Research Article

A Game-Based Secure Localization Algorithm for Mobile Wireless Sensor Networks

Tianyue Bao, 1, 2 Jiangwen Wan, 1 Kefu Yi, 1 and Qiang Zhang 1

1 School of Instrumentation Science and Optoelectronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191, China
2 Northeast Petroleum University, Daqing 163318, China

Correspondence should be addressed to Jiangwen Wan; jwwan@buaa.edu.cn

Received 25 March 2015; Revised 23 June 2015; Accepted 3 August 2015

Academic Editor: Feng Hong

Copyright © 2015 Tianyue Bao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The issue of node localization is a fundamental problem in wireless sensor networks. Recently, the localization problem for mobile sensor networks in hostile environment has received significant attention. Due to the mobility of the sensor nodes, it is more challenging to achieve node localization in attacked sensor networks than in static ones. To address these challenges, the paper presents a novel game-based secure localization algorithm. The nodes’ strategy level can be indicated through the results of trust evaluation and then by means of constructing reasonable strategy space and payoff function using game theory; all kinds of nodes within the network can achieve the optimal payoffs. The performance of our algorithm is evaluated by extensive simulation experiments. The simulation results show that the localization error of our proposed algorithm is lower than those of the existing ones in attacked environment.

1. Introduction

With the development of microcomputer technology, mobile wireless sensor networks (MWSNs) are widely used in many fields, such as underwater sensor, border detection, and animal tracking [1, 2]. Location awareness is very important because many applications of MWSNs depend on the information of locations of sensor nodes. Localization is to obtain the nodes position [3, 4].

In most existing sensor networks, nodes are static. However, in some modern applications, localizations become a difficulty, when nodes are moving and being attacked [5]. A mobile node is unable to receive location information rapidly and accurately when it is attacked [6]. The false coordinates or distance estimation will cause a major localization error for normal sensor nodes. In this case, some methods should be explored to eliminate or reduce the adverse influence caused by malicious beacon nodes and ensure safe localization in mobile WSNs.

In this paper, we propose a game-based security localization (GSL) algorithm for solving the mobile node self-localization problem with the existence of malicious node. Firstly, node in multiple hop transmission decides the behavior grade according to the time and space information. Secondly, according to the behavior grade, the complete multirisk level strategy space is constructed and is updated over time. Finally, node selects a behavior grade to obtain optimal benefits. Simulation experiment results show that the algorithm can effectively restrain node's malicious behaviors and boost the cooperation ability of the network. The localization error with GSL is lower than those without GSL in mobile and attacked environment.

The remainder of this paper is organized as follows. Section 2 introduces related works on secure localization algorithms. Section 3 presents the network model, attack model, and game model. Section 4 provides the detail of GSL algorithm. Section 5 presents the simulation results and Section 6 concludes the paper.

2. Related Works

The research in security localization algorithm for wireless sensor networks is mainly divided into two methods. The first method is based on sensor nodes. It can prevent nodes...
from being affected by the attack through the establishment of protection mechanisms (Verifiable Multilateration, SeRLoc, etc.), or removing malicious nodes from the network using the effective detection and filtering methods (DRBTS, ARMMSE, and a voting-based algorithm, etc.). The second method is based on security equipment. It can improve the defense capability of the network by adding security equipment in the physical layer.

Lazos et al. [7] present a robust positioning system called ROPE which utilizes a location verification technique to identify the location claims of the sensor nodes before data collection.

Yang et al. [8] analyze the outlier data detection problem and design a stray monitoring algorithm based on general cycle bilateration, which reduced to data from the group to improve localization accuracy.

Yu et al. [9] propose a BRS-based robust secure localization (BRSL) algorithm, aiming at reducing the impact of the malicious attackers in the network. The BRSL method includes two phases: the setup trust evaluation framework and the localization stage.

Wei and Guan [10] introduce a novel scheme called a lightweight positioning verification algorithm (LPVA); it does not rely on dedicated hardware equipment under the condition of network attack resistance and can be used in the low-cost network.

