Hindawi
Mobile Information Systems
Volume 2017, Article ID 3243570, 12 pages
https://doi.org/10.1155/2017/3243570

Research Article

A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks

Gulshan Kumar,[1] Mritunjay Kumar Rai,[2] Hye-jin Kim,[3] and Rahul Saha[4]

[1] *School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India*
[2] *School of Electronics and Communication Engineering, Lovely Professional University, Phagwara, Punjab, India*
[3] *Business Administration Research Institute, Sungshin W. University, 2 Bomun-ro 34da gil, Seongbuk-gu, Seoul, Republic of Korea*
[4] *School of Computer Applications, Lovely Professional University, Phagwara, Punjab, India*

Correspondence should be addressed to Hye-jin Kim; hyejinaa@daum.net

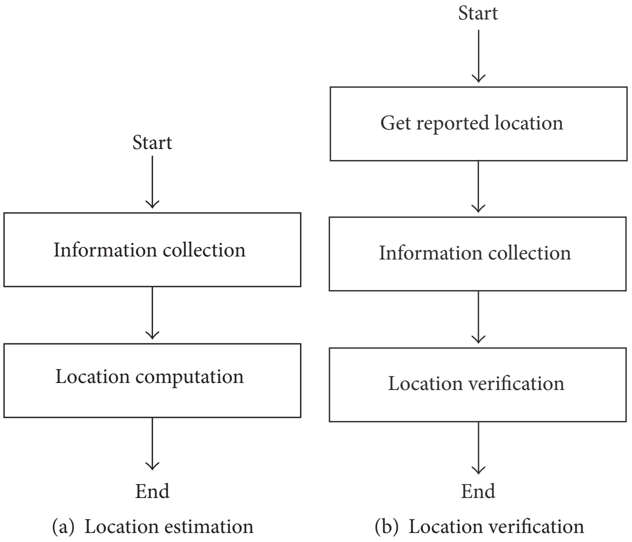
Received 20 September 2016; Accepted 17 November 2016; Published 26 February 2017

Academic Editor: Jaegeol Yim

Localization is a concerning issue in the applications of wireless sensor networks. Along with the accuracy of the location estimation of the sensor nodes, the security of the estimation is another priority. Wireless sensor networks often face various attacks where the attackers try to manipulate the estimated location or try to provide false beacons. In this paper, we have proposed a methodology that will address this problem of security aspects in localization of the sensor nodes. Moreover, we have considered the network environment with random node deployment and mobility as these two conditions are less addressed in previous research works. Further, our proposed algorithm provides low overhead due to the usage of less control messages in a limited transmission range. In addition, we have also proposed an algorithm to detect the malicious anchor nodes inside the network. The simulated results show that our proposed algorithm is efficient in terms of time consumption, localization accuracy, and localization ratio in the presence of malicious nodes.

1. Introduction

Localization [1, 2] defines the calculation of the location or position of sensor nodes in wireless sensor networks (WSNs). The dynamic need of the applications has made the deployment of WSNs extended from static to mobile. Such networks are dynamic and therefore the localization of nodes is also changeable and thus makes the process a critical factor in WSNs. The knowledge of the physical location of a network entity helps in different applications and services [3–5]. The main consideration of location discovery is a set of special nodes known as anchor nodes, which are resource privileged having more storage and computational capacity. Using the location of anchor nodes, other unknown nodes compute their location in different ways. Therefore, it is critical that malicious anchor nodes need to be prevented from providing false location information as the unknown nodes completely depend on the anchor nodes for computing their own location [6]. WSNs attract the adversaries in a very general way. Attacks are executed by the internal nodes as well as external nodes. Therefore, it is compulsory that the localization techniques should be secured enough [7]. The secured localization process must prevent both malicious insider nodes from misrepresenting their location and outside entities from performing intrusion with the location determination process. The security requirements for localization techniques must include privacy of the location information, authorization for legitimate nodes and the integrity to identify any kind of deviation from true location. Further, information availability to compute proper location is also required for a secured localization process. The accuracy of nodes' locations can be considered on the basis of two aspects. On one hand, nodes (anchor or unknown) need to calculate their correct position depending upon some references, which is called localization estimation (Figure 1(a)). On the other hand, the Base Station (BS) also needs to ensure that the location estimations it has received are correct. Thus, we need to verify the locations received from the nodes. This is called location verification (Figure 1(b)). In this paper, we have introduced a secured localization process using mutual



(a) Location estimation (b) Location verification

Figure 1: Localization system.

authentication and validation of insider nodes. The rest of the paper has been organized as follows. Section 2 explains the attack model, that is, the different attacks on localization systems in WSNs. Related work in this line of work has been cited in Section 3. The proposed algorithm is discussed in Section 4 along with the detailed network model and its related assumptions are in Section 5. The results of the simulation have been explained in Section 6. Finally, we have concluded the paper in Section 7.

2. Attack Model

Many attacks [8] have been studied on localization system. Attacks are executed in the information collection process in location estimation phase as well as location verification phase. There are several types of elementary and combinational attacks that can be executed in localization systems. Table 1 summarizes the layer wise attacks in WSNs localization process [9].

2.1. Elementary Attacks. Elementary attacks are the prime attacks which have their own technical aspects of execution. Some of such attacks are discussed below.

Range Change Attack. In this attack an attacker changes the range or Angle of Arrival (AoA) measurements among nodes. This attack affects both localization estimation and location verification systems. For example, reducing or increasing the range measurement between node A and node B will lead to malicious estimation of locations of B shown by green dotted circles in Figure 2.

False Beacon Location Attack. In this attack an attacker makes the victim node receive false estimated locations. For example, an attacker gains control over a beacon or anchor node and then it make the node broadcast false location. False reported location attack is generally executed in a location verification system where a malicious anchor node or unknown node reports false location.

2.2. Combinational Attacks. Combinational attacks are those who merge different technicalities of elementary attacks and create overall malicious affect. Some of the important combinational attacks are listed below.

Impersonation. In this attack an attacker makes its identity be as a legitimate node in the network. For example, in localization systems, an attacker spoofs the anchor nodes' identity and broadcasts false locations. This leads to erroneous range measurements. In location verification systems, an attacker impersonates a victim node to make verifiers believe that the original node is at the attacker's location.

Sybil Attack. In this attack a malicious node has the capability of presenting itself as different identities in a network to function as distinct nodes. These multiple identities are called Sybil nodes. It sends false information like position of beacon nodes and erroneous strength of signal. By masquerading and disguising as multiple identities, this type of malicious node gains control over the network.

Location-Reference Attack. This attack is executed against the localization phase. Each common node gets a location-reference set $\langle \mathrm{loc}_i, d_i \rangle$ for localization where loc_i is the location of beacon i and d_i is the distance between the beacon and the common node. In this attack the attacker makes the compromised beacons broadcast false locations and distorts the distance measurements between beacons and common nodes. The attack can be classified into three types: (a) uncoordinated attack, (b) collusion attack, and (c) pollution attack. Exemplary scenarios are shown in Figures 3(a), 3(b), and 3(c), respectively. Red nodes represent the attacker nodes,

Table 1: Summarization of layer wise attacks on localization in WSNs [9].

