Xue et al. EURASIP Journal on Wireless Communications and Networking (2020) 2020:39
https://doi.org/10.1186/s13638-020-1658-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A type of energy-efficient secure localization algorithm FM based in dynamic sensor networks

Wei-cheng Xue[1,2,3], Bao Peng[4*], Shan-he Wang[1,3] and Yu Hua[1]

Abstract

Since dynamic wireless sensor networks are widely used in the military field, the location information is the basis of various applications, because each node in the dynamic sensor network is moving continuously, and it is quite possible to be attacked by various forms of information. Aiming at the problem of secure localization in dynamic sensor networks, a new secure localization algorithm—frequency modulation secure localization (FMSL)—for dynamic sensor networks is proposed with the support of FM signal and Monte Carlo method. The algorithm uses FM signals which are widely covered to locate randomly distributed nodes loaded with FM signal receiving module, filters some malicious attack anchors in the network, and uses the improved Monte Carlo algorithm to locate the nodes, so as to improve the positioning accuracy. Meanwhile, according to the moving path and the localization time, energy consumption of the network could be estimated and also give the sleep scheduling strategy for the node to be localized. The simulation results show that the FMSL algorithm can significantly improve the security performance and positioning accuracy of mobile sensor networks compared with the existing security positioning algorithms such as Monte Carlo and convex programming. In the process of motion, the positioning accuracy can reach less than 10%.

Keywords: Wireless sensor networks, Mobility, Secure localization, FM, Safety check

1 Introduction

The security, energy efficiency, and positioning accuracy of a positioning system are considered as the three main indicators for evaluating the positioning design of sensor networks [1–3]. The limited energy of the sensor network increases the difficulty of its positioning. Frequent communication and information interaction and complex positioning calculations will have a serious impact on the energy consumption of the nodes. In addition, the addition of various additional devices (such as FM) on the node will also increase the energy cost of the node invisibly [4]. Therefore, how to design and implement a lightweight positioning algorithm becomes the development trend of wireless sensor network positioning technology [5–7].

Security, as a key index of a positioning system, has received wide attention only in the past 5 years. Relevant research results are few, and these methods have their own trade-offs in hardware cost, algorithm complexity and communication, computing overhead, and node deployment requirements [8–12]. In order to effectively solve the security problem of node self-localization system, L. Hu and Devin introduced a localization scheme-based Monte Carlo method for mobile wireless sensor network (MWSN). Simulation results show that the Monte Carlo localization (MCL) algorithm gives lower estimation error than both the centroid and the amorphous localization algorithms. Monte Carlo method-based MCL scheme is also developed in [2, 3]. Based on FM signal and Monte Carlo algorithm, this paper proposes a secure localization algorithm, which has low complexity, low communication, and computational overhead and does not require any hardware environment to be deployed in advance. It is called FMSL (mobile sensor network security localization) algorithm based on FM and Monte Carlo.

* Correspondence: pengb@sziit.edu.cn
[4]Shenzhen Institute of Information Technology, Shenzhen 518172, China
Full list of author information is available at the end of the article

2 System model and analysis

In this section, the algorithm principle and the assumptions are described first, and then the FMSL algorithm is presented (Fig. 1).

2.1 Methods

The mobile location problem can be described as follows: let t denote the discrete time, s_t is the location distribution of nodes at time t and is an implicit state variable, and o^t denotes the observation information received from seed nodes at time $t-1$ to t and is an observation state variable. The transfer equation $p(s_t \mid s_t - 1)$ describes the location distribution of t time based on the location distribution of a node $t-1$. The observation equation $p(s_t \mid o^t)$ describes the probability of the node location at s_t at t time, given the observation o^t. In the formula, s_t^i is a possible state of a node in mobile sensor network at t time, $w^i{}_t$ is a weight parameter, which indicates the probability that the state of a node in mobile sensor network at t time is s_t^i, that is [7]:

