Hindawi
Security and Communication Networks
Volume 2017, Article ID 6102780, 12 pages
https://doi.org/10.1155/2017/6102780

Research Article

Research on Secure Localization Model Based on Trust Valuation in Wireless Sensor Networks

Peng Li,[1,2] Xiaotian Yu,[1] He Xu,[1,2] Jiewei Qian,[1] Lu Dong,[1] and Huqing Nie[1]

[1] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2] Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Jiangsu Province, Nanjing 210003, China

Correspondence should be addressed to Peng Li; lipeng@njupt.edu.cn

Received 5 October 2016; Revised 6 January 2017; Accepted 19 January 2017; Published 8 March 2017

Academic Editor: Qing Yang

Secure localization has become very important in wireless sensor networks. However, the conventional secure localization algorithms used in wireless sensor networks cannot deal with internal attacks and cannot identify malicious nodes. In this paper, a localization based on trust valuation, which can overcome a various attack types, such as spoofing attacks and Sybil attacks, is presented. The trust valuation is obtained via selection of the property set, which includes estimated distance, localization performance, position information of beacon nodes, and transmission time, and discussion of the threshold in the property set. In addition, the robustness of the proposed model is verified by analysis of attack intensity, localization error, and trust relationship for three typical scenes. The experimental results have shown that the proposed model is superior to the traditional secure localization models in terms of malicious nodes identification and performance improvement.

1. Introduction

WSNs (wireless sensor networks) are composed of a large number of static or mobile sensors. Positioning technologies based on WSN [1] estimate the current location of unknown nodes using the cooperation of position nodes and localization algorithm. In the locating, the nodes whose positions are known are called anchor nodes, while the nodes whose positions are unknown are called unknown nodes. The information on distance of anchor nodes and unknown nodes can be obtained via cooperation. Afterwards, that information and the localization algorithm are used to determine the positions of unknown nodes.

Due to random deployment and network topology dynamicity, the locating in the WSN is more vulnerable to various attacks [2, 3]. On this basis, the secure localization algorithms are widely used. Namely, they can be divided into three categories [4]: (1) secure localization algorithms based on robust observation; (2) secure localization algorithms based on isolation of malicious beacon node; and (3) secure localization algorithms based on localization verification. In the first group, the upper-bound limitation of the nodes' distance disables the attack node to reduce the measure distance. In the second group, the beacon nodes are used as checkpoints for mutual monitoring, in order to prevent the false localization. In the third group, a predetermined deployment location combined with a set of neighbor nodes is used to determine whether the localization process is attacked or not. However, these algorithms have different shortcomings [5]. The first group's algorithms are unable to resist to the attack, which causes the increase of the measured distance. In addition, the algorithms can only roughly confirm whether the unknown node is in certain area or not. The second group relies too much on the base station node, which might cause the base station overload during the processing of a large amount of node information. Namely, the base station becomes the bottleneck of algorithm performance. The third group's defense capability is greatly influenced by deployment of the nodes. In order to compensate the inadequacy of the above algorithms and to improve their resistance to various attacks, a secure localization model based on trust valuation is designed.

The remainder of the paper is organized as follows. Section 2 introduces related work. In Section 3, we detail the secure localization model and give the formal description. Section 4 makes some simulation and analysis on secure localization model based on trust valuation. Section 5 concludes the paper.

2. Related Works

According to the usage of distance in the positioning, the positioning technologies can be divided into two main categories: distance-based (range-based) positioning technologies and distance-independent (range-free) positioning technologies. In the distance-based positioning algorithms, the absolute distance, or angle, between anchor node and unknown node is required. On the other hand, in distance-independent localization algorithms, there is no need to obtain the exact distance between anchor and unknown nodes. The distance-based localization algorithms usually consist of two steps: firstly, the distance (or angle) is measured, and, secondly, the measured distance is used to calculate the coordinates of unknown node. The distance measurement methods can be divided into following categories: methods based on time, methods based on signal arrival angle, and methods based on received signal strength.

The principle of distance-independent localization is simple and easy to implement, and it has advantages in terms of cost and power consumption. Besides, its performance is not affected by environmental factors. These algorithms can be divided into four categories: APTI algorithm, DV-Hop algorithm [6], Amorphous algorithm [7], and N-hop algorithm.

In the WSN, the localization algorithm can be attacked in many ways. The attacks can be divided into two categories: internal attacks and external attacks. Four types of external attacks are concerned: Sybil attack [8], selective forwarding attack, wormhole attack, and node capture attack [9–11].

Due to limitation on sensor nodes, it is impossible to have a well-integrated defense system in the traditional WSN. The secure localization algorithms intended for WSN need to balance availability and integrity. According to that, the security localization algorithms can be divided into three categories: secure localization algorithms based on robust observation, secure localization algorithms based on isolation of malicious beacon node, and secure localization algorithms based on localization verification.

The gradual application of WSN localization caused the appearance of various attack methods [12]. Nowadays, the main secure localization algorithm in the WSN has no ability to deal with the internal attacks and to identify the malicious nodes. Moreover, in the case of nodes compromising, the secure localization cannot be achieved. Thus, the trust management, which has been widely studied in various network environments, is considered as an effective complement to the traditional localization.

In 1994, Marsh proposed a model of trust and cooperation for the first time, which has been regarded for a long time as a scope of sociology and psychology. In addition, Marsh introduced the concept of trust relationship formalization. In 1996, Blaze et al. proposed the concept of trust model in order to solve the complex security problems in the Internet [13].

The trust management models can be roughly divided into two categories: objective trust management models and subjective trust management models. The objective trust management models abstract the trust value into Boolean value; thus, there are only two possibilities for trust value. Due to the aforementioned, the commonly used trust management models are subjective trust management models. The most popular subjective trust management models are presented in the following.

(1) Pervasive Trust Management. Pervasive Trust Management (PTM) represents a subresearch project of the UBISEC project, which defines a dynamic trust model based on a pervasive environment. The method of average weight is used for trust evaluation, and the evaluation result for two interactive entities can be expressed as

$$\begin{gathered} R(A,B)=\alpha, \quad \alpha\in[0,1], \\ \exists R(A,B)=\alpha \mid G\left(\alpha^{+} \longrightarrow R(A,B)\geq\alpha\right) \\ \wedge G\left(\alpha^{-} \longrightarrow R(A,B)<\alpha\right), \end{gathered} \tag{1}$$

where α represents the trust value, α^{+} indicates that trust increases when feedback is positive, and α^{-} indicates that trust decreases when feedback is negative.

The disadvantage of this model is that the arithmetic mean is used to calculate the indirect trust degree. In addition, this method processes data roughly and cannot accurately reflect the characteristics of the fuzzy trust value.

(2) Hassan's Model. Hassan's model is based on vector mechanism. If there are n entities, namely, $Q_1, Q_2, Q_3, \dots, Q_n$, then, the relationship between entity Q_i and other entities can be represented as a trust vector: $\overrightarrow{Q_i} = (t_{Q_iQ_1}, t_{Q_iQ_2}, \dots, t_{Q_iQ_{i-1}}, t_{Q_iQ_{i+1}}, t_{Q_iQ_n})$.

The disadvantage of this model is that it is not resistant to the collusion attacks. Namely, malicious nodes can give each other a high trust value.

