

Distributed Localization in Wireless Sensor Networks Under Denial-of-Service Attacks

Lei Shi^{ID}, Qingchen Liu^{ID}, Jinliang Shao^{ID}, and Yuhua Cheng^{ID}, *Senior Member, IEEE*

Abstract—In this letter, we study the problem of localizing the sensors' positions in presence of denial-of-service (DoS) attacks. We consider a general attack model, in which the attacker action is only constrained through the frequency and duration of DoS attacks. We propose a distributed iterative localization algorithm with an abandonment strategy based on the barycentric coordinate of a sensor with respect to its neighbors, which is computed through relative distance measurements. In particular, if a sensor's communication links for receiving its neighbors' information lose packets due to DoS attacks, then the sensor abandons the location estimation. When the attacker launches DoS attacks, the AS-DILOC algorithm is proved theoretically to be able to accurately locate the sensors regardless of the attack strategy at each time. The effectiveness of the proposed algorithm is demonstrated through simulation examples.

Index Terms—Localization, sensor networks, denial-of-service attacks, distributed algorithm.

I. INTRODUCTION

LOCALIZATION, which is a fundamental problem in wireless sensor networks, has attracted extensive attention in the past few decades. In some networks with centralized information structures, such as agricultural monitoring networks and road traffic monitoring networks, it is very convenient to use centralized localization method because

Manuscript received March 17, 2020; revised May 22, 2020; accepted June 14, 2020. Date of publication June 19, 2020; date of current version July 3, 2020. This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme through the Marie Skłodowska-Curie Agreement under Grant 754462, in part by the National Science Foundation of China under Grant U1830207, Grant 61772003, and Grant 61903066, in part by the China Postdoctoral Science Foundation under Grant 2017M612944 and Grant 2018T110962, and in part by the National Key Research and Development Program of China under Grant 2017YFC1501005 and Grant 2018YFC1505203. Recommended by Senior Editor M. Guay. (Corresponding author: Qingchen Liu.)

Lei Shi and Yuhua Cheng are with the School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: shilei@std.uestc.edu.cn; chengyuhua_auto@uestc.edu.cn).

Qingchen Liu is with the Chair of Information-Oriented Control, Technical University of Munich, 80869 Munich, Germany (e-mail: qingchen.liu@tum.de).

Jinliang Shao is with the School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: jinliangshao@uestc.edu.cn).

Digital Object Identifier 10.1109/LCSYS.2020.3003789

the measurement data of all nodes in the network are collected in a central processor [1], [2]. However, as described in [3], the centralized method is usually not suitable for large-scale sensor networks, and it requires higher computational complexity and lower reliability than the distributed method due to the accumulated information loss caused by the multi hop transmissions on the wireless network.

In 2009, Khan *et al.* [4] proposed a distributed iterative localization (DILOC) algorithm based on barycentric coordinates representation, where there are anchors, i.e., the nodes with known accurate locations, and sensors to be localized. The remarkable feature of the DILOC algorithm is that the sensor localization is represented by an iterative process with matrix-vector form through relative distance measurements. It has been proved that the DILOC algorithm can converge to the exact locations of sensors. Based on the framework of DILOC, the localization problem in different scenarios have been studied. In [5], the DILOC algorithm was utilized to achieve precise localization in a noisy environment. Deghat *et al.* [6] established an algebraic condition for the DILOC algorithm to achieve global convergence in a finite-time horizon. The global convergence with measurement noise and local convergence with least squares solutions of the DILOC algorithm were analyzed in [7]. Based on three types of hybrid measurements, including distance, azimuth and relative position, Lin *et al.* [8] presented a necessary and sufficient graphic condition for sensor localization. In addition, [9] proposed a more general iterative form for the DILOC algorithm by adding a gain parameter based on consensus of multi-agent systems (e.g., see [10], [11]). This consensus-based iterative form includes the iterative form in [4] as a special case.

Network security issues have gradually become the focus of public attention [12]–[14]. In recent years, various cyber attacks have appeared with different purposes. A common type of network attack is called denial of service (DoS), whose purpose is to block communication, thereby forcing network resources unavailable to its target users, i.e., packet loss. In most previous studies (e.g., [15], [16]), packet loss was always assumed to follow a probability distribution. In fact, it is not feasible for a defender to assume that packet loss caused by attackers follows a given probability distribution [17]. With this in mind, the reference [17] proposed a general attack model without any assumptions on the underlying attack strategy, where the attacker action is only constrained through the frequency and duration of DoS attacks.

To the best of our knowledge, most work based on the DILOC algorithm is carried out in a perfect communication environment [4]–[9]. It is of practical significance to analyze the localization problem of wireless sensor networks under DoS attacks, which is also the research motivation of this letter. According to the general DoS attacks model proposed in [17], we first uses a simulation example to show that the classical DILOC algorithm may not achieve localization, while the attackers can attack the communication network in a changing active time period. Then, we propose a new consensus-based distributed iterative localization algorithm using an abandonment strategy, which is called the AS-DILOC algorithm. By introducing the composition of binary relations and casting the iteration of the AS-DILOC algorithm as a convergence problem of the product of infinite sub-stochastic matrices, we prove that the AS-DILOC algorithm converges globally to the accurate locations of sensors in presence of DoS attacks.

The outline of this letter is shown as follows. Section II introduces some preliminary knowledge. Section III presents the AS-DILOC algorithm under DoS attacks in detail. In Section IV, the global convergence of the AS-DILOC algorithm is theoretically proved. This letter is concluded in Section V.