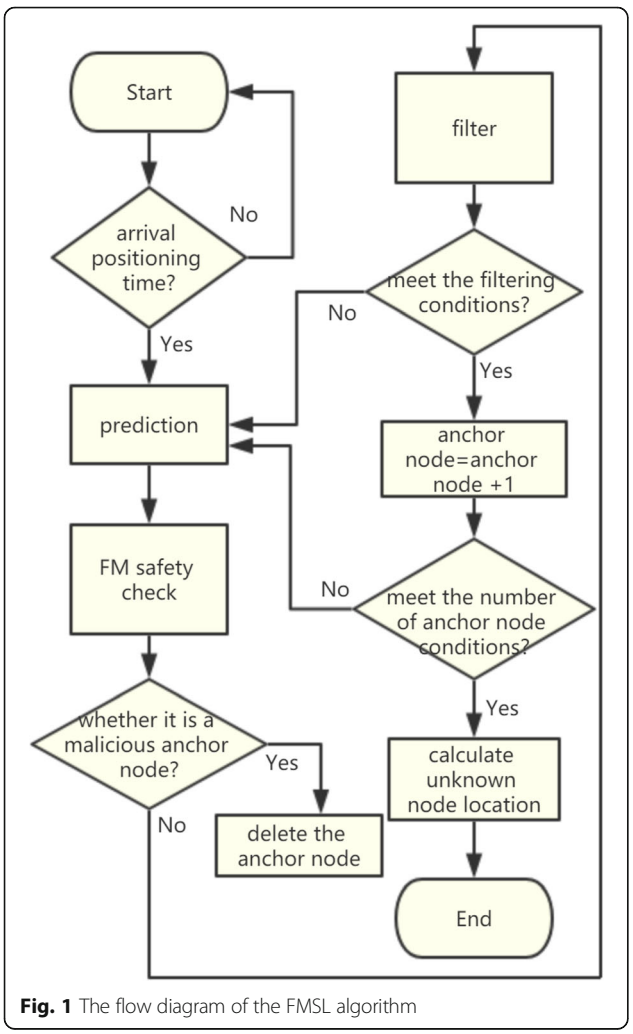

Fig. 1 The flow diagram of the FMSL algorithm

$$p\left(s_t^i \mid o^t\right) \approx w_t^i \quad \sum_{i=1}^{N} w^i{}_t = 1 \quad \} \tag{1}$$

$$p(|LH_s| = K) = \frac{\left(\rho_L \pi R^2\right)^k}{k!} e^{-\rho_L \pi R^2} \tag{2}$$

$$p(l_t|l_{t-1}) = \begin{cases} \frac{1}{\pi(\Delta t \times v)^2} & if \ \ d(l_t, l_{t-1}) \le \Delta t \times v \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

Here, the localization estimation of a particular sensor node at time t is denoted by l_t, Δt is the time interval, and $v_{\max}$ is the supreme motion speed that an anchor or a sensor node can travel between localization steps and assume o_t denoting this localization observation.

The description of a mobile sensor network security positioning problem is as follows: let $\{(x_i, y_i), \mathrm{RSSI}_i, m_i\}$ denote the real position coordinates of node i, signal reception intensity value, and information string data sent to other nodes. In mobile sensor networks, after node i is attacked and its information is altered in series, it is put back into the network to affect the location calculation of other nodes. The position coordinates, signal reception intensity, and information string data sent to other nodes after the attack are made into triples $\{(\tilde{x}_i, \tilde{y}_i), \tilde{\mathrm{RSSI}}_i, \tilde{m}_i\}$. Then:

$$d_i = \sqrt{(x_i - \tilde{x}_i) + (y_i - \tilde{y}_i)} \ge \lambda \tag{4}$$

$$RSSI_i \ne \tilde{RSSI}_i \ or \ m_i \ne \tilde{m}_i \tag{5}$$

Among them, λ is the maximum set distance error. According to the number of attack nodes and cooperation mode, common attack modes can be divided into three types:

- Attack by a single malicious node (the direction of attack is to find the direction from the node to the malicious node)
- Non-collusion attack of three malicious nodes (the attack direction is from the sphere node to each malicious node)
- Three malicious nodes collusion attack (first, calculate the coordinates of three malicious nodes and then coordinate and coordinate the three-node collusion attack)

2.2 FM safety check

When locating unknown nodes, each unknown node needs to refer to the location information of multiple anchor nodes and the distance information between these anchor nodes and unknown nodes. But when the network is attacked, the adversary may capture some of

these anchor and propose incorrect data as reference information. For this reason, when calculating the location of unknown nodes, it is necessary to consider the reliability of the information provided by the anchor nodes. In this paper, FM signal location technology is introduced to achieve the regional location of anchor nodes. The credibility weight of each anchor node is established, and this process is called FM security verification [13, 14].