Xiao et al. [11] propose a robust network localization algorithm call RobustLoc, based on a robust patch merging operation that can reject outliers for both multilateration and patch merging.

The above studies mainly eliminate the fake beacon information (ROPE, RobustLoc, etc.) or detect malicious nodes (LPVA, BRSL, etc.) or increase equipment to improve localization accuracy but seldom deal with action information of sensor nodes, when nodes are mobile. Our proposal utilized an improved game theory and the sensor nodes’ pluralistic behavior in the network to establish a trust-preferential strategy, which make the beacons cooperate effectively.

3. Network Model

3.1. Network Environment. In an environment under attack, a mobile wireless sensor network consists of anchor nodes, unknown nodes, and malicious nodes; nodes with known coordinates are called anchor nodes, nodes whose coordinates are unknown are called unknown nodes, and nodes which are captured and possibly attack are called malicious nodes. All nodes are randomly distributed in the two-dimensional space of the network and on the move.

As shown in Figure 1, the communication radius of each node in the network is represented by $r$ and the maximum moving speed is represented by $V_{\text{max}}$. Each node has a unique ID, and the coordinates of unknown nodes are estimated by obtaining the coordinate information of adjacent anchor nodes.

3.2. Attack Model. In the sequential Monte-Carlo localization algorithm, coordinates of unknown nodes are calculated through sample set [12]. The unknown node will select locations of anchor nodes within single hop and two hops as members of the sample set, and therefore the accuracy of location information of anchor nodes within this scope determines the accuracy of positioning [13]. The attack models used in this paper are shown in Figures 1 and 2. The unknown node $N$ can monitor the information of anchor nodes $(b_1$–$b_6)$. Meanwhile, it may be attacked by the malicious node $a_1$. The malicious node $a_1$ obtains the information of anchor nodes $(b_7$–$b_{10})$ provided by $a_2$ (from the region of $a_2$) through the attack channel and transmits this information to the unknown nodes. Nodes to be positioned will mistakenly take such beacon nodes as reference information within its two-hop range, causing localization errors of unknown nodes. We assume that the attack channel between malicious nodes is independent of distance. Potential cases of attacks are shown in Figure 1 where the distance between malicious nodes is long, and estimation of coordinates of unknown nodes based on coordinates transmitted by malicious nodes will cause large errors. In Figure 2, the distance between malicious nodes is relatively short, and the two-node scopes of malicious nodes have an area of intersection in which the node $b_6$ is located.

In a multihop network, we use $T$ to represent the time of each hop. For the unknown node $N$, the distance between it and $d_1$–$d_6$ is one hop and the communication time is $T$. 

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{Attack model with long attack distance.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure2.png}
\caption{Attack model with short attack distance.}
\end{figure}
To obtain data, d7 channel has to cover three hops, so its communication time is \(3T\).

3.3. Game Model

3.3.1. Game Participants. In the process of mobile positioning, every unknown node will obtain the information of beacon nodes within one hop or two hops [14]. For attacks which may exist in data transmission links, all nodes involved in the transmission of information are game participants. Therefore, participants in the game model include information sender \(T\), information recipient \(R\), and \(n\) information forwarders \(E\). Throughout information transmission, the data sent by the sending node may travel through \(n\) forwarding nodes to reach the receiving node, so the number of participants of the game is \(n + 2\).

3.3.2. Strategy Space. In this paper, we define the strategy space according to the different behaviors of nodes. Node behaviors include cooperative, uncooperative, and attack behavior. According to the different attack effect, the attack behavior is divided into \(n\) level, and the attack level is determined by the attack effect. For example, the influence of the attack in Figure 1 is much greater than that in Figure 2, so the attack level in Figure 1 is higher than in Figure 2. We divide node actions into multiple levels according to their effects. We call the behaviors taken by nodes, which are shown in Table 1, strategy space.