Layers	Attacks	Attack behaviour	Results
Physical layer	Stealing	Signal eavesdropping and tampering	Packet error and packet loss
	Jamming	Sending jamming signal in the working frequency range	Packet loss
Data link layer	Collision	Repetition of messages	Packet loss
	Exhaustion	Sending of unnecessary message	Packet loss
	Unfairness	Explicitly take the control of the channel	Packet loss
Network layer	DoS Attacks	Exhaustion of energy of the unknown nodes	Packet loss
	Selective forwarding	Selectively forward packets	Packet loss
	Sybil	Possessing multiple identities	Packet error
	Sinkhole	Maliciously tamper with routing	Packet error
	Wormhole	Shortening the distance to make a fast routing path	Packet loss
Transport layer	Flooding	Establishing false connections	Packet loss
	Tampering	Tampering localization beacons	Packet error

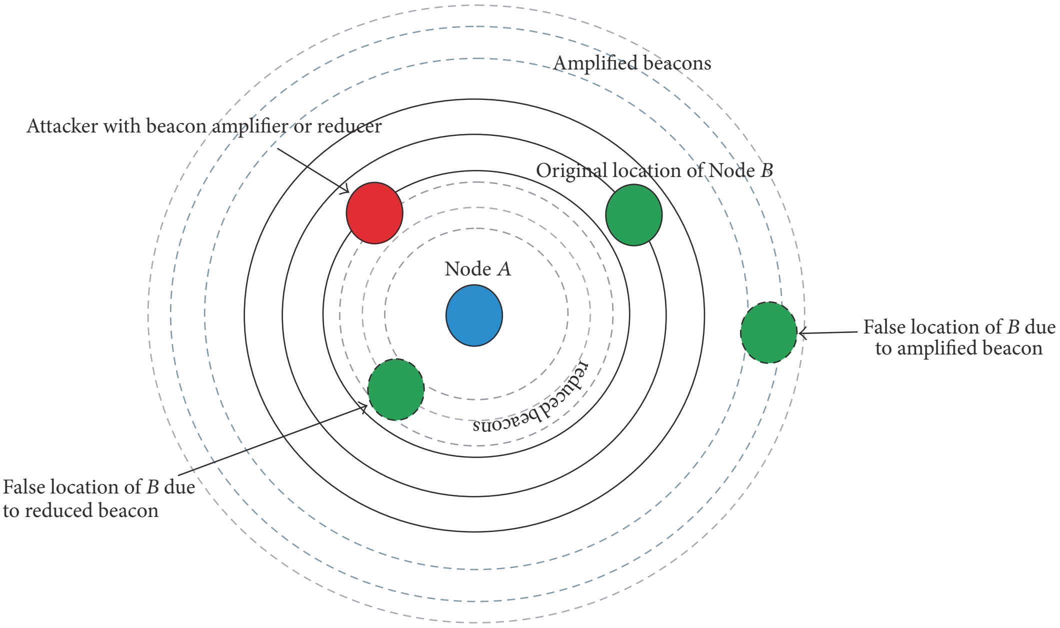

Amplified beacons
Attacker with beacon amplifier or reducer
Original location of Node *B*
Node *A*
False location of *B* due to amplified beacon
reduced beacons
False location of *B* due to reduced beacon

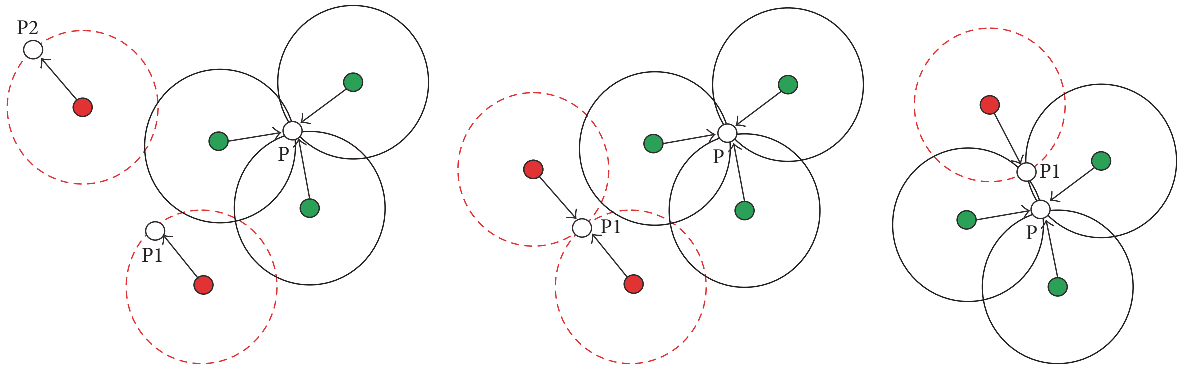
Figure 2: Effects of range change.

green nodes represent beacon nodes, and the white nodes represent common nodes.

In uncoordinated attack, different false location references are provided to mislead the unknown node to different false locations, for example, P1 and P2 in Figure 3(a). In collusion attack, all false location references mislead the common node to the same randomly chosen false location, say P1 in Figure 3(b). In pollution attack, all false location references misguide the unknown node, to a specially chosen false location P1, as in Figure 3(c), which still conforms to some normal location references. This attack succeeds even when normal location references are in the majority. In all the categories as shown in Figure 3, P is the original location.

3. Related Work

Whenever we talk about the secure localization [10] several related problems emerge like location privacy and location reporting. To mitigate the attacks on location identification or location calculation many researchers have proposed different schemes and approaches. They are classified into two types, node-centric and infrastructure-centric. Node-centric approaches deal with the calculation of information at node level. Based on their design goals, existing solutions can be further classified into three methods: (1) the prevention method, to prevent the adversaries from producing erroneous information, for example, HiRLOC [11], SeRLOC [12], ROPE [13], and SPINE [14]; (2) the detection method, to detect



(a) Uncoordinated (b) Collusion (c) Pollution

Figure 3: Location-reference attack variation.

and revoke the nodes producing erroneous information, for example, DRBTS [15], TSCD [16], and LAD [17]; and (3) the filtering method, to filter the received erroneous information in the location computation step such as ARMMSE [18] and i-Multihop [19]. On the other side, infrastructure-centric approaches emphasize the overall network structure for localization security, such as SLA [16] and SLS [20]. If a localization system is infrastructure-centric, the infrastructure will trust the estimation locations and no verification is needed, because the locations are computed by the infrastructure itself. However, if a localization system is node-centric, the nodes may be compromised and may intentionally report false locations. So the infrastructure may not simply trust the reported locations. Thus, when localization system is node-centric, location verification is a sound method for the infrastructure to check the validity of nodes' reported estimation. Different types of secure location verification methods [21] have been introduced such as Sector [22] and Distance Bounding Protocol [23].

Some of the recent research works in this direction have been identified. A very recent collaborative approach for secure localization has been shown in [9]. The proposed approach is based upon a trust model applied for under water wireless sensor networks. A cryptography based approach [24] is used for the secure localization using signature and encryption to provide confidentiality and integrity of the location information. It uses public key infrastructure along with Hash Message Authentication Code (HMAC) digest. Further, trilateration is used to calculate the coordinates of the unknown nodes. The proposed algorithm in [25] uses iterative gradient descent with selective pruning of inconsistent measurements to achieve high localization accuracy. The authors have also shown the accuracy of estimated location in mobile environment but have not emphasized the external nodes or elementary attacks. The proposed algorithm has not addressed the issue of false alarm. Different class of distance based localization algorithms have classified in [26]. The authors have also proposed a polynomial-time algorithm and two heuristic-based algorithms using a threshold value of the compromised nodes. A novel approach of secure localization has been observed in [27]. The authors have used Global Positioning System (GPS) systems and inertial guidance modules on special master node to provide the location accuracy. They have also used an efficient key distribution process in the algorithm. An encryption based secure localization algorithm is shown in [28]. The proposed algorithm, based on Paillier cryptosystem, provides a multilateral privacy preserving solution for secured least square estimation. A novel approach of secured localization using Connected Dominating Set (CDS) is discussed in [29]. Another secure localization technique is shown in [30]. The proposed method uses triangle inequality to detect the attack and then applies localization process based upon some reference points. Both processes use voting mechanism.