2.2.1 Establishment of fingerprint database

Firstly, in the network deployment area, the fingerprint database is established by using FM signal acquisition equipment. Expressed as follows:

$$U = \left\{ \left(u_{ji}, p_i \right) | j = 1, \cdots, N, i = 1, \cdots, k \right\} \tag{6}$$

In the formula, j is the frequency used, i is the number of reference points, u_{ji} is the fingerprint data of the reference point of the jth frequency at the ith position, $p_i = (x_i, y_i)$ is the reference point position of the ith position, N is the total number of frequencies used, k is the total number of location reference points, and U is the FM fingerprint database. Anchor nodes loaded with FM signal receivers are calculated by measured FM signal data and fingerprint database data, then:

$$\Delta E = \left\{ \left(\sum_{j=1}^{N} \left(u_{jc} - u_{ji} \right)^2 \right)^{1/2} | i = 1, \cdots, k \right\} \tag{7}$$

In the formula, ΔE is a set of Euclidean distances between anchor nodes loaded with FM signal receivers and position reference points. ΔE_i is arranged in ascending order according to the Euclidean distance, and h pieces of ΔE_i are selected from small to large to calculate the location information of anchor nodes loaded with FM signal receivers.

2.2.2 Trustworthiness weight of anchor node

Let the location information of anchor node O loaded with FM signal receiver be (x_O, y_O) calculated by fingerprint database, and the position reference information sent by anchor node O to the node to be located be $(x_O^{'}, y_O^{'})$; then, the mean square deviation of anchor node O is:

$$\begin{aligned} \Delta E = & \left\{ \left(\sum_{j=1}^{N} \left(u_{jc} - u_{ji} \right)^2 \right)^{1/2} | i = 1, \cdots, k \right\} \\ s.t. \quad & \sigma_o \le \lambda \end{aligned} \tag{8}$$

In the formula, (x_{oq}, y_{oq}) represents the location information of the qth reference point in ΔE_i in anchor node O. λ is the maximum error of FM signal location calculation in a network. If $\sigma_o \ge \lambda$, anchor node O is included in the high-risk list. The location data of the node is not used as a reference in location calculation.

Definition 1 The σ of all anchor nodes in the network is arranged in ascending order. If the O of anchor node is in l position in the array, the corresponding weight of the credibility of anchor nodes is:

$$\omega_o = 1 - \frac{(l-1)}{M} \tag{9}$$

Among them, M is the number of network anchor nodes, and ω_o is the credibility weight of anchor node O.

3 Algorithm design

Based on the FM security verification mechanism, the traditional Monte Carlo algorithm was optimized, and a new algorithm, FM MCL security positioning algorithm, for mobile sensor network security positioning was proposed which greatly reduced the complexity of location generation. The algorithm is divided into the following three steps [15–17]:

1. Position prediction: According to the filtered estimated position, the next possible position is predicted, and around N position estimates combined with the motion model, N prediction points are generated in a circular area with the position estimate at this step as the center, and v is the radius of the circular area.

Definition 2: Sample number (N): the estimated number of unknown nodes to estimate their own position and the next position prediction.

2. Receiving observation information: Since it is a location algorithm based on ranging, the unknown node can directly measure the distance r from anchor node to itself within its ranging radius d, and save this distance.
3. Position filtering and position generation: According to the above observation information, the $\sigma_o \ge \lambda$, $o = 1, 2, \cdots, M$ and the anchor nodes of impossible position estimation are deleted from the estimation matrix. After deletion, the number of deleted anchor nodes and predicted points is complemented according to the observation information. Assuming r is the measured distance and e is the ranging error, the deletion and prediction strategies are as follows:
   (a) If there is only one anchor node in the self-ranging radius d, the prediction point not on the circle with the anchor node as the center of the circle, r as the radius, and e as the ranging error, and the next position estimation will be

deleted in the prediction. The coordinates of the estimated points of the step are randomly generated in the circle, and the coordinates of the next step are predicted according to the motion model.