(3) Sun's Model. Sun's model is based on entropy; namely, it uses T to express trust relationship, while P represents the probability that the agent nodes take action to the target nodes. The calculation process of trust value used in Sun's model is shown as

$$T=\begin{cases} 1-H(p), & 0.5\leq p\leq 1, \\ H(p)-1, & 0\leq p\leq 0.5, \end{cases} \tag{2}$$

where $H(p) = -p\log_2^{(p)} - (1-p)\log_2^{1-p}$ represents the entropy function. Then, the trust value is defined by

$$T_{ABC}=R_{AB}T_{BC}, \tag{3}$$

where T_{ABC} represents the trust degree of node A to node C, T_{BC} denotes direct trust value of node B to node C, and R_{AB} denotes the recommendation trust value of node A to node B.

The convergence rate of Sun's model is limited by the length of trust chain, and it is difficult to get the trust value when the trust chain length increases.

3. Secure Localization Model Based on Trust Valuation

3.1. Trust Valuation Basis. The concepts in trust valuation and roles of nodes are listed as follows.

Definition 1. Comprehensive trust value is based on the localization error and time consumption of the beacon nodes, and it refers to the adoption level of the information provided by the beacon nodes.

Definition 2. Direct trust value refers to the confidence of unknown node in the anchor node, which is directly involved in the localization process.

Definition 3. Indirect trust value refers to the confidence of unknown node in the anchor node based on recommendation from other nodes.

Definition 4. Recommended trust value refers to the confidence of unknown node in the recommended nodes.

Definition 5. Source node represents an unknown node in the localization process.

Definition 6. Target node represents an anchor node needed for the localization.

Definition 7. Recommended nodes represent all nodes used in the localization except source node and target node.

3.1.1. Trust Valuation Framework. In the WSN localization, the unknown node N sends the localization request, *Loc_req*, and the beacon node B, which is within communication range of node N, sends the response, *Loc_ack*, to node N after receiving of its request. Then, N calculates direct trust value D for node B using the valuation algorithm. Other beacon nodes, which are within the communication range of node N, form the recommended node set defined as $R = \{B_1, B_2, \ldots, B_i\}$. In order to get indirect trust value of node B, node N calculates the recommended trust value of nodes in R. Therefore, the indirect trust value of node B for node N is obtained and labeled as M. According to all mentioned, the comprehensive trust value is defined as

$$C = \alpha D + \beta M, \tag{4}$$

where α and β represent weight coefficients of direct and recommended trust values, respectively, and C represents the comprehensive trust value. The frame diagram of trust validation is shown in Figure 1.

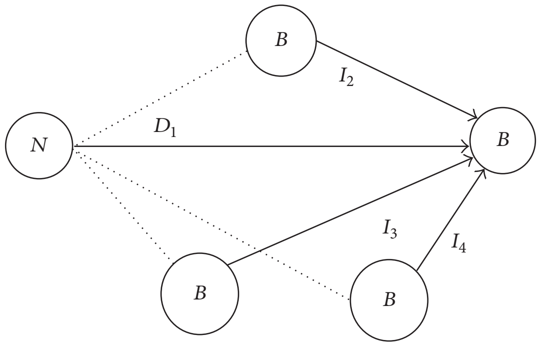


FIGURE 1: Frame diagram of trust validation.

3.1.2. Direct Trust. According to the multidimensional decision theory [14], the direct trust of source node for target node consists of n attributes that form a set of attributes $S = \{p_1, p_2, \ldots, p_i, \ldots, p_n\}$ $(0 \le p_i \le 1)$.

Each attribute value has different influence on calculation of direct trust value; thus, the weight vector is defined as $V = \{v_1, v_2, \ldots, v_i, \ldots, v_n\}$ $(0 \le v_i \le 1, \sum_{i=1}^{n} v_i = 1)$. Moreover, the time decay function, $T(k)$, defined by (5), is used to calculate the direct trust value:

$$T(k) = \begin{cases} 0 & k = 0, \\ 1 & k = 1, \\ T(k-1) - \left(\dfrac{1}{2}\right)^{k-1} & 1 \le k \le n. \end{cases} \tag{5}$$

Based on the above function, the kth calculation of direct trust value is obtained. The direct trust value function is defined by

$$W_k^{(p,v)} = T(k) \times \sum_{i=1}^{n} v_i \times p_i. \tag{6}$$

All previous direct trust values are combined in order to obtain the final result:

$$D_{xy} = \prod_{k=1}^{n} W_k^{(p,v)}, \tag{7}$$

where D_{xy} indicates the direct trust value of the source node x for target node y. The difference between direct trust values of attack node and normal node is enlarged by this calculation method. In case of attack, the node is close to zero according to the calculated $W_k^{(p,v)}$ value, and the node will be abandoned.

3.1.3. Indirect Trust and Recommended Trust. The trust model is composed of three types of nodes, the source node, the target node, and the recommended node, which form the trust chain as shown in Figure 2.

In Figure 2, S, R, and O represent the source node, the recommended node, and the target node, respectively, while I and D indicate the recommended trust value and the direct trust value, respectively.

Received Signal Strength Indicator (RSSI) represents the strength of the received signal [15], with the RSSI signal attenuation model in WSN defined by

$$\mathrm{RSSI}(d) = C_0 - 10\lambda \log_{10}^{d}, \tag{8}$$

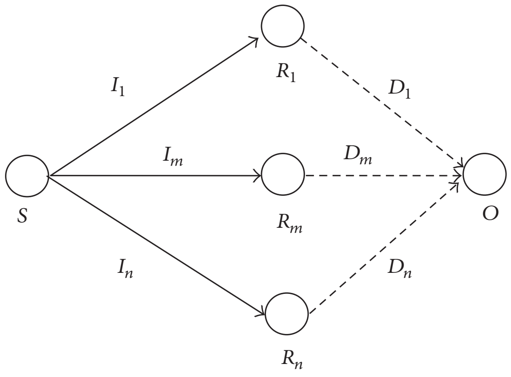


Figure 2: Trust chain.

where RSSI(d) represents the signal strength at distance d from the transmitter, C_0 indicates the signal strength reference value from the transmitter, and λ denotes the path loss factor.

Due to the influence of environmental noise, there may be errors when measuring RSSI. Thus, (8) can be modified to

$$\mathrm{RSSI}(d) = C_0 - 10\lambda \log_{10}^{d} + E, \tag{9}$$

where the measurement error E follows the normal distribution defined by

$$E \sim N\left(0, \sigma^2\right), \tag{10}$$

where σ is random variable changes depending on the existing environment [16].

Some experiments were carried out in article [17], in order to describe the relationship between the RSSI error and the corresponding distance. It adopts regular pattern as the communication model, and the communication radius of the nodes is 20 m. The distance between two nodes is fixed and RSSI values are observed 100 times. It repeats the observation of RSSI value as the distance between two nodes increases; it comes to the conclusion as shown in Figure 3.

As can be seen from Figure 3, the error of RSSI gradually increases with the increasing of distance within communication range. However, the error decreases gradually when distance is beyond the scope of communication. Since the distance is calculated according to the RSSI value, the variation law of distance error is coincident with RSSI error. Thus we get Theorem 8.

Theorem 8. *The error, that is, the difference between measured and actual distance values, increases with the increase of distance between nodes [18].*

According to Theorem 8, three anchor nodes that are closest to the target node will be selected as recommended nodes and labeled as R_l, R_m, and R_n. Recommendation trust value is then defined as

$$I_{xy}(k, s, n) = \begin{cases} \dfrac{1}{2} & i = 1, \\ \dfrac{1 + \sum_{i=1}^{n} T(k) \times s_i}{2 + n} & i > 1, \end{cases} \tag{11}$$

where n denotes the total number of nodes that participate in the trust calculation and s_i represents the Boolean value that indicates whether the node is being trusted in calculation of direct trust. The initial value of the recommended trust value is 1/2. After a certain period, the value fluctuates due to performance of recommended node.