A novel approach of using game theory has been applied in [31]. The proposed algorithm combines two methods: Least Trimmed Square (LTS) algorithm is used in regression to identify and remove regression factors which are anomalous and Game Theoretic Aggregation (GTA) solves the problem of combining outputs from a number of predictors to generate a more accurate predictive model. To improve the performance of LTS, a single phase weight-based combination of factors is used by combining GTA with LTS, without any threshold specification. Another game based approach has been shown in [32]. The proposed approach uses trust evaluation and optimal payoff calculation to identify the strategy space of the nodes.

The use of decentralized dynamic key generation for secure localization has been researched in [33]. The proposed algorithm uses symmetric key encryption process with XOR operations and produces robustness with low overhead. A smart card based approach has been utilized in [34]. The proposed algorithm implements a secure and lightweight authentication scheme for heterogeneous wireless sensor networks using smart cards dynamic identities to prevent threats to users' privacy. Mutual trust in wireless sensor network has been discussed in [35]. The algorithm predistributes the random keys securely and uses identity based cryptography. Mutual trust is built up depending upon this identities and keys. A three-tier security framework is shown in [36]. The proposed framework uses two polynomial pools: the mobile polynomial pool and the static polynomial pool. Authentication mechanism used between stationary access nodes and sensor nodes makes it more capable of withstanding to node replication attacks. The node capture attacks and flooding of packets in DV-hop localization are addressed in [37]. The proposed approach has used broadcast authentication and weight-based computation for secure localization purpose. A secure localization algorithm against wormhole attack has been discussed in [38]. The algorithm uses Round Trip Time (RTT) to collect information about the local subgraph. Ordinal Multidimensional Scaling (MDS) is used to adapt the topology changes. A verification method is also used here to minimize the false negatives. Another wormhole resistant localization solution has been observed in [39]. The algorithm uses different labels for pseudoneighbors and identifies the forbidden links. The algorithm is efficient in preventing the attack with the limitation that the nodes must have the identical radii. A number of approaches have been identified in the literature review. Almost all the existing works deal with the static network scenario. They also have a number of drawbacks such as extra hardware usage, more beacons, and control message transmission and predefined knowledge of the network topology. As per the need of mobility in the network environment, the security services in a mobile resource constrained environment are somehow critical to provide and therefore have received a less consideration in the previous works of the researchers. In this paper, we have provided a solution to the problem using an efficient certificate distribution and validation of distance estimation by the Base Station using a very less number of control messages. This will help for the WSNs to provide less overhead, better throughput, and better security from different types of attacks.

4. Proposed Algorithm

Our proposed algorithm considers only the anchor nodes, unknown nodes, and Base Station where anchor nodes and unknown nodes are deployed randomly. The anchors are having a variable range of transmission with an average transmission range R_{avg} given as

$$R_{\text{avg}} = \frac{\min \sum_{e \in E} \psi(|e|)}{m}, \tag{1}$$

where m is the number of anchor nodes in the network, e is an edge between two nodes, E is the set of the edges in the network, and $\psi(|e|)$ is the weighing function of a connection between an anchor node and an unknown node and interpreted as $\psi(|e|) \sim |e|^{\alpha}$, $2 \leq \alpha \leq 4$.

The algorithm starts with an initialization phase that deals with distribution of certificates by the BS. After the distribution of the certificates, distance estimation phase starts among the anchor nodes and the unknown nodes. Once the distances are estimated, the BS is able to localize the unknown nodes applying Minimum Mean Square Error (MMSE) method. The algorithm is summarized in Algorithm 1.

As we have used the speed of light, c, to estimate the distance, the process shown above will prevent the generation of high speed link required to execute wormhole attack because there cannot be any high speed link in which the transmission speed will be more than that of the light. The utilization of mutual authentication with certificates provided by the BS will help to avoid or prevent any kind of authentication attack such as Sybil attack and impersonation attack executed by the outsider nodes. The encryption method will help to securely transmit the estimated distance to the BS. The $t_{\text{retransmit}}$ value will help to detect the jamming attack so that further the avoidance and detection process can applied following the methods as shown in [40]. But it can be a fact that the insider nodes are compromised and can generate distance reduction or enlargement attacks. To prevent these attacks, we have to follow the further process.

Let us assume that the deviation of the true position of the unknown node due to measurement error and/or malicious distance estimates is δ which is tolerable for the system. We know that the unknown node (x_{u_i}, y_{u_i}) must be in the intersection region of the anchor nodes' bound circles in the range. Therefore, in Algorithm 2 we can validate the distance estimation provided by the anchor nodes.

5. Network Model and Assumptions

The network model is considered to be self-organizing having no central control of deploying the sensor nodes in the network. For the ease of presentation, the wireless sensor network model $\mathcal{N}$ is considered to be in 2D and represented by a graph $G(V, E)$ which consists of V, a set of vertices, and E a set of edges. The size of the network can be given as

$$|\mathcal{N}| = |A| + |U|, \tag{2}$$

where $|A|$ is the size of anchor node set A, $|U|$ is the size of the unknown node set U, and $A, U \subseteq V$.

In the proposed algorithm, we have divided the network nodes in two categories of nodes. First, the anchor nodes, $a_j \in A$, which are privileged in their storage capacity and computational capacity with additional energy resources. Secondly, the unknown nodes $u_i \in U$, which are not privileged like the anchor nodes and are able to perform minimum computational tasks. Both types of nodes are randomly deployed in the network environment. The location estimation of an unknown node is calculated by using the location information of the anchor nodes in a WSN. Therefore, the integrity of location messages as well as the reliability of message origin is very important during the localization process. Confidentiality of estimated location is also required in some applications, to protect the privacy of the corresponding sensors. In this paper, an appropriate cryptographic scheme is presented to provide the security services. The assumptions for our proposed approach have been listed below.

(i) The unknown nodes and anchor nodes are mobile.

(ii) Base Station (BS) is assumed to be trusted and is considered to be key distributor and certificate authority.