(b) If there are two anchor nodes in the self-ranging radius d, draw a circle with $\omega_o r_o$, $o = 1, 2, \ldots, M$ as the radius. According to the intersection relation of the two circles, two possible positions of the unknown node can be obtained. In the position prediction, the prediction point and the next step position estimation outside the small circle with these two positions as the center of the circle and ranging error as the radius are deleted, and the position estimation point coordinates are generated within the two small circles, and the next step coordinates are predicted according to the motion model.

(c) If there are more than two anchor nodes in the radius d of the self-ranging, the position of the unknown node can be determined by drawing a circle with $\omega_o r_o$, $o = 1, 2, \ldots, M$ as the radius. Then, the prediction points and the next position estimation outside the small circle with the center of the circle and the radius of the ranging error are deleted, and the coordinates of the position estimation points are generated in the small circle, and the next coordinates are predicted according to the motion model.

(d) If there is no message, the location estimate and location prediction are not deleted.

4 Simulation results and discussions

In this section, the localization algorithms are implemented by MATLAB. For our performance evaluation, the sensor nodes are initially randomly distributed over a square area of 100 m × 100 m. The sample number N = 30, i.e., the sum of the numbers, which are the self-location estimations and the next location predictions obtained by the unknown node is 30. The ranging error e, such as e = 10%, means that the ranging error is 10% of the measured distance. If the measured distance is d, the actual distance is between $(1 - e)d$ and $(1 + e)d$ [18–20].

The transmission range r of both the sensor nodes and seeds is assumed to be a circle with a radius of 25 m. Then, the following equation can be drawn:

$$n_d = \frac{\pi r^2 n_m}{\text{TotalArea}} \tag{10}$$

$$s_d = \frac{\pi r^2 s_m}{\text{TotalArea}} \tag{11}$$

where n_m denotes all of the unknown nodes in the whole deployment, s_m denotes all the anchors in the whole deployment, and A is the square area of the deployment.

The percent of the rate between the communication radium and the distance between the estimating coordinate (x_e, y_e) of the nodes determined by the localization error δ_e, and the actual coordinate (x_r, y_r) is shown as the follows:

$$\delta_e = \frac{\sqrt{(x_e - x_r)^2 + (y_e - y_r)^2}}{r} \times 100\% \tag{12}$$

4.1 FMSL algorithm complexity and accuracy

The FMSL algorithm is based on the traditional dynamic sensor network localization algorithm and introduces the FM safety check, result its algorithm time complexity to increase the safety check process, but uses a linear mathematical operation relationship. Therefore, the added time and space complexity is low. When $n_d = 10$, $v = d = 25$, $N = 10$, $s_d = 4$, $e = 0$, in the absence of malicious attacks, compared with the MCL and convex methods, the FMSL algorithm shows that its accuracy and efficiency are significantly improved.

Figure 2 shows that in the absence of malicious attacks, the performance of the FMSL algorithm is significantly better than the MCL and convex programming algorithms. If there is a malicious attack in the system because there is no safety check for MCL and convex, the malicious attack information cannot be identified, and the ranging error caused by the malicious attack will be introduced for positioning calculation, which makes the entire algorithm unable to achieve effective localization. The FMSL algorithm introduces the FM safety check. When the ranging error introduced by a malicious attack is less than 1.5r, the effect is similar to

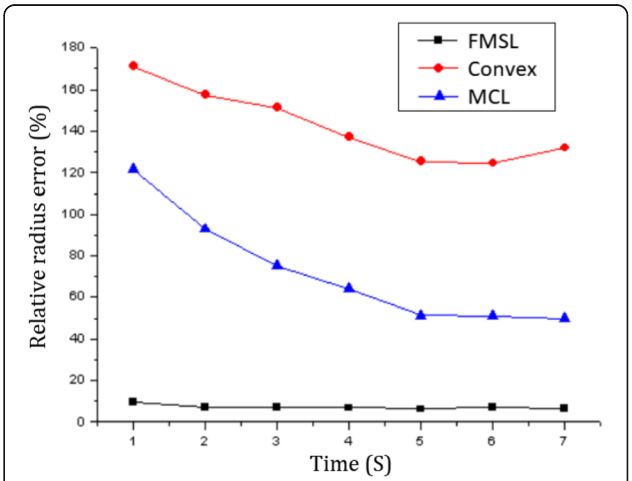

Fig. 2 Accuracy comparison

the ranging error. Its affect is shown in Fig. 3. When the ranging error introduced by the malicious attack is greater than 1.5r, almost all malicious attacks can be identified and deleted, lead to changes for the anchor density, which will affect the performance of the algorithm. Its affect is shown in Fig. 4.

