A Source Location Privacy Preservation Method Using Mixed Fake Sources and Phantoms

Zhen Hong *Member, IEEE,* Wentao Chen, Taotao Li, Jie Su

***Abstract*—Industrial cyber-physical systems (ICPS) have significantly improved production efficiency, e.g., Siemens applied ICPS in its Amberg factory, which achieved 75% production automation. However, the security problems involved have not been completely solved, e.g., the source Location privacy (SLP). Currently, with the expansion of the ICPS network size and the increasing number of devices, the existing defense process uses these device nodes as false nodes to enhance the security of the ICPS. However, this approach also results in additional energy consumption and transmission delays. To address the above challenges, we propose a solution to mix false sources and phantom strategies (i.e., Phantom-backbone-Fake, PBF). Firstly, a relay phantom node selection algorithm is proposed because adversaries are prone to track source nodes through fixed routes. We aim to optimize the path from the source node to the relay node and then to the sink node to minimize transmission delays. Ultimately, we devise a comprehensive strategy that considers both energy efficiency and distance indicators for the selection of appropriate false nodes. Through simulation and analysis, we demonstrate that our approach improves security and overall network performance.**

***Index Terms*—Industrial Cyber-Physical Systems, Source Location Privacy, Fake Source**

I. Introduction

In recent years, the emergence of Industrial Cyber-Physical Systems (ICPS) has made a unique and specialized advancement within the industry [1]. However, as the interconnections between devices within the system deepen, the potential attack will further enlarge. While external physical attacks pose a significant threat, the risks from inadvertent behavior or deliberate attacks by insiders are even more dangerous since they can easily access the ICPS network [2]–[5].

Once the location of a critical node has been determined, an attacker can exploit its vulnerabilities and weaknesses to compromise the system, tamper with data, disrupt production, or damage equipment. These actions can have a serious impact on infrastructure, production processes, and public safety. An example of this is the incident at Maroochy Shire's new wastewater treatment system in Queensland, where for some reason internal staff took control of 150 sewage pumping stations via wireless transmitters, misdirecting key sensors and ultimately leading to the release of one million liters of untreated sewage and causing severe damage to the local environment. [6]. Preventing internal attacks therefore becomes critical, especially when external attacks can be prevented [7], [8].

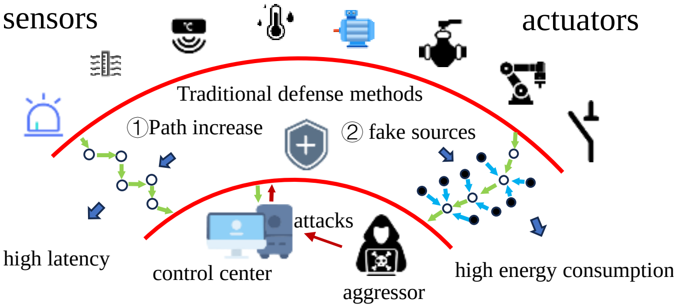


Figure 1: Consequences of high latency and high consumption

However, some of the currently proposed solutions such as Source Location Privacy Protection (SLP) are inadequate [9], [10]. They more or less enhance security at the expense of the performance of the system. As shown in Figure 1, random walk (RW) [11] and phantom routing (PR) [10], This approach comes at the cost of increased system transmission delay. and false source schemes like [12]–[14] at the cost of consuming the energy of other sensing nodes. Most of these methods enhanced security by increasing the distance from the source node to the sink node and by using a large number of false sources to interfere with the attacker. In some small systems, energy consumption and delays may be ignored, but in large Industrial Cyber-Physical Systems, such as smart grid systems and intelligent transportation systems, real-time and cost requirements are extremely high. Tiny transmission delays as well as unnecessary energy losses may lead to delays in control signals, and energy voids in some of the sensing nodes [15]. This may affect the system's real-time adjustments to equipment or processes, as well as increase the system's operating costs, which may ultimately force companies to cut production capacity or reduce equipment uptime, thus affecting productivity.

Therefore, it takes more than a simple solution to improve the privacy of ICPS. A routing scheme that enhances security while reducing energy consumption and transmission delay is essential. To improve privacy without increasing the energy consumption and transmission delay of the existing schemes, and at the same time to solve the problems of an unbalanced distribution of false sources and energy voids, we propose a scheduling scheme called PBF. PBF consists of three components: phantom deployment, backbone construction, and false

This work was supported by National Natural Science Foundation of China under Grant 62072408, Zhejiang Provincial Science Fund for Distinguished Young Scholars under Grant LR24F020004, and Zhejiang Provincial New Century 151 Talent Project. (*Corresponding author: J. Su*).

Z. Hong, W. Chen, T. Li, and J. Su are with the Institute of Cyberspace Security, and College of Information Engineering, Zhejiang University of Technology, Hangzhou, Zhejiang 310023 China. e-mail: {zhong1983, 211122030044, 2111903074, jiesu}@zjut.edu.cn.

message scheduling.

The contributions of this paper are concluded as follows.

- We propose a novel framework for backbone network construction aimed at phantom node selection throughout the network area and hierarchy. It delineates the entire network space and hierarchy that facilitates the construction of efficient backbone networks. The goal of our method is to reduce information transmission delays while significantly improving privacy protection measures.
- A novel fake-source scheduling method is devised to carefully select suitable fake sources through a dual screening process of energy consumption and distance metrics. It not only significantly extends the safety period of the entire network but also keeps lower energy consumption.

The subsequent sections of the paper are organized as follows. Section II discusses the related work about SLP. Afterward, we introduce the system model including the network and attack model in Section III. The detailed descriptions of the PBF algorithm are proposed in Section IV. Section V evaluates the algorithm's performance through simulation. Finally, we conclude our paper and give the future work in Section VI.

II. Related Work

Since the inception of source location privacy (SLP), many researchers have moved the focus to its challenges [10]. Generally, the previous studies can be classified into five groups based on variations in routing structures: false data, random wandering, multipath routing, phantom routing, and anonymous cloud-based schemes.

A. False Data

The method incorporates false nodes to disrupt potential attackers. Specifically, Wang et al. [16] proposed a hierarchical source location privacy-preserving scheme (SSLP-NC) for autonomous underwater vehicles, introducing a hierarchical network structure and different fake source selection mechanisms. Recognizing the dynamic nature of underwater sources, Wang et al. [17] employ fuzzy processing to safeguard the location privacy of dynamic sources. Furthermore, to address challenges in balancing security and efficiency inherent in traditional schemes, He and Han et al. [18], [19] intervene in the adversary's tracking of data sources and enhance performance through the strategic planning of fake packets and concealed traffic, respectively.