(iii) Anchor nodes and unknown nodes are deployed with their private keys.

```
Input. anchor node set $A$, unknown node set $U$
Step 1. BS creates identities $\text{ID}_{a_j}$ for all anchor nodes and identities $\text{ID}_{u_i}$ for all unknown nodes
Step 2. BS provides certificates: $\text{Cert}_{a_j}$, $\text{Cert}_{u_i}$
Step 3. $\forall a_j \in A$ do
            $a_j$ sends $u_i$ random nonce $\varkappa$, $\text{Cert}_{a_j}$; for $i = 1, 2, \ldots, n$ and $j = i = 1, 2, \ldots, m$
            $a_j$ waits for a threshold time $t_{\text{retransmit}}$ to retransmit the message
Step 4. $\forall u_i$ under $R_{\text{avg}}$ for any $a_j \in A$
                        $u_i$ sends $a_j$: $[\varkappa, \text{time}_{\text{proc}_u}]_{K_{a_j+}}$, $\text{Cert}_{u_i}$
Step 5. Calculate $\text{time}_{\text{prop}}$
Step 6. $d_{u_i}^{a_j} = c \times \text{time}_{\text{prop}}$
Step 7. $a_j$ sends $d_{u_i}^{a_j}$ to the Base Station (BS)
Step 8. end loop
Step 9. Apply MMSE
```

Algorithm 1: Distance estimation by anchor nodes.

```
Input. Set of anchor nodes $A$ with locations $(x_{a_j}, y_{a_j})$, location estimate of an unknown node $(x_{u_i}, y_{u_i})$, error parameter $\delta$
Step 1. $\forall a_j \in A$, $j = 1, 2, \ldots, m$
If $(\text{true}_{d_{u_i}^{a_j}} - \delta)^2 \le (x_{u_i} - x_{a_j})^2 + (y_{u_i} - y_{a_j})^2 \le (\text{true}_{d_{u_i}^{a_j}} + \delta)^2$
then exit
else go to Step 2
Step 2. calculate the algebraic centre $x^*$ of intersection region $\mathscr{R}$
Step 3. Initialize $r^* = 0$ //radius of the intersection region $\mathscr{R}$ as
Step 4. $\forall v$ inside the region $\mathscr{R}$ do
          if $\|v - r^*\| > r^*$
        then $r^* \leftarrow \|v - r^*\|$
       end if
Step 5. $\forall a_j \in A$, $j = 1, 2, \ldots, m$ do
    $\overline{\overline{\overline{\text{true}_{d_{u_i}^{a_j}}}}} = \dfrac{\text{true}_{d_{u_i}^{a_j}}}{1 + \varepsilon_{\max}}$
Step 6. if $\overline{\overline{\text{true}_{d_{u_i}^{a_j}}}} > \|x^* - a_j\| + r^*$ then
            Anchor node $a_j$ is malicious
       else
            $a_j$ is not malicious
Step 7. end if
```

Algorithm 2: Validation of distance estimation and detection of malicious anchors by BS.

(iv) Base Station (BS) shares the public key only to the legitimate unknown nodes and anchor nodes predefined.

Initialization Phase. Base Station (BS) provides the identity for all anchor nodes and unknown nodes as ID_{a_j} and ID_{u_i} where a_j is an anchor node and u_i is an unknown node. BS also provides certificates for each anchor node and unknown node as Cert_{a_j} and Cert_{u_i}.

$$\text{BS} \longrightarrow \text{Cert}_{a_j} = \left[\text{ID}_{a_j}, K_{a_j+}, t, e_t\right] \text{BS}_{K-}, \qquad (3)$$

where ID_{a_j} is the identity of an anchor node a_j, K_{a_j+} is the public key of that anchor node, t is the timestamp when the certificate was created, and e_t is the expiry time of the certificate. This total certificate is digitally signed by BS_{K-} which is the private key of the Base Station. All anchor nodes must make them update themselves by having a fresh certificate as required. For an legitimate unknown node u_i, we can rewrite the above format in the following way:

$$\text{BS} \longrightarrow \text{Cert}_{u_i} = \left[\text{ID}_{u_i}, K_{u_i+}, t, e_t\right] \text{BS}_{K-}, \qquad (4)$$

where ID_{u_i} is the identity of an unknown node u_i, K_{u_i+} is the public key of that unknown node, and e_t is the expiry time of the certificate.

Distance Estimation Phase. The anchor node a_j sends a random nonce $\varkappa$, along with the certificate Cert_{a_j} to all the one-hop neighborhood unknown nodes u_i in the range R_{avg}

and starts the timer on. When the unknown nodes receive the message, verify the certificate using the public key BS_{K+} given by BS. As, only legitimate anchor nodes are having the certificate to provide, by verifying the certificates, the authentication of the anchor nodes can be proved. Then, the unknown nodes u_i response back to the anchor node a_j with the same nonce $\varkappa$, time duration between of receiving the last bit of message sent by anchor node and transmitting the first bit of message to the anchor node, given as $\mathrm{time}_{\mathrm{proc}_u}$ encrypted with anchor node's public key K_{a_j+} along with its own certificate.

$$\begin{gathered} a_j \longrightarrow u_i : \varkappa, \mathrm{Cert}_{u_i}, \\ u_i \longrightarrow a_j\text{: } \left[\varkappa, \mathrm{time}_{\mathrm{proc}_u}\right]_{K_{a_j+}}, \mathrm{Cert}_{u_i}. \end{gathered} \tag{5}$$

When a_j sends message to u_i, it waits for a bounded time value $t_{\mathrm{retransmit}}$ to retransmit the message if no response starts arriving to the anchor in that bounded time. This value is precomputed at the starting of the network deployment assuming all the favourable conditions of the network environment with a noise effect of Δt and given as

$$t_{\mathrm{retransmit}} = \mathrm{time}_{\mathrm{normal}} + \Delta t, \tag{6}$$

where $\mathrm{time}_{\mathrm{normal}}$ is the normal time duration of getting a response back from the unknown node.

When the anchor node receives the response back from the unknown nodes, it decrypts the message using its own private key K_{a_j-}, verifies the certificate of the unknown nodes, stops the timer, and calculates the signal propagation time as

$$\mathrm{time}_{\mathrm{prop}} = \frac{\left(\mathrm{time}_j - \mathrm{time}_{\mathrm{proc}_u} - \mathrm{time}_{\mathrm{proc}_a}\right)}{2}, \tag{7}$$

where $\mathrm{time}_{\mathrm{prop}}$ is the signal propagation time, time_j is the timer interval at the anchor side, and $\mathrm{time}_{\mathrm{proc}_a}$ is the time duration between receiving the first bit of the response and last bit of the response. The interaction between unknown node and anchor node is shown in Figure 4.

Once the propagation time is calculated, the estimated distance between anchor node a_j and unknown node u_i is calculated as

$$d_{u_i}^{a_j} = c \times \mathrm{time}_{\mathrm{prop}}, \quad \text{where } c \text{ is the speed of light.} \tag{8}$$

Once the anchor node calculates this estimated distance, it is then forwarded to the BS encrypted with the public key of BS and along with the anchor node's certificate.

$$a_j \longrightarrow \mathrm{BS} : \left[d_{u_i}^{a_j}\right]_{\mathrm{BS}_{K+}}, \mathrm{Cert}_{a_j}. \tag{9}$$

After receiving the message from the anchor nodes, BS decrypts the message with is private key and gets the estimated distances. Finally, it uses Minimum Mean Square Error (MMSE) [41] to estimate the location of an unknown node (x_{u_i}, y_{u_i}). One thing needs to remember is that we need at least three noncollinear anchor nodes to apply MMSE. Another important attribute of our proposed algorithm deals with the mobility of the nodes. We consider that the nodes (whether the anchor or the unknown) are mobile. The relative mobility between an unknown node u_i and anchor node a_j at a given time t is given by

$$\mathrm{RM}_t^{a,u} = d_{a,u_t} - d_{a,u_{t-1}} \tag{10}$$

$\mathrm{RM}_t^{a,u}$ is positive if node u_i is moving away from a_j and negative if u_i is coming closer to a_j.

Though the mobility is incorporated in the algorithm, nodes (both the anchor nodes and the unknown nodes) are assumed to be pseudostatic; that is, they are static for a very short time interval for the localization process and this does not incorporate any significant error in the estimation.