4.2 Localization error vs. ranging error

When $s_d = 4$, $n_d = 10$, $v = d = 25$, $N = 10$, the ranging error is set to $e = 0$, $e = 5\%$ and $e = 15\%$, respectively. The analysis results are shown in Figs. 3 and 4.

The analysis shows that the ranging error is also an important parameter affecting the positioning accuracy. When the ranging error is increased, the accuracy is obviously reduced. It is obvious that there is an error in the ranging. Then, the calculation of the estimated position of the node will be followed by an error. The overlap of the error leads to the error of the result. Therefore, the selection of the high-precision ranging module is also a useful method to improve the positioning accuracy.

4.3 Localization error vs. anchors density

When $n_d = 10$, $v = d = 25$, $N = 10$, $e = 0$, the anchor node density is $s_d = 1$, $s_d = 2$, $s_d = 4$ and $s_d = 8$, respectively. The analysis results are shown in Fig. 4.

The analysis shows that when the anchor node density is low, such as $s_d = 1$, the positioning accuracy is poor, and the result is not much better than the traditional non-ranging sequence Monte Carlo algorithm. However, when the anchor node density increases, the positioning accuracy increases obviously. When the other conditions are unchanged, $s_d = 4$, the positioning accuracy of 13.13% is much better than about 40% of the traditional sequence Monte Carlo method, so this positioning algorithm has strong practicability.

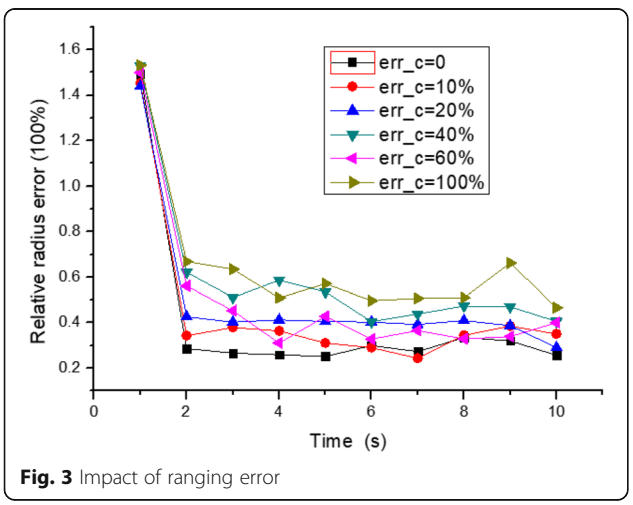

Fig. 3 Impact of ranging error

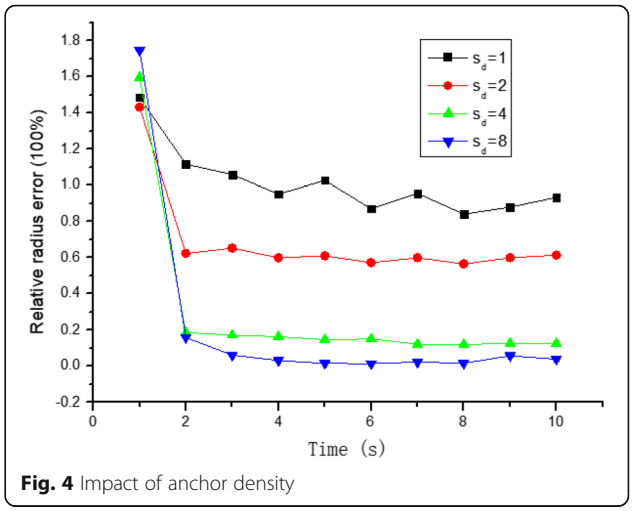

Fig. 4 Impact of anchor density

4.4 Localization error vs. security performance

When the malicious anchor node accounts for 10% of all anchor nodes, the number of unknown nodes in the region n_m = 150, the ranging error caused by malicious nodes is $\overrightarrow{e}$, then the effects of $\overrightarrow{e}$ on algorithm performance is shown in Fig. 5a; malicious anchor node accounts for 10% of all anchor nodes, $\overrightarrow{e}/r$=10%, then, the effects of n_m on algorithm performance are shown in Fig. 5b.