B. Randomized Wandering

To mitigate energy consumption, Bradbury et al. [20] proposed an SLP algorithm named Dynamic Single Routing (DynamicSPR), employing directed random wandering as a strategy for spurious source allocation to reduce energy usage. Additionally, Chen et al. [21] proposed a forward random walk (FRW) scheme, forwarding to next-hop nodes by randomly selecting nodes with smaller hop counts from the set of neighboring nodes. However, the FRW scheme establishes only a single path between the receiver and the source, leading to insufficient SLP protection. To address this limitation, Mukamanzi et al. [22] adopted three-phase or four-phase routing strategies with biased random wandering and greedy wandering, aiming to enhance the cycle and lifetime of the network.

C. Multi-Path Routing

To protect data from attacks, Han et al. [23] generate dynamic multipath routing packet slices for transmission from the perspective of sink nodes, while Wang et al. [24] designs a routing protocol for multipath distribution from the viewpoint of message flow, aiming to maximize the average backtracking time of the adversary. Both approaches aim to maximize source location privacy. Conversely, Sun et al. [25] effectively increases the number of randomized directional paths by intensifying the randomization of data transmission paths and employing directional routing algorithms to divert packets away from source locations. However, this protocol incurs significant energy consumption and delay. To address this concern, Koh et al. [26] select optimal paths using the Bayesian maximum a posteriori (MAP) estimation method, striking a balance between energy cost and location privacy to preserve network performance.

D. Phantom Routing

To overcome the limitations of the fake source packet routing protocol, Mutalemwa et al. [27] introduce randomized secondary phantom nodes instead of fake source packets to mitigate its drawbacks. Although this protocol achieves robust Source Location Privacy (SLP) protection with low communication overhead, its security level is comparatively lower. In response, Ozturk et al. [10] propose a two-stage phantom routing approach. In the initial phase, source packets are randomly unicast, and in the second phase, messages are disseminated to the base station using the flooding technique, extending the safe period but also leading to high energy consumption. To address this issue, He et al. [28] reduce energy consumption by dividing the network into multiple sectors, relaying neighboring packets through nodes in different sectors to obtain random routing paths, and controlling the routing range by setting a hopping threshold for the packets. Additionally, Mahmoud et al. [29] leverage the coordinates of sector regions and center nodes to enhance the geographic diversity of virtual nodes for source location security.

E. Anonymization-Based Cloud Solutions

The solution typically involves blending real and fake packets from a specific region, rendering it impossible for the attacker to discern the specific transmission path. Wang et al. [13] establish an anonymous cloud with minimal energy consumption using a lightweight threshold message-sharing algorithm, preventing the attacker from pinpointing the source node through traffic patterns. Simultaneously, Han et al. [12] confound adversaries and offer comprehensive privacy location protection by randomly altering packet destinations and creating multiple routing paths using multiple receivers from the perspective of fake hotspots and fake packets. In a similar vein, Mahmoud et al. [30] counteract the inconsistency of traffic patterns from a fake traffic cloud perspective, effectively safeguarding the location privacy of the source nodes.

In summary, past approaches sacrifice network performance to provide better source location privacy. Simply using phantom nodes and creating a fake source mechanism can obfuscate the global attacker's backtracking path. This process ensures source location privacy, but excessively long communication paths and a high frequency of false message flooding can significantly degrade network performance. Therefore, in this paper, we improve the deployment method of phantom nodes and the propagation pattern of false messages, reducing the communication paths in conjunction with the use of a small number of false source nodes, which improves the overall performance while enhancing security. This paper provides a better solution.

III. System Model

In this section, we abstract real-world application scenarios into network models and then provide a comprehensive description of all models.

A. Network Model

In the designated monitoring area, a multitude of sensor nodes, encompassing both source and sink nodes, are uniformly distributed. Each node is equipped with transceivers for communication and sensing information. The attacker's objective is to trace the location of the sending node by analyzing the signal in reverse until the source node is identified. All nodes share identical characteristics, including computational power, initial energy, and cache memory. The communication distance is equal to the sensing distance, enabling neighboring nodes to communicate if the distance between them is less than the communication radius. Information such as hop count and ID can be exchanged between adjacent nodes.

B. Attack Model

The attackers exploit signals in the vicinity to locate nodes transmitting messages, refraining from altering or disrupting routing paths, packets, or sensor nodes to maintain the network's normal operation. Their perceived distance aligns with the communication distance of the sensor nodes. Starting at the sink node, the attacker intercepts the signal, analyzes the traffic information, and then proceeds to the next node in the signal's trajectory, awaiting a new packet. By carefully following the message hop by hop, the attacker ultimately reaches the source node.

C. Performance Metrics

Safe period: The safe period represents the count of cycles before an attacker can identify a source node. Assuming data sources are produced at a high frequency, the attacker can only backtrack once within a sampling period. Consequently, the maximum safe period is determined.

$$\max T_s \tag{1}$$

where $T_s \leq T_{max}$, $T_{max}$is the potential maximum safety period which is a constant. In the ideal scenario, the safety period can be set to a large value without considering node failure. However, a high maximum safety period may result in a large amount of computational overhead. Therefore, combined with the node's lifetime, the boundary of the safety period (i.e., T_{max}) is determined by enumeration with the minimum simulation time to ensure the value is as large as possible. The minimum simulation time is the shortest running period required by the system to ensure the reliability and validity of the simulation results during the operation of the simulated system. By setting a reasonable minimum simulation time, it can be verified that the value of Tmax can be accurately calculated and applied in the simulation process. As well as avoiding excessive computational overhead caused by setting Tmax too high. The simulation time is usually modeled to simulate the operation of the actual system, thus providing a relative measure.