Handling Distance Estimation Error. Distance estimations in a wireless environment are very common to have error due to the noise or delay in the medium. Assume that the estimation error is $\epsilon \in [-\epsilon_{\max}, \epsilon_{\max}]$, where $\epsilon_{\max}$ is a system parameter and given as $0 \le \epsilon_{\max} \le 1$. Therefore, the estimated distance can be given as

$$d_{u_i}^{a_j} \in \left[\mathrm{true}_{d_{u_i}^{a_j}} \times \left(1 - \epsilon_{\max}\right), \mathrm{true}_{d_{u_i}^{a_j}} \times \left(1 + \epsilon_{\max}\right)\right], \tag{11}$$

where $\mathrm{true}_{d_{u_i}^{a_j}}$ is the true distance between a_j and u_i and can be calculated by applying Euclidean method.

Further, the presence of compromised insider anchor nodes can create an error factor θ. Following this, the estimated distance between a_j and u_i in presence of malicious anchor node can be given as

$$d_{u_i}^{a_j} = \mathrm{true}_{d_{u_i}^{a_j}} \times \left(1 + \epsilon_{\max}\right) \times (1 + \theta), \quad \text{for } \theta > 0. \tag{12}$$

As we know that $\epsilon \in [-\epsilon_{\max}, \epsilon_{\max}]$, the value of ϵ can create both the positive estimation error and negative estimation error. Positive estimation error will create multiple intersection points of the convex region of the anchor nodes' ranges leading to the distance enlargement attacks. On the other hand, negative estimation error creates an empty intersection region assuming that the location of the unknown node is in the intersection of bounds of anchors leading to the distance reduction attack. This concept is shown in Figure 5. The black solid circles are anchor nodes and green circle is the original estimated location. If the anchor nodes are compromised and provide reduced distance estimations, the intersection will be empty and if the malicious anchor nodes provide enlarged distance estimations, the position of the unknown node deviates from the original position shown as light blue circle.

Distance reduction is not a severe in WSN localization. If we find the empty intersection region $\mathscr{R}$, the distance estimates can be increased with a factor of $1/(1-\varepsilon_{\max})$ to get a nonempty intersection region $\mathscr{R}'$, where the unknown node must exist.

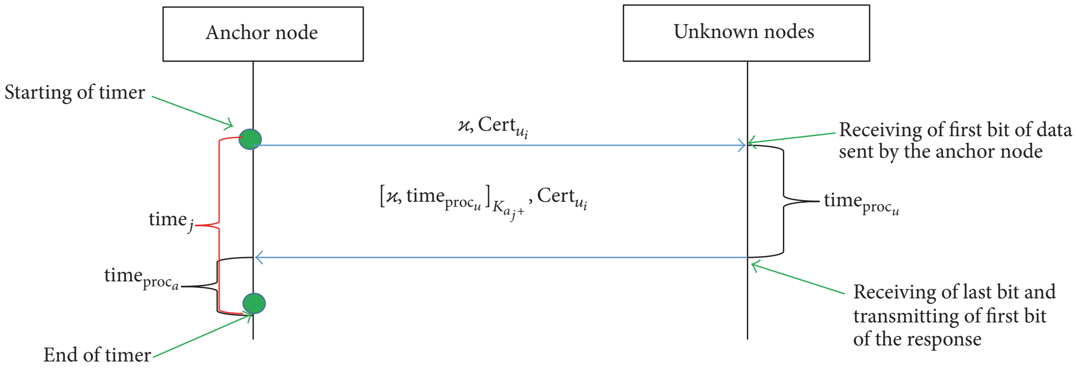
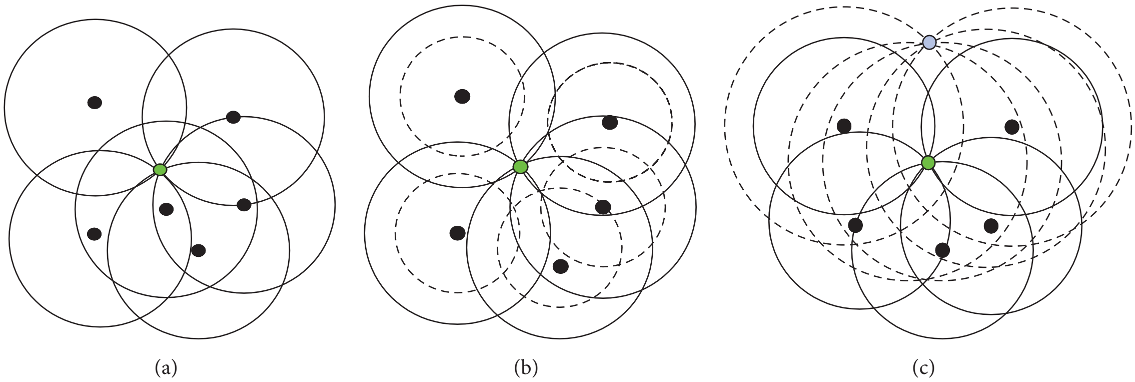

Anchor node
Unknown nodes
Starting of timer
$\varkappa$, Cert_{u_i}
Receiving of first bit of data sent by the anchor node
$[\varkappa, \text{time}_{\text{proc}_u}]_{K_{a_j+}}$, Cert_{u_i}
time_j
$\text{time}_{\text{proc}_u}$
$\text{time}_{\text{proc}_a}$
Receiving of last bit and transmitting of first bit of the response
End of timer

Figure 4: Propagation time estimation process.


(a)

(b)

(c)

Figure 5: (a) Truthful estimation. (b) Distance reduction. (c) Distance enlargement.

To prevent distance enlargement situation, the BS need to follow the process summarized in Algorithm 2. The tolerable error parameter δ can be derived from the following equation as

$$\delta = w_1 \epsilon + w_2 \theta, \qquad (13)$$

where ϵ is the system measurement error due to noise and θ is the error included by malicious anchor nodes. We assume that the unknown nodes are error free and do not provide any false distance estimation. w_1, w_2 are used as weighing values for the errors depending upon the network conditions. This δ will provide an upper bound and lower bound of the estimated distance in presence of error given as

$$\begin{aligned}\left(\text{true}_{d_{u_i}^{a_j}} - \delta\right)^2 &\leq \left(x_{u_i} - x_{a_j}\right)^2 + \left(y_{u_i} - y_{a_j}\right)^2 \\ &\leq \left(\text{true}_{d_{u_i}^{a_j}} + \delta\right)^2, \qquad (14) \\ \text{true}_{d_{u_i}^{a_j}} &= \sqrt{\left(x_{u_i} - x_{a_j}\right)^2 + \left(y_{u_i} - y_{a_j}\right)^2}.\end{aligned}$$

The algebraic centre x^* in Algorithm 2 can be calculated using barrier method on the unconstrained optimization problem given as

$$\begin{aligned}\min \quad & (x, \delta) - \lambda \cdot \delta \\ & - \sum_{j=1}^{m} \log \left[\left(\overline{\text{true}_{d_{u_i}^{a_j}}} \cdot (1 - \delta) \right)^2 - \left\| x - a_j \right\|^2 \right] \qquad (15) \\ & - \log (\delta),\end{aligned}$$

where λ is the Lagrangian multiplier and $\overline{\text{true}_{d_{u_i}^{a_j}}}$ is given by $\overline{\text{true}_{d_{u_i}^{a_j}}} = \text{true}_{d_{u_i}^{a_j}} / (1 - \varepsilon_{\max})$, that is, the increased distance estimation in case of negative estimation error.

