Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9935780, 11 pages
https://doi.org/10.1155/2021/9935780

Research Article

A Novel Privacy-Preserving Mobile-Coverage Scheme Based on Trustworthiness in HWSNs

Chunyang Qi,[1] **Jie Huang**,[1,2] **Bin Wang**,[3] **and Hongkai Wang**[4]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China*
[2]*Purple Mountain Laboratories, Nanjing 211111, China*
[3]*College of Electrical Engineering, Zhejiang University, Hangzhou 310058, China*
[4]*State Grid Zhejiang Electric Power Corporation Information & Telecommunication Branch, Hangzhou 310007, China*

Correspondence should be addressed to Jie Huang; jhuang@seu.edu.cn and Bin Wang; bin_wan@zju.edu.cn

Received 3 March 2021; Accepted 21 May 2021; Published 17 June 2021

Academic Editor: Lihua Yin

To solve the problem of security deployment in a hybrid wireless sensor network, a novel privacy-preserving mobile coverage scheme based on trustworthiness is proposed. The novel scheme can efficiently mitigate some malicious attacks such as eavesdropping and pollution and optimize the coverage of hybrid wireless sensor networks (HWSNs) at the same time. Compared with the traditional mobile coverage scheme, the security of data transmission and mobility are considered in the deployment of HWSNs. Firstly, our scheme can mitigate the eavesdropping attacks efficiently utilizing privacy-preserving signature. Then, the trust mobile protocol based on the trustworthiness is used to defend the pollution attacks and improve the security of mobility. In privacy-preserving signature, the hardness of discrete logarithm determines the degree of security of the privacy-preserving signature. The correctness and effectiveness of signature algorithm are proven by the probabilities of the native messages which can be recovered and forged which is negligible. Furthermore, a mobile scheme based on the trustworthiness (MSTW) is proposed to optimize the network coverage and improve the security of mobility. Finally, the simulation compared with a previous algorithm is carried out, in which the communication overhead, computational complexity, and the coverage are given. The result of the simulation shows that our scheme has roughly the same network coverage as the previous schemes on the basis of ensuring the security of the data transmission and mobility.

1. Introduction

As wireless sensor networks (WSNs) have been rapidly developing and growing popularity, the mobile deployment in an interested area with maximum coverage has become an important challenge in the field of research. However, the security of the data transmission and the mobility are generally not considered in the mobile deployment. Hybrid wireless sensor networks (HWSNs) usually include two types of nodes, such as mobile nodes and static nodes, where the mobile nodes have the ability of movement to increase the coverage in the monitored area. If there are eavesdropping and pollution attacks in the network, the innocent nodes can be eavesdropped and quickly polluted during the adjustment. For the mobile deployment in HWSNs, the previous researchers had done tremendous researches.

A large number of network coverage optimization schemes for HWSNs had been proposed in [1–6]. Unlike the previously proposed mobile coverage schemes, our mobile coverage scheme based on privacy-preserving signature and trustworthiness can mitigate the eavesdropping and pollution attacks effectively and ensures that the network coverage will not be significantly reduced at the same time.

Due to the limited resources of HWSNs, traditional symmetric or asymmetric cryptographic algorithms are not available. The trustworthiness is an emerging security technology based on network dynamic parameters, which can estimate the level of network security in HWSNs. The problems of node integrity and authentication are addressed utilizing the trustworthiness in [7–10]. The investigations and studies have shown that the recommended trust and the dynamic network information of the current node can effectively evaluate the node security level. Moreover, another solution [11] to achieve evaluation is that the sensor nodes will be equipped with additional computing units to evaluate trust. For more related work in detail, please refer to Section 2.

1.1. Motivation and Contribution. In the past decade, the previous researchers had conducted tremendous studies for mobile coverage. However, many issues are not addressed. A genetic scheme utilized virtual force and a particle swarm to optimize network coverage for HWSNs were proposed in [12]. However, the security issues in mobile deployment also need to be considered. If there are eavesdropping and pollution attacks in the HWSNs, the eavesdropping attack can result in the disclosure of location information of a mobile node, thereby attackers launched a premeditated attack. Relatively, the pollution attack will quickly infect malicious information to its neighbor nodes in a communication phase. Figure 1 shows the probability that nodes are vulnerable to infection when there is an attack in the network. If a node is malicious, the area within the communication radius is marked as polluted region. While the Euclidean distance between the sensor nodes and the malicious node is less than $2r$, the sensor nodes will be marked as high-risk nodes. If the Euclidean distance is equal to $2r$, the sensor nodes are labeled secondary risk nodes. All other sensor nodes are low risk. During the deployment process, it is an arduous task against pollution attack by protecting the sensor nodes integrity and realizing sensor nodes authentication. Bao and Chen [13] proposed a scalable trust management protocol, in which the multidimensional trust attributes extracted from communication and social networks are considered. However, many subjective factors were added in the process of selecting trust attributes.

Considering that and the target of mobile coverage in HWSNs, the main contributions of this paper are summarized as follows:

(1) We proposed a novel trust evaluation and update scheme including information entropy theory to resist the pollution attacks, in which the probability of trust can be objectively evaluated and updated

(2) At the same time, a privacy-preserving signature scheme which can sign the data transmission during the lifetime of HWSNs is proposed to defend against eavesdropping attacks

(3) Moreover, a mobile scheme based on the trustworthiness (MSTW) including an optimized virtual force algorithm is proposed to reduce the probability of being polluted. Meanwhile, the maximum network coverage is obtained under the overall network trust

1.2. Organization. The other chapters of this paper are introduced as follows. Related researches regarding mobile coverage based on the trust and privacy-preserving signature technologies are introduced in Section 2. The network and attack model are demonstrated in Section 3, where the mobile framework is also given. In Section 4, a mobile scheme based on the trustworthiness (MSTW) is proposed to improve the network coverage and reduce the probability of the sensor nodes being polluted. In Section 5, a suitable privacy-preserving signature scheme is introduced to ensure the security of data transmission. In Section 6, the full construction of the privacy-preserving mobile coverage scheme based on the trustworthiness (PP-MSTW) and the virtual force are presented, and the results of performance analysis are also given. Finally, the conclusion is presented in Section 7.