Energy consumption: This paper adopts the energy consumption model in [31], [32], which applies to a topical adversary. The energy consumption model can be chosen according to the distance between nodes. Assuming that the transmission distance between the sender and the receiver is l, The energy consumed by the node to send γ the bit data is E_{TX}.

$$E_{TX}(\gamma, l)) = \begin{cases} E_{elec} \cdot \gamma + E_{mf} \cdot \gamma \cdot l^4, l > l_0 \\ E_{elec} \cdot \gamma + E_{fs} \cdot \gamma \cdot l^2, l \leq l_0 \end{cases} \tag{2}$$

where l_0 is the threshold distance. When $l > l_0$, the nodes communicate with each other using the multipath fading model and the path loss coefficient is E_{mf}. When $l \leq l_0$, the nodes communicate with each other using the free space model and the path loss coefficient is E_{fs}. E_{elec} denotes the energy consumed for each unit of bit data received or sent. The energy consumed by the node to receive γ bits of data is E_{RX}:

$$E_{RX}(\gamma) = \gamma \cdot E_{elec} \tag{3}$$

To alleviate the impact of node energy depletion on network communication and extend the network's lifecycle, we aim to optimize node energy consumption, reducing additional overhead. We denote (E_i) as the maximum average overhead per period when the first battery runs out of power. The objective of minimizing energy consumption can be expressed as

$$minE_i = \frac{1}{T_s} \max_{1 \leq i \leq |V|} \sum_{j=1}^{T_s} E_i^j \tag{4}$$

where E_i^j refers to the overhead of node i in period j that results from data processes such as broadcasting, receiving, and aggregation. Specifically, the analysis and processing of fake messages are regarded as parts of data fusion. V is a set of nodes in the cycle.

Transmission delay: transmission delay in wireless communication networks involves factors such as antenna height gain and system loss factor. When ε bits of data are transmitted between node i and node j at a distance of l, the transmission delay due to communication link instability is ignored to simplify the calculation method of transmission delay. Consider the transmission delay D_t from the source node to the sink as the superposition of the transmission delays of all single-hop $hop_{ij} \in R$ on the transmission path R:

$$D_{i,j} = \sum_{hop_{ij} \in R} \frac{\varepsilon \cdot t}{1 - exp(-0.5\gamma_{ij})} \tag{5}$$

Where, t denotes the time taken by the node to receive and process a unit bit of data in an ideal environment without interference, and $\gamma_i j$ denotes the signal-to-dry ratio, which is affected by the ambient noise and is calculated as follows:

$$\gamma_{ij} = \begin{cases} \frac{g_{ij} \cdot P^t_{ij}}{(P_e + \sum_{k \in N_i, k \neq i} P^r_{kj}) l^4}, l > l_0 \\ \frac{g_{ij} \cdot P^t_{ij}}{(P_e + \sum_{k \in N_i, k \neq i} P^r_{kj}) l^2}, l \leq l_0 \end{cases} \tag{6}$$

in where P_e denotes the ambient noise power around the receiver, N_i denotes the set of neighboring nodes other than the sender within the receiver's communication range, P^r_{kj} denotes the power of the signal received by the receiver. g_{ij} is related to the transmission power and the transmission distance of the wireless device, and P^t_{ij} denotes the energy consumption for transmitting a unit of bit of data. To simplify the transmission delay, link quality and message retransmission are not considered. The transmission delay T_R from source to aggregation can be expressed as a superposition of the single-hop communication delay R on the transmission path as follows.

$$T_R = \sum_{e_{i,j} \in R} D_{i,j} \tag{7}$$

However, high latency also affects the performance of the network, so in this paper, the transmission latency is also optimized as follows

$$minT_R = minmax_j T^{(j)}_R, j = 1, 2, ..., T_{safe} \tag{8}$$

where $T^{(j)}_R$ is the delay of j cycles on path R, and its maximum value is used as an evaluation metric for the transmission delay of the routing protocol. In this paper, to simplify the transmission, we do not consider the additional delay caused by the link quality and retransmission mechanism.

IV. Proposed Technique

This section introduces a novel scheme that integrates multi-objective holistic planning models to enhance source location privacy, minimize energy consumption, and reduce transmission delay. The scheme is structured into four phases: initialization, phantom node selection, backbone path construction, and false source scheduling, As shown in Figure 2. In this section, according to Algorithm 1, all the real nodes outside the visibility region have a chance to act as ghost nodes, by constructing the backbone path, and all the remaining nodes will be calculated as to whether they can act as fake nodes or not according to Algorithm 3.

A. Initialization Phase

To initialize the network, the sink nodes employ a breadth-first search using a flood routing protocol to establish a hierarchical structure throughout the network. The sink node initially sets its depth value to zero, incrementing it by broadcasting to a value of 1. Each node within its transmission range receives and updates the depth information. This process continues until the entire network is covered. Consequently, all sensor nodes acquire information regarding the number of hops to the sink node, details about neighboring nodes, and unique identification, denoted as the network's id. The initialization phase is executed once when the network is deployed and the initialization is not re-executed when subsequent nodes are started. This is to prevent an attacker from inferring important information about the network structure by monitoring the initialization process at the startup of each node.

B. Selection of Phantom Nodes

Phantom nodes are located near the source node and simulate the data transmission behavior of the source node to lure attackers away from the source node. Therefore, choosing a suitable phantom node can effectively improve security and confidentiality.

The visibility region around the source node must be considered when selecting a suitable phantom node. Here,R, H, L, and Y represent the perceptual radius of the node, the distance from the source node to the sink node, the distance from the phantom node to the sink node, and the distance from the source node to the phantom node, respectively. As shown in Fig. 2, θ denotes the angle of the visible region around the source node. α and β denote the angle between the phantom node and two nodes, the source node and the sink node, respectively. An attacker's presence in this region greatly increases the risk of source node exposure. By ensuring that $\alpha > \theta . \beta > \theta$, the phantom node we choose must be located outside the visible region around the source node to ensure that the attacker cannot directly recognize the source node in the visible region, therefore, the selection of a suitable phantom node should satisfy the following conditions:

$$\begin{cases} \theta = asin\frac{R}{H} \\ \beta = cos\frac{H^2 + L^2 - Y^2}{2 \cdot H \cdot L} \\ \alpha = acos\frac{H^2 + Y^2 - L^2}{2 \cdot H \cdot Y} \\ \alpha > \theta . \beta > \theta \end{cases} \tag{9}$$

Nodes meeting these conditions form the set of visible phantom nodes. This set of visible phantom nodes is then categorized into tiers determined by the distance from the source node, denoted as $h_1, h_2, ..., h_m$. Where

$$\begin{cases} h_1 > R \\ h_m < Dist_{(source,sink)} \end{cases} \tag{10}$$

Fixing or centralizing the chosen phantom nodes' location may escalate the capture risk and increase energy consumption. To mitigate this, the forward region is uniformly segmented into Q_1, Q_2, Q_3, Q_4, utilizing the line between the source and sink nodes as the central axis. During each iteration, a phantom node $P^{(j)}, (j = 1, 2, ..., T_s)$, is randomly