II. PRELIMINARIES

A. Notations

The set of natural numbers is denoted by \mathbb{N} . I_n is an n -order identity matrix. Let $\mathbf{0}$ be compatible dimensions of zeros, and $\mathbf{1}$ be an all 1's column vector. $M(i, :)$ denotes the i th row of matrix M . $\det[M]$ represents the determinant of matrix M . For a nonnegative matrix $M \in \mathbb{R}^{n \times n}$, its infinite norm is represented as $\|M\|_\infty = \max\{\sum_{j=1}^n M_{ij} : i = 1, 2, \dots, n\}$. A nonnegative matrix M is row-stochastic if $M\mathbf{1} = \mathbf{1}$, and it is sub-stochastic if $M\mathbf{1} \leq \mathbf{1}$. Let $\prod_{w=1}^s M_w = M_s M_{s-1} \cdots M_1$ represent the left products of matrices $M_i, i = 1, 2, \dots, s$.

Definition 1 [18]: The convex hull of the set $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ is the minimum convex set containing all points $x_i, i = 1, 2, \dots, n$, represented by $Co\{\mathcal{X}\} = \{\sum_{i=1}^n a_i x_i : a_i \geq 0, \sum_{i=1}^n a_i = 1\}$.

B. Graph Theory

Let $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ represent a digraph containing a node set $\mathcal{V} = \{1, 2, \dots, n\}$ and an arc set \mathcal{E} . An arc with initial node i and terminal node j is represented by (i, j) . There are no self-loops, namely, such arcs as $(v_i, v_i), i = 1, 2, \dots, n$. A directed path from nodes i_1 to i_z in \mathcal{G} is a finite non-null edge sequence $\mathcal{P}_{i_1 \rightarrow i_z} = (i_1, i_2)(i_2, i_3) \cdots (i_{z-1}, i_z)$, in which $i_1, i_2, \dots, i_z \in \mathcal{V}$ are different from each other. The directed distance from i_1 to i_z is indicated as $d_{i_1 \rightarrow i_z}$, which is the number of arcs in the shortest path from i_1 to i_z .

Definition 2 [19]: Let \mathcal{E}_1 and \mathcal{E}_2 be relations on a set \mathcal{V} . The composition of \mathcal{E}_1 and \mathcal{E}_2 is the relation consisting of order pairs (b, d) , where $b, d \in \mathcal{V}$, and for which there exists $c \in \mathcal{V}$ such that $(b, c) \in \mathcal{E}_1$ and $(c, d) \in \mathcal{E}_2$. The composition of \mathcal{E}_1 and \mathcal{E}_2 is represented by $\mathcal{E}_1 \circ \mathcal{E}_2$.

C. Barycentric Coordinate Representation

The barycentric coordinate describes the relative position of a node relative to other nodes. For four nodes i, j, k, l in the 2-dimension Euclidean space, the coordinates are expressed by

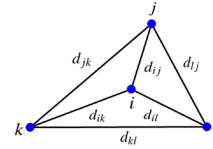


Fig. 1. An example of node i lying in the convex hull of nodes j, k, l .

p_i, p_j, p_k, p_l , respectively. The barycentric coordinates of point i relative to j, k, l are a_{ij}, a_{ik}, a_{il} , satisfying

$$p_i = a_{ij}p_j + a_{ik}p_k + a_{il}p_l, \quad (1)$$

where $a_{ij} + a_{ik} + a_{il} = 1$. In particular, the barycentric coordinates can be expressed as the ratio of regions between specified triangles. For instance, in Fig. 1, the barycentric coordinates are given by

$$a_{ij} = \frac{S_{\Delta ikl}}{S_{\Delta jkl}}, \quad a_{ik} = \frac{S_{\Delta ilj}}{S_{\Delta jkl}}, \quad a_{il} = \frac{S_{\Delta ljk}}{S_{\Delta jkl}},$$

where $S_{\Delta ikl}, S_{\Delta ilj}, S_{\Delta ljk}, S_{\Delta jkl}$ are the areas of the corresponding triangles $\Delta ikl, \Delta ilj, \Delta ljk, \Delta jkl$, which can be calculated with Euclidean distance measurements between nodes by *Cayley-Menger* determinant [20], i.e.,

$$S_{\Delta ikl}^2 = -\frac{1}{16} \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & d_{ik}^2 & d_{il}^2 \\ 1 & d_{ki}^2 & 0 & d_{kl}^2 \\ 1 & d_{li}^2 & d_{lk}^2 & 0 \end{bmatrix},$$

in which d_{ik}, d_{il}, d_{lk} are Euclidean distance measurements among nodes i, l, k .

III. PROBLEM FORMULATION

A. DILOC Algorithm

Consider a wireless sensor network with a node set $\Theta = \{1, 2, \dots, n\}$ in the 2-dimension Euclidean space. A node is called an anchor if its location is known, and a node is called a sensor if its location is unknown and to be determined. As shown in [4], at least three anchors that are not in a straight line are necessary to locate any sensor with unknown location in the 2-dimension Euclidean space. Therefore, without loss of generality, we let $\Xi = \{1, 2, 3\}$ and $\Omega = \{4, 5, \dots, n\}$ represent the set of anchors and the set of sensors, respectively. The set of the neighbors of node i in a given radius, μ_i , is

$$\Phi(i, \mu_i) = \{r \in \Theta : d_{ri} < \mu_i\},$$

which may include anchors as well as sensors. In the classical DILOC algorithm, the following three deployment assumptions are required.