The radius of the intersection region $\mathscr{R}$ is initialized with 0 with an assumption that the unknown node is positioned at the intersection point itself and no convex region has been generated by the intersection. Moreover, the radius of the intersection region can be updated by verifying the distance between any point v inside the region and the algebraic centre x^*. Finally, we can detect the malicious insider anchor nodes depending upon the increased estimated distance.

So the attacks, those are identified in localization process as shown in Table 1, are addressed in the proposed model. The

Table 2: Prevention of attacks by the proposed model.

Attacks	Attack behaviour	Prevention by our proposed model
Stealing	Signal eavesdropping and tampering	Our proposed model uses encryption to prevent such attacks
Jamming	Sending jamming signal in the working frequency range	Detection is addressed in the proposed algorithm
Collision	Repetition of messages	Not applicable in the proposed model, as the maximum calculation is done by BS and anchor node with minimum message controls
Exhaustion	Sending of unnecessary message	No scope to provide unnecessary message as transmission range is limited to and the distance estimation process is secured
Unfairness	Explicitly taking the control of the channel	Not possible due to the minimum size of the packets
DoS Attacks	Exhaustion of energy of the unknown nodes	Can be monitored directly by the Base Station
Selective forwarding	Selectively forward packets	Using the approach of one-hop neighborhood forwarding is not necessary
Sybil	Possessing multiple identities	Mutual authentication is used
Sinkhole	Maliciously tamper with routing	Mutual authentication is used with the certificates
Wormhole	Shortening the distance to make a fast routing path	The distance estimation is done based upon the light speed which is the maximum speed of transmission can be and therefore no faster route can be created between an anchor and an unknown node
Flooding	Establishing false connections	Broadcasting is limited by the anchor nodes within a limited range of R_{avg}
Tampering	Tampering localization beacons	Both encryption and mutual authentication are used
Insider attack	Compromised anchor nodes may provide false information	Both the distance reduction and distance enlargement attack have been addressed
Range change attack	Changing the range or Angle of Arrival (AoA)	Our proposed model does not incorporate the mechanism of AoA as it works on time interval to calculate the distance and therefore can easily avoid such attack
False beacon location attack	Compromising a beacon and then he can make the beacon broadcast false location	Authentication, limited range, and validation of distance estimation in the proposed approach will help to avoid such attack
False reported location attack	Malicious node reports false	Verification is done at the BS, so there is less chance to report falsified verification

Table 3: Simulation parameters.

Simulation area	500 m × 500 m
Number of unknown nodes	500
Communication range	120 m
Node deployment	Random
Mobility model	Random Way Point model

summarization of countermeasures by our proposed model has been shown in Table 2.

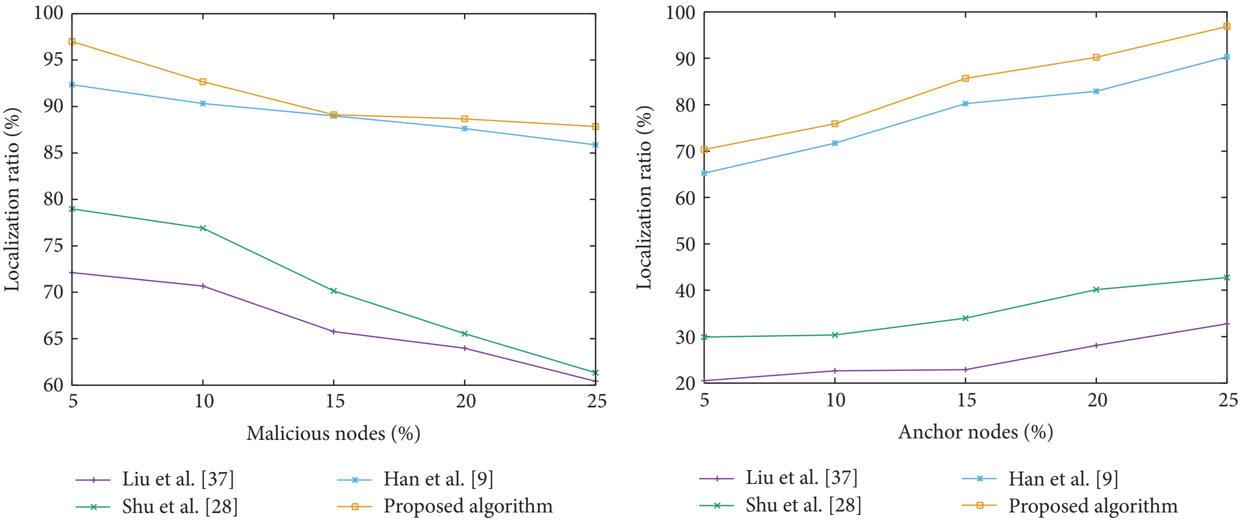
6. Results and Discussion

In this section, we have evaluated the proposed algorithm based on the parameters as shown in Table 3.

We have compared the simulated results with the three recent algorithms: (1) Collaborative Secure Localization algorithm based on Trust model (CSLT) proposed by Han et al. [9], (2) Multilateral Privacy Algorithm (MPA) for secured localization proposed by Shu et al. [28], and (3) Authenticated Weight-based Secured (AWS) DV-hop proposed by Liu et al. [37]. The performances of the algorithms are measured on the following three parameters: localization efficiency, localization accuracy, and malicious detection ratio.

The attacks described in Table 2 are also simulated to show the efficiency of the proposed algorithm. The localization ratio is defined as the percentage of successful location estimation of unknown nodes. The result in Figure 6(a) shows that, with the increasing malicious nodes' percentage, every algorithm in our comparison faces a significant decrease in successful localization of unknown nodes. However, the proposed algorithm still performs better as compared to others. Figure 6(b) shows that the proposed algorithm outperforms the other algorithms in the successful localization of unknown nodes with the increasing percentage of anchor nodes. Localization accuracy is a valuable metric for evaluating the efficiency of localization algorithms.

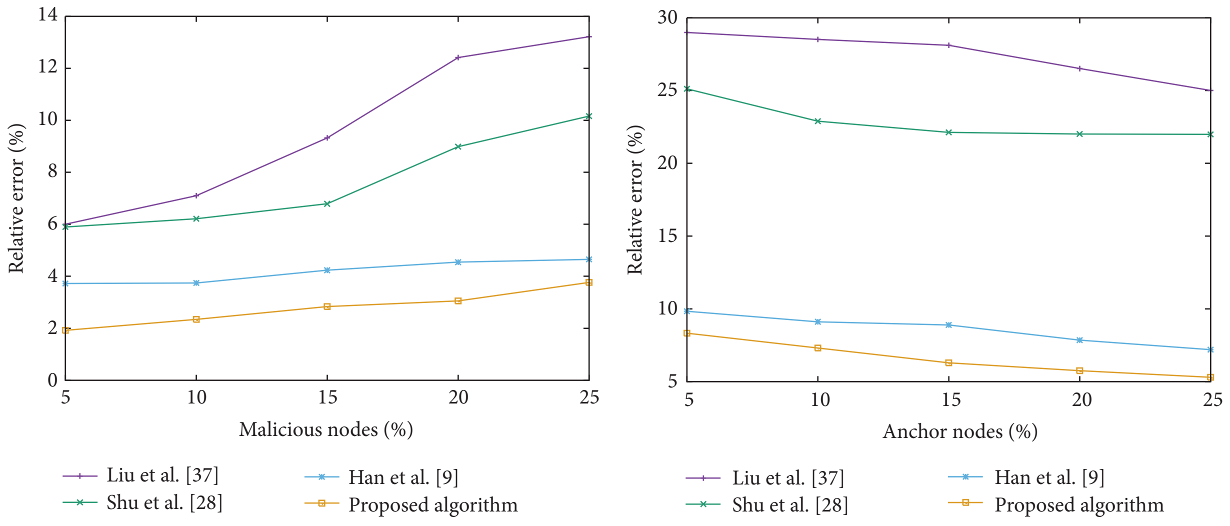
In the proposed work, the localization accuracy is defined by the relative error between the actual location and the calculated node position. In our simulation, we have varied the ratio of malicious nodes from 5% to 30% with increments



(a)

(b)

Figure 6: Comparison of localization ratio: (a) impact of malicious nodes and (b) impact of anchor nodes.