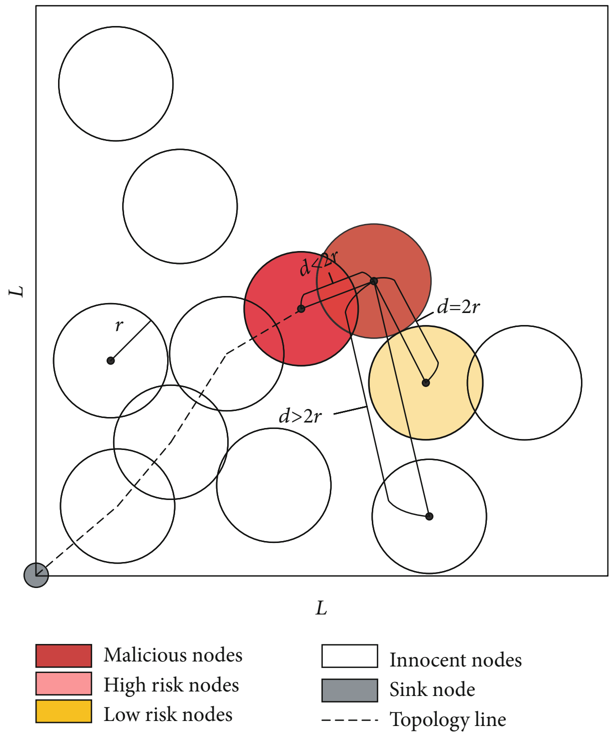

FIGURE 1: The distribution of different types of node security level.

2. Related Works

Mobile coverage in the deployment of HWSNs has always been a research hotspot, in which tremendous researches had been proposed. However, the security of HWSNs during the deployment is always not considered. The trust evaluation scheme can replace the traditional encryption mechanism with minimal resource. Some works in the field of mitigating eavesdropping attacks, trustworthiness for pollution attacks, and network coverage are discussed below.

2.1. Privacy-Preserving Signature. In HWSNs, attackers often obtain the dynamic information of the entire network by monitoring certain sensor nodes in the network. Yang et al. [14] studied several typical network structures and proved that as long as the eavesdropper monitors the data of one sensor node in each cycle, the entire network system can be completely observed.

There are two ways to defend against eavesdropping attacks including information theoretic and computational approaches. In information theoretic schemes, Zhang et al. [15] proposed a novel type of network $\boldsymbol{P}$-coding scheme, which prevented the network from being eavesdropped globally by performing lightweight sorting encryption on each native message and its encoding vector. Furthermore, Chen and Wang [16] applied the fake signature to network coding in the environment of IOT devices, which can resist both external and internal attacks at the same time and can also achieve the highest security level. In computational approaches, Nikravan et al. [17] proposed a lightweight computing scheme based on identity online and offline information to resist eavesdropping attacks with high computing power. Huang and Zhu [18] used the method of strategic equilibrium game to capture deception or eavesdropping, which can achieve Bayesian Nash equilibrium under an iterative algorithm.

2.2. Trust Evaluation and Update. Currently, most traditional trust evaluation models focus on sensor radio and the number of successful data transmission. Sensor nodes build a trust model through the measurable parameters such as remaining energy and the recommendation from the neighboring nodes. Ganeriwal et al. [19] proposed a framework for evaluating the communication trust of neighbor nodes to ensure the security of sensor network. Though the framework had good robustness, the recommendations of other neighboring nodes were not considered. With the continuous development of trust evaluation framework, the trust model was trained by the neural network fuzzy inference [20], in which the parameter accuracy was optimized by the sorting genetic theory. Finally, they proposed a trust management framework with the higher security. However, the scheme neglected the recommendations from the neighboring nodes, which resulted in the trust values being not soundest. For this problem, an effective clustered trust model was proposed [21] to consider more external and human intervention factors, in which the trust weight between the subtrust sets is adaptive. However, the calculation cost will increase continuously due to weight updating, in which the method needs to learn repeatedly interaction information between sensor nodes.

2.3. Maximum Mobile-Coverage in HWSNs. For sensor network coverage issues, researchers had done a lot of research in the previous decades.

A novel distributed and centralized aggregation method is proposed in [22] to reduce the sensor density in a limited area, which can also prolong the sensor network life to the greatest extent. Chen et al. [23] proposed a supplementary solution for network coverage to dynamically maintain the coverage during the network life. When the nodes in the network are depleted or damaged due to the reasons such as energy exhaustion or damage, the sensor nodes with redundant coverage are dynamically adjusted to supplement the missing coverage. Naveen and Kumar [24] studied the problem of minimizing the cost of network deployment under the constraint of average vacancy, which calculated the density function of the relay nodes to preset the initial position of the nodes and verified the effectiveness of the scheme. In dynamic HWSNs, Cao et al. [25] proposed an improved social spider optimization strategy to reduce the network coverage blind spots and redundancy, which simulated the movement law of spiders and cooperation mechanism to achieve the optimal solution of network coverage.

3. Problem Statement

3.1. Hybrid Network Model. Suppose that hybrid sensor nodes with two groups of different attributes are randomly deployed in a two-dimensional space, and each node is assigned a unique identifier. The different two groups of nodes include static and mobile sensor nodes. The network topology of this HWSNs is $L-G=(L, V, E, r_s)$, in which L expresses the side length of the rectangular deployment region, V denotes the combination of two types of nodes, E means the topological connection combination between sensor nodes, and r_s shows the sensing radius.

Generally, the communication radius r_c of the sensor nodes is $r_c = 2r_s$ in the HWSNs. The characteristics of nodes and conversion rules are given as follows:

(1) Static sensor nodes: such nodes do not have the ability to move. After the deployment is completed, the position of the nodes is not allowed to be changed. At the same time, the energy consumption of nodes is mainly caused by data communication.

(2) Mobile sensor nodes: if there are no restrictions, mobile nodes can move freely within the deployment range. Such nodes usually have higher energy and computing resources than static nodes. Here, we specify the energy of mobile nodes as $E_m = 5 * E_s$.

(3) Node conversion rules: the mobile sensor nodes need to consume a lot of energy in the process of moving. When the current remaining energy of the mobile nodes drops below 50% of the average energy of the entire network, the mobility of nodes will be removed. At this time, the mobile node will participate in information perception as a static node.

Each WSN has its cluster selection scheme to gather information from sensors. Figure 2 shows the deployment structure in our hybrid WSNs. The hybrid network model including static nodes and mobile nodes will execute cluster formation (CF) and optimal cluster head (CH) selection algorithm after deployment. In a window period, each cluster only has one CH. The nodes within a cluster usually communicate with the cluster head. The cluster head nodes are generally mobile nodes or the higher energy static nodes in the cluster. In addition, when the nodes in the network can directly communicate with the BS, such nodes can directly send data to the BS.