Finally, the indirect trust value is obtained by

$$M_{xy}(k, s, n, p, v) = \frac{\left(I_{xu}(k, s, n) \times D_{uy}(p, v) + I_{xv}(k, s, n) \times D_{vy}(p, v) + I_{xw}(k, s, n) \times D_{wy}(p, v)\right)}{3}. \tag{12}$$

3.1.4. Comprehensive Trust. Based on direct and indirect trust values, the comprehensive trust value of the source node for the target node is obtained, namely, $C = \alpha D + \beta M$. Similar to that in the ordinary trust valuation, α and β are generally considered as fixed values; thus, the trust model has no dynamic adaptability. Therefore, an adjustment method based on information entropy theory [19] is proposed.

In the calculation of comprehensive trust value, the information entropy of direct trust value is defined by

$$\begin{aligned} H_{sd} &= \sum_{i=1}^{n} p_i I_{\varepsilon} = -\sum_{i=1}^{n} p_i \log_2(p_i) \\ &= -D_{xy}(p, v) \times \log_2\left(D_{xy}(p, v)\right) \\ &\quad - \left(1 - D_{xy}(p, v)\right) \times \log_2\left(1 - D_{xy}(p, v)\right). \end{aligned} \tag{13}$$

Similarly, the information entropy of indirect trust value is defined by

$$\begin{aligned} H_{sm} &= \sum_{i=1}^{n} p_i I_e = -\sum_{i=1}^{n} p_i \log_2(p_i) \\ &= -M_{xy}(k, s, n, p, v) \times \log_2\left(M_{xy}(k, s, n, p, v)\right) \\ &\quad - \left(1 - M_{xy}(k, s, n, p, v)\right) \\ &\quad \times \log_2\left(1 - M_{xy}(k, s, n, p, v)\right). \end{aligned} \tag{14}$$

Through the calculation of direct and indirect trust values of information entropy, the certain information can be acquired. The weight distribution is obtained as

$$\begin{aligned} \alpha &= \frac{H_{sm}}{H_{sd} + H_{sm}}, \\ \beta &= \frac{H_{sd}}{H_{sd} + H_{sm}}. \end{aligned} \tag{15}$$

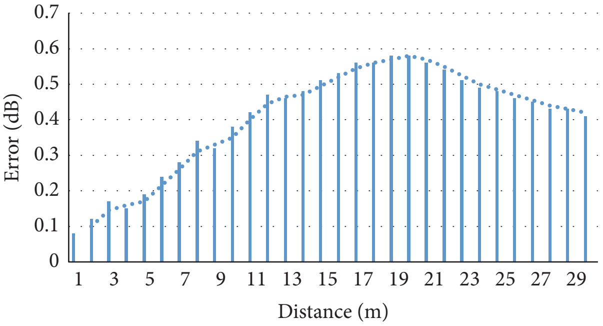


Figure 3: Relationship between distance and error.

3.2. Key Technologies

3.2.1. Attribute Set Selection

(1) Distance Measurement. The difference between measured and actual distances in the WSN positioning obeys to the normal distribution [20]. Therefore, the error function can be defined by

$$\sigma_N(d) = ae^{-(d-d_0)^2/b^2}, \quad (16)$$

where $\sigma_N(d)$ refers to the Gaussian function of distance d. When $d = d_0$, the measurement error reaches its maximal value. In summary, the p_1 attribute of the measured distance value is defined as

$$p_1(d) = \begin{cases} \dfrac{d}{d_0} & d \le d_0, \\ \dfrac{d-d_0}{d_0} & d > d_0. \end{cases} \quad (17)$$

(2) Localization Performance

Definition 9. The unknown node's location reference set is defined as $R = \{(x_1, y_1, d_1), (x_2, y_2, d_2), \ldots, (x_i, y_i, d_i), \ldots, (x_n, y_n, d_n)\}$, where (x_i, y_i) represents the coordinates set of the anchor node i and d_i is the distance between anchor node i and unknown node.

Definition 10. The residual represents the deviation of observed distance value and real distance value, and the total localization residual is defined as

$$\sigma_{\text{sum}} = \sum_{i=1}^{n} \left| \sqrt{(x-x_i)^2 + (y-y_i)^2} - d_i \right|, \quad (18)$$

where x and y represent the measured coordinates of unknown node, x_i, and y_i denote the coordinates of anchor node, and d_i is measured distance between beacon node i and unknown node.

In (18), the coordinates x and y are obtained by the least square method and the least squares regression model [21, 22], while the estimation function is defined by

$$\begin{gathered} d_i^2 = (x-x_i)^2 + (y-y_i)^2 + \eta, \\ (x, y) = \arg\min \sum_{i=1}^{n} \left(\sqrt{(x_i-x_0)^2 + (y_i-y_0)^2} - d_i \right)^2, \end{gathered} \quad (19)$$

where η is the measurement error and $\eta \sim U(-\varepsilon, \varepsilon)$ [23], while ε is the maximal measurement error defined as

$$\max \left| d_i - \sqrt{(x_i-x)^2 + (y_i-y)^2} \right| \le \varepsilon. \quad (20)$$

The residuals are used to indicate the degree of each node's deviation from its true location. The mean residual error is defined as

$$\rho = \frac{\sigma_{\text{sum}}}{n} \le \xi, \quad (21)$$

where n represents the number of anchor nodes involved in positioning. In order to define a threshold, value of ε is needed. When the mean residual error is smaller than the threshold value, the localization result is considered as consistent. Otherwise, the presence of malicious nodes is indicated. The attribute value of localization performance p_2 is defined as

$$p_2 = \begin{cases} \dfrac{\rho}{\zeta}, & \rho \le \zeta, \\ 0, & \rho > \zeta. \end{cases} \quad (22)$$

(3) Detection of Anchor Node Position. Based on (22), the major attacks can be filtered by comprehensive trust value. Nevertheless, in the case of Sybil attack, the above attribute value is not enough to fight against the attack.

Definition 11. The concept of Sybil attack in the WSN indicates that a single node has a multiple identity.

The RSSI signal attenuation model in WSN environment is defined by (8).

According to the attenuation model, the distance ratio can be deduced as

$$\frac{d_r^i}{d_r^j} = 10^{(\text{RSSI}(d_r^i) - \text{RSSI}(d_r^j))/10\lambda}, \quad (23)$$

where d_r^i is the distance between receiver and transmitter. From (23), it can be concluded that the distance ratio is related only to the RSSI difference. Therefore, (23) can be rewritten as

$$\frac{d_r^i}{d_r^j} = f\left(\text{RSSI}\left(d_r^i\right) - \text{RSSI}\left(d_r^j\right)\right). \quad (24)$$

Based on the above analyses, we know that if the distance between receiver and transmitter is constant, the RSSI difference is stable. The positioning in the case of Sybil attack is presented in Figure 4.

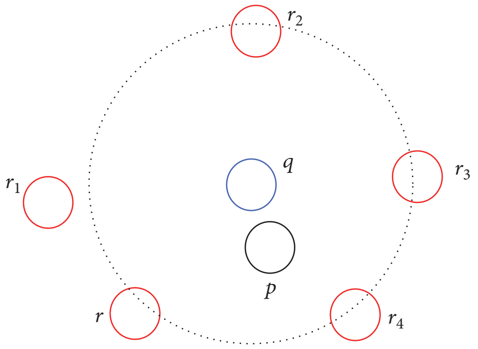


Figure 4: Localization in the case of Sybil attack.