(a)

(b)

Figure 7: Comparison of localization accuracy: (a) impact of malicious nodes and (b) impact of anchor nodes.

of 5%. Simulation result, shown in Figure 7(a), shows that the relative error percentage of location estimation increases with the increasing number of malicious nodes. However, the proposed algorithm proves its efficiency in location estimation accuracy. Similarly, location accuracy is also tested by varying the anchor nodes' percentage. Result shown in Figure 7(b) signifies to the fact that the proposed algorithm significantly reduces the relative error percentage with the increasing number of anchor nodes. It is also seen in the result that the other algorithms also decrease the relative error with the increasing number anchor nodes, but the percentage of relative error is less in our proposed algorithm.

Simulation time is defined as the time taken for the algorithms to detect a particular malicious attack. The result in Figure 8 shows that the proposed algorithm is efficient in detecting 90% of the malicious attack with less time as compared to the other algorithms in comparison.

7. Conclusion

Security in localization has always been a vital part of localization algorithms. Though there are a number of algorithms which are introduced with security aspects, but the algorithm designers have somehow overlooked the complexity issue of the algorithms in the resource constrained WSNs. In this paper, we have addressed this problem and provided a solution with our proposed algorithm. The proposed algorithm not only prevents a number of outsider attacks but

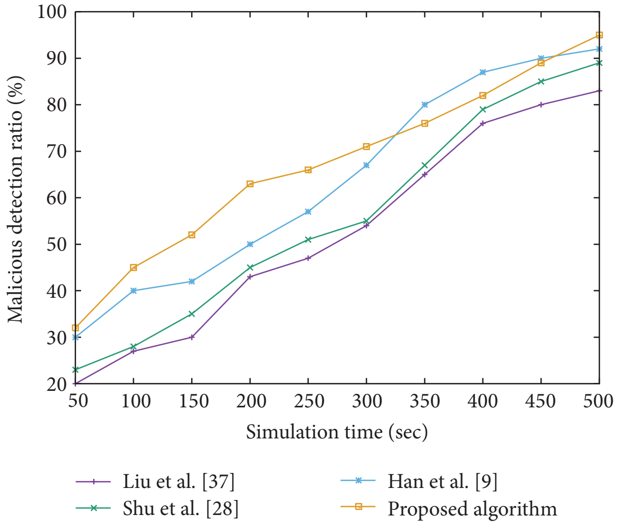


Figure 8: Comparison of malicious detection ratio.

also provides a check on the insider nodes. Moreover, the algorithm provides low overhead and major functionality is based on Base Station. The simulation results also prove the efficiency of the proposed algorithm in terms of localization efficiency, localization accuracy, and malicious detection ratio. The most important feature of our algorithm is that it supports mobility of the nodes and therefore it is suitable for dynamic network environments.

Competing Interests

The authors declare that they have no competing interests.

References

[1] D. Niculescu and B. Nath, "Localized positioning in ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 247–259, 2003.

[2] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkon-Jak, "Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pp. 106–116, 2001.

[3] D. D. Perkins, R. Tumati, H. Wu, and I. Ajbar, "Localization in wireless ad hoc networks," in *Resource Management in Wireless Networking*, pp. 507–542, Kluwer Academic Publishers, Boston, Mass, USA, 2005.

[4] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular ad hoc networks: a new challenge for localization-based systems," *Computer Communications*, vol. 31, no. 12, pp. 2838–2849, 2008.

[5] K. K. Chintalapudi, "On the feasibility of Ad-Hoc localization systems," Tech. Rep. 117, Computer Science Department, University of Southern California, Los Angeles, Calif, USA, 2003.

[6] G. Kumar and M. K. Rai, "An energy efficient and optimized load balanced localization method using CDS with one-hop neighbourhood and genetic algorithm in WSNs," *Journal of Network and Computer Applications*, vol. 78, pp. 73–82, 2017.

[7] X.-M. Cao, B. Yu, G.-H. Chen, and F.-Y. Ren, "Security analysis on node localization systems of wireless sensor networks," *Journal of Software*, vol. 19, no. 4, pp. 879–887, 2008.

[8] J. Jiang, G. Han, C. Zhu, Y. Dong, and N. Zhang, "Secure localization in wireless sensor networks: a survey (Invited Paper)," *Journal of Communication*, vol. 6, p. 123, 2011.

[9] G. Han, L. Liu, J. Jiang, L. Shu, and J. J. P. C. Rodrigues, "A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks," *Sensors*, vol. 16, no. 2, article 229, 2016.

[10] A. Srinivasan and J. Wu, "A survey on secure localization in wireless sensor networks," in *Encyclopedia of Wireless and Mobile Communications*, p. 126, CRC Press, 2007.

[11] L. Lazos and R. Poovendran, "HiRLoc: high-resolution robust localization for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, 2006.

[12] L. Lazos and R. Poovendran, "SeRLoc: secure range-independent localization for wireless sensor networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04)*, pp. 21–30, Philadelphia, Pa, USA, October 2004.

[13] L. Lazos, R. Poovendran, and S. Čapkun, "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, IEEE, April 2005.

[14] S. Capkun and J. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[15] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: distributed reputation-based beacon trust system," in *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06)*, pp. 277–283, IEEE, Indianapolis, Ind, USA, October 2006.

[16] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 195–203, Washington, DC, USA, November 2005.

[17] W. Du, L. Fang, and P. Ning, "LAD: localization anomaly detection for wireless sensor networks," in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS '05)*, p. 41, IEEE, April 2005.

[18] D. Liu, P. Ning, and W. K. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 99–106, IEEE, April 2005.

[19] C. Wang and L. Xiao, "Sensor localization in concave environments," *ACM Transactions on Sensor Networks*, vol. 4, no. 1, article 3, 2008.

[20] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 4 I, pp. 829–835, 2006.

[21] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM Workshop on Wireless Security (WiSE '03)*, p. 110, San Diego, Calif, USA, 2003.

[22] S. Čapkun, L. Buttyn, and J.-P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 21–32, 2003.

[23] K. B. Rasmussen and S. Čapkun, “Location privacy of distance bounding protocols,” in *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS ’08)*, pp. 149–160, ACM, Alexandria, VA, USA, October 2008.

[24] T. Zhang, J. He, X. Li, and Q. Wei, “A signcryption-based secure localization scheme in wireless sensor networks,” *Physics Procedia*, vol. 33, pp. 258–264, 2012.

[25] 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.

[26] 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.

[27] Q. Mi, J. A. Stankovic, and R. Stoleru, “Practical and secure localization and key distribution for wireless sensor networks,” *Ad Hoc Networks*, vol. 10, no. 6, pp. 946–961, 2012.