The analysis shows that malicious modification of anchor node location information and node density in the region are also important parameters that affect positioning accuracy. When the distance error value of malicious anchor node is increased, the accuracy decreases but not greatly, mainly because the FM security check effectively inhibits the positioning effect caused by this attack. When the number of nodes in the region exceeds 150, the positioning performance of the whole algorithm gradually stabilizes, and the positioning accuracy also improves slightly.

4.5 Analysis of energy-efficient localization

In the case of a certain network size, the proportion of sleepy nodes remains basically stable, and most of the nodes to be located in the network are dormant. Due to the existence of node state switching energy consumption, not every node to be located can save energy when sleeping, and the energy consumption is calculated as follows [20–22]:

$$\Delta T(S_i) \times P_s + 2 \times E_s < \Delta T(S_i) \times P_l \tag{13}$$

wherein P_s and P_l respectively are the power consumption of the node to be located in the dormant and listening state. E_s is the energy consumption cost of the node switching between the two states. $\Delta T(S_i)$ is the time

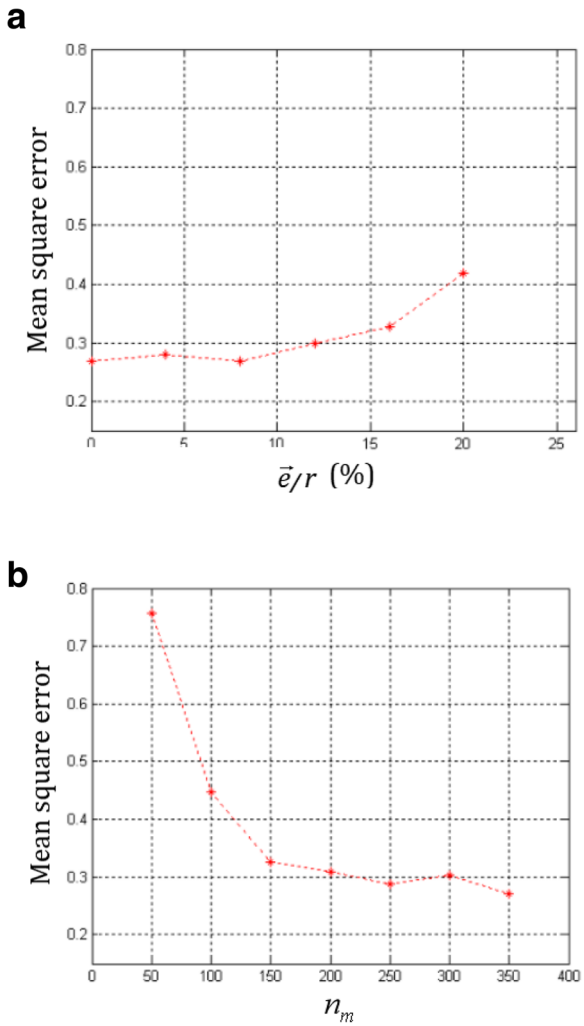

Fig. 5 Analysis of security performance. **a** Impact of ranging errors caused by malicious attacks. **b** Impact of the total number of nodes

interval for receiving the anchor node information twice for the node to be located. If and only if Eq. 13 is established, the node to be located is in a dormant state during the two information reception time intervals, which will be more energy efficient. At this time, the energy saved by the node to be located is [16, 17]:

$$\Delta E = \Delta T(S_i) \times (P_l - P_s) + 2 \times E_s \tag{14}$$

It can be known in Eqs. 13 and 14 that the value of the node to be located is largely dependent on the $\Delta T(S_i)$ value, and from the above analysis, the $\Delta T(S_i)$ value of the network scale and the movement path will remain unchanged. Therefore, the number of sleepy nodes is basically stable, and by controlling the anchor nodes with more energy consumption to sleep longer, the population is optimal. The total energy consumption of the anchor nodes is normalized to 1. The longest sleep time of the anchor nodes is also 1, and the sleep optimized by the equilibrium theory is used. The time allocation rules are shown in Fig. 6.