3.2. Attack Model. The inherent characteristics of HWSNs including open deployment environment and limited resources make it vulnerable to various types of unknown attacks. Previous researches about the mobile coverage usually do not consider the network security during the movement. We assume that before the sensor nodes start to implement the mobile coverage scheme, there are already attacked nodes in the network. These malicious nodes launch

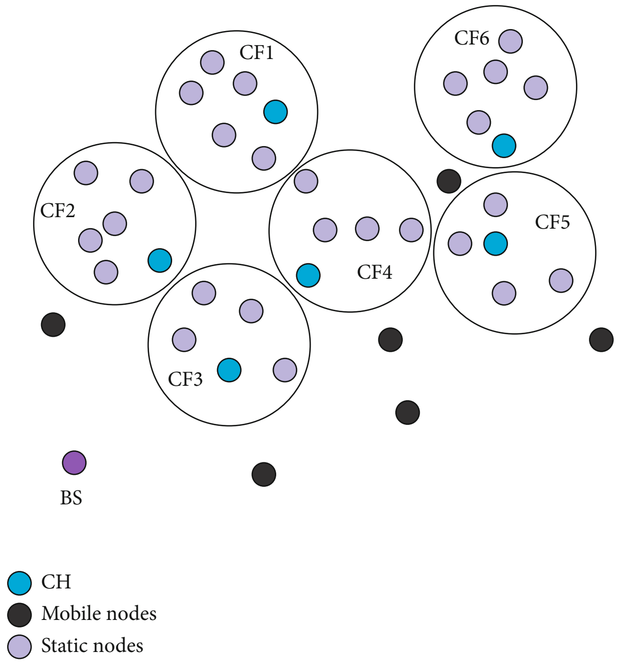

Figure 2: The deployment structure in Hybrid WSNs.

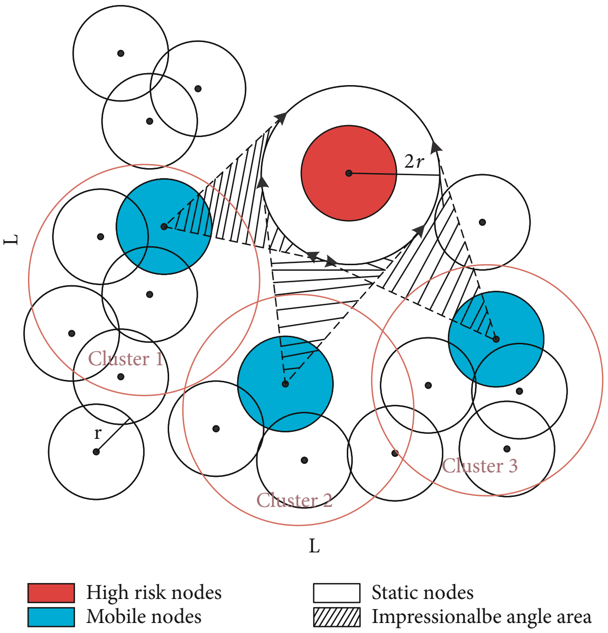

Figure 3: High risk moving angle and range.

attacks on the network by injecting fake data packets or tampering with the content of the transmitted data. The type of attack is usually named a pollution attack. The attack model is proposed as follows:

(1) Suppose there are N_M malicious nodes in our HWSNs. The types of attack occur before the mobile deployment. The malicious nodes usually inject false information or tamper with the contents of data packets

(2) Malicious nodes in the network can randomly select neighbor nodes within their communication range as the next hop pollution nodes

(3) As shown in Figure 3, there are two types of nodes including mobile and static in our HWSNs. Generally, mobile nodes have higher energy and computing resources, so they have higher defense performance than static nodes. Therefore, we think that the static nodes are easier to be attacked. The red area in the figure is the communication range r_s of a certain malicious node. When an innocent mobile node moves into the range of $2r_s$, the mobile sensor node will establish direct communication with the malicious node. At this time, the mobile node will be in a high-probability pollution area. In order to avoid the mobile node from moving into this area, the impressionable angle area is given to reduce the probability of the mobile node being polluted

4. A Multicluster Trust Scheme

According to the given network and attack model, a malicious defense model based on trust evaluation needs to be proposed. In this section, we construct a multicluster trust computing scheme to assess the trustworthiness of each node. The trust degree of the HWSNs is represented by (T, G_i), where G_i is the i-th evaluation window time. The multicluster trust scheme is defined as follows:

Definition 1. A multicluster trust scheme MCTS includes a tuple of four probabilistic distributed algorithms:

(a) Communication $(O_{i,j}, R_{i,j}) \mapsto (T_1(i,j))$: $O_{i,j}$ is the number of the data successfully transmitted, $R_{i,j}$ is the number of forward failures, and the communication trust is $T_1(i,j)$.

(b) Energy $(d_{i,j}, \varepsilon_{\text{amp}}, f_{\text{amp}}, E_{\text{elec}}) \mapsto (T_2(i,j))$: $d_{i,j}$ is the transmission distance, ε_{amp} is in free space, f_{amp} is the unit energy consumption coefficient in multipath attenuation model, E_{elec} represents the energy consumption when receiving data, and $T_2(i,j)$ is the energy trust.

(c) Probabilistic trust against attacks $(V_M, r_s, L) \mapsto (T_3(i,j))$: the set V_M is the malicious nodes, r_s is the sensing radius, L represents the side length of rectangular detection area, and $T_3(i,j)$ is the attacked trust.

(d) Aggregation $(T_n(i,j), w_n) \mapsto (T(i,j))$: $T_n(i,j)$ is the multitype trust values containing all the above types of trust variables. w_n symbols the weight set of each trust variable. Then, the aggregation $T(i,j)$ will be output.

4.1. The Multitype Trust Evaluation Method. The previous section has given the network and attack model, combined with the definition of the multicluster trust scheme. The specific trust evaluation method is given. We separately calculated communication trust, energy trust, and attacked trust. Finally, a weight distribution scheme combined with information entropy is proposed to aggregate the mentioned multitype trust. The multitype trust aggregation model is expressed as

$$T(i,j)=\sum_{i=1}^{n} w_n T_n(i,j), \tag{1}$$

where $0 \le w_n \le 1$, $w_1 + w_2 + \cdots w_n = 1$; w_n is the weight factor of the multitype trust; and $T_n(i,j)$ is the multitype trust.

4.1.1. Communication Trust. The communication methods between nodes in the communication trust calculation are mainly divided into two modes: (1) node i directly interacts with node j, and (2) node i communicates with node j indirectly through k intermediate nodes. This paper uses the simplified beta trust model to calculate the trust value. The trust evaluation model adopts the model of previous research work [26], which is expressed as

$$f(t)=\frac{\alpha+1}{\alpha+\beta+2}\left(1-\frac{\beta}{W}\right)\left(1-\frac{1}{\alpha+\delta}\right), \tag{2}$$

where the successful interactions is α and the unsuccessful number is β, $1-\beta/W$ is the penalty function, and $1-1/(\alpha+\delta)$ is the adjustment function.