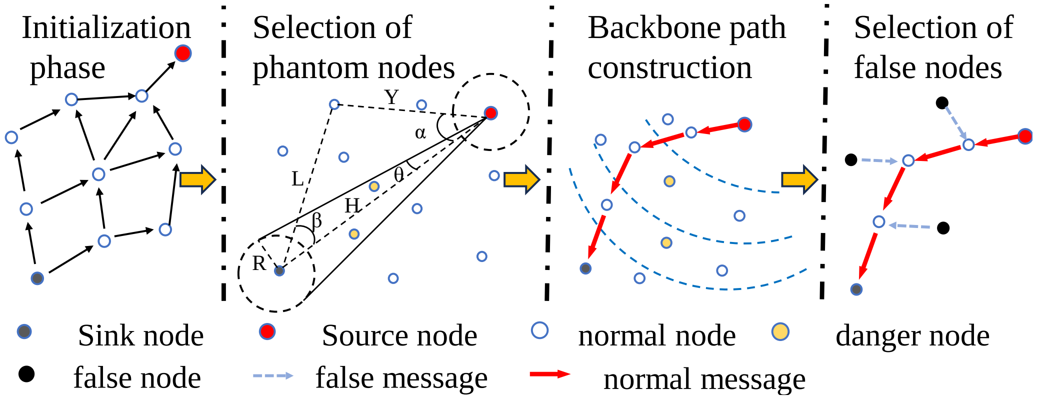


Figure 2: Programmatic framework

selected from various positions within h and Q to enhance randomness.

In this paper, we propose a method for selecting phantom nodes, see Algorithm 1 for details. The basic implementation process of the algorithm is as follows: First, calculate the distance H from the source node to the converging node and update the angle θ. Then iterates over all the nodes in the network and builds a set of candidate nodes, Pset. Each node in the set of candidate nodes is filtered. The nodes that satisfy the conditions are added to the phantom node set P according to Eq. 9. Finally, the auxiliary sets h_set and Q_set are generated. Through this algorithm, The nodes suitable to serve as phantom nodes can be selected, thereby enhancing the security and confidentiality of the source nodes.

C. Backbone Path Construction

The backbone path's construction directly affects the source location's confidentiality and network performance. Usually, the attacker can quickly infer the source location from a short path, which results in low privacy. By contrast, a long path provides better privacy but results in additional latency and overhead. Therefore, the key to backbone path design is to create optimal transmission paths and ensure enough idle nodes on these paths to act as decoy sources.

Regarding the design of paths after constructing the network hierarchy (i.e., tree topology) specified, we use the idea of heuristic search to find the paths from source to aggregation, optimized for a single objective search. The objective function $f(x)$ is constructed based on the current node x:

$$f(x) = g(x) + h(x) \tag{11}$$

$f(x)$ is an estimate of the cost, from the initial state to the goal state via state x. $g(x)$ is the actual cost, of going from the initial state to state x in the state space. $h(x)$is the estimated cost of the best path from state x to the goal state. In the node selection process, the node with the highest aggregate priority is consistently chosen for traversal.

In this network, an optimal path can be found which reduces the latency.

Proof. Let the coordinates of the parent node be (x_0, y_0) and the coordinates of any of its children be (x_i, y_i), so for $h(x)$ between the two, it must satisfy.

$$h(x_0) \leq h(x_i) + Cost_{0,i} \tag{12}$$

$cost0, i$ is the value of generation from the parent node to the next child node, constant greater than or equal to 0, i.e., to satisfy that the cost function is monotonically increasing. According to this objective function, it can be seen that for $f(x)$ of the parent and child nodes, there are always

$$\begin{cases} f(x_0) = g(x_0) + h(x_0) \\ f(x_i) = g(x_i) + h(x_i) \end{cases} \tag{13}$$

During the search process of the algorithm, the actual cost $g(x)$ is increasing, which can be introduced by the following equation:

$$g(x_i) = g(x_0) + Cost_{0,i} \tag{14}$$

The generation value of a child node is equal to the generation value of the parent node plus the generation value from the parent to the next child node. Substituting into the second equation of Eq. 13, the following equation is obtained:

$$f(x_i) = g(x_0) + h(x_i) + Cost_{0,i} \tag{15}$$

resulting in

$$g(x_0) + h(x_0) \leq g(x_0) + h(x_i) + Cost_{0,i} \tag{16}$$

obtainable

$$f(x_0) \leq f(x_i) \tag{17}$$

During the execution of the algorithm, the succeeding $f(x)$value is greater than the current $f(x)$value at times, i.e., $f(x)$ is monotonically increasing in the subsequent search extension to the child nodes, and there will be no local minima, so the paths planned using this algorithm must be optimal paths.

Where $h(x)$ is the expected cost of node x from the endpoint, using the Manhattan distance.

$$d_{0,i} = |x_0 - x_i| + |y_0 - y_i| \tag{18}$$

□

In addition, when choosing the above function to construct the backbone path, in which the backbone node selection also needs to be filtered, this paper is based on the centrality theory [33], i.e., the more the number of neighbors of a node, the lower the probability of the attacker to capture the node.the probability of captureCP_i of node i is calculated as follows:

$$CP_i = \frac{1}{|N_i|} \tag{19}$$

Where $|N_i|$ denotes the number of neighbor nodes of the node. Nodes with a greater number of neighboring nodes are in a more secure position.In addition, when selecting nodes on the backbone path, nodes with as much residual energy as possible need to be considered to avoid energy voids caused by energy depletion of the nodes during information transmission. It is also important to consider the size of the average distance to the neighboring nodes, because after that false nodes are generated to a large extent in these nodes, and the smaller the average distance the smaller will be the additional energy overhead caused by false nodes. The probability of being selected $C_{(u,v)}$ is as follows:

$$C_{(u,v)} = \frac{E_u}{\sum dist(v,u)} \tag{20}$$

Where $dist(V,u)$ is the distance of nodes $u, v \in V$, V is the set of neighboring nodes, and u is the selected node. E_u is the current node energy value, for which we propose an energy-efficient minimum trunk capture probability path search method as in Algorithm 2.