- A1** The locations of all the sensors lie inside the convex hull of the anchors, i.e., $Co\{\Omega\} \subseteq Co\{\Xi\}$.
- A2** For every sensor $i \in \Omega$, there are some $\mu_i > 0$ such that a triangulation set, $\mathcal{N}_i \subseteq \Phi(i, \mu_i)$, satisfying $|\mathcal{N}_i| = 3$ exists, where $|\mathcal{N}_i|$ is the number of the elements in \mathcal{N}_i .
- A3** For any sensor $i \in \Omega$, there is a communication link between all nodes in the set $\{i\} \cup \mathcal{N}_i$.

Finding the triangulation set \mathcal{N}_i is an important step in the DILOC algorithm. Given the deployment density, sensor i can set an initial communication radius μ_i to determine its neighbor set $\Phi(i, \mu_i)$. Then, sensor i selects any three neighbors in $\Phi(i, \mu_i)$ and tests whether it is located in the convex hull of

these neighbors. If all tests fail, sensor i adaptively increases its communication radius in small increments. By repeating this process, the triangulation set will be finally determined.

Let $p_a = [p_1, p_2, p_3]^T$ and $p_s = [p_4, p_5, \dots, p_n]^T$ be the locations of anchors and sensors, respectively. According to the representation of the barycentric coordinates of each node relative to its neighbors, we get

$$\begin{bmatrix} p_a \\ p_s \end{bmatrix} = \begin{bmatrix} I_3 & \mathbf{0} \\ F & H \end{bmatrix} \begin{bmatrix} p_a \\ p_s \end{bmatrix}, \quad (2)$$

where there are three nonzero elements in each row of $[F \ H]$. These are the barycentric coordinates of the nodes relative to their neighbors. In addition, the matrix $[F \ H]$ is row-stochastic and the block matrix H is sub-stochastic. In particular, the row sums of matrix H satisfy: if the neighbor set \mathcal{N}_{i+3} of the sensor $i+3$ contains anchors, where $i = 1, 2, \dots, n-3$, then $\sum_{j=1}^{n-3} H_{ij} < 1$, and if there are no anchors in \mathcal{N}_{i+3} , then $\sum_{j=1}^{n-3} H_{ij} = 1$.

The iteration of the DILOC algorithm in [4] is written as

$$\tilde{p}_i(t+1) = \sum_{r \in \mathcal{N}_i} a_{ir} \tilde{p}_r(t), \quad i \in \Omega, \quad (3)$$

where $\tilde{p}_i(t)$ is the location estimation of sensor i at time t , and a_{ir} are the barycentric coordinates of sensor i relative to its three neighbors in \mathcal{N}_i . By the assumption **A3**, a_{ir} are known to sensor i . The iteration process (3) can also be computed in another form [9], which can be written as

$$\tilde{p}_i(t+1) = \tilde{p}_i(t) + \gamma \sum_{r \in \mathcal{N}_i} a_{ir} (\tilde{p}_r(t) - \tilde{p}_i(t)), \quad i \in \Omega, \quad (4)$$

where γ is a constant. Obviously, (4) is a more general form, which covers (3) as a special case of $\gamma = 1$. Define $\tilde{p}_s(t) = [\tilde{p}_4(t), \tilde{p}_5(t), \dots, \tilde{p}_n(t)]^T$. Eq. (4) can be expressed equivalently as the following compact form

$$\tilde{p}_s(t+1) = \gamma F p_a + Q \tilde{p}_s(t), \quad (5)$$

where $Q = (1 - \gamma)I_{n-3} + \gamma H$. It has been shown in [4]–[9] that the final location estimations of the sensors updating through (4) or (5) are expressed as

$$\lim_{t \rightarrow \infty} \tilde{p}_s(t) = [I_{n-3} - H]^{-1} F p_a, \quad (6)$$

which is also the exact locations of the sensors. $[I_{n-3} - H]^{-1} F$ is the matrix of the barycentric coordinates of the sensors in terms of the anchors.

Remark 1: For each sensor i , its three neighbors in \mathcal{N}_i may contain both anchors and other sensors. Sensor i can determine its barycentric coordinates relative to its three neighbors in \mathcal{N}_i by measuring the Euclidean distance, thereby estimating its own location. Because the locations of anchors are known, sensor i can localize itself in one single step if its three neighbors in \mathcal{N}_i are all anchors. And if \mathcal{N}_i contains location-unknown sensors, sensor i 's one-step location estimation is not its accurate location. The purpose of the DILOC algorithm is to determine the final location estimation of sensor i completely by the locations of anchors through distributed iteration, so that accurate localization is achieved.

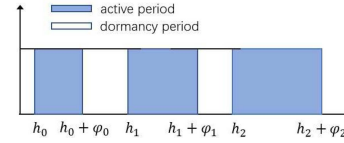


Fig. 2. An example of attack schedules.

B. DoS Attacks Model

DoS attacks refer to a kind of attacks in which an attacker controls some or all components of the system. DoS attacks can affect the timeliness of information exchange, resulting in a loss of data [17]. Without loss of generality, it is assumed that the attacker can attack the communication network in the changing active time period, which means the attacked communication channels can neither be used for sending nor receiving data. Next, the attacker needs to pause the attack activity and move to sleep time to save energy for the next attack.

Let $\{s_k\}_{k \in \mathbb{N}}$, where $s_0 \geq 0$, represents the time sequence of DoS attacks off/on conversion, i.e., the time instants when the attacker launches DoS attacks. Specifically, the attack instant s_k and its dwell time φ_k determine the k -th active period of DoS attacks, i.e., $S_k := [s_k, s_k + \varphi_k]$, in which the attacker attacks parts or all of the communication channels, and then the information transmitted by the attacked channels will be lost. If $\varphi_k = 0$, the k -th DoS takes the form of a single pulse at time s_k . Let

$$\mathbf{S} = \bigcup_{k \in \mathbb{N}} S_k, \quad \mathbf{M} = \mathbf{T} \setminus \mathbf{S} \quad (7)$$

represent a set of time instants where communication is denied and allowed, respectively, where $\mathbf{T} = \{t : t = 0, 1, 2, \dots\}$ is the set of all iteration time instants. To illustrate DoS attacks, a simple example is shown in Fig. 2.

C. Simulations by the DILOC Algorithm Under DoS Attacks

In the DILOC algorithm, each sensor always uses the received information from its neighbors to estimate the location. In other words, when a part of the communication links arriving at a certain sensor i are attacked, the sensor i estimates its location by using the information received from the remaining communication links. Define

$$\mathcal{N}_i^D(t) = \{j : j \in \mathcal{N}_i \text{ and } (j, i) \text{ is attacked at } t \in \mathbf{S}\}. \quad (8)$$

For any $i \in \Omega$, the iteration form of the DILOC algorithm under DoS attacks is written as

$$\tilde{p}_i(t+1) = \begin{cases} \tilde{p}_i(t) + \gamma \sum_{r \in \mathcal{N}_i \setminus \mathcal{N}_i^D(t)} a_{ir} (\tilde{p}_r(t) - \tilde{p}_i(t)), & t \in \mathbf{S}, \\ \tilde{p}_i(t) + \gamma \sum_{r \in \mathcal{N}_i} a_{ir} (\tilde{p}_r(t) - \tilde{p}_i(t)), & t \in \mathbf{M}. \end{cases} \quad (9)$$

It is worth noting that the DILOC algorithm may not accurately locate the sensors due to the diversity of attack strategies of DoS, which is illustrated by the following example.

Example 1: Consider a sensor network consisting of seven nodes, see Fig. 3, where the sets of anchors and sensors are $\Xi = \{1, 2, 3\}$ and $\Omega = \{4, 5, 6, 7\}$, respectively. The locations of anchors are $p_1 = (1, \sqrt{3})$, $p_2 = (0, 0)$, $p_3 = (2, 0)$. The triangulation sets are chosen as $\mathcal{N}_4 = \{2, 5, 7\}$, $\mathcal{N}_5 = \{3, 6, 7\}$,

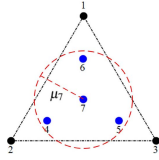


Fig. 3. A network consisting of seven nodes, where 1, 2, 3 and 4, 5, 6, 7 represent the anchors and the sensors, respectively.

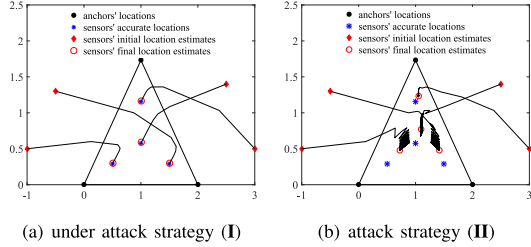


Fig. 4. Trajectories of the sensors' location estimations obtained by the DILOC algorithm under the DoS attack strategies (I) and (II).

$\mathcal{N}_6 = \{1, 4, 7\}$, $\mathcal{N}_7 = \{4, 5, 6\}$. We can see that there are no anchors in the sensor 7's triangulation set, and there is only one anchor in the triangulation sets of other sensors. Since no sensors communicate directly with all anchors, all sensors can not achieve accurate localization in one step. For each sensor $i \in \Omega$, its barycentric coordinates relative to its three neighbors in the triangulation set \mathcal{N}_i can be calculated by using Euclidean distance among the nodes in the set $\{i\} \cup \mathcal{N}_i$ in the Cayley-Menger determinant. For example, we can use the distances $d_{74} = d_{75} = d_{76} = \frac{\sqrt{3}}{3}$, $d_{45} = d_{46} = d_{56} = 1$ to compute $a_{74} = a_{75} = a_{76} = \frac{1}{3}$. Let the gain parameter be $\gamma = 1/2$ in Eq. (9). Suppose the attacker attacks at time instants $s_k = 3k$, $k \in \mathbb{N}$, and the dwell time is $\varphi_k = 1$, $k \in \mathbb{N}$. We below consider two DoS attack strategies:

- (I) The attacker attacks communication links (2, 4), (5, 4), (7, 4) at time instants $3k$, $k \in \mathbb{N}$ and communication links (4, 7), (5, 7), (6, 7) at time instants $3k + 1$, $k \in \mathbb{N}$.
- (II) The attacker attacks communication links (2, 4), (3, 5), (6, 7) at time instants $3k$, $k \in \mathbb{N}$ and communication links (1, 6), (4, 7), (5, 7) at time instants $3k + 1$, $k \in \mathbb{N}$.

It can be observed from Fig. 4 that the DILOC algorithm can precisely determine the locations of the sensors under attack strategy (I), but not under attack strategy (II).