In the strategy space set of nodes \(G = \{C, U, A_1, A_2, \ldots, A_n\}\), \(\{C, U\}\) represent cooperative behaviors and uncooperative behaviors, respectively. Cooperative behaviors refer to the cooperative response of nodes, such as receiving or forwarding after listening to signals. Uncooperative behaviors refer to the fact that the nodes do not deal with the information which needs receiving or forwarding; that is, no response will be carried out where the set \(\{A_1, A_2, \ldots, A_n\}\) represents a collection of different levels of attacks. Attack level depends on the degree of influence of reference coordinates on the positioning accuracy. In the positioning process, for example, different attacks have different effects on the accuracy of positioning. The longer the distance between false coordinates and actual coordinates (Figure 1) is, the stronger the attack’s destructive power will be, the bigger the positioning error will be, and the higher the attack level will be. The false coordinate information (Figure 2) with short distance can help localization when anchor nodes are sparse, so its attack level is low.

3.3.3. Game Payoff. In the game process of transmission of positioning information, the payoff of a participant after choosing a strategy at the moment of \(t\) can be \(u_{k(t)}(t)\), where \(k(t) \in G\). For the attack node and each information sender, every gamer who participates in the information transmission will choose a behavior mode in the strategy space \(G\), resulting in payoff. The payoff of gamers comes mainly from the gain obtained by behaviors \(m_{k(t)}\) and their own loss \(c_{k(t)}\), and therefore the payoff function is \(u_{k(t)} = m_{k(t)} - c_{k(t)}, k(t) \in G\). The information recipient will obtain the maximum payoff from the correct information provided or forwarded by the sending node or forwarding node. On the contrary, rejection or attack will reduce the payoff. At the moment of \(t\), the payoff function of normal nodes can be expressed as \(u_C(t) \geq u_U(t) \geq u_{A_1}(t) \geq \cdots \geq u_{A_n}(t)\), while the payoff function of attack nodes can be expressed as \(u_{A_n}(t) \geq \cdots \geq u_{A_1}(t) \geq 0 \geq u_U(t) \geq u_C(t)\).

3.3.4. Trust Level. In the attack models mentioned above, the attacks are characterized by changing time reference and tampering with the spatial reference. Changes of time reference reflect on the increase of the number of hops from the beacon node to the receiving node. Information of each anchor node obtained by unknown nodes has time weights which can be used to determine attack payoff. The bigger the time weight is, the greater the attack payoff will be, and so the higher the influence of attacks on the accuracy of coordinates of unknown nodes will be. In Figure 1, the malicious coordinate data of the beacon node \(b7\) reaches the unknown node \(N\) through 3 hops, of which the time information is \(3T\) (\(T\) is the time interval of each segment). Obviously, the longer the time is, the greater the influence of attacks on positioning will be. Tampering of spatial reference data reflects on the fact that coordinate information is changed by the malicious node. In Figure 1, the malicious node \(a1\) changes its coordinates to the coordinates of \(b7-b10\), and the distance between these coordinates and the node to be positioned is much larger than two hops of the unknown node \(N\), seriously affecting the positioning accuracy of the unknown node.

Dempster Shafer (abbreviated D-S) evidence theory is adopted in this paper to calculate the trust values [15] based on the data information of time and space. Trust levels are defined by trust values. We use three variables, \(a_i, b_j, c_i\), to quantify the degree of a node behavior. \(a_i\) represents the measurement of a note that is not attacked, \(b_i\) represents the measurement of a note that has been attacked, and \(c_i\) represents the measurement of a note whose behavior is unknown. The measurement of node behavior can be divided into the following situations:

\[(1)\] Measurement analysis of behavior of time parameter.
Assuming that \(\beta_i = (t - \Delta t)/\Delta t\):

\[\begin{align*}
\alpha_i' &= \alpha_i' + 1, \\
\beta_i' &= \beta_i'.
\end{align*}\]
\[ c'_i = c'_i; \]
\[ a'_i = a'_i, \]
\[ b'_i = b'_i + \beta_i, \]
\[ c'_i = c'_i; \]
\[ -1 \leq \beta_i \leq 1 \]
\[ \beta_i > 1. \]  

(1)

(2) Measurement analysis of behavior of spatial parameter. To represent the Euclidean distance between any two beacon nodes, we use
\[ d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \]
\[ a_{ij} = a_{i,j} + 1, \]
\[ b_{ij} = b_{i,j}, \]
\[ c_{ij} = c_{i,j}; \]
\[ 0 \leq d_{ij} \leq 2r \]
\[ a_{ij} = a_{i,j}, \]
\[ b_{ij} = b_{i,j}, \]
\[ c_{ij} = c_{i,j} + \left[ \frac{d_{ij} - 2r}{r} \right]; \]
\[ d_{ij} > 2r. \]  

(2)

(3) Quantitative classification of trust levels. If there is information of \( n \) anchor nodes around the unknown node, we can determine the quantized values of each node based on the measurement of time and space with the following formula:
\[ m_i(A) = \frac{a''_i}{a''_i + b''_i + c''_i} \]
\[ m_i(B) = \frac{b''_i}{a''_i + b''_i + c''_i} \]
\[ m_i(C) = \frac{c''_i}{a''_i + b''_i + c''_i}, \]
where \( a''_i = a'_i + a, b''_i = b'_i + b, \) and \( c''_i = c'_i + c, \) where \( A, B, \) and \( C \) represent three exclusive trust states of nodes, namely, "trust," "distrust," "impossible," and "uncertainty."  

(3.3.5. Level Mapping. By the above methods, the time and space parameters of mobile positioning can be converted into trust levels, and a parameter \( M \) can be determined in the trust levels of each node, where \( M = \text{MAX}(m(A), m(B), m(C)). \) The game space of behaviors of a node is \( \{A_1, A_2, \ldots, A_n, U, C\}, \) consisting of \( n + 2 \) elements. We construct the following rules (Figure 3) to map the trust value to game behavior one by one. The bigger the trust value is, the higher level the mapped behavior will be. The trust levels of nodes can be used to identify the elements of the behavior space by establishing the mapping relationship.

3.3.5. Level Mapping. By the above methods, the time and space parameters of mobile positioning can be converted into trust levels, and a parameter \( M \) can be determined in the trust levels of each node, where \( M = \text{MAX}(m(A), m(B), m(C)). \) The game space of behaviors of a node is \( \{A_1, A_2, \ldots, A_n, U, C\}, \) consisting of \( n + 2 \) elements. We construct the following rules (Figure 3) to map the trust value to game behavior one by one. The bigger the trust value is, the higher level the mapped behavior will be. The trust levels of nodes can be used to identify the elements of the behavior space by establishing the mapping relationship.

4. Game Calculation with Strategy Evolution

4.1. Strategic Game. Every node has a trust vector \( T = (T_{A_1}, T_{A_2}, \ldots, T_{U}, T_{C}) \), so we define the behavior game space of each node as \( j \in \{A_1, A_2, \ldots, A_n, U, C\}. \) In the mapping relationship, every element of the trust vector \( M \) is the probability of the behavior space; hence \( 0 \leq T_j \leq 1, \) and \( \sum_{j=1}^{N+2} T_j = 1. \) We assume that in the process of positioning the behavior of the information sender is identified as \( i \) and the behavior of participating node is identified as \( j, \) where \( i, j \in \{A_1, A_2, \ldots, A_n, U, C\}. \) We define the trust assignment relationship matrix as \( T_{ij}; \) then the element of this matrix model is the trust level of a node when it faces the sender with the behavior.
identification of \( j \) and the mode selection identification of \( i \):