The basic implementation process of the algorithm is as follows: Calculating the value of $f(x)$ from the start node to the child nodes, selecting the child node with the smallest $f(x)$ from it as the next point of the search, and taking the current node as the parent of the next node, iterating back and forth until the next child node is the target point, and finally backtracking to the starting point through the parent of the target node.

Algorithm 1 Phantom Node Select

```
**require**:$R$ : perceptual radius, $N$ : All nodes, source, sink
**Output**:P : phantom node set
Calculates $H$:Distance between sink and source
update $\theta \leftarrow \arcsin \frac{R}{H}$
**for** $vi$ *in* $N$ **do**
    Build the candidate set $P_{set}$
**end**
**for** $i$ *in* $P_{set}$ **do**
    L$\leftarrow$ distance(i,source)
    Y$\leftarrow$ distance(i,sink)
    $\alpha \leftarrow \arccos \frac{H^2+Y^2-L^2}{2*H*Y}$
    $\beta \leftarrow acos\frac{H^2+L^2-Y^2}{2*H*L}$
    **if** $\alpha>\theta$ ,$\beta>\theta$ **then**
        $P \leftarrow i$
    **end**
    $h_1, h_2, ..., h_m \leftarrow h\_set(P)$
    $Q_1, Q_2, Q_3, Q_4 \leftarrow Q\_set(P)$
**end**
```

Algorithm 2 Backbone Path Building

```
**Input**:start point: $s$, target point:$t$
**Output**:path
Calculates $f_s \leftarrow G_s + H_s$
open list :O,close list :C
**while** *$O$ is not empty* **do**
    get $u$ from O
    **if** *$u$ is target* **then**
        path $\leftarrow$ reconstruct_path($u$)
        return path
    **end**
    **else**
        $O \setminus \{u\}, C \cup \{u\}$
        v$\leftarrow$ neighbors($u$)
        **for** *$i$ in $v$* **do**
            The parent of node $i$ is node $u$
            V$\leftarrow$ neighbors(i)
            $C_{(i,V)} \leftarrow \frac{E_i}{\sum dist(V,i)}$,$CP_i \leftarrow \frac{1}{|N_i|}$
        **end**
        Sort $v$ $s.t.$ $C_{(1,V)} \geq C_{(2,V)} \geq ... \geq C_{(v,V)}$
        $v \leftarrow itertools.islice(v, 5)$
        Sort $v$ $s.t.$ $CP_1 \leq CP_2 \leq ... \leq CP_v$
        $point \leftarrow argmin(f_s)$ in $v$
        **if** *point not in O* **then**
            put the dot into O
        **end**
    **end**
**end**
```

D. Selection of False Nodes

Diverging from phantom nodes, fake nodes imitate the behavior of regular communicating nodes without actually transmitting data. Their purpose is to mislead observers and obscure the real communication nodes' locations. Throughout the network, non-backbone nodes can function as false sources and disseminate false information to protect privacy, although at the cost of increased latency and energy consumption.

Furthermore, in the absence of artificially introduced false sources, the attacker will solely retreat to the backbone network in subsequent traceability attempts. To address this challenge, this chapter proposes an optimal virtual false source dispatch mechanism that leverages the retrospective behavior of the Markov chain to simulate attacker movements. Given the stochastic nature of the attacker and other probability-driven random movements, each anti-tracking maneuver operates independently. Thus, their mobility pattern adheres to Markovian principles, enabling their movement processes to be effectively represented by Markov chains.The state space of the attacker is $X = \{v_1, ...v_V\}$,$v_j \in X$ represents the position of the node corresponding to state j,.the transition relationship between the state space satisfies

$$\begin{aligned} &P\left\{X_{i+1} = v_j | X_1 = v_{i_1}, ..., X_{i-1} = v_{i_{i-1}}, X_i = v_i\right\} \\ &= P\left\{X_{i+1} = v_j | X_i = v_i\right\} \end{aligned} \tag{21}$$

The state space can be expressed as

$$P = [p_{i,j}]_{V \times V}$$

$$
\begin{aligned}
s.t. \quad p_{i,j} =& P\left\{X_{n+1} = v_j | X_n = v_j\right\} \\
=& \begin{cases} \frac{1}{|I_i+1|} & v_j \in I_i \bigcup \left\{v_i\right\} \\ 0 & otherwise \end{cases}
\end{aligned} \tag{22}
$$

Among them, i_i represents the neighbor node of node i. At the same time, there is a single source node in the network that captures the node to stop the attacker's activity. Therefore, the characteristics of the attack process are a separate absorption state (that is, the location of the source node v_i), and its probability of conversion is

$$
P_{i,j} = \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases} \tag{23}
$$

Moreover, given that the attacker's movement process conforms to a Markov chain, the concept of first reach time is applicable. For any pair of nodes i and j, $T_{i,j}(\omega)$ represents the duration until the attacker initially arrives at node j while retracing its steps from node i.

$$
T_{i,j}(\omega) = min\left\{n : X_0 = i, X_n(\omega) = j, n \geq 1\right\} \tag{24}
$$

WhereX_0 denotes the initial state, and $X_n(\omega)$ represents the state reached after implementing the state transfer strategy ω from the initial moment.

In summary, the first arrival time from location i to location j, excluding the source node, is denoted by $T_{i,j}(\omega)$. Leveraging the Markovian nature of the attacker's movement pattern, the probability of his initial arrival at state j after n time steps from state i can be expressed as

$$
f_{i,j}^{(n)} = P\left\{T_{i,j} = n | X_0 = i\right\} \tag{25}
$$

The first arrival probability is characterized by the following: for any states i and j and for all $1 \leq n \leq \infty$, there exists

$$
p_{i,j}^{(n)} = \sum_{l=1}^{n} f_{i,j}^{(l)} p_{j,j}^{(n-l)} \tag{26}
$$

where $p_{j,j}^{(0)} = 1$. Ultimately, the conditional mathematical expectation of $T_{i,j}$ yields $\mu_{i,j}$, signifying the average transition time from state i to state j, originating from state i and culminating in the initial arrival at state j.

$$
\mu_{i,j} = E\left\{T_{i,j} | X_0 = i\right\} = \lim_{T^{max} \to \infty} \sum_{n=1}^{T^{max}} n f_{i,j}^{(n)} \tag{27}
$$