[28] T. Shu, Y. Chen, and J. Yang, “Protecting multi-lateral localization privacy in pervasive environments,” *IEEE/ACM Transactions on Networking*, vol. 23, no. 5, pp. 1688–1701, 2015.

[29] A. Srinivasan, “SecLoc—secure localization in WSNs using CDS,” *Security and Communication Networks*, vol. 4, no. 7, pp. 763–770, 2011.

[30] W. T. Zhu, Y. Xiang, J. Zhou, R. H. Deng, and F. Bao, “Secure localization with attack detection in wireless sensor networks,” *International Journal of Information Security*, vol. 10, no. 3, pp. 155–171, 2011.

[31] S. Jha, S. Tripakis, S. A. Seshia, and K. Chatterjee, “Game theoretic secure localization in wireless sensor networks,” in *Proceedings of the International Conference on the Internet of Things (IOT ’14)*, pp. 85–90, IEEE, Cambridge, Mass, USA, October 2014.

[32] T. Bao, J. Wan, K. Yi, and Q. Zhang, “A game-based secure localization algorithm for mobile wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 642107, 8 pages, 2015.

[33] Z. Merhi, A. Haj-Ali, S. Abdul-Nabi, and M. Bayoumi, “Secure localization for wireless sensor networks using decentralized dynamic key generation,” in *Proceedings of the 8th International Wireless Communications and Mobile Computing Conference (IWCMC ’12)*, pp. 543–548, 2012.

[34] C.-C. Chang, W.-Y. Hsueh, and T.-F. Cheng, “A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks,” *Wireless Personal Communications*, vol. 89, no. 2, pp. 447–465, 2016.

[35] C.-H. Lin, Y.-H. Huang, A. D. Yein, W.-S. Hsieh, C.-N. Lee, and P.-C. Kuo, “Mutual trust method for forwarding information in wireless sensor networks using random secret pre-distribution,” *Advances in Mechanical Engineering*, vol. 8, no. 4, pp. 1–9, 2016.

[36] A. Rasheed and R. N. Mahapatra, “The three-tier security scheme in wireless sensor networks with mobile sinks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 5, pp. 958–965, 2012.

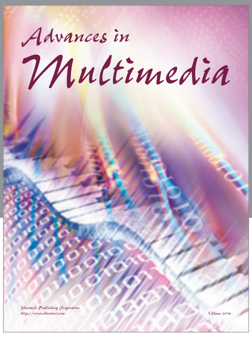
[37] X. Liu, R. Yang, and Q. Cui, “An efficient secure DV-Hop localization for wireless sensor network,” *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 275–284, 2015.

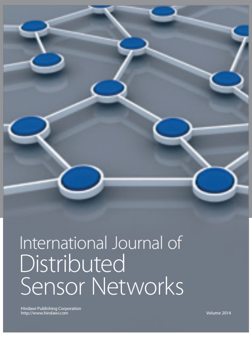
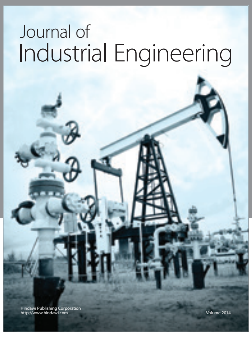
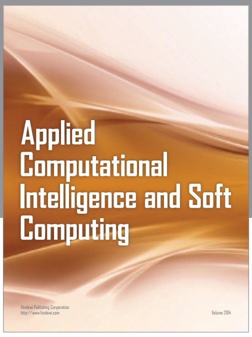
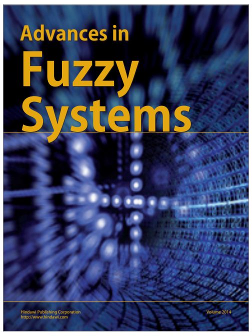
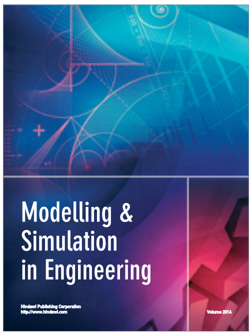
[38] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, “Wormhole detection based on ordinal MDS using RTT in wireless sensor network,” *Journal of Computer Networks and Communications*, vol. 2016, Article ID 3405264, 15 pages, 2016.

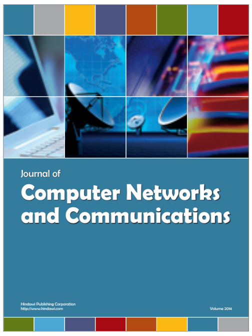
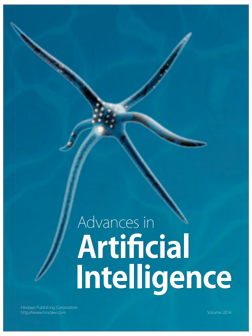
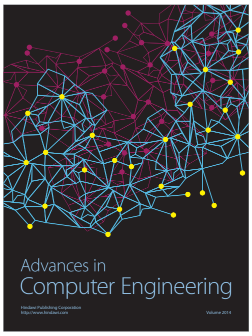
[39] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, “Securing DV-Hop localization against wormhole attacks in wireless sensor networks,” *Pervasive and Mobile Computing*, vol. 16, pp. 22–35, 2015.

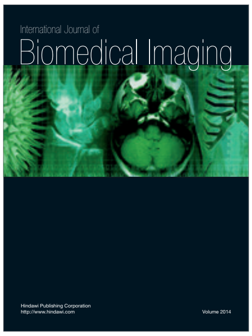
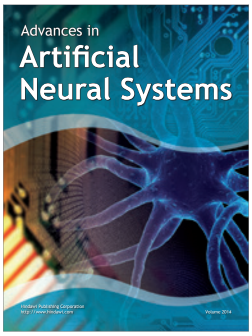
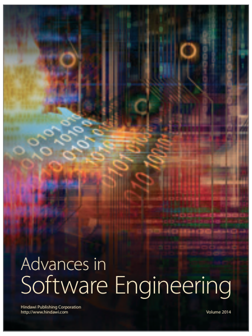
[40] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: attack and defense strategies,” *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

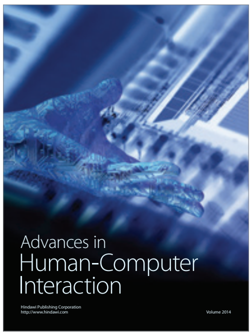
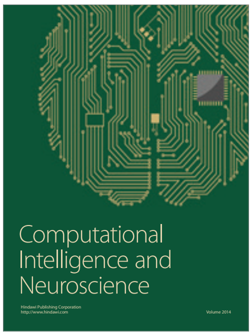
[41] A. Savvides, C.-C. Han, and M. B. Strivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors,” in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 166–179, July 2001.


Advances in
Multimedia

The Scientific
World Journal

International Journal of
Distributed
Sensor Networks

Journal of
Industrial Engineering

Applied
Computational
Intelligence and Soft
Computing

Advances in
Fuzzy
Systems

Modelling &
Simulation
in Engineering


Journal of
Computer Networks
and Communications

Advances in
Artificial
Intelligence

Advances in
Computer Engineering

International Journal of
Computer Games
Technology

International Journal of
Biomedical Imaging

Advances in
Artificial
Neural Systems

Advances in
Software Engineering

Journal of
Robotics

Advances in
Human-Computer
Interaction

Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering