)}(\delta_8)=\{2,3,7\},\ \Delta_8^{(3)}(\delta_8)=\{2,3,9\}$$

$$\Delta_9^{(1)}(\delta_9)=\{3,4,10\},\ \Delta_9^{(2)}(\delta_9)=\{3,4,8\},\ \Delta_9^{(3)}(\delta_9)=\{3,8,10\}$$

$$\Delta_{10}^{(1)}(\delta_{10})=\{4,6,8\},\ \Delta_{10}^{(2)}(\delta_{10})=\{6,7,9\},\ \Delta_{10}^{(3)}(\delta_{10})=\{5,7,9\}.$$

As shown in Fig. 3, nodes in black refer to anchors and nodes in red are non-anchors to be localized. The communication interactions among sensors are indicated by directional arrows.

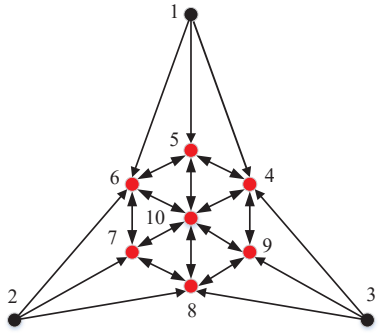

Fig. 3. Interactive topology among sensors.

Here, we suppose that non-anchor 4 is under deception attack, hence the related triangulation sets $\Delta_5^{(1)}(\delta_5)$, $\Delta_5^{(2)}(\delta_5)$, $\Delta_9^{(1)}(\delta_9)$, $\Delta_9^{(2)}(\delta_9)$ and $\Delta_{10}^{(1)}(\delta_{10})$ are affected by attack during localization. Let $\phi=0.2$, $\gamma=0.6$, $\lambda=0.05$, $n=3$, $\beta=0.85$, $t=100$. The initial location estimates of non-anchors are chosen as $\check{p}_4(0)=(36,70)$, $\check{p}_5(0)=(5,66)$, $\check{p}_6(0)=(-20,35)$, $\check{p}_7(0)=(65,75)$, $\check{p}_8(0)=(95,50)$, $\check{p}_9(0)=(100,15)$, $\check{p}_{10}(0)=(60,5)$.

With the provided parameters, the trust weights of triangulation sets of non-anchors 5, 9, 10 which receive information from node 4 subject to deception attacks are depicted in Figs. 4–6, respectively. As expected, the trust weights of triangulation sets involving information received from the attacked nodes can be reduced through the localization process with trust assessment and weight update. As can be seen from the figures above, the trust weights of the triangulation sets containing the attacked node 4, i.e., $\Delta_5^{(1)}(\delta_5)$, $\Delta_5^{(2)}(\delta_5)$, $\Delta_9^{(1)}(\delta_9)$, $\Delta_9^{(2)}(\delta_9)$ and $\Delta_{10}^{(1)}(\delta_{10})$ finally approach 0, while the sum of the weights of trusted triangulation sets converge to 1.

Moreover, Fig. 7 reveals that all the non-anchors cannot converge to the exact locations because the distance measurements obtained by some nodes are tampered, which illustrates the deficiency of DILOC [7] under deception attacks. In contrast, it can be proven from Fig. 8 that our proposed algorithm based on trust assessment is capable of achieving accurate localization while suffering from deception attacks. Therefore, the proposed localization algorithm has been numerically verified.

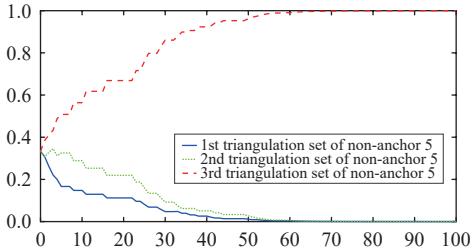

Fig. 4. Trust weight of the triangulation sets of non-anchor 5.

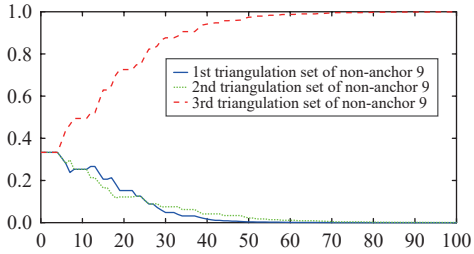

Fig. 5. Trust weight of the triangulation sets of non-anchor 9.

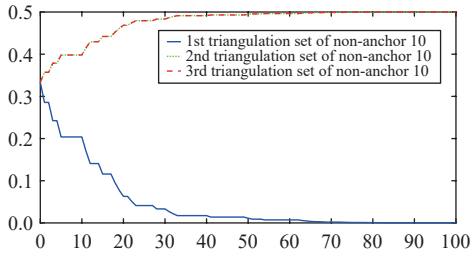

Fig. 6. Trust weight of the triangulation sets of non-anchor 10.