Suppose that the number of successful direct interaction is $O_{i,j}$; otherwise, it is $R_{i,j}$. Therefore, the trust expression for direct communication between nodes i and j is

$$P=\frac{O_{i,j}+1}{O_{i,j}+R_{i,j}+2}\left(1-\frac{R_{i,j}}{W}\right)\left(1-\frac{1}{O_{i,j}+\delta}\right). \tag{3}$$

The mathematical trust expectation probability from i to j is expressed as the communication trust value in a round. So, the directly connected node communication trust is

$$T_d(i,j)=\sum_{t=1}^{n}\frac{E\left(P_{i,j}\right)}{n}. \tag{4}$$

Here, n represents the amount of time windows within the effective operation time of the HWSNs.

In the case of the relay communication, node i needs to use k relay nodes to communicate with node j. The relay node z recommends an indirect trust value of node j to node i in the trust calculation model of node i for node j. The indirect trust calculation model in communication trust is shown as follows:

$$T_{id}(i,j)=\frac{\sum_{k=1}^{n} T_d(i,z)\cdot T_d(z,j)}{n}. \tag{5}$$

When node i and node j are neighbor nodes, the communication trust model will be calculated by Equation (4). Otherwise, Equation (5) will give the indirect communication trust value.

4.1.2. Energy Trust. In hybrid sensor networks, energy consumption is divided into two types, namely, communication and mobile consumption. Static nodes only include communication loss, while mobile nodes include both communication and mobile loss. In communication energy loss, when node i sends n bits information to node j successfully, the communication energy consumption model can be given as follows:

$$E_c(i,j)=\begin{cases} n\cdot E_{\text{elec}}+n\cdot\varepsilon_{\text{amp}}\cdot d_{ij}^2, & d_{ij}<d_0,\\ n\cdot E_{\text{elec}}+n\cdot f_{\text{amp}}\cdot d_{ij}^4, & d_{ij}\ge d_0,\end{cases} \tag{6}$$

where d_{ij} is the realistic transmission distance, d_0 represents the threshold of distance, E_{elec} represents the consumption of energy by the circuit for transmitting or receiving data per bit, and ε_{amp} and f_{amp} denote the energy loss in the free space and the multipath attenuation. So d_0 can be expressed as $d_0=\sqrt{\varepsilon_{\text{amp}}/f_{\text{amp}}}$.

Additionally, the energy consumption during the movement should also be considered. The energy consumption can be expressed as follows:

$$E_m=2d\sum_{i=0}^{n}\sqrt{{F_{x_i}}^2+{F_{y_i}}^2}, \tag{7}$$

where d represents the side length of a square grid in the network and F_{x_i} and F_{y_i} are the virtual force received by node i.

In a mobile period, the remaining energy of the node is

$$T_2(i,j)=\begin{cases}\dfrac{E_N-E_m-E_c(i,j)}{E_t}, & E_N>\dfrac{E_t}{2},\\ 0, \quad E_N\leqslant\dfrac{E_t}{2},\end{cases} \tag{8}$$

where E_N symbols the remaining energy of the current node and E_t represents the initial energy. Usually, mobile nodes have a higher initialization energy level than static nodes.

4.1.3. Probabilistic Trust against Attacks. When there are malicious nodes in the HWSNs, the innocent nodes communicating with the malicious nodes have the probability of being polluted.

In this subsection, the Euclidean distance relationship analysis between nodes is utilized to assess the probability of defense against attacks between innocent sensor nodes. The ability of an innocent node defending against attacks indicates the trust degree of the sink node to those nodes. The higher the probability of an innocent node being attacked, the lower the trust degree, and vice versa.

According to the Euclidean distance between innocent nodes and a malicious node. E_1 and E_2 are defined as two different events. E_1 denotes the Euclidean distance between innocent nodes, and a malicious node j is less than the r_c of malicious nodes, and it can be expressed as $V_n \cap N\_(j) \neq \varnothing$. E_2 denotes the Euclidean distance is longer than the communication radius, and it can be showed as $V_n \cap N_{-}(j) = \varnothing$, where $j \in V_M$ and $N_{-}(j)$ is the neighbor of malicious node j.

Lemma 2. *Nodes i and j are randomly deployed in the $L \times L$ rectangular monitoring region, in which the communication radius $r \in (0, W/2)$. The distribution of nodes i and j is given as*

$$D\left(d_{i,j} \leq r\right) = \frac{\left((3\pi/2) + \left(4\sqrt{2}/3\right) - (25/12)\right) r^4 - (8/3)Lr^3 + \pi L^2 r^2}{L^4}. \tag{9}$$

According to Lemma 2, if two nodes in the monitoring area can communicate with each other, the probability is $D(d_{i,j} \leq r)$. For node a, i.e., $\forall a \in V_n$, the probabilty of the node a that can communicate with malicious node j is

$$P(a \in N_{-}(j)) = \frac{D(r)}{2}. \tag{10}$$

Therefore, the probability of E_1 and E_2 can be given as follows:

$$\begin{aligned} P(E_1) &= P(V_i \cap N_{-}(j) \neq \varnothing) = 1 - \left(1 - \frac{D(r)}{2}\right)^{N_i}, \\ P(E_2) &= P(V_i \cap N_{-}(j) = \varnothing) = \left(1 - \frac{D(r)}{2}\right)^{N_i}. \end{aligned} \tag{11}$$

Finally, the probability trust against attacks can be expressed as follows:

$$T_3(i,j) = \begin{cases} P(E_1), & E_1 = \text{true}, \\ P(E_2), & E_2 = \text{true}. \end{cases} \tag{12}$$

4.2. Trust Aggregation. The weight relationships between the trust measures are more objectively determined. Information entropy can express the probability of a certain specific information, so it can be used to calculate the weights of uncorrelated subtrust distributions. The probability formula of information entropy is as follows:

$$H(\mu) = -\sum Q(\mu) \log_2(\mu), \tag{13}$$

where μ is the information variable and $Q(\mu)$ is the probability distribution function. Supposing that R is the recommended trust from three types of subtrust evaluation parameters, $1 - R$ is the degree to which these trust levels are suspected. With the above assumptions, the recommendation function of trust degree is

$$H(R) = -R \log_2 R - (1 - R) \log_2 (1 - R). \tag{14}$$

When there are multiple types of recommended trust values, not all trust values have the same recommendation weight. The weight of each trust value is independent, and it occupies a different degree of importance in the overall recommendation. Therefore, the weight entropy of R_{ij}^k can be given as follows:

$$H\left(R_{ij}^k\right) = -R_{ij}^k \log_2 R_{ij}^k - \left(1 - R_{ij}^k\right) \log_2 \left(1 - R_{ij}^k\right). \tag{15}$$

In practical applications, malicious nodes in the HWSNs usually disguise or slander the recommended trust value to deviate from the correct estimated value. Moreover, the previous trust weight distribution schemes often adopt artificial weight preset methods, which further leads to the deviation of trust weight distribution from objectivity. The information entropy weight distribution scheme can effectively reduce the degree of defamation of malicious nodes. According to Equation (15), the trust weight distribution can be given as follows:

$$\omega_k = \frac{1 - \left(\left(H\left(R_{ij}^k\right)\right) / \left(\log_2 R_{ij}^k\right)\right)}{\sum_{k=1}^{n} \left[1 - \left(\left(H\left(R_{ij}^k\right)\right) / \left(\log_2 R_{ij}^k\right)\right)\right]}. \tag{16}$$

Therefore, the final trust can be expressed as follows:

$$T(i,j) = \sum_{k=1}^{n} \left(\omega_k T_{ij}^k\right). \tag{17}$$

5. The Privacy-Preserving Signature Scheme

In the HWSNs, the trust evaluation of each nodes can drive the mobile nodes to a safer location. However, the data transmission security should also be considered to prevent pollution attacks. To solve the above problem, a novel privacy-preserving signature scheme is proposed.

5.1. Related Knowledge. In this subsection, some mathematical knowledge is related to the hardness and bilinear cyclic map is provided to support our scheme.

Suppose there are two bilinear cyclic groups H and H_T with the same prime number. They both have nondegeneracy and bilinearity and are computable. Generally, the security strength of privacy-preserving signature scheme depends on the hardness of the bilinear cyclic. For $F = (h, h^x)$, where $x \in \mathbb{Z}_p^*$, no polynomial algorithm can be calculated to obtain x.

5.2. Privacy-Preserving Signature Scheme. According to the above assumption of the cyclic group of the bilinear mapping, we give a complete privacy-preserving signature scheme including six probabilistic subalgorithms. The detailed scheme construction is given as follows:

(a) Construct a bilinear cyclic group $e : H \times H \mapsto H_T$, and output $k \xleftarrow{R} \kappa$, $sk = \{sk_1, \cdots, sk_{m+n+1}\}$ such that $sk_i \xleftarrow{R} \mathbb{F}_p$, and $pk = (\mu, h, H, H_T, g)$, where $\mu \xleftarrow{R} H \setminus \{1\}$ and $g := \{h^{sk_1}, \cdots, h^{sk_{m+n+1}}\}$, where m and n are two random positive integers

(b) The resource data transmitted in the network is divided into n data blocks $w \in \prod_i$. $f : \{0,1\}^* \times \{0,1\}^* \times \kappa \mapsto \mathbb{F}_p$ is a random function; the encryption matrix is

$$G_E = \begin{bmatrix} e_{i,1} & & \\ & \ddots & \\ & & e_{i,m} \end{bmatrix}. \tag{18}$$

The coding vector is $c = (w_1, \cdots, w_m)$, and the payload of w is $w_p = (w_{m+1}, \cdots, w_{m+n})$. Then, $\text{Encrypt}(k, Id_i, w) = (c_E, w_p) \in \prod_i^E$, where $c_E = c \cdot G_E = (w_1 e_{i,1}, \cdots, w_m e_{i,m})$

(c) According to the above parameters sk and w, the signature of the data block σ can be given as follows:

$$\sigma = \mu^{\sum_{m+n}^{z=1} w_z sk_z + \left(\sum_{m}^{z=1} w_z\right) G(Id_i) sk_{m+n+1}}. \tag{19}$$

Then, the combined signature of the encoded data block is (w^r, σ^r), w^r, and σ^r are computed as follows:

$$\begin{aligned} w^r &= \sum_{j=1}^{\wp} \alpha_j w_j, \\ \sigma^r &= \prod_{j=1}^{\wp} \sigma_j^{\alpha_j}. \end{aligned} \tag{20}$$

The combined signature is $\xi^r = (Id_i, w^r, \sigma^r)$

(d) According to the given public key, the signature is verified as follows:

$$\begin{aligned} v_1 &= e(\sigma, h), \\ v_2 &= e\left(\mu \prod_{\tau=1}^{m+n} g_\tau^{w_\tau} \cdot \prod_{\tau=1}^{m} g_{m+n+1}^{G(Id_i) w_\tau}\right). \end{aligned} \tag{21}$$

When $v_1 = v_2$, the verification is successful

(e) The $e_{i,1}, \cdots, e_{i,m}$ is computed by the decryption matrix as

$$G_D = \begin{bmatrix} e_{i,1}^{-1} & & \\ & \ddots & \\ & & e_{i,m}^{-1} \end{bmatrix}. \tag{22}$$

The coding data is decrypted as $c_D = c_E \cdot G_D$. Then, the original block is calculated as follows:

$$w_D = \text{Decrypt}(k, Id_i, w) = (c_D, w_p) \tag{23}$$

5.3. Defense against Eavesdropping Attacks

Definition 3. When the i-th data block $\{w_i\}_{i=1}^q$ is maliciously eavesdropped, the probability function of the native data recovery is negligible.

Theorem 4. *The privacy-preserving signature scheme can resist the eavesdropping attacks.*

Proof. When the eavesdroppers collect the i-th linear combination of data blocks $\{w_i\}_{i=1}^q$, the data block can be analyzed as another expression as follows:

$$\begin{bmatrix} w_1 \\ \vdots \\ w_q \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{q1} & \cdots & \alpha_{qm} \end{bmatrix} \cdot \begin{bmatrix} eb_{i,1} \\ \vdots \\ eb_{i,m} \end{bmatrix}, \tag{24}$$

where $eb_{i,j} = (c_{i,j}, x_{i,j}) \in \mathbb{F}_p^{m+n}$ and $x_{i,j}$ is the native message.

Then, the encryption matrix of the encoding vector w_i can be expressed as follows:

$$C_E = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{q1} & \cdots & \alpha_{qm} \end{bmatrix} \cdot G_E. \tag{25}$$

If the attackers want to successfully native message, $\alpha_{i,j} (1 \le i \le q, 1 \le j \le m)$ must be randomly selected from $\mathbb{F}_p$, and the randomly selected matrix is denoted as C_D. According to [27], the probability that the native message is recovered can be expressed as

$$P = P(C_D) \cdot P[\text{rank } (C_D) = m], \tag{26}$$

where $P(C_D)$ is the probability of decryption matrix is computed and $P[\text{rank } (C_D) = m]$ is the probability of matrix with same rank, which can be expressed as $\prod_{i=0}^{r-1} (1 - p^{i-r}) \le 1$. Meanwhile, $P(C_D) = 1/p^m$, then, the recover probability can be rewritten as $P = P[\text{rank } (C_D) = m]/p^m$.

Finally, the probability that the native message is recovered can be expressed as

$$P = \frac{\prod_{i=0}^{q-1} \left(1 - p^{i-q}\right) \le 1}{p^m} \le \frac{1}{p^m} \le \frac{1}{2^{\lambda m}}. \tag{27}$$

This completes the proof.

6. The Privacy-Preserving Mobile-Coverage Scheme Based on Trustworthiness

In Section 5, we proposed a privacy-preserving signature scheme and proved its effectiveness against eavesdropping attacks, after ensuring the security of data transmission

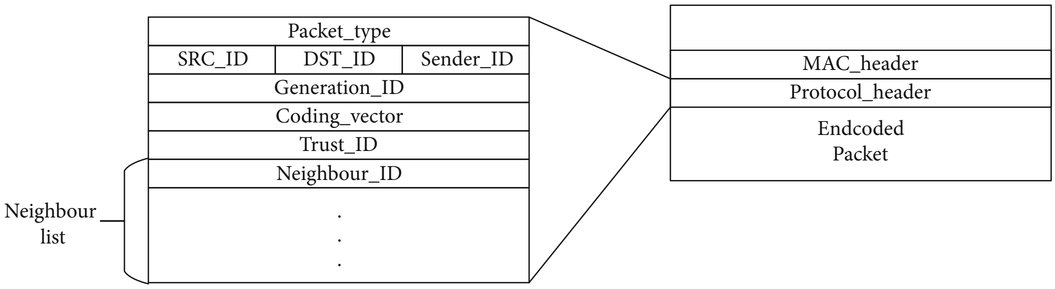

FIGURE 4: The flowchart of PP-MSTW.

during the movement. Then, how to select the safest mobile nodes to move in an iteration should be considered.

The privacy-preserving mobile coverage scheme based on trustworthiness (PP-MSTW) we proposed is shown in Figure 4. The mobile coverage scheme contains four phases, namely, destinations, mobility control, mobile coverage, and trust computation. Meanwhile, the privacy-preserving scheme will run during the network life when nodes exchange data. The data transmission format between nodes is shown in Figure 5. The data packet type, trust mark, neighbor node information, and the trust generation are defined in the transmitted data.

6.1. Full Construction. The definition of MCTS has be given in Section 4. Combined with the virtual force algorithm, the full construction of PP-MSTW is showed as follows:

(a) Setup (L^{λ}): a hybrid wireless sensor network is deployed in rectangular area A. The HWSN includes mobile and static sensor nodes. Moreover, the mobile nodes have higher energy than static nodes.

(b) Trust evaluation ($P \mapsto T_i, T_h$): suppose the collection of polluted nodes is $P = [M_1, \cdots, M_t]$, T_i of each node can be calculated by probabilistic trust against attacks in a generation, and the highest trust T_h will be given.

(c) Trust movement ($T_h \mapsto F_m$): the virtual force and Voronoi diagram are used to calculate the resultant force F_m experienced by the mobile nodes. Moreover, the resultant force F_m determines the distance and angle of movement.

(d) Trust update ($T_i \mapsto T_{i+1}$): after the sink node obtains the trust T_i of the previous generation, the highest trusted mobile node will perform the movement operation in a round G. When the movement is completed, the next-generation trust T_{i+1} will be calculated according to the new topology in the HWSNs.

(e) Maximum coverage: as the nodes of each generation move, the network coverage will gradually increase. When the network coverage reaches the highest value and does not change, the network deployment is completed.

As shown in Figure 4, the execution flowchart of PP-MSTW is as follows:

(1) Hybrid wireless sensor network initialization and two types of nodes are randomly deployed in the $L \times L$ rectangular region

(2) The trust of all nodes in the network will be calculated. The static node with the lowest degree of trust is confirmed as the next-generation pollution node

(3) The sink node selects the highest trusted mobile node to move within a generation G. The virtual force algorithm and the Voronoi diagram strategy determine the moving direction and distance of the node

(4) After performing the above operations, the trust of each node will be updated according to the location of the next-generation pollution node and the updated network topology

(5) As long as there is traffic between nodes in the network, the privacy-preserving scheme will be implemented

The MSTW algorithm shows the specific execution process of trust mobile, which will give updated trust U_m and network coverage p.

6.2. Simulation Result Analysis. The PP-MSTW is composed of two parts including privacy-preserving signature scheme and mobile coverage based on trustworthiness (MSTW) algorithm. In Subsection 5.3, the theoretical correctness of the signature scheme is proven. In this subsection, the communication and computation overhead of the MSTW are analyzed in detail. Simulation experiment is constructed in the softwares OMNET++ and MATLAB.

6.2.1. Communication Overhead. According to the definition of communication trust, the communication overhead can be expressed as follows:

$$O_{\text{communication}} = \frac{[(n(s) + l + 1)/(n(f + s) + l + 2)]^2}{N}, \quad (28)$$

where s is the number of successful data exchanges between nodes in each generation and f represents the failures. Meanwhile, the sink node will calculate the position of the next generation of nodes according to the virtual force algorithm, and the mobile signal l will be sent to the mobile node that needs to move. Generally, mobile nodes have the highest trust.