\[
[T_{ij}](N+2) \times (N+2) = \theta \begin{bmatrix}
N & N & \cdots & N & N & N \\
N & N & \cdots & N & N & N \\
N & N & \cdots & N & N & N \\
1 & 1 & \cdots & 1 & 1 & 1 \\
N+2 & N+2 & \cdots & N+2 & N+2 & N+1 \\
N & N+1 & \cdots & N+1 & N+1 & N+1 \\
N+2 & N+2 & \cdots & N+2 & N+2 & N+2 
\end{bmatrix} + (1-\theta) \begin{bmatrix}
N & N & \cdots & N & N & N \\
N & N & \cdots & N & N & N \\
N & N & \cdots & N & N & N \\
1 & 1 & \cdots & 1 & 1 & 1 \\
N+2 & N+2 & \cdots & N+2 & N+2 & N+1 \\
N & N+1 & \cdots & N+1 & N+1 & N+1 \\
N+2 & N+2 & \cdots & N+2 & N+2 & N+2 
\end{bmatrix}.
\]

(4)

The matrix \( T_{ij} \) defines the trust level identifications of a node based on different behaviors of the information sender when the node is receiving the information (\( \theta = 0 \)) and forwarding the information (\( \theta = 1 \)). For example, when the receiving node or forwarding node receives the behavior of the information sender \( A_1 \), the higher the level of the selected attack is, the lower its trust value will be.

For a node, the purpose of adopting strategic game during positioning is to choose a behavior with higher trust degree through behavior identification, thus achieving the best positioning results. According to this rule, the expected behavior of each node which participates in the game is \( T^* \):

\[
T^* = \theta \begin{bmatrix}
U(N+1) \\
U(N+1) \\
\vdots \\
C(N+2) \\
C(N+2) \\
\vdots \\
C(N+2) 
\end{bmatrix} + (1-\theta) \begin{bmatrix}
C(N+2) \\
C(N+2) \\
\vdots \\
C(N+2) \\
C(N+2) \\
\vdots \\
C(N+2) 
\end{bmatrix}.
\]

(5)

4.2 Update Mechanism. At the initial phase, the node has a higher willingness to collaborate, and its initial trust vector is defined as \( T(0) = (0, 0, \ldots, 0, 1) \). At the time point of \( t \), the level identification of instantaneous trust \( K_{ij} \) can be obtained according to the trust matrix \( [T_{ij}](N+2) \times (N+2) \), the relay node identity \( \theta \), the behavior identity of the information transmission node \( j \), and the behavior identity of the participating node \( i \).

The update equation of the trust vector can be expressed as

\[
T(t+1) = A \delta_{ij} T(t) + (1 - \delta_{ij}) K_{ij},
\]

(6)

where \( \delta_{ij} \) is the time factor \( \delta_{ij} = (\delta_{A_1}, \delta_{A_2}, \ldots, \delta_{U}, \delta_{V}) \), describing the degree of coupling between the transient effect and the trust vector of the previous moment. The greater the \( \delta \) is, the more dependent the trust vector will be on the value of the previous moment in the system, whereas the instantaneous trust has a relatively small impact on it, and vice versa. \( A \) is the trust transmission matrix, whose role is to overcome the misjudgment of the trust vector caused by monitoring errors or transmission mistakes. The specific form is below:

\[
A(N+2) \times (N+2) = 
\begin{bmatrix}
p_N & 1-p_N & \cdots & 1-p_N & 1-p_N \\
1-p_{N-1} & p_{N-1} & \cdots & 1-p_{N-1} & 1-p_{N-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1-p_1 & 1-p_1 & \cdots & p_1 & 1-p_1 \\
1-p_{N+1} & 1-p_{N+1} & \cdots & 1-p_{N+1} & p_{N+1} \\
1-p_{N+2} & 1-p_{N+2} & \cdots & 1-p_{N+2} & p_{N+2} 
\end{bmatrix},
\]

(7)

where \( p_N \) represents the probability of the trust level being correctly identified.