Remark 2: As can be seen from Example 1, the DILOC algorithm cannot achieve accurate sensor localization under arbitrary attack strategy. In fact, the DILOC algorithm is only effective for one kind of attack strategy, that is, the attacker either attacks all three communication links to a node or does not attack any communication link to the node. If the attacker launches other attack strategies, the DILOC algorithm will fail. In addition, the effectiveness of DoS attacks is independent of the communication structure and initial location estimations.

D. AS-DILOC Algorithm

In this letter, we propose a consensus-based distributed iterative algorithm which can accurately locate sensors under any DoS attack strategy under the deployment assumptions **A1** – **A3**, where each node estimates its location by using an abandonment-strategy rule. The proposed algorithm is shown in Algorithm 1.

Algorithm 1 AS-DILOC Algorithm

- 1: Set the time sequence $\{s_k\}_{k \in \mathbb{N}}$ of DoS attacks off/on conversion, dwell time φ_k , $k \in \mathbb{N}$, and the initiate location estimates $\tilde{p}_i(0)$, $i = 1, 2, \dots, n$;
- 2: For each location-unknown sensor $i \in \Omega$, the following update strategy is designed.

- I) If sensor i can receive the neighbors' information from all three communication links arriving at itself, then the following location estimate rule is designed:

$$\tilde{p}_i(t+1) = (1-\gamma)\tilde{p}_i(t) + \gamma \sum_{r \in \mathcal{N}_i} a_{ir} \tilde{p}_r(t), \quad (10)$$

- II) If sensor i detects that the information on at least one communication link arriving at it is intercepted, then a strategy of abandoning update is adopted, i.e.,

$$\tilde{p}_i(t+1) = \tilde{p}_i(t). \quad (11)$$

- 3: Advance the time to $t+1$, then go to step 2.

Remark 3: In the DILOC algorithm (9), if some communication links arriving at node i are attacked by the attacker, namely, node i cannot receive the neighbor information on these communication links, then node i will use the neighbor information received from the remaining communication links to estimate its location. The difference between the AS-DILOC algorithm and the classic DILOC algorithm is reflected in the strategy of processing neighbor information when the sensor network is attacked. For example, in the AS-DILOC algorithm, even if only one communication link arriving at node i is attacked, node i adopts a strategy of abandoning update, i.e., $\tilde{p}_i(t+1) = \tilde{p}_i(t)$.

IV. CONVERGENCE ANALYSIS

The global convergence of the AS-DILOC algorithm is analyzed by using the sub-stochastic matrix and the composition of binary relations.

We first convert Eqs. (10) and (11) to a matrix-vector form:

$$\tilde{p}_s(t+1) = \gamma F(t) p_a + [I_{n-3} - \gamma(N(t) - H(t)g)] \tilde{p}_s(t), \quad (12)$$

where $N(t) = \text{diag} \{ \sum_r [F(t) H(t)]_{1r}, \dots, \sum_r [F(t) H(t)]_{n-3,r} \}$,

$$[F(t) H(t)](i, :) = \mathbf{0}, \quad \text{if } t \in \mathbf{S}, \mathcal{N}_i^D(t) \neq \emptyset,$$

$$[F(t) H(t)](i, :) = [F H](i, :), \quad \text{if } t \in \mathbf{M} \text{ or } t \in \mathbf{S}, \mathcal{N}_i^D(t) = \emptyset,$$

for $i = 1, 2, \dots, n-3$. Let $Q(t) = I_{n-3} - \gamma(N(t) - H(t)g)$, then the solution of iterative process (12) can be written as

$$\lim_{t \rightarrow \infty} \tilde{p}_s(t) = \prod_{t=0}^{\infty} Q(t) \tilde{p}_s(0) + \lim_{t \rightarrow \infty} \Gamma(t) p_a, \quad (13)$$

where $\Gamma(t) = \gamma F(t) + \gamma \sum_{j=1}^t \prod_{i=j}^t Q(i) F(j-1)$.

We observe from (5) that the final location estimations of the sensors are located in the convex hull of the anchors and linearly represented by the locations of the anchors. Therefore, the following equation should be proved first

$$\prod_{t=0}^{\infty} Q(t) = \mathbf{0}. \quad (14)$$

Furthermore, in order to ensure that the final location estimations of sensors are the same with the accurate locations, it is also necessary to prove that

$$\lim_{t \rightarrow \infty} \Gamma(t) = [I_{n-3} - H]^{-1}F. \quad (15)$$

Our next major task is to give detailed proofs of Eqs. (14) and (15), respectively. Before proceeding, we construct a digraph $\mathcal{G}[M(t)] = \{\mathcal{V}[M(t)], \mathcal{E}[M(t)]\}$, $t \in \mathbb{N}$, where

$$M(t) = \begin{bmatrix} 1 & \mathbf{0} \\ \gamma F(t)\mathbf{1} & Q(t) \end{bmatrix}$$

is the corresponding weighted adjacency matrix, $\mathcal{V}[M(t)] = \{0, 1, \dots, n-3\}$ is the node set in which the elements are the row indexes of matrix $M(t)$ except the first one which is labeled as 0, and $\mathcal{E}[M(t)]$ is the set of arcs.

We first present the result of directed edges composition to prove Eqs. (14) and (15).

Theorem 1: Consider the AS-DILOC algorithm. Under the deployment assumptions **A1** – **A3**, if the parameter γ is selected within the interval $(0, 1)$, then for any time intervals $[s_k, s_{k+P})$, $k \in \mathbb{N}$, where $P = \max\{d_{i \rightarrow j}; i \in \Xi, j \in \Omega\}$, we have

$$(0, i) \in \mathcal{E}[M(s_k)] \circ \dots \circ \mathcal{E}[M(s_{k+P} - 1)], \quad (16)$$

for $i = 1, 2, \dots, n-3$.

Proof: The communication links among the nodes are described by a digraph \mathcal{G} . It is known from [9] that there is a directed path from the anchor set to each location-unknown sensor in the digraph \mathcal{G} under the assumptions **A1** – **A3**. Assume that the directed path from the anchors set Ξ to each sensor $i_z + 3$ is described as $\mathcal{P}_{a \rightarrow i_z+3} = (a, i_1 + 3), (i_1 + 3, i_2 + 3), \dots, (i_{z-1} + 3, i_z + 3)$, where $a \in \Xi$ and $i_1 + 3, i_2 + 3, \dots, i_z + 3 \in \Omega$ with $i_1, i_2, \dots, i_z \in \{1, 2, \dots, n-3\}$.

We first consider the arc $(a, i_1 + 3)$ and the time interval $[s_k, s_{k+1})$. Since the communication channels reaching node $i_1 + 3$ may be attacked in the interval $[s_k, s_k + \varphi_k)$, so the arc $(a, i_1 + 3)$ may not belong to the digraph \mathcal{G} at time $t \in [s_k, s_k + \varphi_k)$. And since $[s_k + \varphi_k, s_{k+1})$ is the dormant period of nodes, node $i_1 + 3$ can get information about all its neighbors at any $t \in [s_k + \varphi_k, s_{k+1})$. According to the definition of $[F(t) H(t)]$, we can get $\sum_j [H(s_k + \varphi_k)]_{i_1 j} < 1$, equivalently, $\sum_j [Q(m\delta + T_d)]_{i_1 j} < 1$. This implies that $(0, i_1) \in \mathcal{E}[M(m\delta + T_d)]$. Furthermore, it can be observed that the row-stochastic matrix $M(t)$ has diagonal elements under the condition $0 < \gamma < 1$, namely, the digraph $\mathcal{G}[M(t)]$ has self-loops on all nodes $0, 1, \dots, n-3$. Consequently,

$$(0, i_1) \in \mathcal{E}[M(s_k)] \circ \dots \circ \mathcal{E}[M(s_{k+1} - 1)], \quad (17)$$

where $(0, 0) \in \mathcal{E}[M(s_k)], \dots, (0, 0) \in \mathcal{E}[M(s_k + \varphi_k - 1)], (0, i_1) \in \mathcal{E}[M(s_k + \varphi_k)], (i_1, i_1) \in \mathcal{E}[M(s_k + \varphi_k + 1)], \dots, (i_1, i_1) \in \mathcal{E}[M(s_{k+1} - 1)]$.

Consider the arc $(i_r + 3, i_{r+1} + 3)$ and the attack period $[s_{k+r}, s_{k+r+1})$, where $r = 1, 2, \dots, z-1$. Obviously, each node can get information about all its neighbors during the dormant period $[s_{k+r} + \varphi_{k+r}, s_{k+r+1})$. From the definition of $[F(t) H(t)]$, we have $[H(s_{k+r} + \varphi_{k+r})]_{i_r+3, i_r+3} > 0$, and further $[Q(s_{k+r} + \varphi_{k+r})]_{i_r+3, i_r+3} > 0$. This means that $(i_r, i_{r+1}) \in \mathcal{E}[M(s_{k+r} + \varphi_{k+r})]$. It thus follows that

$$(i_r, i_{r+1}) \in \mathcal{E}[M(s_{k+r})] \circ \dots \circ \mathcal{E}[M(s_{k+r+1} - 1)], \quad (18)$$

where $(i_r, i_r) \in \mathcal{E}[M(s_{k+r})], \dots, (i_r, i_r) \in \mathcal{E}[M(s_{k+r} + \varphi_{k+r} - 1)], (i_r, i_{r+1}) \in \mathcal{E}[M(s_{k+r} + \varphi_{k+r})], (i_{r+1}, i_{r+1}) \in \mathcal{E}[M(s_{k+r} + \varphi_{k+r} + 1)], \dots, (i_{r+1}, i_{r+1}) \in \mathcal{E}[M(s_{k+r+1} - 1)]$.

Combining (17) and (18), it can be obtained that

$$(0, i_z) \in \mathcal{E}[M(s_k)] \circ \dots \circ \mathcal{E}[M(s_{k+z} - 1)], \quad (19)$$

where z is the length of the path $\mathcal{P}_{a \rightarrow i_z+3}$ and satisfies $z \leq P$. In addition, the fact that the nodes have self-loops in the digraph $\mathcal{G}[M(t)]$, $t \in \mathbb{N}$ guarantees that

$$(i_z, i_z) \in \mathcal{E}[M(s_{k+z})] \circ \dots \circ \mathcal{E}[M(s_{k+P} - 1)]. \quad (20)$$

By (17) and (20), we have

$$(0, i_z) \in \mathcal{E}[M(s_k)] \circ \dots \circ \mathcal{E}[M(s_{k+P} - 1)]. \quad (21)$$

Equivalently, we have $(0, i) \in \mathcal{E}[M(s_k)] \circ \dots \circ \mathcal{E}[M(s_{k+P} - 1)]$ for any $i = 1, 2, \dots, n-3$. ■

Based on the conclusion of Theorem 1, we analyze Eq. (14) and Eq. (15) in detail in Theorem 2.