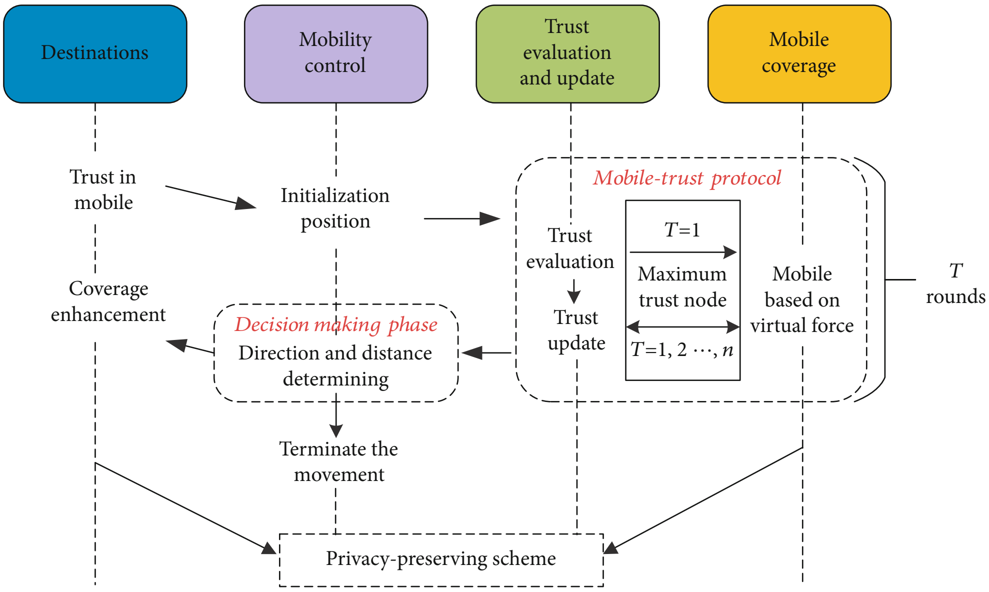

Figure 5: The definition of transmitted data format.

```
Input: Static nodes $\boldsymbol{S}_s = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_s\}$ and mobile nodes $\boldsymbol{S}_m = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_m\}$, in which $s + m = N$ and an $L \times L$ initial rectangular region, coverage difference accuracy $\kappa$, communication radius $r_c$, sensing radius $r_s$, $r_c = 2r_s$, iterations $\boldsymbol{G}$, all network sensor nodes initialization trust $\boldsymbol{U} = \{\boldsymbol{U}_{\boldsymbol{s}_1}, \boldsymbol{U}_{\boldsymbol{s}_2} \cdots, \boldsymbol{U}_{\boldsymbol{s}_s}, \cdots, \boldsymbol{U}_{\boldsymbol{s}_{s+1}}, \boldsymbol{U}_{\boldsymbol{s}_{s+2}}, \cdots, \boldsymbol{U}_{\boldsymbol{s}_{s+m}}\}$.
Output: The mobile sensor nodes trust set $\boldsymbol{U}_m$ and the network coverage $\boldsymbol{p}$.
for$i = 0, 1, \cdots, \boldsymbol{G}_n$do
    According to the virtual force and voronoi theory, the combined force $\boldsymbol{F}_s = \{\boldsymbol{F}_{s_1}, \boldsymbol{F}_{s_2}, \cdots, \boldsymbol{F}_{s_m}\}$of mobile nodes in a rectangular region $L \times L$ is calculated.
    Select Max $(\boldsymbol{U}_s)$; Where there are first generation pollution nodes in the network.
    while$\boldsymbol{p}_{\boldsymbol{G}_i} - \boldsymbol{p}_{\boldsymbol{G}_{i-1}} \le \kappa || \boldsymbol{F}_{s_m} = \varnothing$, stop.
    Calculate the mobile nodes trust $\boldsymbol{U}_{\boldsymbol{m}}$.
    Select Max $(\boldsymbol{U}_m)$ to move for avoiding the high-risk area and improving the network coverage $\boldsymbol{p}$.
end for
```

Algorithm 1: Mobile scheme based on the trustworthiness.

The growth rate of communication overhead about the MSTW is shown in Figure 6. As the sink node sends more and more mobile signal, the growth rate of communication overhead in the HWSNs is the lowest compared to previous studies. In HWSNs, the number of successful communications between nodes is much higher than the number of failures.

6.2.2. Computation Overhead. Network computation overhead is mainly divided into four parts including communication trust, energy trust, probabilistic trust against attacks, and virtual force. All calculations are performed on $\mathbb{F}_q$, where the number of multiplications implies the computation overhead.

In communication trust, Equation (5) shows that communication trust needs to be calculated $n^2 - n + 1$ times on a finite filed $\mathbb{F}_q$, and so the computation overhead is $O_c = n^2 - n + 1$.

In energy trust, the computation overhead in energy trust can be easily derived as $O_e = n^4$.

Our scheme is compared with other trust computing schemes; ours mainly includes probabilistic trust against attacks. According to the above formula for resisting attacks probability, the computation overhead can be expressed as follows:

$$O_a = n\left(qr^4 - pr^3 + mr^2\right). \tag{29}$$

In addition to the computation overhead in the trust evaluation process, the computation overhead of the trust mobile algorithm should also be considered. The computation overhead in trust mobile mainly includes virtual force algorithm. Research [28] shows that the computation overhead of the virtual force algorithm is $O_v = n(n-1)$.

Finally, the overall computation overhead of the MSTW within a generation G is expressed as follows:

$$\begin{aligned} O_{\text{computation}} &= O_c + O_e + O_a + O_v \\ &= n^4 + 2n^2 + n\left(qr^4 - pr^3 + mr^2 - 2\right) + 1. \end{aligned} \tag{30}$$

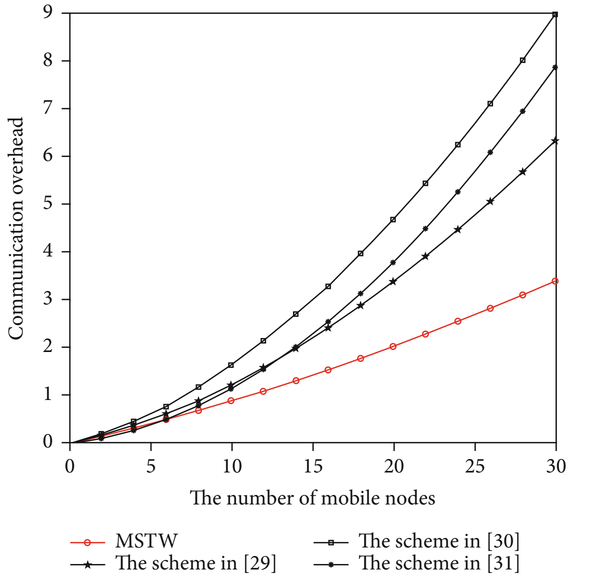

Figure 6: The communication overhead of different schemes.

Table 1: Computational comparison of different schemes.

Items	Computational complexity
The scheme in [29]	$n^4 + 2n^2$
The scheme in [30]	$n^4 + n^2 + kn + p$
MSTW	$n^4 + 2n^2 + n\left(qr^4 - pr^3 + mr^2 - 2\right) + 1$
The scheme in [31]	$n^4 + n^2 + kn$

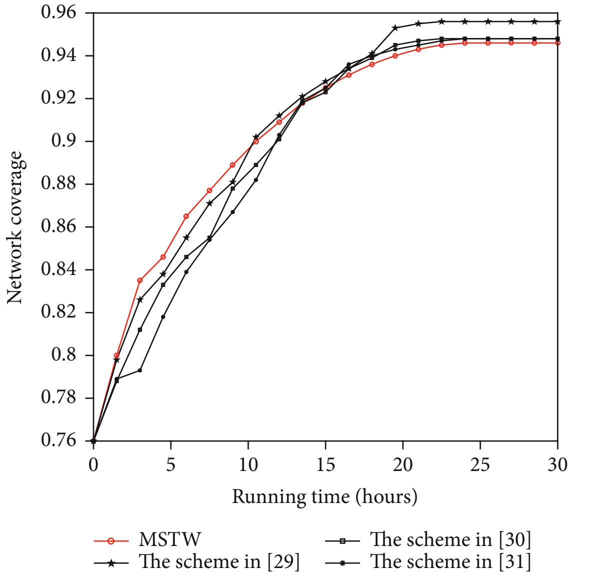

Figure 7: The coverage of different schemes in [29–31].