The analysis shows that more sleeping time is allocated for the anchors that consume more power in the positioning process. This can make the amount of energy consumption of the nodes in the network more equal, so that the network lifetime is prolonged.

5 Conclusions

In this paper, we propose a novel approach for secure localization in dynamic sensor networks. The optimized MCL method is used to calculate the location of unknown nodes in dynamic sensor networks. Then, the safety check mechanism is applied to the location process to enhance the algorithm's ability to resist malicious attacks. The proposed model has been evaluated in MATLAB simulation environment, and the experimental results demonstrate that our model achieves state-of-the-art performance. In future work, we will conduct a comprehensive analysis of multi-dimensional signals and characteristics for the surrounding environment to support the model for low-cost secure localization, through which we would like to see a more effective secure localization method.

Abbreviations

FM: Frequency modulation; FMSL: Frequency modulation secure localization; MATLAB: Matrix laboratory; MCL: Monte Carlo localization

Acknowledgements

The authors acknowledged the anonymous reviewers and editors for their efforts and valuable comments and suggestions.

Authors' contributions

WX and PB proposed the innovation ideas. The other authors also have contributed jointly to the manuscript. All authors read and approved the final manuscript.

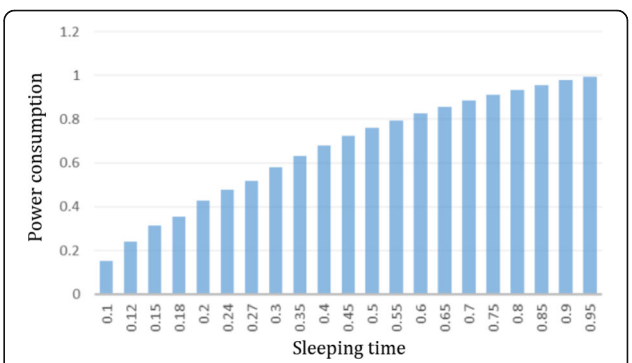

Fig. 6 The allocation rule of sleeping time

Funding
This work was supported in part by Guangdong Province Higher Vocational Colleges & Schools Pearl River Scholar Funded Scheme (2016) and project of Shenzhen Science and Technology Innovation Committee (JCYJ20170817114522834).

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]National Time Service Center, the Chinese Academy of Sciences, Xi' an 710600, China. [2]Jiangsu Broadcasting corporation, Nanjing 210008, Jiangsu, China. [3]University of Chinese Academy of Sciences, Beijing 100049, China. [4]Shenzhen Institute of Information Technology, Shenzhen 518172, China.

Received: 25 October 2019 Accepted: 26 January 2020
Published online: 11 February 2020