In Figure 4, p is an unknown node, q is an auxiliary judgment node, and r_1, r_2, r_3, and r_4 denote the false localization information, while the anchor node r is the attacked node. The RSSI value is affected by environment; thus, the measured distance between node r and node p will change according to the RSSI fluctuation. Therefore, the auxiliary node q is introduced. According to the above analysis, the difference between RSSI(d_r^p) and RSSI(d_r^q) is stable. Thus, according to (23), the value of d_r^q/d_r^p remains stable.

The coordinates of q are (x_q, y_q), the coordinates of p are (x_p, y_p), and the coordinates of r are (x_r, y_r).

(1) When $k = \pm 1$, (26) can be simplified as (23). According to the form of (27), it can be concluded that the equation represents a straight line.

(2) When $k \neq \pm 1$, (26) can be simplified as (28).

The discriminant of circle defined as $D^2 + E^2 - 4F$ is substituted into (29).

When $k \neq \pm 1$, the result is always greater than zero. In summary, the trajectory of r is a circle or a straight line.

According to the above conclusions, the difference of RSSI is stable only when the faked nodes are distributed strictly in standard circle or straight line. Therefore the difference between RSSI(d_r^p) and RSSI(d_r^q) can be used against the witch attack.

At time moment t_1, node p is an unknown node, nodes q and r are the auxiliary nodes, and nodes s, t are the anchor nodes. In the following moments, t_2 and t_3, RSSI is detected by these values.

Definition 12.

$$\begin{aligned}
&\operatorname{diff}_{t_1}(p,q,r) = \left|\operatorname{RSSI}\left(d_r^p\right) - \operatorname{RSSI}\left(d_r^q\right)\right| \\
&\qquad\qquad \text{when the current moment is } t_1, \\
&\operatorname{diff}_{t_1}(p,q,r,s,t) \\
&\quad = \max\left(\left|\operatorname{diff}_{t_1}(p,q,s) - \operatorname{diff}_{t_1}(p,q,t)\right|,\right. \\
&\quad \left|\operatorname{diff}_{t_1}(p,q,s) - \operatorname{diff}_{t_1}(p,q,t)\right|, \\
&\quad \left.\left|\operatorname{diff}_{t_1}(p,q,s) - \operatorname{diff}_{t_1}(p,q,t)\right|\right), \\
&\operatorname{diff}(p,q,r,s,t) = \max\left(\operatorname{diff}_{t_n}(p,q,r,s,t)\right) \\
&\qquad\qquad 1 \leq n \leq 3.
\end{aligned} \tag{25}$$

Thus, the definition of attribute value p_3 is defined as (30).

$$\begin{aligned}
&\frac{\sqrt{\left(x_r - x_q\right)^2 + \left(y_r - y_q\right)^2}}{\sqrt{\left(x_r - x_p\right)^2 + \left(y_r - y_p\right)^2}} = k \Longrightarrow \\
&\left(x_r - x_q\right)^2 + \left(y_r - y_q\right)^2 = k^2\left(\left(x_r - x_p\right)^2 + \left(y_r - y_p\right)^2\right) \Longrightarrow \\
&\left(k^2 - 1\right)x_r^2 + \left(k^2 - 1\right)y_r^2 - 2x_r\left(x_q - k^2 x_p\right) - 2y_r\left(y_q - k^2 y_p\right) = k^2\left(x_p^2 + y_p^2\right) - \left(x_q^2 + y_q^2\right),
\end{aligned} \tag{26}$$

$$y_r = \frac{x_p - x_q}{y_q - y_p}x_r + \frac{x_q^2 + y_q^2 - x_p^2 - y_p^2}{2\left(y_q - y_p\right)}, \tag{27}$$

$$x_r^2 + y_r^2 - \frac{2\left(x_q - k^2 x_p\right)}{k^2 - 1}x_r + \frac{2\left(y_q - k^2 y_q\right)}{k^2 - 1}y_r + \frac{\left(x_q^2 + y_q^2\right) - k^2\left(x_p^2 + y_p^2\right)}{k^2 - 1} = 0, \tag{28}$$

$$\begin{aligned}
&\frac{4\left(x_q - k^2 x_p\right)^2}{\left(k^2 - 1\right)^2} + \frac{4\left(y_q - k^2 y_p\right)^2}{\left(k^2 - 1\right)^2} - \frac{4\left(x_q^2 + y_q^2\right) - 4k^2\left(x_p^2 + y_p^2\right)}{k^2 - 1} \\
&\quad \Longrightarrow \frac{4x_q^2 - 8k^2 x_q x_p + 4k^4 x_p^2 + 4y_q^2 - 8k^2 y_q y_p + 4k^4 y_p^2}{\left(k^2 - 1\right)^2} - \frac{4\left(x_q^2 + y_q^2\right) - 4k^2\left(x_p^2 + y_p^2\right)}{k^2 - 1}
\end{aligned}$$

$$\begin{aligned}&\Longrightarrow \frac{8x_q^2 - 8k^2 x_q x_p + 8y_q^2 - 8k^2 y_q y_p - 4k^2 x_q^2 - 4k^2 y_q^2 + 4k^2 x_p^2 + 4k^2 y_p^2}{\left(k^2 - 1\right)^2} \\ &\Longrightarrow \frac{4k^2\left(y_p - y_q\right)^2 + 4k^2\left(x_p - x_q\right)^2 + \left(1 + k^2\right)\left(8x_q^2 + 8y_q^2\right)}{\left(k^2 - 1\right)^2},\end{aligned} \tag{29}$$

$$p_3 = \begin{cases} \dfrac{\left|\operatorname{diff}(p, q, r, s, t)\right|}{\tau} & \left|\operatorname{diff}(p, q, r, s, t)\right| \le \tau, \\ 1 & \left|\operatorname{diff}(p, q, r, s, t)\right| > \tau. \end{cases} \tag{30}$$

(4) Transit Time Detection. As it is well known, there are many attacks in the WSN [24, 25], which mainly consist of replayed attacks, Sybil attacks, and wormhole attacks. In these attacks, the certain time is needed to tamper the information. As a result, the time used for positioning will increase. Figure 5 represents the node communication process.

Node p is the source node, while node q is the target node. The observation time of the target node is $T = t_3 - t_2$. Before positioning, the n group of experiment were conducted. In the experiments, a set of times T was obtained. The maximum value $T_{\max}$ was selected from the set.

Based on the experimental results, the definition of attribute value p is obtained by

$$p_4 = \begin{cases} 0 & T > T_{\max}, \\ \dfrac{T}{T_{\max}} & T \le T_{\max}. \end{cases} \tag{31}$$

3.2.2. Discussion on Threshold. In Section 3.2.1, the attribute set selection and calculation processes are presented. Equations (20), (21), and. (26) are all crucial for the threshold. According to (20), the threshold ε and the maximal measurement error should be discussed.

In the environment without obstacles, according to Definition 9, the localization error follows the normal distribution defined by

$$d_E \sim N\left(0, \sigma^2\right). \tag{32}$$

The second parameter of normal distribution is determined in the literature [26]. The relationship between the parameter σ and the distance d can be fitted into the Gaussian function shown as

$$\sigma(d) = ae^{-(d-d_0)^2/b^2}. \tag{33}$$

According to the above analysis, when distance between unknown node and anchor node is d_0, the standard deviation of the distance error reaches the maximum. Therefore, the maximal deviation value between measured and calculated distances can be used as a threshold. The positioning in the presence of obstacles is presented in Figure 6.