Theorem 2: Under the deployment assumptions **A1** – **A3**, if the parameter γ is selected within the interval $(0, 1)$, then Eq. (14) and Eq. (15) can be derived, that is, the AS-DILOC algorithm can converge to the exact sensor locations under DoS attacks.

Proof: For any time interval $[s_{mP}, s_{(m+1)P})$, where $m \in \mathbb{N}$, we know from Theorem 1 that $(0, i) \in \mathcal{E}[M(s_{mP})] \circ \dots \circ \mathcal{E}[M(s_{(m+1)P} - 1)]$, $i = 1, 2, \dots, n-3$. Let δ_m denote the number of time instants in the interval $[s_{mP}, s_{(m+1)P})$. According to Definition 2, there are a series of nodes $i_1, i_2, \dots, i_{\delta} \in \{1, 2, \dots, n-3\}$ such that $(0, i_1) \in \mathcal{E}[M(s_{mP})], (i_1, i_2) \in \mathcal{E}[M(s_{mP} + 1)], \dots, (i_{\delta_m-1}, i_{\delta_m}) \in \mathcal{E}[M(s_{(m+1)P} - 1)]$, where $i_{\delta_m} = i$ and there may be duplicate elements in the nodes set $\{i_1, i_2, \dots, i_{\delta_m}\}$.

Below we analyze the matrices product $\prod_{t=s_{mP}}^{s_{(m+1)P}-1} Q(t)$ associated with the interval $[s_{mP}, s_{(m+1)P})$. Define

$$\sigma = \min \left\{ \gamma a_{ir}, 1 - \gamma \sum_{r \in \mathcal{N}_i} a_{ir} : i, r = 1, 2, \dots, n \right\}, \quad (22)$$

then all elements of $M(t)$ are greater than or equal to σ . By $(0, i_1) \in \mathcal{E}[M(s_{mP})]$, we have $[\gamma F\mathbf{1}]_{i_1} \geq \sigma$, it follows that

$$\sum_{j=1}^{n-3} [Q(s_{mP})]_{i_1 j} = 1 - [\gamma F\mathbf{1}]_{i_1} \leq 1 - \sigma < 1. \quad (23)$$

For any $q = 1, 2, \dots, \delta_m - 1$, since $(i_q, i_{q+1}) \in \mathcal{E}[M(s_{mP} + q)]$, we get $[Q(s_{mP} + q)]_{i_q+1, i_q} \geq \sigma$. It thus follows that

$$\begin{aligned} & \left[\prod_{t=s_{mP}+1}^{s_{(m+1)P}-1} Q(t) \right]_{i_{\delta_m} i_1} \\ & \geq [Q(s_{(m+1)P} - 1)]_{i_{\delta_m} i_{\delta_m-1}} \cdots [Q(s_{mP} + 1)]_{i_2 i_1} \geq \sigma^{\delta_m-1}. \end{aligned} \quad (24)$$

Combining with (23) and (24), we can further deduce that

$$\begin{aligned} & \sum_{j=1}^{n-3} \left[\prod_{t=s_{mP}}^{s_{(m+1)P}-1} Q(t) \right]_{i_{\delta_m} j} \\ & = \sum_{\substack{j_1=1 \\ j_1 \neq i_1}}^{n-3} \left[\prod_{t=s_{mP}+1}^{s_{(m+1)P}-1} Q(t) \right]_{i_{\delta_m} j_1} \sum_{j=1}^{n-3} [Q(s_{mP})]_{j_1 j} \end{aligned}$$

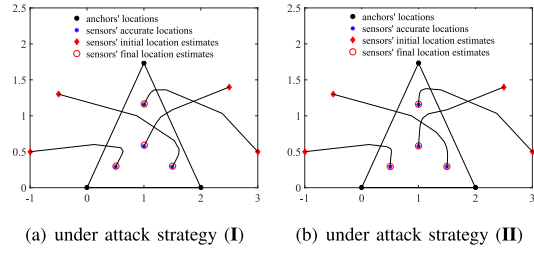


Fig. 5. Trajectories of the sensors' location estimates obtained by the AS-DILOC algorithm under the DoS attack strategies (I) and (II) in Example 1.

$$\begin{aligned}
 & + \left[\prod_{t=s_m P+1}^{s_{(m+1)P}-1} Q(t) \right]_{i_{s_m} i_1} \sum_{j=1}^{n-3} [Q(s_m P)]_{i_1 j} \\
 & \leq (1 - \sigma^{\delta_m - 1}) + \sigma^{\delta_m - 1} (1 - \sigma) = 1 - \sigma^{\delta_m} < 1. \quad (25)
 \end{aligned}$$

Equivalently, we have

$$\left\| \prod_{t=s_m P}^{s_{(m+1)P}-1} Q(t) \right\|_{\infty} \leq 1 - \sigma^{\delta_m} \leq 1 - \sigma^{\hat{\delta}} < 1 \quad (26)$$

for any $m \in \mathbb{N}$, where $\hat{\delta} = \max\{\delta_m : m \in \mathbb{N}\}$. Consequently,

$$\begin{aligned}
 \left\| \prod_{t=0}^{\infty} Q(t) \right\|_{\infty} & \leq \prod_{m=0}^{\infty} \left\| \prod_{t=s_m P}^{s_{(m+1)P}-1} Q(t) \right\|_{\infty} \left\| \prod_{t=0}^{s_0-1} Q(t) \right\|_{\infty} \\
 & \leq \lim_{m \rightarrow \infty} (1 - \sigma^{\hat{\delta}})^m = 0. \quad (27)
 \end{aligned}$$

This guarantees the establishment of Eq. (14).