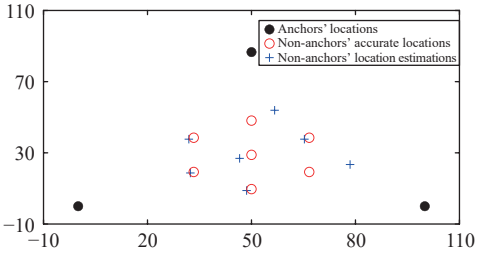

Fig. 7. Localization using DILOC [7] under deception attacks.

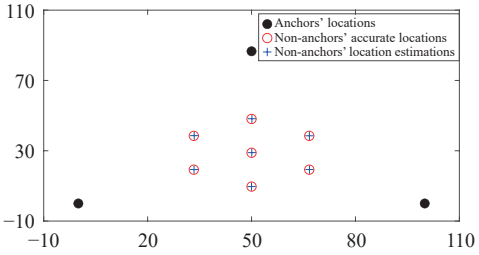

Fig. 8. Localization using our algorithm under deception attacks.

Conclusion: In this letter, the localization issue of wireless sensor networks under deception attacks has been investigated. A distributed iterative localization algorithm based on trust assessment has been presented for ensuring the accurate positioning of sensors subject to malicious tampering. By utilizing data fusion of barycentric coordinates combined with trust assessment model, the coordinates of non-anchors converge to their precise locations. Furthermore, the validity of the algorithm has been verified by numerical examples.

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (62103080), the Natural Science Foundation of Sichuan Province (2022NSFSC0878), the National Postdoctoral Program for Innovative Talents (BX2021056), the China Postdoctoral Science Foundation (2021M700696), and the Sichuan Science and Technology Program (2021YFH0042).

References

[1] N. Saeed, H. Nam, T. Y. Al-Naffouri, and M. Alouini, "A state-of-the-art survey on multidimensional scaling-based localization techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3565–3583, 2019.

[2] M. Ye, D. Li, Q.-L. Han, and L. Ding, "Distributed nash equilibrium seeking for general networked games with bounded disturbances," *IEEE/CAA J. Autom. Sinica*, 2021, DOI: 10.1109/JAS.2022.105428.

[3] 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 Trans. Signal Process.*, vol. 57, no. 2, pp. 752–763, Feb. 2009.

[4] P. Tseng, "Second-order cone programming relaxation of sensor network localization," *SIAM J. Optimiz.*, vol. 18, no. 1, pp. 156–185, Feb. 2007.

[5] Q. Zhang, G. E. Sobelman, and T. He, "Gradient-based target localization in robotic sensor networks," *Pervasive and Mobile Computing*, vol. 5, no. 1, pp. 37–48, Feb. 2009.

[6] Y. Shu, Y. Huang, J. Zhang, P. Coué, P. Cheng, J. Chen, and K. G. Shin, "Gradient-based fingerprinting for indoor localization and tracking," *IEEE Trans. Ind. Electr.*, vol. 63, no. 4, pp. 2424–2433, Apr. 2016.

[7] U. A. Khan, S. Kar, and J. M. F. Moura, "Distributed sensor localization in random environments using minimal number of anchor nodes," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 2000–2016, May 2009.

[8] L. Shi, Q. Liu, J. Shao, and Y. Cheng, "Distributed localization in wireless sensor networks under denial-of-service attacks," *IEEE Contr. Syst. Lett.*, vol. 5, no. 2, pp. 493–498, Apr. 2021.

[9] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomput.*, vol. 275, pp. 1674–1683, 2018.

[10] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 3595–3608, Jun. 2022.

[11] W. He, Z. Mo, Q.-L. Han, and F. Qian, "Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1326–1334, Sep. 2020.

[12] K. Tsang, M. Huang, K. Johansson, and L. Shi, "Sparse linear injection attack on multi-agent consensus control systems," *IEEE Control Syst. Lett.*, vol. 5, no. 2, p. 665670, Apr. 2021.

[13] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, p. 38213834, Sep. 2020.

[14] A. Sargolzaei, B. Allen, C. Crane, and W. Dixon, "Lyapunov-based control of a nonlinear multi-agent system with a time varying input delay under false-data-injection attacks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2693–2703, Apr. 2022.

[15] W. Fu, J. Qin, Y. Shi, W. X. Zheng and Y. Kang, "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4868–4877, Jul. 2020.

[16] H. S. M. Coxeter, *Introduction to Geometry*, New York, USA: John Wiley & Sons, 1961.

[17] M. Sippl and H. Scheraga, "Cayley-Menger coordinates," *Proc. National Academy of Sciences*, vol. 83, no. 8, pp. 2283–2287, Apr. 1986.