4.3. The Conditions of Game Equilibrium. In the process of mobile localization, the steady-state convergence condition of the above mentioned game model is solved by means of evolutionary game ideas and principles for maximizing payoff. According to the evolutionary game theory, when the system is in initial operation, each member node \( n \) that participates in localization selects the appropriate action participation way in accordance with the expectation action...
Table 2: Default parameter settings.

| Model parameter          | Default setting |
|--------------------------|-----------------|
| The number of node $N$   | 5000            |
| The ratio of beacon node $\rho$ | 0.2             |
| Communication radius $r$ | 50 m            |
| Maximum moving speed $V_{\text{max}}$ | 10 m/s         |
| Probability of identifying trust level $p_N$ | 0.75         |
| Time factor $\delta_{i,j}$ | $(\delta_{A_1}, \delta_{A_2}, \ldots, \delta_{U}, \delta_{V})$ | $(0.5, 0.5, \ldots, 0.5, 0.5)$ |

The space $T^*$ and the trust decision-making framework. At the time point of $t+1$, the probability of the node $n$ selecting the action $a_n(t+1) = i \in \{A_1, A_2, \ldots, A_n, U, C\}$ is obtained by the following formula:

$$
\Pr[a_n(t+1) = i] = \frac{\Pr[a_n(t) = i] P_{n,i}(t)}{\sum_{j=1}^{N+2} \Pr[a_n(t) = j] P_{n,j}(t)}, \quad (8)
$$

where $P_{n,i}(t)$ is the instantaneous payoff the participating node $n$ obtains by selecting the action of which the action space is identified as $i$, at the time point of $t$.

The sufficient condition for the evolutionary convergence is proven in the literature, and ultimately the acquired game convergence condition is

$$
P_1^\theta - P_{N+2}^\theta < 0, \quad \theta = 0, 1
$$

$$
p_i > \frac{1}{N+2}.
$$

5. Performance Evaluation

5.1. Simulation Setting. In this section, we designed a mobile network simulation experiment to verify the effects of the trust game-based mobile localization method on cooperation and localization performance of the mobile sensor network node and conducted the simulation in Matlab. The default setting is with 5,000 nodes deployed and moving within the 10000 m × 10000 m area at random. The moving speed is in the range of $[0, V_{\text{max}}]$ (where $V_{\text{max}}$ is the maximum moving speed). The default parameters are as in Table 2.

5.2. Simulation Results

1. The simulation has analyzed the effect of the game algorithm on node cooperation. In the case of different ratios of malicious nodes (20%, 40%, and 60%, resp.), the situations of nodes participating in cooperation via game are shown in Figure 4. The Figure shows that, with the increase of the game number, the ratio of nodes which select cooperation also increases. Finally, the ratio value of nodes which select cooperation tends to be stabilized. In the initial state, the ratios of malicious nodes are 20%, 40%, and 60%; after the game is stable, the ratios of cooperative members have been raised from 45.8%, 36%, and 19.6% to 83.9%, 78.6%, and 72.4%. Simulation results show that the algorithm can effectively improve cooperation of nodes, ensure transmission of localization data, and maintain the proper work of the network even under the situation of malicious attack.

2. In the case of different ratios of malicious nodes (20%, 40%, and 60%, resp.), the mobile game-based secure localization (GSL) algorithm and the mobile localization algorithm without using the game are compared, as shown in the figure. Figures 5 and 6 show the situations of localization accuracy under the 20%, 40%, and malicious nodes coverage conditions. It can be clearly seen from the figure that by using the game approach the localization accuracy has been improved significantly, and the rate of improvement reaches about 20%–50%. Meanwhile, for network environment with a higher ratio of malicious nodes (60%) (Figure 7), the localization results can converge to achieve localization in harsh environments by applying this algorithm. Simulation results show that the game-based localization algorithm can effectively inhibit aggressive behaviors of malicious nodes and improve the localization accuracy of mobile nodes.

3. We compare the following three methods in the simulations: the GSL algorithm (the game theory is used); the DBSLS algorithm (the improved D-S fusion method is used [15]); the BRSL-based robust secure localization (BRSL) algorithm [9]. Figure 8 shows the comparison results of localization error under different malicious ratio. The proportion of attackers ranges from 5% to 60%. As the number of attackers
increases, the localization error increases as well. GSL can obtain more accurate results compared with DBSL and BRSL. In particular, when malicious ratio is high, GSL has better inhibition effect on attacker's number.

6. Conclusions

This paper presents a mobile network node localization algorithm based on game strategies. Features are extracted under the situation of the mobile sensor network being attacked and the mapping relation between the attack level and the trust level is established. At the same time, trust and cooperation model and the payoff space of the strategy game are built, effectively suppressing the behavior of malicious nodes in network. Finally, the game update mechanism and equilibrium conditions are provided to ensure the stability and convergence of the algorithm. Simulation results show that the proposed mobile node localization algorithm based on game strategies takes full advantage of the dynamic characteristics of the algorithm and motivates cooperative behavior of member nodes; this algorithm can achieve nodes' localization and improve localization accuracy in harsh environments, especially in the situation with a higher ratio of initial malicious nodes.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.
Acknowledgments

The authors are grateful to the anonymous reviewers for their industrious work and insightful comments. This work is supported by Natural Science Foundation of China under Grant no. 61371135.

References

[1] H. Chenji and R. Stoleru, “Toward accurate mobile sensor network localization in noisy environments,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1094–1106, 2013.

[2] Z. Wang, Y. Wang, M. Ma, and J. Wu, “Efficient localization for mobile sensor networks based on constraint rules optimized Monte Carlo method,” *Computer Networks*, vol. 57, no. 14, pp. 2788–2801, 2013.

[3] K. W. K. Lui, W.-K. Ma, H. C. So, and F. K. Chan, “Semi-definite programming algorithms for sensor network node localization with uncertainties in anchor positions and/or propagation speed,” *IEEE Transactions on Signal Processing*, vol. 57, no. 2, pp. 752–763, 2009.

[4] G. J. Han, H. H. Xu, T. Q. Duong, J. Jiang, and T. Hara, “Localization algorithms of wireless sensor networks: a survey,” *Telecommunication Systems*, vol. 52, no. 4, pp. 2419–2436, 2013.

[5] Z. Li and H. Shen, “Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287–1303, 2012.

[6] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, “Game theory for wireless sensor networks: a survey,” *Sensors*, vol. 12, no. 7, pp. 9055–9097, 2012.

[7] L. Lazos, R. Poovendran, and S. Capkun, “ROPE: robust position estimation in wireless sensor networks,” in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN ’05)*, pp. 324–331, University of California, Los Angeles, Los Angeles, Calif, USA, August 2005.

[8] Z. Yang, L. Jian, C. Wu, and Y. Liu, “Beyond triangle inequality: sifting noisy and outlier distance measurements for localization,” *ACM Transactions on Sensor Networks*, vol. 9, no. 2, article 26, 2013.

[9] N. Yu, L. R. Zhang, and Y. J. Ren, “BRS-based robust secure localization algorithm for wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 107024, 9 pages, 2013.

[10] Y. Wei and Y. Guan, “Lightweight location verification algorithms for wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, pp. 938–950, 2013.

[11] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, “Indirect reciprocity security game for large-scale wireless networks,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1368–1380, 2012.

[12] R. Feng, X. Xu, X. Zhou, and J. Wan, “A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory,” *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[13] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, “A survey of security challenges in cognitive radio networks: solutions and future research directions,” *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012.

[14] Q. Xiao, K. Bu, Z. Wang, and B. Xiao, “Robust localization against outliers in wireless sensor networks,” *ACM Transactions on Sensor Networks*, vol. 9, no. 2, article 24, 2013.

[15] N. Yu, L. Zhang, and Y. Ren, “A novel D-S based secure localization algorithm for wireless sensor networks,” *Security and Communication Networks*, vol. 7, no. 11, pp. 1945–1954, 2014.
Submit your manuscripts at
http://www.hindawi.com