Table 1 demonstrates the comparison of computation overhead, in which our MSTW has almost the same computation overhead as several other previous schemes, and both are approximately equal to $O_{\text{computation}} \approx O(n^4)$. Figure 6 shows our scheme has the lowest communication overhead in each generation of data communication. In Figure 7, the maximum coverage that all nodes in HWSNs can reach is given during the network life. Compared with the previous schemes, the network coverage of our scheme is 1.3% lower than the maximum coverage achieved by the previous schemes. In summary, our MSTW can guarantee a high coverage under the condition of deployment security and does not increase the computation and communication overhead at the same time.

7. Conclusion

For security HWSN deployment, a novel privacy-preserving mobile coverage scheme based on the trustworthiness is proposed. The scheme can ensure the communication data integrity and confidentiality in the network coding communication. Firstly, a comprehensive trust evaluation method based on historical communication data, energy, and the probability of nodes being attacked is constructed. Then, a privacy-preserving signature scheme is applied to the network for resisting pollution and eavesdropping attacks. Finally, the PP-MSTW is constructed to maximize network coverage under the premise of ensuring the security of node communication.

From analyzing the mathematical theory and result of simulation, the PP-MSTW we proposed can guarantee the security in data communication under the theoretical analysis. The communication and computation overhead of the scheme are lower than those of the previous algorithms. Moreover, the scheme we proposed can obtain the optimal solution for coverage under the premise of security in the network deployment.

In the future research, we will use artificial intelligence methods to analyze network trust and then study game theory methods to adjust network defense strategies and ultimately further improve network robustness.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Key Research and Development Program of China (No. 2018YFB2100400).

References

[1] M. R. Senouci and A. Mellouk, “A robust uncertainty-aware cluster-based deployment approach for WSNs: coverage, connectivity, and lifespan,” *Journal of Network and Computer Applications*, vol. 146, p. 102414, 2019.

[2] R. R. Priyadarshini and N. Sivakumar, “Enhancing coverage and connectivity using energy prediction method in

underwater acoustic WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 2751–2760, 2020.

[3] P. Le Nguyen, K. Nguyen, H. Vu, and Y. Ji, "Telpac: a time and energy efficient protocol for locating and patching coverage holes in wsns," *Journal of Network and Computer Applications*, vol. 147, article 102439, 2019.

[4] S. Shao, L. Wu, Q. Zhang, N. Zhang, and K. Wang, "Cooperative coverage-based lifetime prolongation for microgrid monitoring WSN in smart grid," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, Article ID 249, 2020.

[5] P. Natarajan and L. Parthiban, "k-coverage m-connected node placement using shuffled frog leaping: Nelder–Mead algorithm in WSN," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–6, 2020.

[6] A. Verma, S. Kumar, P. R. Gautam, T. Rashid, and A. Kumar, "Broadcast and reliable coverage based efficient recursive routing in large-scale WSNs," *Telecommunication Systems*, vol. 75, no. 1, pp. 63–78, 2020.

[7] M. S. Abdalzaher and O. Muta, "A game-theoretic approach for enhancing security and data trustworthiness in IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11250–11261, 2020.

[8] N. A. Khalid, Q. Bai, and A. Al-Anbuky, "Adaptive trust-based routing protocol for large scale WSNs," *IEEE Access*, vol. 7, pp. 143539–143549, 2019.

[9] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN [J]," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–3, 2020.

[10] K. Cho and Y. Cho, "HyperLedger fabric-based proactive defense against inside attackers in the WSN with trust mechanism," *Electronics*, vol. 9, no. 10, p. 1659, 2020.

[11] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and S. Islam, "Trustworthiness of self-driving vehicles for intelligent transportation systems in industry applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 961–970, 2020.

[12] Y. Yoon and Y. H. Kim, "An efficient genetic algorithm for maximum coverage deployment in wireless sensor networks," *IEEE Transactions on Cybernetics*, vol. 43, no. 5, pp. 1473–1483, 2013.

[13] F. Bao and R. Chen, "Trust management for the internet of things and its application to service composition," in *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pp. 1–6, San Francisco, CA, USA, 2012.

[14] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, "Security analysis of a distributed networked system under eavesdropping attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1254–1258, 2019.

[15] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, "P-coding: secure network coding against eavesdropping attacks," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, San Diego, CA, USA, 2010.

[16] Y. J. Chen and L. C. Wang, "Privacy protection for internet of drones: a network coding approach [J]," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1719–1730, 2018.

[17] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks," *Wireless Personal Communications*, vol. 99, no. 2, pp. 1035–1059, 2018.

[18] L. Huang and Q. Zhu, "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems," *Computers & Security*, vol. 89, p. 101660, 2020.

[19] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, pp. 1–37, 2008.

[20] J. Kaur and S. Kaur, "Novel trust evaluation using NSGA-III based adaptive neuro-fuzzy inference system," *Cluster Computing*, pp. 1–12, 2021.

[21] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[22] J. Yu, S. Wan, X. Cheng, and D. Yu, "Coverage contribution area based k -coverage for wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8510–8523, 2017.

[23] C. P. Chen, S. C. Mukhopadhyay, C. L. Chuang et al., "A hybrid memetic framework for coverage optimization in wireless sensor networks," *IEEE transactions on cybernetics*, vol. 45, no. 10, pp. 2309–2322, 2015.

[24] K. P. Naveen and A. Kumar, "Coverage in one-dimensional wireless networks with infrastructure nodes and relay extensions," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 140–153, 2019.

[25] L. Cao, Y. Yue, Y. Cai, and Y. Zhang, "A novel coverage optimization strategy for heterogeneous wireless sensor networks based on connectivity and reliability," *IEEE Access*, vol. 9, pp. 18424–18442, 2021.

[26] A. Saidi and K. Benahmed Pr, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," *Ad Hoc Networks*, vol. 106, p. 102215, 2020.

[27] D. Laksov and A. Thorup, "Counting matrices with coordinates in finite fields and of fixed rank," *Mathematica Scandinavica*, vol. 74, pp. 19–33, 1994.

[28] C. Qi, J. Huang, X. Liu, and G. Zong, "A novel mobile-coverage scheme for hybrid sensor networks," *IEEE Access*, vol. 8, pp. 121678–121692, 2020.

[29] Z. Liao, J. Wang, S. Zhang, J. Cao, and G. Min, "Minimizing movement for target coverage and network connectivity in mobile sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 7, pp. 1971–1983, 2014.

[30] M. Abo-Zahhad, S. M. Ahmed, N. Sabor, and S. Sasaki, "Rearrangement of mobile wireless sensor nodes for coverage maximization based on immune node deployment algorithm," *Computers & Electrical Engineering*, vol. 43, pp. 76–89, 2015.

[31] Z. Fu and K. You, "Optimal mobile sensor scheduling for a guaranteed coverage ratio in hybrid wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, Article ID 740841, 2013.