In Figure 6, M represents an obstacle between the anchor node p_3 and the unknown node q. According to the trilateral localization algorithm principle, when the RSSI is much smaller than the normal value, the localization fails.

In the case of localization failure, the RSSI values of the nodes are RSSI(p_1q), RSSI(p_2q), RSSI(p_3q), RSSI(p_1p_2), RSSI(p_2p_3), and RSSI(p_1p_3). Because RSSI(p_3q) is much smaller than the normal value, the distance calculated by the distance attenuation model is larger than distance of p_3q.

If $p_3q > p_1p_3 + p_1q$ and $p_3q > p_2p_3 + p_2q$, there is a barrier between node q and node p_3. In the environment with obstacles, the distance between two nodes, which are affected by the obstacles, is the maximal distance between the obstacles. The maximal measurement error can be obtained by derivations as

$$\begin{aligned}\cos\left(\angle p_3p_1p_2\right) &= \frac{p_1p_3^2 + p_1p_2^2 - p_2p_3^2}{2p_1p_3} \times p_1p_2, \\ \cos\left(\angle qp_1p_2\right) &= \frac{p_1q^2 + p_1p_2^2 - p_2q^2}{2p_1q} \times p_1p_2.\end{aligned} \tag{34}$$

At the same time, (35) can be obtained:

$$\begin{aligned}\cos\left(\angle p_3p_1q\right) &= \cos\left(\angle p_3p_1p_2\right)\cos\left(\angle qp_1p_2\right) \\ &\quad + \sin\left(\angle p_3p_1p_2\right)\sin\left(\angle qp_1p_2\right).\end{aligned} \tag{35}$$

According to the values of cos($\angle p_3p_1q$), p_1p_3 and p_1q, p_3q can be obtained by

$$p_3q = \sqrt{p_1q^2 + p_1p_3^2 - 2p_1q \times p_1p_3 \times \cos\left(p_3p_1q\right)}. \tag{36}$$

In an environment with obstacles, $\varepsilon = d_{p_3q} - p_3q$. d_{p_3q} is the distance value obtained by distance attenuation model.

In (21), $\rho = \sigma_{\text{sum}}/n \le \xi$, and threshold ξ is a mean residual.

Definition 13. In the WSN positioning, the reference node set is $Loc\_refer = \{l_1, l_2, l_3, l_4, l_n\}$, and the information frame format of each reference node is $(x_i, y_i, d_{\text{rssi}_i})$, wherein (x_i, y_i) are the reference node coordinates, and d_{rssi_i} is the distance between reference node and unknown node.

According to Definition 13, the localization error of each reference node in the security localization can be obtained by

$$e_i = \left| d_{\text{rssi}_i} - \sqrt{\left(x_i - x\right)^2 + \left(y_i - y\right)^2} \right|, \tag{37}$$

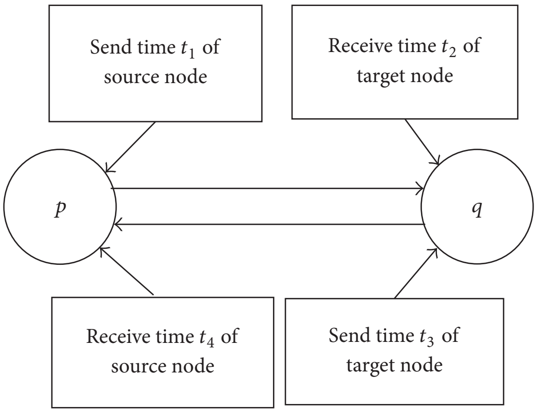

Send time t_1 of source node
Receive time t_2 of target node
p
q
Receive time t_4 of source node
Send time t_3 of target node

Figure 5: Communication process between nodes.

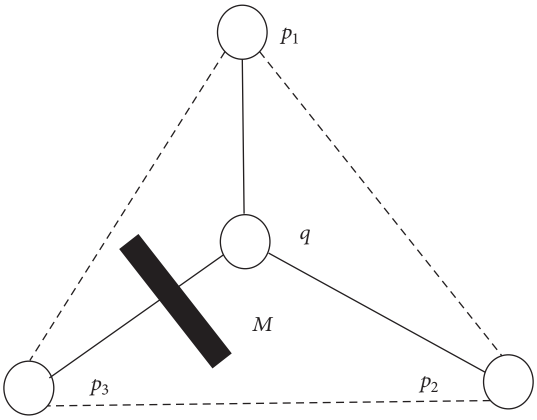


Figure 6: Localization in the presence of obstacles.

where e_i is the localization error of each reference node, and (x, y) refers to the actual position of the unknown node.

$$p_n = \frac{\sum_{i=1}^{n} e_i}{n}. \tag{38}$$

In (38), p_n represents the average localization error, and e_i obeys the normal distribution; thus p_n also obeys the normal distribution. In the experimental environment, the mean μ and the variance σ of the p_n were obtained by the actual measurement.

According to the central limit theorem [27], when $n \to \infty$, the distribution function of $Y_n = (\sum_{k=1}^{n} p_k - n\mu_0)/n\sigma_0$ obeys the standard normal distribution, where $\mu_0 = \mu$, $\sigma_0 = \sqrt{n}\sigma$. If q_n is equal to $n * p_n$, then we may get

$$\lim_{n\to\infty} p\left(\frac{q_n - \mu_0}{\sigma_0} \le x\right) = \Phi(x). \tag{39}$$

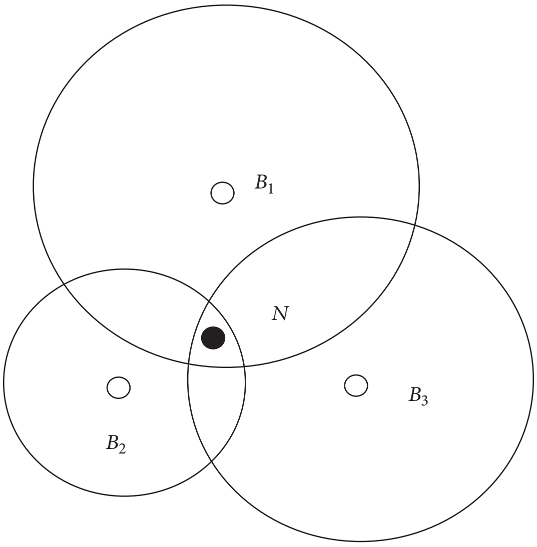


Figure 7: Trilateral-centroid localization.

Based on the above conclusions, (40) can be obtained:

$$\begin{aligned} \lim_{n\to\infty} P(p \le \xi) &= \lim_{n\to\infty} P(q_n \le n\xi) \\ &= \lim_{n\to\infty} \left(\frac{q_n - \mu_0}{\sigma_0} \le \frac{n\xi - \mu_0}{\sigma_0}\right) \\ &= \Phi\left(\frac{n\xi - \mu_0}{\sigma_0}\right). \end{aligned} \tag{40}$$

According to (40), the standard normal distribution can be obtained. Therefore, the standard normal distribution table can be used to set the appropriate threshold ξ in different environments.

3.2.3. Localization Process. According to the trust valuation model, the trust value of each anchor node can be obtained in the communication range of the unknown node. Three anchor nodes with the largest value of trust are used for computing.

Trilateral-centroid localization [28] is used for unknown node localization. The unknown node is N, and the three beacon nodes are B_1, B_2, B_3. Trilateral-centroid localization is shown in Figure 7.