Indeed, the average transfer time for an attacker to reach the source node location from the initial location can be evaluated in terms of $\mu_{i,j}$, which reflects the system's security. To optimize the privacy level, we set the optimization objective of maximizing the average transfer time as shown in the following equation. $\mu_{src,asset}$ denotes the average transfer time for the attacker to reach the source node location from the initial location. Ultimately, we transform the fake message scheduling problem into a problem of estimating the Markov chain state transfer matrix.

$$
\max_{[p_{i,j}]} \mu_{src,asset}\left(\left[p_{i,j}\right]\right) \tag{28}
$$

Table I: The model parameters

Notation	Description	Value
E_{elec}	energy dissipated per bit	50 nJ/bit
ε_{fs}	radio amplifier energy in free space	10 $pJ/bit/m^4$
ε_{mp}	radio amplifier energy with Rayleigh fading	0.0013 $pJ/bit/m^2$
E_{da}	energy for data agrregation	5 nJ/bit/signal
d_0	crossover distance	231 m
$t_{i,j}$	packet forwarding capacity	100 ns/bit
p_e	noise power for the environment	0
$g_{i,j}$	parameter of wireless device	$9.488 * 10^{-5} m^2 (d<d_0)$ $5.0625 m^4 (d \geq d_0)$
$p_{i,j}^{t}$	transmitting power	5 nJ/bit/singal

The task of estimating the state transfer matrix during the false message scheduling phase fundamentally entails establishing communication links among individual nodes within the network. In recent years, topology control has advanced energy efficiency and facilitated low-latency transmission in network systems. Leveraging the topology control framework, this paper introduces a distributed false message scheduling scheme founded on probabilistic selection. The scheme factors in nodes' residual energy and their neighbors' average distance in each cycle to determine the probability $p_i^{T(l)}$ for nodes to propagate false.

$$
p_i^{T(l)} = \frac{exp^{\frac{n_b}{m}} \cdot \frac{E_i}{E_{init}}}{exp^{\frac{\sum dist_{i,j \in V}}{m}} + exp(dist_{(i,source)})} \tag{29}
$$

Where n_b is the set of the adjacent backbone of node i, m is the number of neighboring nodes, E_i node i current node energy, E_{init} node's initial energy, $\sum dist_{i,j \in V}$ is the cumulative distance between node i and neighboring nodes, and $dist_{(i,source)}$ is the distance between node i and the source node, because the selection of phantom nodes is mostly concentrated near the source node, the false source node may be treated as the next backbone node thus making the attacker closer to the real path, so selecting false source node in the proximity to source node interferes with the security of the whole network. Algorithm 3 gives the pseudo-code for fake message scheduling.

The basic implementation process of the algorithm is as follows: Step 1:Each node broadcasts a query to update the state of neighboring nodes. Step 2:Phantom nodes are selected and the backbone network is constructed. Step 3:Calculate the probability of each node being a fake source and decide whether to act as a fake source or not. Step 4:The source transmits data along the backbone network and the fake source broadcasts a fake message. Then the process moves to the next cycle and returns to step 1.

V. Performance Evaluation

In this section, we assess the performance of PBF and conduct a comparative analysis with PR, BLS, TDR, EBBT, and FSSE under both dense and sparse environments, representing varying numbers of nodes in different networks. We evaluate three key metrics: source location privacy security, transmission latency, and energy consumption. To ensure robustness, each experiment is repeated across 20 networks, These are all

Algorithm 3 Calculate Fake Source Node

```
Input:current node:$C_n$
output: Whether to send a false message
require: A fully connected network, P: path
source, sink,backbone$\in$ A fully connected network
V $\leftarrow$ neighbors($C_n$), m$\leftarrow$ $|V|$
init $N_b \leftarrow 0, dist \in \emptyset$
if $C_n \notin \{source, sink, backbone\}$ then
    for $v$ in $V$ do
        if $v$ in $P$ then
            $N_b \leftarrow N_b + 1$
        end
        $\sum$ dist$\leftarrow$Distance(v, $C_n$)
    end
    $D_v \leftarrow \frac{\sum dist}{m}$ $D_n$ $\leftarrow$Distance(source, $C_n$)
    $D_s$ $\leftarrow$Distance(source, sink)
    $Q \leftarrow \frac{N_b}{m}$, $E \leftarrow \frac{E\_node}{E\_init}$, $D \leftarrow \frac{D_n}{D_s}$
    calculate $P_i \leftarrow \frac{exp^Q \cdot E}{exp^{D_v} + exp^D}$
    Take a random number R
    if $R < P_i$ then
        return $P_i$
    end
end
```

distinct networks with 1000 nodes randomly and uniformly distributed, following the methodology outlined in this paper. All simulation results are presented as averages.

A. Simulation Setup

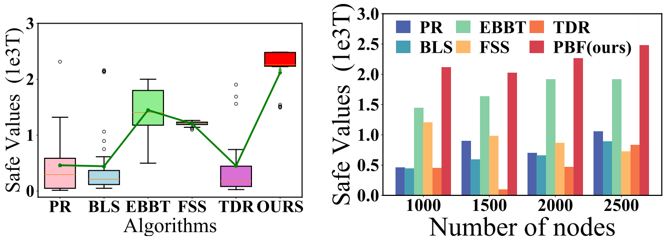
Let us consider a 1000 m × 1000 m network deployment model. 1000 sensor nodes are deployed uniformly at random. The sensor nodes are deployed uniformly and the communication radius between the sensor nodes and the attacker is all 50 m. Each sensor node is initially loaded with 1 Joule of energy. The location of the source node and the location of the aggregation node are (-333, 0), (333, 0). The specific parameters of the configuration are shown in Table 1. Assume that the attacker starts its backtracking task from the aggregation node as this is the focal point of all network traffic. The Tmax is set to 3000 and each trial ends when the adversary reaches the source node or reaches the maximum safe period. The simulation results given here are averaged over 100 trials.

B. Results Analyses

We conducted an initial comparison within a 1000-node environment. The outcomes, depicted in Table II, consistently favor our approach, showcasing distinct advantages in enhancing safe periods without excessively elevating energy consumption or latency. Here T_safe is the number of cycles before the attacker recognizes the source node. Ideally, Tsafe should be as large as possible to ensure that the location of the source node is not easily discovered by the attacker. Subsequently, our scheme will undergo validation through diverse experiments conducted in various environments.

Table II: Comparison results of the six schemes in 1000 nodes

	$T_{safe}(hop) \uparrow$	$E_{cost}(nJ) \downarrow$	$latency(ns)\downarrow$
PR [34]	461	11297231	6159550
BLS [35]	442	15680436	5811720
EBBT [36]	1448	51081738	65304066
FSSE [15]	1205	54261618	241073322
TDR [37]	451	43261090	28393850
PBF(ours)	2117	8436043	22383970



(a)

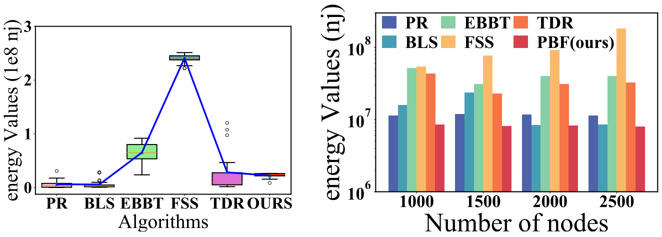
(b)

Figure 3: (a).safety period under six algorithms, our program is significantly better than other (b).safety period of six algorithms with different numbers of nodes, where our scheme is at an advantage no matter in which node

Comparing the results in Fig 3,it verifies that our method has a good enhancement effect on the safe period. It is observed that the safety period of the algorithm proposed in this paper is significantly better than PR, BLS, FSS, and TDR, and slightly higher than EBBT. Even in the PBF algorithm, there are a few cases where the safety period is shorter. This is because our algorithm may have a smaller number of initial fake sources when using a random scheduling strategy, generating fake sources far away from the backbone network. As a result, fake sources close to the backbone may not effectively induce the attacker, allowing them to quickly locate the source. Despite the presence of a shorter safe period, our algorithm still outperforms other algorithms overall. It is worth noting that as the number of nodes increases, our algorithms continue to perform well in terms of security.

Analyzing the results presented in Fig 4, we compare the energy consumption under several algorithms. The increase in energy consumption per node can be attributed to the large number of false messages generated by numerous false sources. However, our algorithm schedules the false nodes based on the actual energy consumption of each node and uses probabilistic selection, meaning that no node consistently broadcasts fake messages. Consequently, it achieves a high level of privacy protection at the cost of less energy consumption and additional communication overhead. As illustrated in the figure, our algorithm consumes much less energy than EBBT, TDR, and FSS, while providing more stable energy consumption overall.

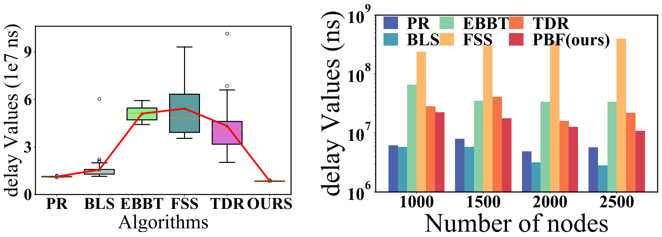
Examining the results depicted in Fig 5, we compare the transmission delay performance of the six algorithms, including both instantaneous delay and the number of hops



(a)

(b)

Figure 4: (a).energy consumption under six algorithms, our scheme has low energy consumption with a high safety period. (b). Energy consumption of six algorithms with different number of nodes, we are in an advantageous position



(a)

(b)

Figure 5: (a) .Delay under six algorithms, our scheme has low energy consumption with a high safety period. (b). delay for six algorithms with different numbers of nodes, we are in an advantageous position

from source to reception. PR, BLS, and TDR exhibit lower latency due to their shorter safety periods. Conversely, EEBT and FSS demonstrate higher delay. FSS employs a large number of false sources to mislead the attacker, thereby increasing transmission delay, while EEBT incurs a high base delay owing to its long backbone. In contrast, our algorithm considers optimal paths and the distance between nodes during backbone construction, resulting in lower latency. Moreover, as the number of nodes increases and the safety period lengthens, our algorithm consistently maintains better performance.

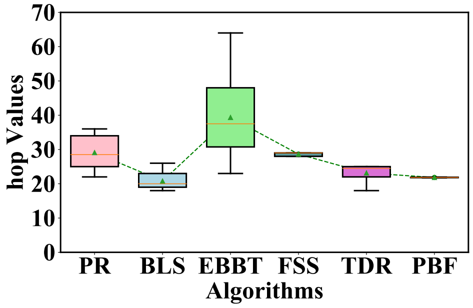


Figure 6: The minimum number of hops between the attacker and the source.

Furthermore, we conducted an analysis of the impact of these six algorithms on the attacker's ability to obfuscate, based on the minimum hop count between the source and the attacker. Generally, a larger minimum hop count indicates a better ability to obfuscate the attacker. As depicted in Fig 6, it is evident that BLS exhibits the lowest minimum hop count, indicating ineffective obfuscation of the attacker. In contrast, EEBT successfully keeps the attacker at a distance from the source node. Although EEBT has a relatively high safety period, it comes with increased delay and energy consumption as the hop count rises. Therefore, our approach does not solely aim for an excessively high hop count. Instead, it ensures relatively low latency and energy consumption while confusing the attacker through false sources. By reducing reliance on the backbone network and incorporating fake sources, we successfully achieve a balance between overall latency, energy consumption, and increased safety period.

VI. Conclusion

In this paper, we have enhanced source location privacy and system performance by introducing a protective scheme against attacks. The algorithm comprises three key components. Firstly, we propose the dynamic generation of phantom nodes, which are the basis for backbone paths. Subsequently, false messages are generated based on the current node conditions. Simulation results demonstrate that our algorithm can effectively reduce energy consumption while achieving a higher safety period than PR, BLS, EEBT, FSS, and TDR algorithms. We verified the algorithm's effectiveness in simulation, but the effectiveness of the algorithm in real environments, such as environments full of interference and background noise, still needs to be improved. Meanwhile, the effectiveness of the algorithm under an attacker model with active learning capability is not further proved. Therefore, given the difference between simulation and real-world applications, in the future, we will build a testbed for small- and medium-sized process industrial control systems similar to smart factories, such as water level control systems. Evaluate their performance in real network environments and against various attacker models.

References

[1] J. Chae, S. Lee, J. Jang, S. Hong, and K.-J. Park, "A survey and perspective on industrial cyber-physical systems (icps): from icps to ai-augmented icps," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 257–272, 2023.

[2] W. Hao, T. Yang, and Q. Yang, "Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Automation Science and Engineering*, vol. 20, no. 1, pp. 32–46, 2023.

[3] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang, and A. W. Colombo, "Advancements in industrial cyber-physical systems: an overview and perspectives," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 716–729, 2023.

[4] F. Tramarin, M. Luvisotto, A. Willig, and K. Yu, "Guest editorial: Industrial cyber–physical systems—new trends in computing and communications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3518–3522, 2021.

[5] H. C. Van Tilborg and S. Jajodia, *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[6] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *International conference on critical infrastructure protection*. Springer, 2007, pp. 73–82.

[7] A. P. Mathur and N. O. Tippenhauer, "Swat: A water treatment testbed for research and training on ics security," in *2016 international workshop on cyber-physical systems for smart water networks (CySWater)*. IEEE, 2016, pp. 31–36.

[8] S. Adepu, J. Prakash, and A. Mathur, "Waterjam: An experimental case study of jamming attacks on a water treatment system," in *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2017, pp. 341–347.

[9] N. Li, N. Zhang, and S. K. Das, "Relation privacy preservation in publishing online social networks," in *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier Inc., 2012, pp. 431–450.

[10] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks*, 2004, pp. 88–93.

[11] Y. Tscha, "Routing for enhancing source-location privacy in wireless sensor networks of multiple assets," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 589–598, 2009.

[12] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "Cpslp: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2739–2750, 2019.

[13] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 100–114, 2019.

[14] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2011.

[15] Z. Hong, R. Wang, S. Ji, and R. Beyah, "Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1337–1350, 2019.

[16] H. Wang, G. Han, Y. Liu, A. Li, and J. Jiang, "Auv-assisted stratified source location privacy protection scheme based on network coding in uasns," *IEEE Internet of Things Journal*, 2023.

[17] H. Wang, G. Han, W. Lai, Y. Hou, and C. Lin, "A multi-round game-based source location privacy protection scheme with auv enabled in underwater acoustic sensor networks," *IEEE Transactions on Vehicular Technology*, 2023.

[18] Y. He, G. Han, M. Xu, and M. Martínez-García, "A pseudopacket scheduling algorithm for protecting source location privacy in the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9999–10 009, 2021.

[19] G. Han, Y. Liu, H. Wang, and Y. Zhang, "A collision-free-transmission-based source location privacy protection scheme in uasns under time slot allocation," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1546–1557, 2022.

[20] M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 115, pp. 67–81, 2018.

[21] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.

[22] F. Mukamanzi, M. Raja, T. Koduru, and R. Datta, "Position-independent and section-based source location privacy protection in wsn," *IEEE Transactions on Industrial Informatics*, 2022.

[23] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in wsns intended for iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5527–5538, 2019.

[24] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.

[25] J. Sun, Y. Chen, X. Lv, and X. Qian, "A multipath source location privacy protection scheme in wireless sensor networks via proxy node," in *2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*. IEEE, 2022, pp. 280–286.

[26] J. Y. Koh, D. Leong, G. W. Peters, I. Nevat, and W.-C. Wong, "Optimal privacy-preserving probabilistic routing for wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2105–2114, 2017.

[27] L. C. Mutalemwa, M. Kang, and S. Shin, "Controlling the communication overhead of source location privacy protocols in multi-hop communication wireless networks," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2020, pp. 055–059.

[28] Y. He, G. Han, H. Wang, J. A. Ansere, and W. Zhang, "A sector-based random routing scheme for protecting the source location privacy in wsns for the internet of things," *Future Generation Computer Systems*, vol. 96, pp. 438–448, 2019.

[29] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "Psspr: a source location privacy protection scheme based on sector phantom routing in wsns," *International Journal of Intelligent Systems*, vol. 37, no. 2, pp. 1204–1221, 2022.

[30] M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2011.

[31] G. Cheng, S. Guo, Y. Yang, and F. Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2015, pp. 1–8.

[32] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on wireless communications*, vol. 1, no. 4, pp. 660–670, 2002.

[33] S. P. Borgatti, "Centrality and network flow," *Social networks*, vol. 27, no. 1, pp. 55–71, 2005.

[34] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *25th IEEE international conference on distributed computing systems (ICDCS'05)*. IEEE, 2005, pp. 599–608.

[35] T. Koduru and R. Manjula, "Source location privacy in wireless sensor networks: What is the right choice of privacy metric?" *Wireless Networks*, vol. 29, no. 4, pp. 1891–1898, 2023.

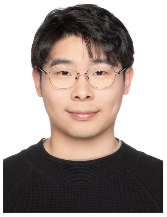
[36] H. Wang, L. Wu, Q. Zhao, Y. Wei, and H. Jiang, "Energy balanced source location privacy scheme using multibranch path in wsns for iot," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 6654427, 2021.

[37] J. Long, M. Dong, K. Ota, and A. Liu, "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," *IEEE Access*, vol. 2, pp. 633–651, 2014.

Zhen Hong (Member, IEEE) received the B.S. degree from Zhejiang University of Technology, Hangzhou, China, and University of Tasmania, Australia in 2006, respectively, and the Ph.D. degree from the Zhejiang University of Technology Hangzhou, China, in 2012. Now he is a full professor at the Institute of Cyberspace Security, and College of Information Engineering, Zhejiang University of Technology, China. He was a research scholar at CAP Research Group, School of Electrical & Computer Engineering, Georgia Institute of Technology from 2016 to 2018. His research interests include Internet of Things, cyberspace security, and data analytics. He received the first Zhejiang Provincial Young Scientists Title in 2013 and the Zhejiang Provincial New Century 151 Talent Project in 2014. He also received Zhejiang Provincial Science Fund for Distinguished Young Scholars in 2023. He is a member of IEEE and ACM, and a senior member of CCF and CAA, respectively.

Wentao Chen Born in Anhui, China. He is currently pursuing the M.S. degree in Control Theory and Control Engineering at the School of Information Engineering, Zhejiang University of Technology, Hangzhou, China. His current research interest is Internet of Things application security.

Taotao Li was born in Zhejiang, China. He is currently working toward the Ph.D. degree in control theory and control engineering with the College of Information Engineering, Zhejiang University of Technology, Hangzhou, China. His current research interests include the security and privacy of the Internet of Things devices, data-driven security.



Jie Su is currently an assistant professor with the Institute of Cyberspace Security and College of Information Engineering, Zhejiang University of Technology, Hangzhou, China. His research interests include deep learning, signal processing, and the IoT security. Su received his Ph.D. degree in computer science from Newcastle University U.K., in 2023.