In the DILOC algorithm, it has been proved that the matrix H is invertible if there is a directed path from the anchors set to each location-unknown sensor, thus $(I_{n-3} - H)^{-1}$ exists. According to the definitions $F(t)$ and $Q(t)$, we deduce that

$$(I_{n-3} - Q(t))(I_{n-3} - H)^{-1}F = \gamma F(t). \quad (28)$$

By substituting (28) into $\Gamma(t)$, we obtain that

$$\begin{aligned}
 \lim_{t \rightarrow \infty} \Gamma(t) & = \lim_{t \rightarrow \infty} \left(\sum_{i=0}^t Q(t) \cdots Q(i+1)(I_{n-3} - Q(i)) \right) (I_{n-3} - H)^{-1}F \\
 & = \lim_{t \rightarrow \infty} (I_{n-3} - Q(t)Q(t-1) \cdots Q(0))(I_{n-3} - H)^{-1}F \\
 & = (I_{n-3} - H)^{-1}F. \quad (29)
 \end{aligned}$$

This also means that (15) is established. ■

Example 2: Consider a sensor network consisting of the anchor set $\Xi = \{1, 2, 3\}$ and the sensor set $\Omega = \{4, 5, 6, 7\}$ in the 2-dimensional Euclidean space. The triangulation sets and location coordinates of the sensors are set the same as Example 1. Let the gain parameter be $\gamma = 1/2$ in Eq. (10). It can be observed from Fig. 5 that the AS-DILOC algorithm can precisely determine the locations of the sensors whether under attack strategies (I) or (II) considered in Example 1.

Remark 4: The main contribution of this letter is to propose an AS-DILOC algorithm based on barycentric coordinates measurement in the situation of DoS attacks. We show through Example 1 that the DILOC algorithm may fail when the attacker changes the attack strategy. We prove that the AS-DILOC algorithm proposed in this letter can achieve accurate sensor localizations under arbitrary attack strategy, which is illustrated by Example 2.

V. CONCLUSION

The problem of determining the sensors' locations in the presence of DoS attacks has been studied in this letter. The AS-DILOC algorithm has been proposed based on the barycentric coordinates which only involve relative distance measurement. The global convergence of the AS-DILOC algorithm has been analyzed by using the sub-stochastic matrix and the composition of binary relations. Moreover, the effectiveness of the AS-DILOC algorithm under DoS attacks has been verified by a simulation example.

ACKNOWLEDGMENT

The authors gratefully acknowledge the suggestions and comments by the Associate Editor and anonymous.

REFERENCES

- [1] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from connectivity in sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, no. 3, pp. 961–974, Nov. 2004.
- [2] A. Pal, "Localization algorithms in wireless sensor networks: Current approaches and future challenges," *Netw. Protocols Algorithms*, vol. 2, no. 1, pp. 45–73, 2010.
- [3] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *Comput. Netw.*, vol. 51, no. 10, pp. 2529–2553, Jul. 2007.
- [4] 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.
- [5] U. A. Khan, S. Kar, and J. M. F. Moura, "DILAND: An algorithm for distributed sensor localization with noisy distance measurements," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1940–1947, Mar. 2010.
- [6] M. Deghat, I. Shames, B. D. O. Anderson, and J. M. F. Moura, "Distributed localization via barycentric coordinates: Finite-time convergence," *IFAC Proc. Vol.*, vol. 44, no. 1, pp. 7824–7829, Jan. 2011.
- [7] S. Zhu and Z. Ding, "Distributed cooperative localization of wireless sensor networks with convex hull constraint," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2150–2161, Jul. 2011.
- [8] Z. Lin, T. Han, R. Zheng, and C. Yu, "Distributed localization with mixed measurements under switching topologies," *Automatica*, vol. 76, pp. 251–257, Feb. 2017.
- [9] X. Z. Huang and Y. P. Tian, "Asynchronous distributed localization in networks with communication delays and packet losses," *Automatica*, vol. 96, pp. 134–140, Oct. 2018.
- [10] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 988–1001, Jun. 2003.
- [11] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.
- [12] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
- [13] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
- [14] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jan. 2014.
- [15] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15.4 communication," in *Proc. Int. Conf. Comput. Commun. Netw.*, Maui, HI, USA, 2011, pp. 1–6.
- [16] J. Xiong and J. Lam, "Stabilization of linear systems over networks with bounded packet loss," *Automatica*, vol. 43, no. 1, pp. 80–87, Jan. 2007.
- [17] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.
- [18] R. Rockafellar, *Convex Analysis*. Princeton, NJ, USA: Princeton Univ. Press, 1972.
- [19] K. Rosen, *Discrete Mathematics and Its Applications*, 7th Ed. New York, NY, USA: McGraw-Hill Company, 2012.
- [20] M. Sippl and H. Scheraga, "Cayley-menger coordinates," *Proc. Nat. Acad. Sci.*, vol. 83, no. 8, pp. 2283–2287, Apr. 1986.