The coordinates of three anchor nodes are (x_1, y_1), (x_2, y_2), and (x_3, y_3). Unknown node coordinate is (x, y). Measurement distance values are d_1, d_2, and d_3. Equation (41) can be listed according to Figure 7:

$$\begin{aligned} \sqrt{(x - x_1)^2 + (y - y_1)^2} &= d_1, \\ \sqrt{(x - x_2)^2 + (y - y_2)^2} &= d_2, \\ \sqrt{(x - x_3)^2 + (y - y_3)^2} &= d_3. \end{aligned} \tag{41}$$

According to (38) and the least square method, unknown node coordinates can be obtained as follows [29]:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_1 - x_3) \, 2(y_1 - y_3) \\ 2(x_2 - x_3) \, 2(y_2 - y_3) \end{bmatrix}^{-1} \cdot \begin{bmatrix} x_1^2 - x_3^2 + y_1^2 - y_3^2 + d_3^2 - d_1^2 \\ x_2^2 - x_3^2 + y_2^2 - y_3^2 + d_3^2 - d_2^2 \end{bmatrix}. \qquad (42)$$

In addition, due to the presence of measurement errors, in some cases, the equations may not be solvable (as shown in Figure 7). In this case, the center of triangle is formed by the intersection of all circles, taken as the coordinates of the unknown point.

There are six intersections among three circles in Figure 8. The coordinates of the three intersection points which are close to the unknown nodes are (x_1, y_1), (x_2, y_2), and (x_3, y_3). The coordinates of the estimated position of the unknown node are (x, y). Thus we can calculate (x, y) via

$$(x, y) = \left(\frac{x_1 + x_2 + x_3}{3}, \frac{y_1 + y_2 + y_3}{3} \right). \qquad (43)$$

4. Simulation and Analysis

4.1. Experiment of Environment Selection and Parameter Setting. Matlab7.0 experimental platform is used as the simulation environment. In this simulation environment, 100 nodes are randomly deployed in the range of 100 m $*$ 100 m [30]. The number of anchor nodes and unknown nodes is 40 and 60, respectively. The communication radius of the nodes is 20 m, and the communication model is the regular pattern. The path loss factor is $\eta = 2.5$ and the range standard deviation is $\sigma = 0.5$.

4.2. Simulation Experiment. In the simulation experiment, three types of nodes are listed as follows: attack node, anchor node, or unknown node. First of all, three groups of experiments are carried out under different environments. The experimental conditions are listed as follows: nonexisting attack nodes, attack nodes existing, and attack nodes existing under trust valuation model.

According to Figures 9, 10, and 11, it can be concluded that the localization error increases with the increasing of attack nodes. When the trust valuation model is added in the localization process, the localization error recovers to normal level.

In addition, the robustness of the model is also investigated. One is attack power and the other is the number of attack nodes.

As can be seen from Figure 12, when the number of attack nodes is less than 20, the localization error of secure localization model is much smaller than normal localization algorithm. However, when the number of attack nodes exceeds 20, the localization error increases sharply, since the attack node produces much fake information with consistency. The system cannot distinguish between malicious nodes and normal nodes through the consistency of the given information.

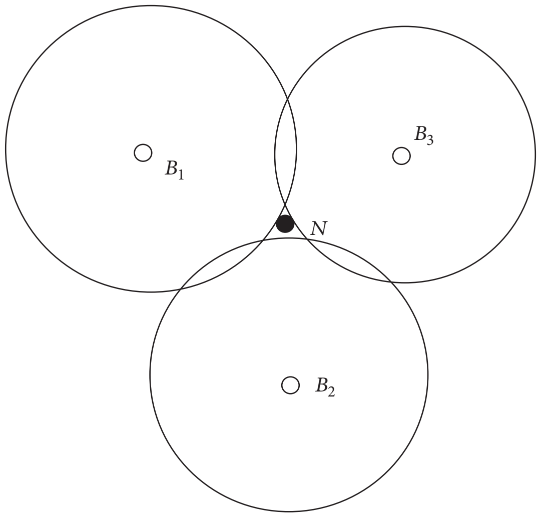


Figure 8: Trilateral-centroid localization.

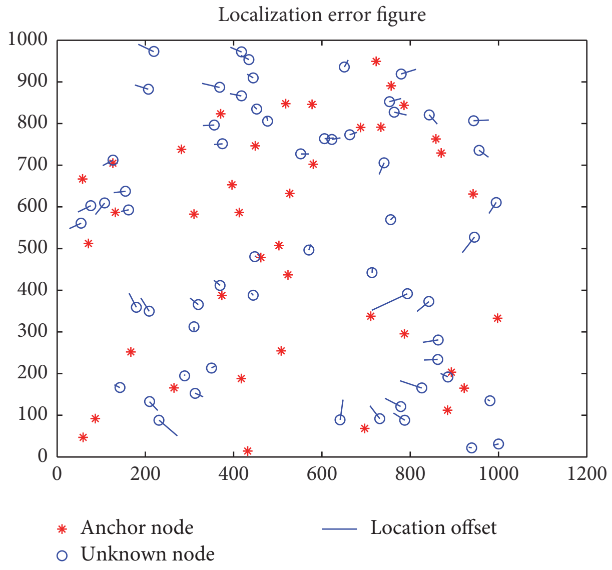


Figure 9: Normal localization.

As can be seen from Figure 13, the localization error of secure localization model remains in a very low level and the localization error of normal localization algorithm increases with the increasing of attack power. The localization error of secure localization model increases with the increasing of attack power, in case the attack power is under 5, with the performance of malicious nodes being similar to normal nodes. However, the system can distinguish between malicious nodes and normal nodes from the values of each attribute with the increasing of attack power. Thus the localization error remains in a low level.

In addition, this algorithm is compared with other secure localization algorithm in localization error.

As can be seen from Figure 14, the overall localization error of this algorithm is smaller than AR-MMSE algorithm. In the AR-MMSE algorithm [31], the localization error

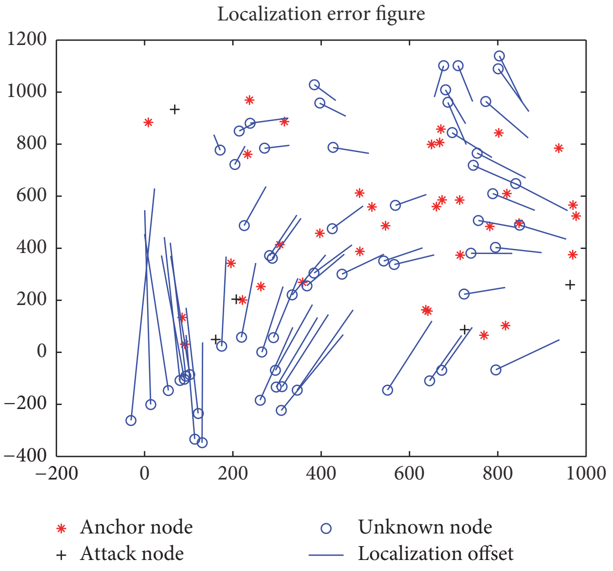


Figure 10: Localization under attack node.

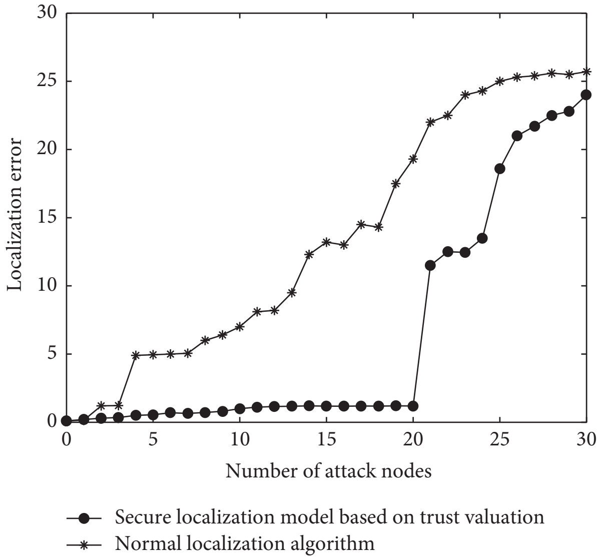


Figure 12: Localization algorithms comparison.

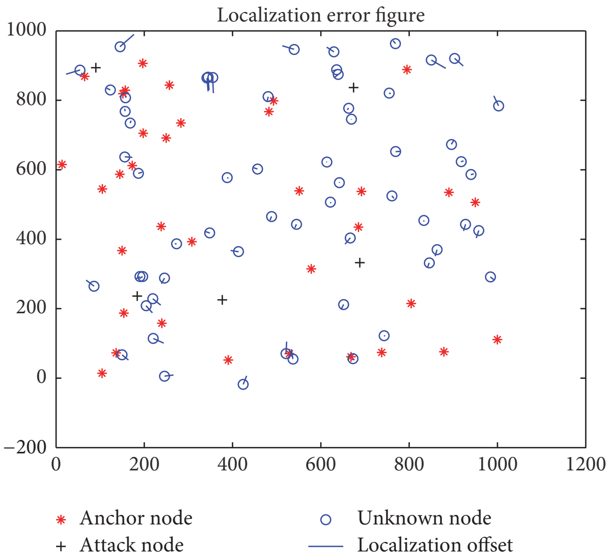


Figure 11: Localization under trust valuation model.

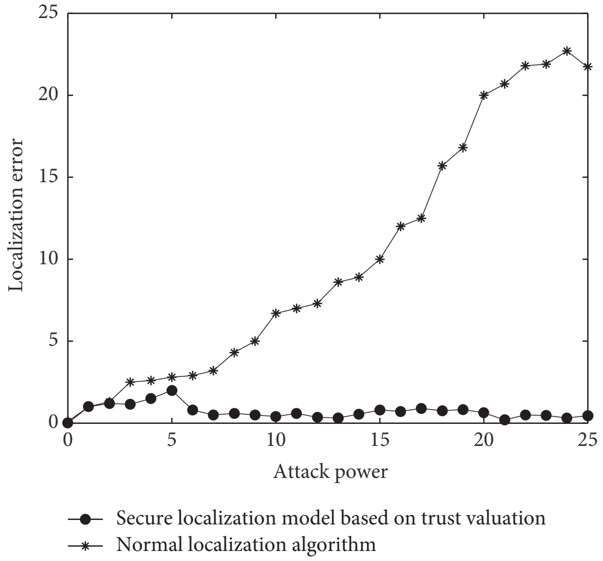


Figure 13: Localization algorithms comparison.

becomes large when the number of malicious nodes exceeds 14. After that, with the increasing of the number of malicious nodes, the localization error is also growing. The algorithm proposed in this paper gets much larger localization error when the number of malicious nodes exceeds 20. AR-MMSE algorithm determines malicious nodes just by the consistency of the location information, while the proposed algorithm is capable of identifying malicious nodes via some additional attributes, such as distance measurement, detection of anchor node position, and detection of transition time.

As can be seen from Figure 15, the trust relationship network becomes tighter as the density of anchor nodes increases. Normal node does not build trust relationship with attack node, so the attack node is removed from the secure localization model.

5. Conclusion

The problem of secure localization is closely related to the structure characteristics and application background in WSN. Traditional security algorithms in WSN are constrained by the limited resources of sensor nodes. Trust management can improve the security and reliability of the localization system with low system overhead. In this paper, a number of attributes related to the localization are adopted and the threshold of the attribute value is discussed to ensure that the method can deal with the internal attacks and a certain degree of collusion attack. This model is superior to the traditional secure localization algorithm based on WSN in the success rate of identifying malicious nodes and performance overhead.

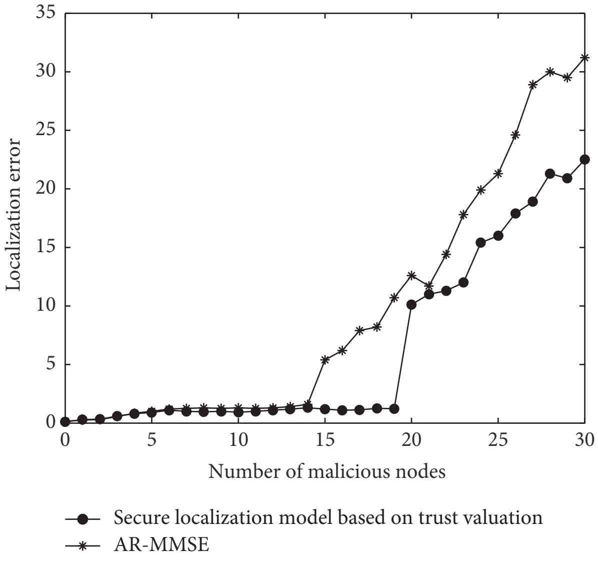


FIGURE 14: Localization algorithms comparison.

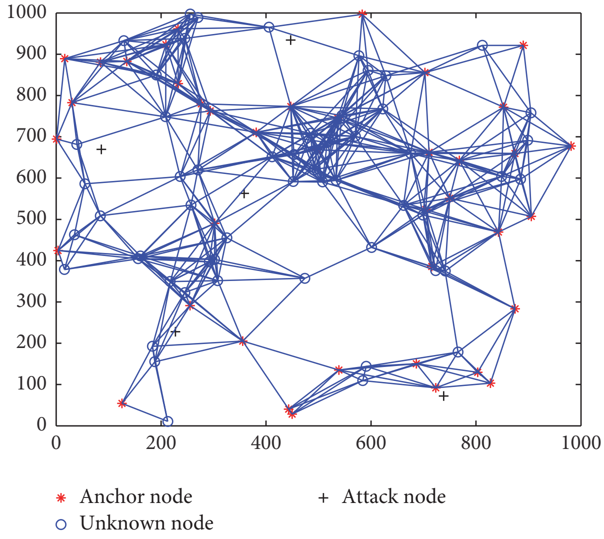


FIGURE 15: Trust relationship.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The subject is sponsored by the National Natural Science Foundation of China (no. 61373017, no. 61572260, no. 61572261, no. 61672296, and no. 61602261), the Natural Science Foundation of Jiangsu Province (no. BK20140886 and no. BK20140888), Scientific & Technological Support Project of Jiangsu Province (no. BE2015702 and no. BE2016777, BE2016185), China Postdoctoral Science Foundation (no. 2014M551636 and no. 2014M561696), Jiangsu Planned Projects for Postdoctoral Research Funds (no. 1302090B and no. 1401005B), Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks Foundation (no. WSNLBZY201508).

References

[1] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 6, pp. 810–823, 2010.

[2] P. R. Vamsi and K. Kant, "Trust and location-aware routing protocol for wireless sensor networks," *IETE Journal of Research*, vol. 62, no. 5, pp. 634–644, 2016.