References

1. L. Chelouah, F. Semchedine, L. Bouallouche-Medjkoune, Localization protocols for mobile wireless sensor networks: a survey. COMPUTERS & ELECTRICAL ENGINEERING 77, 733–751 (2018). https://doi.org/10.1016/j.compeleceng.2017.03.024
2. E.S. Navarro, V. Vivekanandan,V.W.S. Wong. Dual and mixture Monte Carlo localization algorithms for mobile wireless sensor networks. in: Proc. of the IEEE Wireless Communications and Networking Conference (WCNC2007), Kowloon, China, 4027-4031(2007).
3. Abu Znaid, Ammar MA, Idris, Mohd Yamani Idna, Wahab, Ainuddin Wahid Abdul, Qabajeh, Liana Khamis, Mahdi, Omar Adil. Sequential Monte Carlo localization methods in mobile wireless sensor networks: a review. Journal of sensors. 2017. doi:https://doi.org/10.1155/2017/1430145.
4. L. Xin, J. Min, N. Zhenyu, Multi-modal cooperative spectrum sensing based on Dempster-Shafer fusion in 5G-based cognitive radio. IEEE ACCESS **6**(99), 199–208 (2018). https://doi.org/10.1109/ACCESS.2017.2761910
5. Z. Na, Y. Wang, X. Li, J. Xia, X. Liu, M. Xiong, W. Lu, Subcarrier allocation based simultaneous wireless information and power transfer algorithm in 5G cooperative OFDM communication systems. Physical Communication 29, 164–170 (2018)
6. Peng Bao. Research on mobile node location and secure location technology in wireless sensor networks. PhD thesis, Harbin Institute of Technology, 2009.
7. X. Liu, X. Zhang, Rate and energy efficiency improvements for 5G-based IoT with simultaneous transfer. IEEE Internet Things J. 6(4), 5971–5980 (2019). https://doi.org/10.1109/jiot.2018.2863267
8. X. Liu, Y. Zhan, J. Cen, An energy-efficient crowd-sourcing-based indoor automatic localization system. IEEE Sensors J. 18(14), 6009–6022 (2018). https://doi.org/10.1109/JSEN.2018.2842239
9. Z. Na, J. Wang, C. Liu, M. Guan, Z. Gao, Join trajectory optimization and communication design for UAV-enabled OFDM networks. Ad Hoc Netw. 98, 1–10 (2020)
10. J.M. Pak, C.K. Ahn, P. Shi, et al., Distributed hybrid particle/FIR filtering for mitigating NLOS effects in TOA based localization using wireless sensor networks. IEEE Trans. Ind. Electron. 99, 5182–5191 (2016). https://doi.org/10.1109/TIE.2016.2608897
11. X. Liu, M. Jia, X. Zhang, A novel multichannel internet of things based on dynamic spectrum sharing in 5G communication. IEEE Internet Things J. 6(4), 5962–5970 (2019). https://doi.org/10.1109/JIOT.2018.2847731
12. J. Zhang, A two-step filtrate localization method for wireless sensor networks. Journal of Theoretical & Applied Information Technology 47(1), 60–63 (2013)
13. Z. Nagy, F.Y. Yong, M. Frei, A. Schlueter, Occupant centered lighting control for comfort and energy efficient building operation. Energy and Buildings 94, 100–108 (2015). https://doi.org/10.1016/j.enbuild.2015.02.053
14. J.-Y. Chang, T.-H. Shen, An efficient tree-based power saving scheme for wireless sensor networks with mobile sink. IEEE Sensors J. 16(20), 7545–7557 (2016). https://doi.org/10.1109/JSEN.2016.2601327
15. Shun-hua Tan, Miao Chen, Tao Tang. Localization algorithm based on sector scan for mobile wireless sensor networks. in: Proc. of the 2010 International Conference on Biomedical Engineering and Computer Science (ICBECS2010). Wuhan, China, 1-4(2010). doi:https://doi.org/10.1109/ICBECS.2010.5462413.
16. J. Haghighat and W. Hamouda. A power-efficient scheme for wireless sensor networks based on transmission of good bits and threshold optimization. IEEE Trans. Commun.. 4(8)6,3520-3533(2016). doi:https://doi.org/10.1109/TCOMM.2016.2585653.
17. M. Abdelhakim et al., Mobile coordinated wireless sensor network: an energy efficient scheme for real-time transmissions. IEEE J. Sel. Areas Commun 34(5), 1663–1675 (2016). https://doi.org/10.1109/JSAC.2016.2545383
18. S.H.A. Chao, W.A.N.G. Ru-chuan, A type of energy-efficient localization method based on mobile beacons for wireless sensor networks. Computer technology and development 12(12), 51–54 (2012)
19. M. Farooq-I-Azam et al., Intelligent energy efficient localization using variable range beacons in industrial wireless sensor networks. IEEE Trans. Ind. Informat 12(6), 2206–2216 (2016). https://doi.org/10.1109/TII.2016.2606084
20. N. Capurso, T. Song, W. Cheng, et al., An android-based mechanism for energy efficient localization depending on indoor/outdoor context. IEEE Internet Things J. 4(2), 299–307 (2017). https://doi.org/10.1109/JIOT.2016.2553100
21. H. Akcan, C. Evrendilek, Complexity of energy efficient localization with the aid of a mobile beacon. IEEE Communication letters 22(2), 392–395 (2018). https://doi.org/10.1109/LCOMM.2017.2772876
22. Liu Zhuang. Research on localization and energy-efficient technology of wireless sensor networks [D]. PhD thesis, Jilin University, 2012.

Publisher's Note