[3] S. Nandhakumar and N. Malmurugan, "ETIDS: an effective trust based intrusion detection system for wireless sensor networks," *Journal of Computational and Theoretical Nanoscience*, vol. 13, no. 3, pp. 1791–1797, 2016.

[4] N. Labraoui, M. Gueroui, and M. Aliouat, "Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks," *European Transactions on Telecommunications*, vol. 23, no. 4, pp. 303–316, 2012.

[5] W.-W. Chang, T.-J. Sung, H.-W. Huang et al., "A smart medication system using wireless sensor network technologies," *Sensors and Actuators*, vol. 172, no. 1, pp. 315–321, 2011.

[6] J. Wang, R. K. Ghosh, and S. K. Das, "A survey on sensor localization," *Journal of Control Theory and Applications*, vol. 8, no. 1, pp. 2–11, 2010.

[7] K. Jeril, V. Amruth, and N. N. Swathy, "A survey on localization of Wireless Sensor nodes," in *Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES '14)*, pp. 1–6, Chennai, India, February 2014.

[8] M. M. Patel and A. Aggarwal, "Security attacks in wireless sensor networks: a survey," in *Proceedings of the International Conference on Intelligent Systems and Signal Processing (ISSP '13)*, pp. 329–333, Anand, India, March 2013.

[9] A. Ahmed, K. Abu Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A trust aware routing protocol for energy constrained wireless sensor network," *Telecommunication Systems*, vol. 61, no. 1, pp. 123–140, 2016.

[10] E. Goldoni, A. Savioli, M. Risi, and P. Gamba, "Experimental analysis of RSSI-based indoor localization with IEEE 802.15.4," in *Proceedings of the European Wireless Conference (EW '10)*, pp. 71–77, IEEE, Pavia, Italy, April 2010.

[11] R. Garg, A. L. Varna, and M. Wu, "An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 717–730, 2012.

[12] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *Journal of Internet Technology*, vol. 15, no. 6, pp. 929–935, 2014.

[13] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proceedings of the IEEE Symposium on Security and Privacy*, vol. 30, pp. 164–173, 1996.

[14] S. Guo, V. Leung, and Z. Qian, "A permutation-based multi-polynomial scheme for pairwise key establishment in sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '10)*, pp. 1–5, Cape Town, South africa, May 2010.

[15] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1787–1796, 2011.

[16] M. Ye and Y.-P. Wang, "A new malicious nodes attack-resistant security location method in wireless sensor network," *Chinese Journal of Computers*, vol. 36, no. 3, pp. 532–545, 2013.

[17] Y. Guo and X. Liu, "A research on the localization technology of wireless sensor networks employing TI's CC2530 instrument," in *Proceedings of the 11th International Conference on Computational Intelligence and Security (CIS '15)*, pp. 446–449, Shenzhen, China, December 2015.

[18] A. Lewandowski and C. Wietfeld, "A comprehensive approach for optimizing ToA-localization in harsh industrial environments," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS '10)*, pp. 516–525, Indian Wells, Calif, USA, May 2010.

[19] F. G. Mármol and G. M. Pérez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–5, IEEE, Dresden, Germany, June 2009.

[20] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Fingerprinting localization in wireless networks based on received-signal-strength measurements: a case study on wimax networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 283–294, 2010.

[21] S. M. Lasassmeh and J. M. Conrad, "Time synchronization in wireless sensor networks: a survey," in *Proceedings of the Energizing Our Future, IEEE Southeast Con (SOUTHEASTCON '10)*, pp. 242–245, Charlotte-Concord, NC, USA, March 2010.

[22] S. Mohammad Ali and W. Tat-Chee, "Message passing based time synchronization in wireless sensor networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 12, no. 4, pp. 1–21, 2016.

[23] E. Kim and K. Kim, "Distance estimation with weighted least squares for mobile beacon-based localization in wireless sensor networks," *IEEE Signal Processing Letters*, vol. 17, no. 6, pp. 559–562, 2010.

[24] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.

[25] J. Hwang, T. He, and Y. Kim, "Secure localization with phantom node detection," *Ad Hoc Networks*, vol. 6, no. 7, pp. 1031–1050, 2008.

[26] X. Chen, N. C. Rowe, J. Wu, and K. Xiong, "Improving the localization accuracy of targets by using their spatial–temporal relationships in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 72, no. 8, pp. 1008–1018, 2012.

[27] J. Lee, W. Chung, and E. Kim, "A new kernelized approach to wireless sensor network localization," *Information Sciences*, vol. 243, no. 1, pp. 20–38, 2013.

[28] S. Bohidar, S. Behera, and C. R. Tripathy, "A comparative view on received signal strength (RSS) based location estimation in WSN," in *Proceedings of the IEEE International Conference on Engineering and Technology (ICETECH '15)*, pp. 2–5, IEEE, Coimbatore, India, March 2015.

[29] L. Mu, X. Qu, and Z. Zhou, "SARL: a flexible simulation architecture of range-based location in WSN," in *Proceedings of the 35th Chinese Control Conference (CCC '16)*, pp. 8412–8417, Chengdu, China, July 2016.

[30] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 4, pp. 66–77, 2004.

[31] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 4, article 22, 2008.

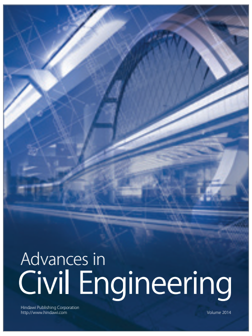
Journal of
Engineering

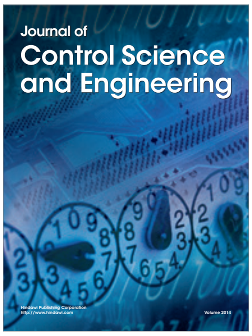
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

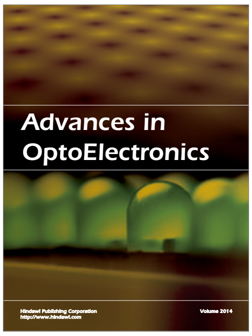
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

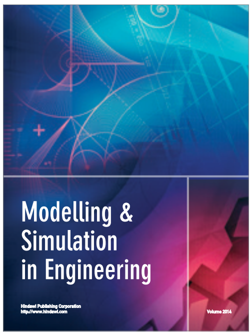
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

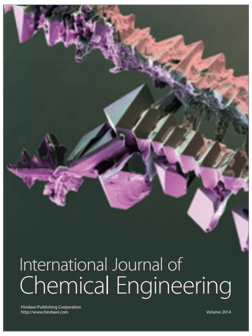

Advances in
OptoElectronics

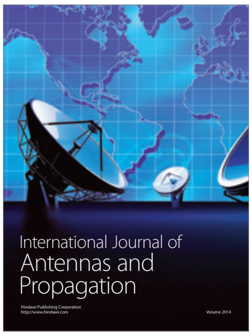
VLSI Design

International Journal of
Navigation and
Observation

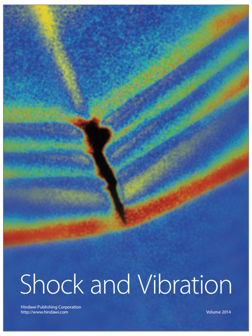

Modelling &
Simulation
in Engineering

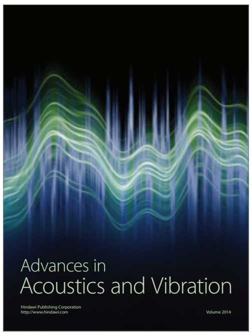
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration