Hindawi
Security and Communication Networks
Volume 2022, Article ID 5026549, 16 pages
https://doi.org/10.1155/2022/5026549

Research Article

Silence is Golden: A Source Location Privacy Scheme for Wireless Sensor Networks Based on Silent Nodes

Chen Gu,[1] **Arshad Jhumka**,[2] **and Carsten Maple**[3]

[1]*School of Computer Science and Information Engineering, Hefei University of Technology, Hefei, China*
[2]*Department of Computer Science, University of Warwick, Coventry, UK*
[3]*WMG University of Warwick, Coventry, UK*

Correspondence should be addressed to Chen Gu; guchen@hfut.edu.cn

Received 24 November 2021; Revised 22 October 2022; Accepted 3 November 2022; Published 18 November 2022

Academic Editor: Tom Chen

Source location privacy (SLP) is an important property for security-critical wireless sensor network applications such as monitoring and tracking. However, cryptology-based schemes cannot protect the SLP effectively since an adversary can capture the source node regardless of the contents of messages. Most techniques use fake sources or message delay to provide SLP, but at the cost of high energy consumption or high message delivery latency. In this paper, we present a new technique to address SLP by selecting sets of nodes that are to be silent for a short period, forcing an attacker to either be delayed or to trace back to the source along a longer route. As such, we make a number of important contributions: (i) we formalise the silent nodes selection (SiNS) problem, (ii) we prove it to be NP-complete, and (iii) to circumvent the high complexity of SiNS, we propose a novel SLP-aware routing protocol. Results from extensive simulations show that our proposed routing protocol provides a high level of SLP under appropriate parameterization at the expense of only negligible latency and messages overhead.

1. Introduction

A sensor node equipped with a low-powered CPU and limited RAM can sense the surrounding environment such as temperature and pressure. A wireless sensor network (WSN) consists of many such nodes and enables many practical applications ranging from animal behavior and habitat monitoring [1, 2], military [3], medical services [4], and other applications [5]. Due to the distributed nature of the WSN, data are often originally produced and sent from a sensor node called *source* to be received by a sensor node called *sink* through many intermediate sensor nodes in the network over a wireless broadcast medium and the communication protocol. In this case, the location privacy of nodes is crucial to be protected in many applications.

Privacy in WSN can be classified into content-based privacy and context-based privacy. Specifically, content-based privacy refers to protecting the contents of broadcast messages from not being revealed to an eavesdropping attacker. There has been much research addressing the issue of providing content privacy using encryption [6]. On the other hand, context-based privacy protects the contextual information of messages not observed or inferred by attackers when messages are transmitted across the network. It is often desirable to keep the location private where the messages are originally from. For example, in the military scenario, a soldier who broadcasts information to neighboring soldiers may disclose its location even though messages are all encrypted. Moreover, in the animal protection application, poachers may be tempted to infer the location of the endangered animal when it broadcasts messages via the equipped sensors. Other real-world examples include monitoring badgers [7] and the WWF's Wildlife Crime Technology Report [8], both of which would benefit from the protection of context privacy. In this paper, we work on protecting context privacy and focus on the source location.

Protecting source location privacy (SLP) is important in many application domains, especially in security-critical situations. The main idea is to delay the attacker from

finding the source location as long as possible via SLP-routing protocols. It has been shown that in a non-SLP protected network, even a weak attacker such as a distributed eavesdropping attacker can backtrack along message paths through the network to find the source location and capture the asset [9]. Thus, different classes of SLP-aware routing algorithms are proposed to address the SLP issue. The phantom routing is proposed to protect the SLP by altering a flooding routing protocol to consist of an initial directed random walk followed by flooding [10]. Although the random walk-based schemes can protect the SLP in theory, they encounter the issue of link failure and messages cannot be successfully delivered to the sink (i.e., low data delivery). The technique of fake source applies sensor nodes in the network as fake sources to broadcast fake messages, such that an adversary cannot identify which source is the real one. It has been shown that this class technique can effectively protect the SLP but at the expense of extremely high energy consumption of sensor nodes. Another technique applicable in delay-tolerant networks adopts a message delay technique to achieve near-optimal SLP, but at the expense of delivery latency [11]. Thus, most state-of-the-art routing protocols incur high overheads (temporal or spatial) to provide SLP.

To solve SLP while reducing the induced overhead, in this paper, we focus on bounding the message overhead (thus, indirect energy). To achieve this, we propose a novel technique where nodes are chosen to become silent, i.e., they drop and do not respond to a received message. Specifically, we adopt an idea contrary to fake sources, but which achieves the same objective of getting an attacker to take a longer route, rather than sending fake messages to force an attacker into taking a diversionary route, we now "turn off" nodes on the main route. This is analogous to putting no entry signs on the original path, rather than putting diversion signs on the road. Besides, unlike existing SLP solutions that actively use diversified transmission paths to protect the SLP, our solution passively forces messages transmitted through a long route to the sink. In this case, the main benefit is that a sensor does not need to identify the neighboring sensor nodes in the WSN and thus there is no extra setup phase for the WSN deployment. As a result, an attacker eavesdrops fewer data transmissions within its reception range and either has to find a longer route to the source, or will be temporarily delayed, thereby potentially increasing the level of SLP provided. As such, the main contributions of this paper are as follows:

(i) We propose a novel problem, namely the silent node selection (SiNS), which is the study of the selection of nodes that are to be silent.

(ii) We prove that SiNS is NP-complete.

(iii) We develop a novel routing protocol, based on a simple solution to the SiNS problem.

(iv) We perform experiments of the routing protocol using TOSSIM. Simulation results show that under certain parameterization, it is possible to obtain high level of SLP at the expense of negligible overhead.

The remainder of this paper is organized as follows: Section 2 surveys related work in SLP and Section 3 presents the models assumed. In Section 4 we present the formalization of SiNS problem, and the silent nodes selection protocol (or heuristics) is shown in Section 5. Section 6 presents the results of the experiments conducted. Finally, We conclude the paper with a summary of contributions in Section 7.

2. Related Work

Ozturk et al. first introduced and formalized the panda hunter game to describe the problem of SLP in WSNs [12]. The scenario involves poachers using network traffic flows to track the location of a panda being monitored in its habitat. It has shown that certain routing techniques, such as flooding, provided no SLP since the attacker can find the source location by simply following the shortest path from the sink to the source of messages. Later several techniques such as random walk-based technique and fake source-based technique have been used to protect the SLP in the literature.

2.1. Random Walk-Based Solutions. The authors proposed a technique called phantom routing [12], where messages are first sent to randomly chosen phantom node in the network via a directed random walk, followed by flooding in order to deliver the message to the sink (shown in Figure 1(a)). There has been much work proposing improvements to phantom routing. A variant was proposed in [10], where messages were routed along a single path from the phantom node to the sink instead of flooding to decrease the energy cost by reducing the number of messages sent. Phantom walkabouts [14] uses a mixture of long and short directed random walks to provide higher protection level of SLP than the phantom routing scheme with a low message overhead. However, it does not provide a high packet delivery rate. Other algorithms use random walk techniques to provide SLP such as forward random walk [15] and two-level phantom routing using a second phantom node [16]. However, this class of solution has a number of weaknesses that can lead to a low level of SLP due to the reuse of routing paths and exposure of direction information [17].

2.2. Fake Source-Based Solutions. Instead of altering the message routes, fake source-based techniques typically add fake messages sent from fake sources to provide SLP. This is achieved by having fake messages obfuscate the real traffic and lure the attacker towards the fake sources instead of the real source as shown in Figure 1(b). The work in [18] examined SLP using fake sources where a short-lived fake source sends dummy messages based on a given probability when it receives a message. However, It has been shown that the performance was poor. Other schemes have also been proposed to address SLP using fake message techniques. In [19] a solution used fake hotspots and fake branches in the network to improve SLP using multiple sinks. K-means cluster is applied to create clusters and fake packets [20]. Fake messages are sent based on the lightweight message

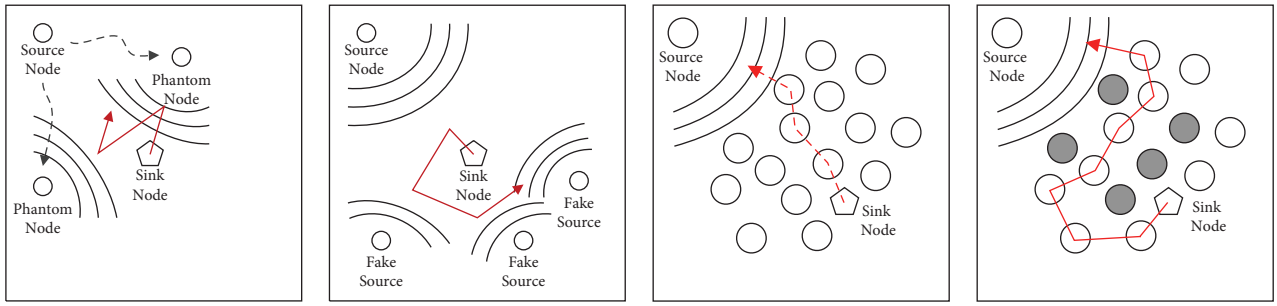

Figure 1: SLP technique attacker movement patterns [13]. The red line starting from the sink node presents the movement of an attacker. The wavy lines denote the messages flooding. In (a) and (b) the attacker zigzags between phantom nodes and fake sources, respectively. The attacker is slowed down on his path to find the source as messages are delayed in transmission shown in (c). In (d), the attacker has to find a long route to catch the source as some nodes (grey color nodes) are in the silent state. (a) Phantom routing. (b) Fake sources. (c) Message delay. (d) Silent nodes.

sharing scheme in [21]. However, the significant drawback of this class of techniques is increased energy consumption and message collision, both of which lead to a decrease in the WSN's lifetime [22, 23].

2.3. Other Solutions. There are some routing protocols that can provide SLP based on other techniques. In [11] a routing protocol was developed based on an integer linear programming (ILP) modeling of SLP to obtain an optimal broadcast schedule. In ILP routing protocol, nodes group received messages together and use delay technique to reduce the progress an attacker can make towards the source (see Figure 1(c)). Besides, the concept of pseudopacket scheduling was used to protect the SLP. This protocol regulates the process of pseudopacket generation to interfere with the adversary's tracking to the data source [24]. Instead of relying on message routing to protect SLP, authors [25] used the MAC layer to provide SLP. Specifically, this scheme set up a TDMA slot assignment that would trap the attacker with following messages and lead it far away from the source. Others include using dynamic routing [26] and virtual sources [27] to address the SLP problem. These solutions tend to either make a trade-off in terms of high latency or a high number of messages sent.

3. Models

In this section we describe models applied in this paper. These models are intentionally the same as previous work in [11, 28, 29] in order to perform a like-for-like comparison in Section 6.

3.1. Network Model. The WSN is modeled as a graph $G = (V, E)$ where V is the nodes and E represent bidirectional links between nodes. The nodes m and n are regarded as neighbors when a link exists between them. Neighboring nodes are able to communicate directly with each other. In practice we do not assume that links are reliable, they may become unidirectional or not be present intermittently. The network is assumed as event-triggered. The source node begins sending messages when it senses an assert. The sink receives all routed messages from WSN and enables to further deliver them to the external world. Intermediate nodes route messages starting from the source to the sink through multiple hops. The messages sent are encrypted so the attacker is unable to identify the source location by the message content.

3.2. Attacker Model. In this paper, we assume a patient distributed eavesdropper [10] in the WSN, which is able to change its location. This attacker is equipped with directional antennas in order to determine the direction a message originated from within a limited range. The attacker is always originally starting at the same location as the sink, because all messages must be delivered to the sink. When the attacker detects a new message that has not been received before, the attacker will physically move to the location of the neighboring node that sent the message. By repeating this movement, the attacker is able to move closer and closer to the source by following unique messages. Once the source location has been found, the attacker captures it and will cease moving in the network.

3.3. Safety Period Model. The aim of a routing protocol that provides SLP is to make sure that an asset (at a specific location in the WSN) is not captured using the context information that is leaked. However, the attacker does not necessarily need to use this information and can instead perform an exhaustive search of the network to find the source of messages and the asset. Here, SLP techniques are irrelevant as the attacker has captured the asset via its search, however, the adversary would use the context information if doing so reveals the location in less time. This means that the SLP problem can only be considered with an upper bound on the search time.

The literature uses two different terminologies for the key principle of safety period. One definition is the amount of time before capture [10], hence, measuring the privacy that is provided. However, this evaluation is not performed under a bounded amount of time. So an alternative

definition (which we adopt in this paper) is that the safety period is the duration an adversary needs to be prevented from capturing an asset [6]. We calculate the safety period $sp(P)$ as follows:

$$sp(P) = \phi \times T_{\text{flooding}}(P), \quad (1)$$

where $T_{\text{flooding}}(P)$ denotes the time taken of flooding routing protocol that provides no SLP protection under some parameterization P and ϕ is a safety factor $(\phi > 1)$. The effectiveness of algorithms is evaluated by capture ratio, which is the number of runs in which an adversary captured the source within the safety period. A lower capture ratio than 100% means improved privacy due to the alternate SLP technique.

4. The SiNS Problem: Formalisation and Complexity

Several solutions to the SLP problem exist. However, all of the solutions suffer from high overhead, e.g., high message complexity or high latency. To address this issue, we pursue the design of a solution whereby the overhead is bounded while maintaining a high privacy level. As such, our solution is based upon the following design decisions:

(i) To bound the number of messages generated, a suitable solution should limit the use of control and/or dummy messages. As such, decisions need to be based on application messages and/or timing.

(ii) A suitable solution needs to be able to force the attacker to follow different (and possibly longer) paths.

(iii) To bound message delivery latency, the solution should not force application messages on long paths in the network.

As such, we introduce the SiNS (silent nodes selection) problem. The SiNS problem is informally defined as the selection of nodes that are to remain silent (do not send messages) for a certain amount of time. When nodes remain silent, they do not introduce further messages into the network (satisfying requirement 1), while forcing the attacker to follow different routes, as the attacker hears from a different node (satisfying requirement 2). Also, by carefully choosing the silent nodes, such that at least one shortest path does not contain silent nodes, message latency will be almost unaffected (satisfying requirement 3). Please observe that the higher the number of silent nodes in the network, the lower the data yield is likely to be. On the other hand, the lower the number of silent nodes, the lower is the SLP level provided.

We now formally define the *SiNS* problem and show that it is NP-complete.

Definition 1 (Silent Nodes Selection). Given a network $G = (V, E)$ of diameter Δ, a size K, a distance δ, find a set $Q \subseteq V$ such that,

(i) $\forall n \in V \backslash Q, \exists q \in Q$, dist $(n, q) \leq \delta$

(ii) $|Q| \leq K$

The first condition captures the fact that silent nodes are not far apart, with the intention of providing a high level of SLP. The second condition bounds the number of such silent nodes so that data yield is not adversely affected.

Please observe that there are some types of networks for which no SiNS solution exist, such as line networks. In such a network, when a node becomes silent (for any duration), it will drop all messages that it receives. The attacker is delayed, thereby reducing the chance of capturing the asset (hence, increasing SLP) however at the expense of poor data yield.

We now prove that SiNS is NP-complete.

Lemma 1 *(SiNS and NP class). SiNS is in NP.*

Proof. To prove this, we need to verify the correctness of the set Q in polynomial time. So, given an instance of SiNS and solution set Q, we can verify whether Q satisfies the following two conditions:

(1) For the first condition, we choose a node $n \notin Q$ and using n as root, we build a spanning tree of depth δ. If there exists a node m in the spanning tree, then the condition is satisfied. Else, choose different node $k \notin Q$, and repeat the same process. After exhausting all possibilities, if no such node is found, then Q is not a solution for SiNS. This evaluation can be performed in $O(|V|)$.

(2) The final condition can be trivially evaluated. □

Lemma 2 *(SiNS and NP-hardness). SiNS is NP-hard.*

Proof. To prove this, we first map and then reduce the problem of minimum dominating sets (MDS) to that of *SiNS*.

We first provide the definition of the MDS problem. □

Definition 2 (MDS). Given a graph $G = (U, A)$, a size M, is there a set $U' \subseteq U$ such that

(i) $\forall n \notin U', \exists u \in U' : (u, n) \in A$

(ii) $|U'| \leq M$

Now, the mapping is as follows:

(i) $V, Q, E \mapsto U, U', A$

(ii) $\Delta \mapsto \alpha$, α is the diameter of U

(iii) $\delta \mapsto 1$

A solution to SiNS exists iff a solution to MDS exists and this is trivial to see.

Theorem 1 *(SiNS and NP-complete). SiNS is NP-complete.*

The proof follows straightforwardly from the two previous lemmas.

5. Heuristics

We have showed that the SiNS problem is intractable. To circumvent this limitation, there are various avenues one can

pursue. For example, one can investigate a special case of the SiNS problem that can be solved in polynomial time. Another example is to develop heuristics that can provide good solutions to the SiNS problem, which we focus on in this paper. In this section, we develop a novel routing protocol (heuristics) that can provide good SLP under specific parameterization. Table 1 summarizes the most commonly used symbols in the paper.

5.1. Overview. Derived from the *SiNS* definition, the heuristics should satisfy that (i) silent nodes are not far apart to provide a high level of SLP, and (ii) the number of such silent nodes are bounded so that data yield is not adversely affected. Now we briefly explain the procedure of the routing protocol based on silent nodes selection, which is shown in Figure 2. Initially a node is selected as the sink to receive data. If a node detects an asset, it becomes the source and periodically sends data to the sink through baseline protocol flooding. Apart from the source and the sink, a node first needs to be selected as either a silent or nonsilent node. Silent nodes can enter the silent state whereas nonsilent nodes will never enter silent state. If silent nodes meet certain criteria, they enter the silent state for a small duration. In the silent state, they will not forward received messages. When the silent state duration expires, silent nodes enter the awake state and resume forwarding messages. Note that our protocol does not require having redundant nodes which may increase additional monetary costs in the network deployment. Silent nodes can still transmit messages when they are in the awake state. An example of silent nodes to be the silent state is shown in Figure 3. We present that the silent nodes selection undergo through 3 stages.

(1) Node Selection: How nodes in the network are selected to be SilentNode or NonSilentNode.

(2) Nodes State Transition**:** When the chosen silent nodes are decided to change their state to silent.

(3) Silent Nodes Duration**:** How long the silent state lasts.

5.2. Node Selection to be Silent. For the first stage, nodes need to be selected as silent nodes or nonsilent nodes. A silent node has two states: (i) awake state and (ii) silent state, whereas the nonsilent node can only be awake to route messages. Given a network $G = (V, E)$, the state of a node $n \in V$ is determined based on three parameters:

(i) D_{Src}: The hop distance of a node to the source.

(ii) D_{Sink}: The hop distance of a node to the sink.

(iii) η: The hop distance from nodes along the shortest route between the sink and the source that enter silent nodes.

Intuitively, as messages are routed from the source to the sink, nodes close to source and sink are not chosen to be silent nodes depending on the specific network configuration. For instance, those nodes are not selected to be silent when only a few nodes are close to the source or the sink. In this case, a node n is not selected to be a silent node if $\Delta^n_{\text{Src}} \le D_{\text{Src}}$ or $\Delta^n_{\text{Sink}} \le D_{\text{Sink}}$.

Table 1: Commonly used symbols.

Symbol	Description
n, σ_i	Specific nodes in the network
Src	The source node
Sink	The sink node
$\Delta^{\sigma_i}_n$	The distance in hops between node n and σ_i
sp	Safety period
P_{src}	Source period
P	Selection probability
T	Silent state duration
D_{Src}	The hop distance boundary to the source
D_{Sink}	The hop distance boundary to the sink
T_{flooding}	Time taken for protectionless flooding

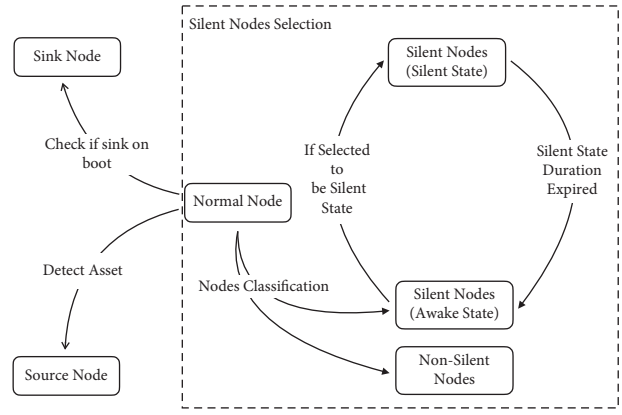

Figure 2: The transformation of node types in this protocol.

We also use η to select if a node is silent or not, which is based on the following analysis: since an attacker can catch the asset through the *shortest* route from the sink, we assume that there is a shortest route $\mathscr{R}_{\min} = \langle \text{Src}, \sigma_1, \sigma_2, \ldots, \sigma_k, \text{Sink} \rangle$ (route length is $|\mathscr{R}_{\min}|$) and a node σ_i fulfilling: $\sigma_i \notin Src \wedge \sigma_i \notin \text{Sink} \wedge \sigma_i \in \mathscr{R}_{\min}$. Thus, we have the following equation:

$$\Delta^{\sigma_i}_{Src} + \Delta^{\sigma_i}_{\text{Sink}} = \left|\mathscr{R}_{\min}\right|. \tag{2}$$

There is another node σ_j, which is not in the $\mathscr{R}_{\min}$ and the distance to any σ_i, where $\sigma_i \in \mathscr{R}_{\min}$ is denoted by η. We also denote the distance between σ_j and source by $\Delta^{\sigma_j}_{\text{Src}}$, and distance between σ_j and sink by $\Delta^{\sigma_j}_{\text{Sink}}$. So we have the following equations:

$$\begin{aligned} \Delta^{\sigma_j}_{\text{Src}} &< \Delta^{\sigma_i}_{\text{Src}} + \eta, \\ \Delta^{\sigma_j}_{\text{Sink}} &< \Delta^{\sigma_i}_{\text{Sink}} + \eta. \end{aligned} \tag{3}$$

From above two equations, we obtain the following equation:

$$\Delta^{\sigma_j}_{\text{Src}} + \Delta^{\sigma_j}_{\text{Sink}} < \Delta^{\sigma_i}_{\text{Src}} + \Delta^{\sigma_i}_{\text{Sink}} + 2\eta. \tag{4}$$

Derived from equations (2) and (4), finally we have the following equation:

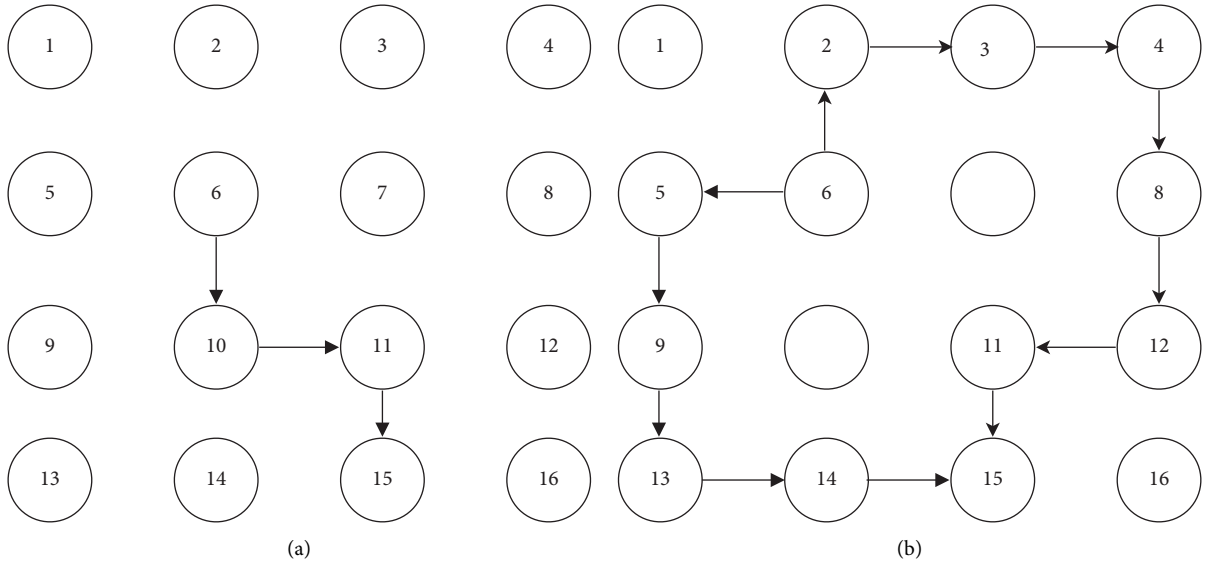

Figure 3: Example of a network with size 4×4. A message is sent from the source node 6 to the sink node 15 through the shortest path $\langle 6, 10, 11, 15 \rangle$ (the source and the sink are not silent nodes). If nodes 7 and 10 enter the silent state, other nodes are involved in transmitting the message from nodes 6 to 15. In this case, a message needs to be routed through a longer path to node 15 such as $\langle 6, 5, 9, 13, 14, 15 \rangle$ or $\langle 6, 2, 3, 4, 8, 12, 11, 15 \rangle$. (a) A message is sent through the shortest path. (b) A message is sent through a long path.

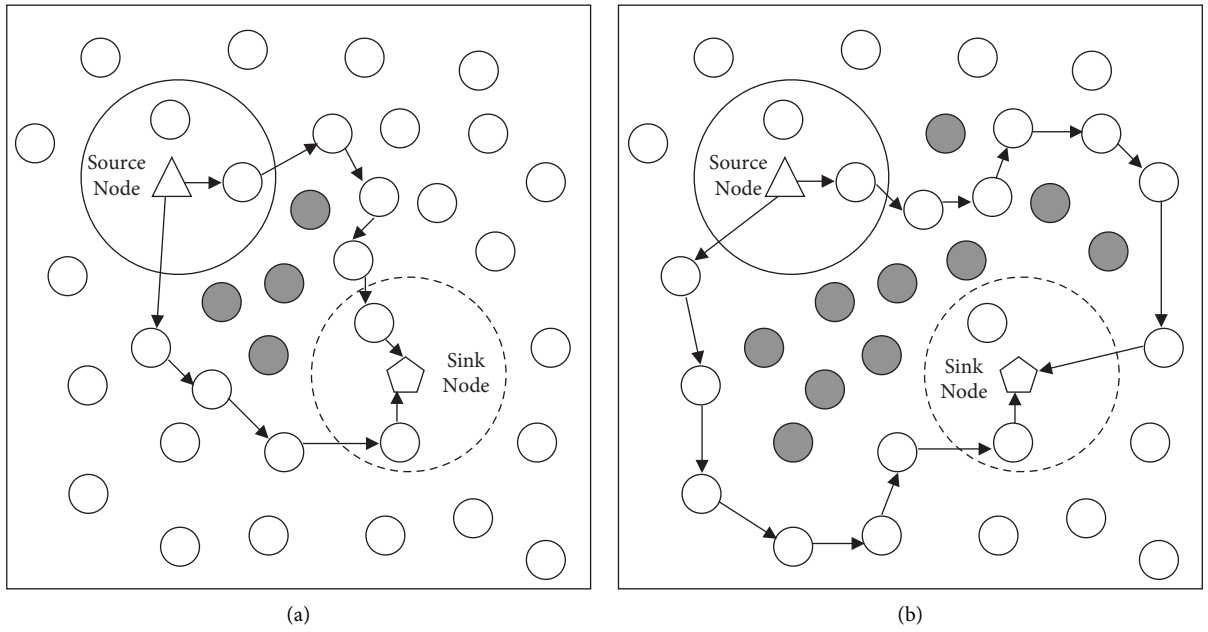

Figure 4: Selection of silent nodes (grey color) with different values η. Circles with solid line and dotted line represent D_{Src} and D_{Sink}, respectively. (a) Small η. (b) Large η.

$$\Delta_{\text{Src}}^{\sigma_j} + \Delta_{\text{Sink}}^{\sigma_j} < \left|\mathscr{R}_{\min}\right| + 2\eta. \tag{5}$$

Equation (5) is used to decide whether a node should be a silent node or not, when the distance to any node in $\mathscr{R}_{\min}$ is less than η. These nodes are chosen to be silent since they are very close to the shortest route $\mathscr{R}_{\min}$. The value of η defines the number of nodes to be selected to be silent nodes, which will be investigated in the results section. Since the value of $|\mathscr{R}_{\min}|$ is equal to $\Delta_{\text{Sink}}^{\text{Src}}$ where the minimum distance from the source to the sink, we select nodes to be silent or nonsilent as per equation (6), respectively.

$$\begin{aligned}
&n \in V \wedge n \notin \text{Src} \wedge n \notin \text{Sink} \wedge \\
\text{SilentNode}(n) = \; &\Delta^n_{\text{Src}} > \mathscr{D}_{\text{Src}} \wedge \Delta^n_{\text{Sink}} > \mathscr{D}_{\text{Sink}} \wedge \\
&\Delta^n_{\text{Src}} + \Delta^n_{\text{Sink}} < \Delta^{\text{Src}}_{\text{Sink}} + 2\eta, \\
&n \in V \wedge n \notin \text{Src} \wedge n \notin \text{Sink} \wedge, \\
\text{NonSilentNode}(n) = \; &\left(\Delta^n_{\text{Src}} \leq \mathscr{D}_{\text{Src}} \vee \Delta^n_{\text{Sink}} \leq \mathscr{D}_{\text{Sink}}\right) \wedge \\
&\Delta^n_{\text{Src}} + \Delta^n_{\text{Sink}} \geq \Delta^{\text{Src}}_{\text{Sink}} + 2\eta.
\end{aligned} \tag{6}$$

An example selection of silent nodes is shown in Figure 4 for two networks with different values of η. Figure 4(a) shows the case in which a small value of η is used for silent node selection, so that a small number of nodes are selected, whereas a large number of nodes are selected as silent nodes with a large value of η in Figure 4(b). However, in both cases, the source, the sink, and the nodes near them (nodes in dashed/solid circles) are not selected to be silent nodes.

5.3. Nodes State Transition. When nodes are classified into silent nodes, they route messages when in the awake state. There is a need to decide when they should be transformed into silent state. Nodes in the silent state will not be involved in transmitting messages. The state transformation from awake state to be silent can be decided by the following:

(i) Approach ($\mathscr{A}$): Approach decides when and which silent nodes are selected to be the silent state

(ii) Probability ($\mathscr{P}$): The probability of a silent node to be silent state

Only if both two conditions are satisfied, should a silent node be put into silent state. In this paper, we consider four different approaches shown in Figure 5.

(i) *Sink to Source*: Silent nodes enter the silent state starting from the sink to the source. When the silent state of a silent node which is closest to the source expires, then the procedure repeats from the sink (see Figure 5(a)).

(ii) *Sink to Source and Back*: Silent nodes enter the silent state starting from the sink to the source. The procedure then works backwards to the sink (see Figure 5(b)).

(iii) *Source to Sink*: Different from Figure 5(a), in this approach silent nodes enter the silent state starting from the source to the sink. When the silent state of a silent node which is closest to the sink expires, then the procedure repeats from the source (see Figure 5(c)).

(iv) *Source to Sink and Back*: Silent nodes enter the silent state starting from the source to the sink. The procedure then works backwards to the source (see Figure 5(d)).

The time when a silent node changes to silent state is decided when it receives a message. Each message contains information, such as message sequence number (SeqNo). If the silent node meets the appropriate constraints, it changes to silent state. Otherwise, the decision will be conducted when receiving the next incoming message. The algorithms are presented in Algorithms 1 and 2.

5.4. Silent Nodes Duration. A silent node in the silent state will need to wake up after a finite duration in order to prevent low packet delivery. Here, we consider the worst case: assume an attacker is located 1 hop from a silent node σ_i which is awake and closer to the source than the attacker, the attacker can reach the location of σ_i by moving 1 hop, i.e., the attacker hears the next message from the σ_i. The time between two interval messages that σ_i receives is P_{src}. To stop the attacker making further moves, the minimum silent state duration of σ_i should be at least P_{src}. Therefore, the silent state duration of node n is defined as follows:

$$\mathscr{T} = \alpha \times P_{\text{src}} \text{where } \alpha \in \mathbb{N} \wedge \alpha \geq 1, \tag{7}$$

where α is a parameter and P_{src} is the constant source period in the network.

6. Results

6.1. Experimental Setup. The simulation environment used to generate our results is based on TOSSIM (V2.1.2). The network layout was configured as a square grid with sizes of 11×11, 15×15, 21×21, and 25×25, totaling 121, 225, 441, and 625 nodes in the network, respectively. The source corner configuration [11] was adopted where the source is in the corner and the sink is located in the centre. The time between messages being sent (the source period) was set to 1.0 seconds per message, meaning 1 message was sent per second. The wireless radio links were generated using the low-asymmetry model provided by LinkLayerModel (LinkLayerModel is a tool provided by the TOSSIM to calculate wireless link strengths between sensor nodes) with parameters from [30]. TOSSIM simulates noise on the wireless links, to do so we provided the first 2500 lines of casino-lab.txt (casino-lab.txt provided by the TOSSIM contains sample noises collected from the real environment). Nodes were positioned 4.5 meters apart from neighboring nodes. Results were generated from at least 2000 repeats for each combination of parameters.

In this work the safety factor is set to 1.3 based on the safety period model. This factor value ensures that the attacker has enough time to capture the source and potentially makes bad moves. Table 2 shows the time taken to capture the source under protectionless flooding ($\mathscr{T}_{\text{flooding}}$) for each network size when the source period is 1.0 second per message. Thus, the safety period can be calculated using these results via equation (1). The parameters we used in the following sections are shown in Table 3.

In this section we will use a metric called capture ratio to evaluate the SLP level. The capture ratio is the percentage of runs in which the source was captured. For example, if the attacker captures the source 20 times within the given safety period out of 100 simulation repeats, the capture ratio is 20%. The lower the capture ratio is, the higher the source location privacy level. Besides, we will also analyze other three key metrics: (i) receive ratio: the percentage of

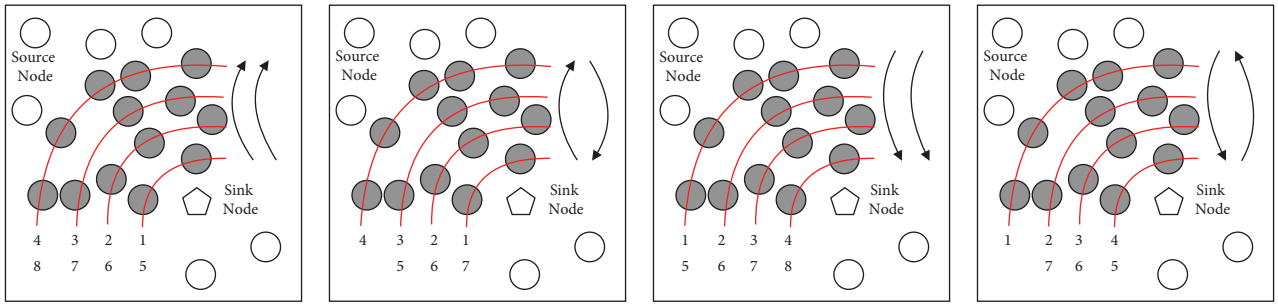

FIGURE 5: Different approaches of state transformation. Nodes in the same string have the same Δ^n_{Sink} in (a) and (b), and same Δ^n_{Src} in (c) and (d). The numbers and arrow denote the temporal sequences of silent nodes to be the silent state. (a) Sink to source. (b) Sink to source and back. (c) Source to sink. (d) Source to sink and back.

```
(1) receive Normal ⟨SeqNo, SDB, ...⟩ ⟶
      ▸ SeqNo generating from the source starts from 1.
      ▸ SBI is the hop distance of silent nodes from the source to the sink.
(2)   SDB ⟵ Δ_ss − 𝒟_Src − 𝒟_Sink.
(3)   IsSilentState ⟵ False.
(4)   switch 𝒜 do ▸ 𝒜 is the state transformation approach
(5)     case SinkToSource
(6)       IsSilentState ⟵ SinkToSource(SeqNo, SDB).
(7)       break
(8)     case SinkToSourceAndBack
(9)       IsSilentState ⟵ SinkToSourceAndBack(SeqNo, SDB).
(10)      break
(11)    case SourceToSink
(12)      IsSilentState ⟵ SourceToSink(SeqNo, SDB).
(13)      break
(14)    case SourceToSinkAn dB ack
(15)      IsSilentState ⟵ SourceToSinkAndBack(SeqNo, SDB).
(16)      break
(17)  if IsSilentStatethen
(18)    pass ▸ Discard the received message
(19)  else
(20)    BCAST Normal ⟨SeqNo, SDB, ...⟩
(21)  end if
```

ALGORITHM 1: Node receives normal messages.

messages sent by the source and received at the sink, (ii) latency: the time it takes a message sent by the source to be received at the sink, and (iii) messages sent per second: the number of messages sent by all nodes in the network per second. We will first show the results of flooding, and then present the results of our quiet nodes-based protocol. Finally, we add state-of-art SLP-aware routing protocols for comparison.

6.2. Simulation Results of Proposed Routing Protocol. In this results section, we discuss the impact of (i) nodes classification, (ii) state transformation, and (iii) silent duration separately. Rather than showing all the results generated by using parameters in Table 3, for each section we choose one result under specific parameters for evaluation. The parameters we used in the following sections are shown in Table 4.

6.2.1. Impact of Classification. Figure 6 shows the results when varying distance (η). One major observation is that the receive ratio decreases as distance increases (see Figure 6(b)). This decrease is due to the fact that there is an increase in the number of silent nodes that are not involving in forwarding messages. As a consequence, the capture ratio decreases (i.e., SLP level increases). However, as the distance increases from 2 hops to 3 hops, the receive ratio decreases from 80% to 70%, whereas the capture ratio does not decrease correspondingly. This suggests that an excessive distance will not benefit the SLP level but impair the data yield.

For latency, as more nodes are classified into silent nodes, messages have to route from the source to the sink through a longer path, hence increasing the latency. On the other hand, messages sent decreases is due to more nodes being silent. However, the impact of latency and message overhead is negligible compared to the baseline results.

```
IsReverse ⟵ False ▸ Whether the direction is backwards
(1) function SINKTOSOURCE(SeqNo, SDB).
(2)   p ⟵ GENERATERANDOMNUMBER(0, 1).
(3)   if (SeqNomodSDB = Δ^n_Sink ∨ (SeqNo + 1) modSDB = Δ^n_Sink) ∧ p ≤ 𝒫 then
(4)     return True
(5)   end if
(6) end function
(7) function SINKTOSOURCEANDBACK(SeqNo, SDB)
(8)   p ⟵ GENERATERANDOMNUMBER(0, 1).
(9)   d ⟵ Δ^n_Src if IsReverse else Δ^n_Sink
(10)  if (SeqNomod SDB = d ∨ (SeqNo + 1) mod SDB = d) ∧ p ≤ 𝒫 then
(11)    if SeqNomod SDB = 0 then
(12)      IsReverse ⟵ IsReverse
(13)    end if
(14)    return True
(15)  end if
(16) end function
(17) function SOURCETOSINK(SeqNo, SDB).
(18)  p ⟵ GENERATERANDOMNUMBER(0, 1).
(19)  if (SeqNomodSDB = Δ^n_Src ∨ (SeqNo + 1) mod SDB = Δ^n_Src) ∧ p ≤ 𝒫 then
(20)    return True
(21)  end if
(22) end function
(23) function SOURCETOSINKANDBACK(SeqNo, SDB)
(24)  p ⟵ GENERATERANDOMNUMBER(0, 1).
(25)  d ⟵ Δ^n_Sink if IsReverse else Δ^n_Src
(26)  if (SeqNomod SDB = d ∨ (SeqNo + 1) mod SDB = d) ∧ p ≤ 𝒫 then
(27)    if SeqNomod SDB = 0 then
(28)      IsReverse ⟵ IsReverse
(29)    end if
(30)    return True
(31)  end if
(32) end function
```

Algorithm 2: State transformation procedure for node n.

Table 2: Time taken for the attacker to capture the source when protectionless flooding is used.

Network size	11×11	15×15	21×21	25×25
Time taken (sec)	9.93	13.98	20.40	24.59

6.2.2. Impact of Nodes State Transition. The procedure for silent nodes to be put into the silent state is due to approach and probability. For approach, we choose a fixed 0.5 (i.e., 50%) probability and vary four approaches introduced in Section 5.3. For probability, the approach of *Sink to source and back* is selected and probabilities are varied as 0.5, 0.6, 0.7, 0.8, and 0.9.

(a) Approach: Figure 7 contains all the results. The receive ratio between 75% and 95% is observed (see Figure 7(b)). Fewer messages were delivered with larger networks. This suggests that the attacker was hearing most of the source messages, meaning that the privacy level imparted by the algorithm is due to the efficiency of the protocol and not due to the unreliability of the network. From Figure 7(a), the approaches of *Sink to source* and *Sink to source and back* performs better SLP level than others. It suggests that approaches which silent state of nodes starts from the sink side preserve much higher levels of SLP than the approaches which silent state starts from the source side, especially in the case of small network size.

(b) Probability: Results are presented in Figure 8. The receive ratio is still at a high level, over 75%. Meanwhile, high levels of SLP are obtained with the increase of the probability. The reason is that the nodes are likely to be selected as silent nodes when

Table 3: Parameters in silent nodes selection simulations.

Parameter	Value
η	1, 2, 3
D_{Src}	2, 3
D_{Sink}	0,1
P	0.5, 0.6, 0.7, 0.8, 0.9
T	P_{src}, $2 \times P_{\text{src}}$, $3 \times P_{\text{src}}$, $4 \times P_{\text{src}}$
$\mathscr{A}$	Sink to Source Sink to Source and back Source to Sink Source to Sink and back

Table 4: Parameters used in the results section. The parameter with * varies in the corresponding section, other parameters are fixed.

	Value		
	Impact of classification	Impact of transformation	Impact of duration
η	*	1	1
D_{Src}	3	3	3
D_{Sink}	0	0	0
$\mathscr{P}$	0.5	*	0.9
$\mathscr{T}$	$4 \times P_{src}$	$4 \times P_{src}$	*
$\mathscr{A}$	*Sink to source and back*	*	*Sink to source and back*

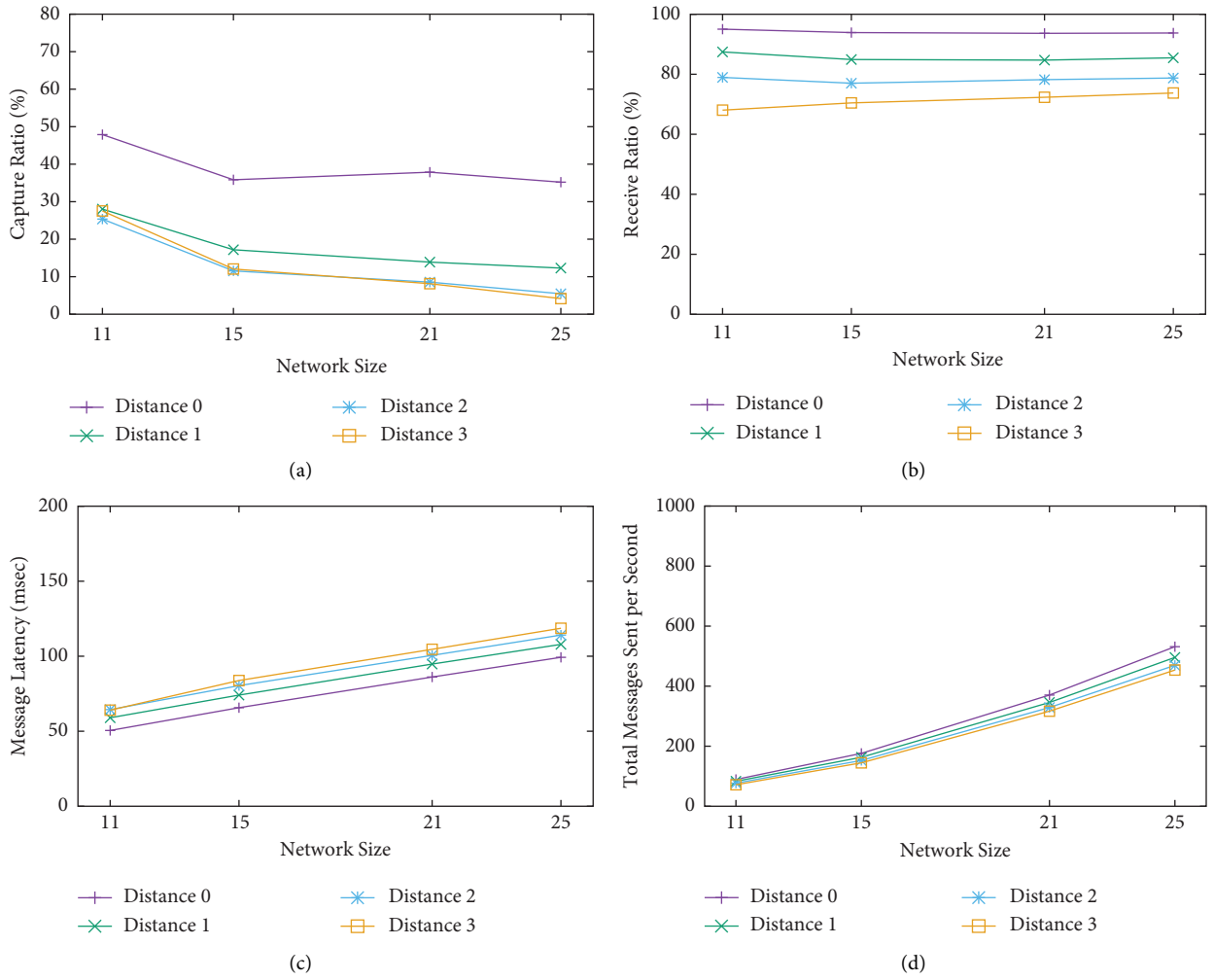

Figure 6: Results showing the impact of selection to be silent. (a) Capture ratio. (b) Receive ratio. (c) Latency. (d) Messages sent.

the probability increases. Specifically in the best case, there is a less than 10% probability of the attacker capturing the source within the safety period.

There is little impact on latency and messages sent when varying approaches and probabilities.

6.2.3. Impact of Silent Nodes Duration. The durations are $\alpha \times P_{\text{src}}$ ($\alpha \in \{1, 2, 3, 4\}$) and results are shown in Figure 9. We observe that a high level of SLP obtained with an increase in duration. The increase of the time duration forces attacker finding a long route to trace back to capture the source, hence the SLP improves. For instance, less than 10% the capture ratio is observed when the duration is $4 \times P_{src}$ while the receive ratio remains at a high level. Furthermore, latency and message sent are still not adversely affected.

6.3. Performance Comparison with Other SLP Schemes. Previous results have shown that our proposed routing protocol can achieve less than 10% capture ratio (see Figure 9(a)) and little overheads. In this section, to further investigate the performance of our solution, we add other

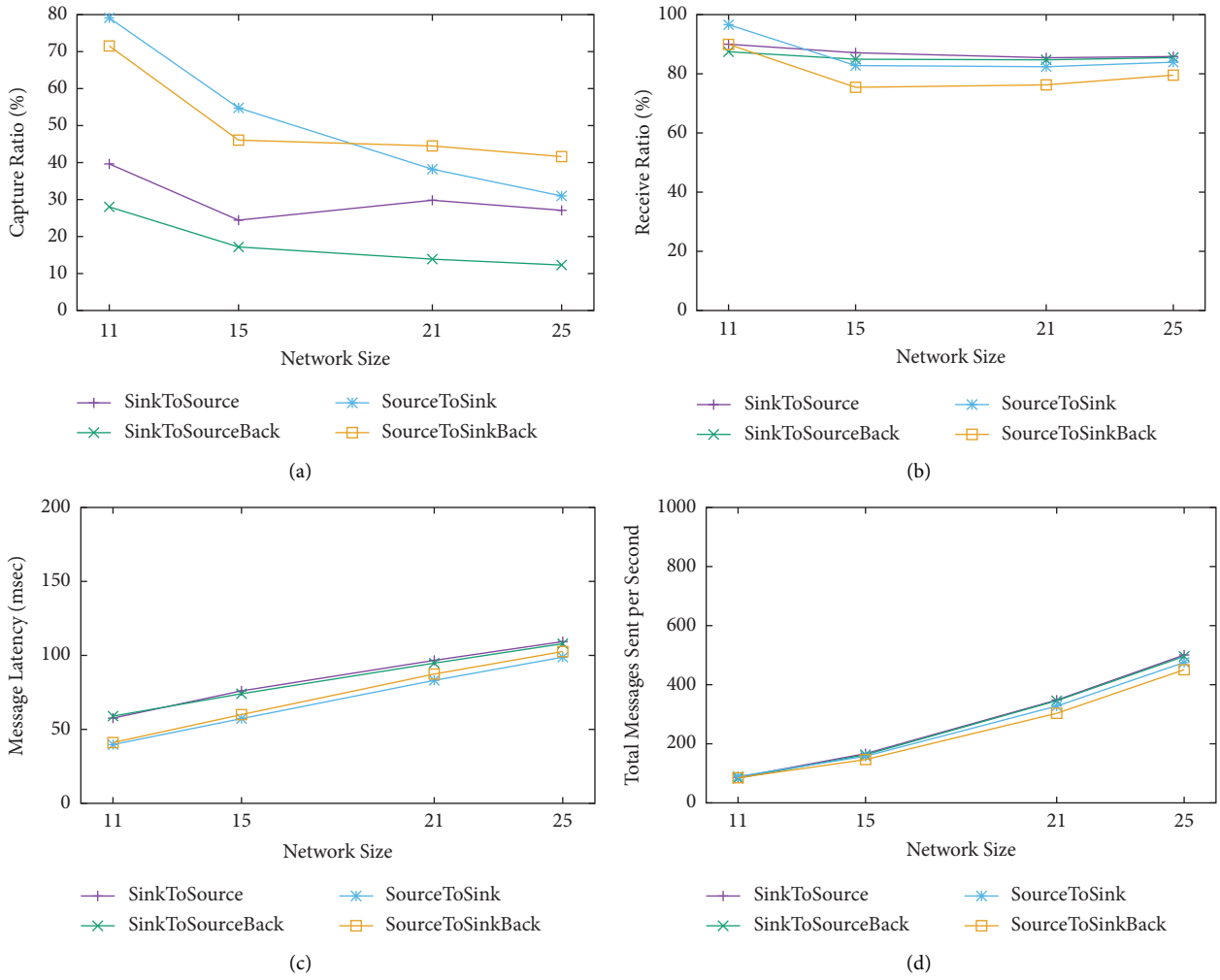

Figure 7: Results showing the impact of approach. (a) Capture ratio. (b) Receive ratio. (c) Latency. (d) Messages sent per second.

three state-of-art protocols that can also achieve SLP for comparison: (i) phantom walkabouts [14], (ii) dynamicSPR [28], and (iii) ILP routing [11].

(i) Phantom Walkabouts: Phantom walkabouts is an algorithm using a mix of short and long random walks to achieve a higher level of SLP than phantom routing. We apply $PW(1,1)$ and $PW(1,2)$ which denote a repeating sequence of 1 short random walk followed by 1 long random walk and 2 long random walk, respectively.

(ii) DynamicSPR: DynamicSPR uses fake source technique where fake sources are allocated away from the real source and determines parameters online to be able to adjust to a dynamic network. The parameter Rnd determining how many fake messages are set to either 1 or 2 messages randomly during the simulation.

(iii) ILP Routing: ILP Routing allows messages that are delayed and grouped at the same sensor node, such that the attacker receives few messages. It also tries to maximize the path from the source to the sink to improve the SLP level. We follow the simulation setup in [11] so that the maximum walk length is 100 hops, the number of messages to group is 1 message, the buffer size is set to 10 messages, and the probability is 20%.

These techniques are chosen because they have each made different trade-offs that we wish to evaluate against. Phantom Walkabouts uses random walk, DynamicSPR uses fake sources, and ILP Routing uses message delay. The results are generated under the simulation environment as same as our solution. The results of our proposed solution is from Figure 8 when the probability is 80%. We also show results of the flooding protocol because it provides *no* SLP. We make observations from Figure 10 for performance of the techniques.

(i) Results for Phantom Walkabouts show a capture ratio of less than 20%, which decreases as the network size increases. There are low costs in terms of the number of messages sent and message latency. However, the receive ratio is poor. Results show 60% or lower receive ratio can be achieved and

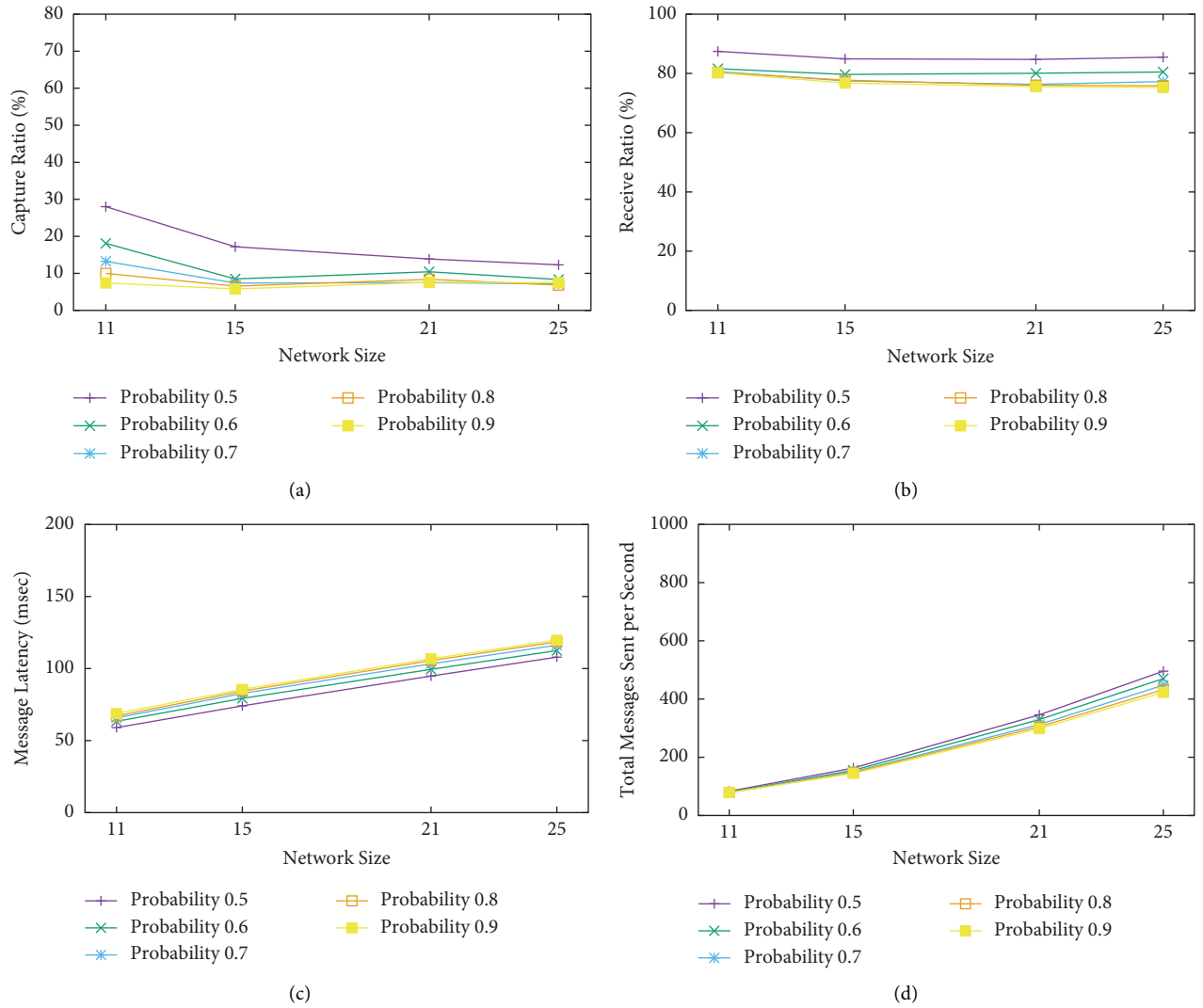

Figure 8: Results showing the impact of probability. (a) Capture ratio. (b) Receive ratio. (c) Latency. (d) Messages sent per second.

the ratio significantly decreases with larger network sizes. This indicates that messages are lost during transmission and a large amount of messages cannot be successfully delivered to the sink as shown in Figure 10(b). This also means that the low capture ratio and low messages sent are due to the low receive ratio (see Figures 10(a) and 10(d)).

(ii) The results show both DynamicSPR and ILP routing can achieve near-optimal SLP (see Figure 10(a)). Meanwhile, the receive ratio between 80% and 95% is observed (see Figure 10(b)). It means that the SLP level is due to the efficiency of the protocol and not due to the unreliability of the network. However, the weaknesses of both algorithms are to introduce much overheads to achieve such high level of SLP. Specifically, for DynamicSPR the messages sent are higher than our solution and increase greatly with larger network size (see Figure 10(d)); latency in ILP routing is near 10 times higher than that in our solution (see Figure 10(c)).

(iii) Results for protectionless flooding show that it indeed provides no SLP, as the capture ratio is 100%. The receive ratio shown in Figure 10(b) is also 100%, as all messages sent from the source are all successfully delivered to the sink. For the latency and messages sent per second, both values in each metric increase with larger network sizes but not significantly as these messages are sent along the shortest path.

(iv) Our proposed solution maintains both a low latency and low number of messages sent per second while keeping a high percentage of messages successfully delivered. While DynamicSPR and Flooding have lower latency, and ILP Routing and Phantom Walkabouts have a lower number of messages sent, we do not select one metric to make a very high trade-off in.

These three algorithms being compared have made trade-offs to achieve high levels of SLP, and their overheads

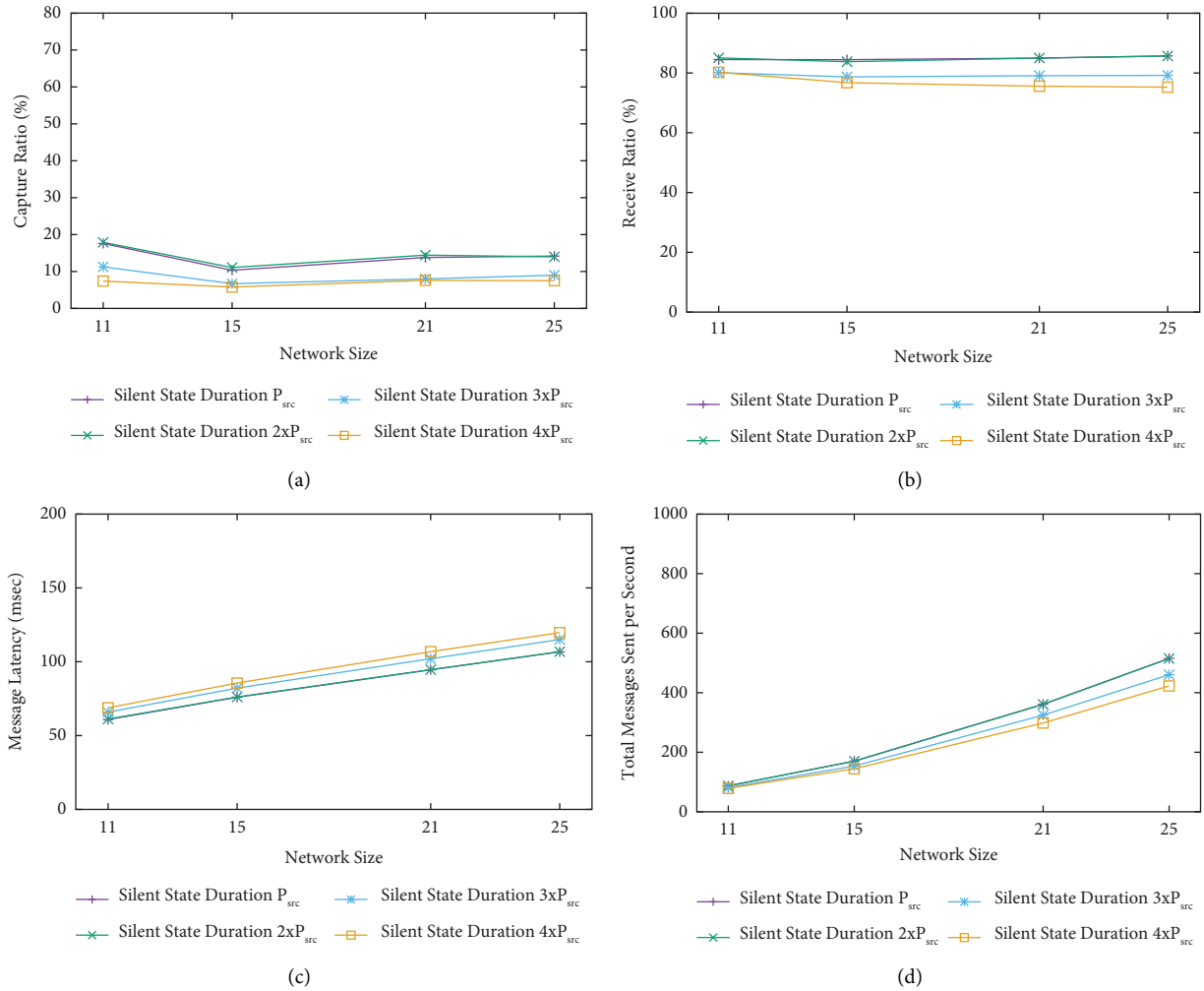

Figure 9: Results showing the impact of duration. (a) Capture Ratio. (b) Receive Ratio. (c) Latency. (d) Messages Sent.

may potentially limit their practical applications. For example, DynamicSPR algorithm will need to be deployed in networks where nodes have a large energy store or perform energy harvesting, and ILP Routing is only suitable for deployment when applications are delay-tolerant. Our proposed routing protocol, instead makes small trade-offs across multiple metrics.

6.4. Discussion

6.4.1. Multiple Attackers. We have assumed a commonly used attacker model in the paper, where a single distributed eavesdropper in the network enables to backtrack on the network traffic flow to find the source location. On the other hand, multiple attackers physically present in the WSN are likely to prove more effective against SLP techniques because of their wider combined visible area. However, there are a number of practical issues that the multiple attacker model has. Having cooperating attackers either entail communication on a different channel for the attackers or the location of attackers can be detected by network nodes or network administrators. For example, nodes in WSN could route messages through areas in which the attackers have not been detected. In this case, the situation is different from a single attacker, which changes our system model and attacker model. To our knowledge, few work deals with multiple attackers [31] and that are the reasons why work on multiple attackers has been rare.

6.4.2. Choice of Parameters. The performance of silent nodes-based protocol relies on the choice of parameters. For example, more nodes can be classified into the silent nodes with a large value of η. A poor choice of parameters may cause the WSN to be disrupted. However, the parameters in the protocol can be generated and finely tuned by the application developers or system administrators for practical scenarios. For example, in other network configuration that

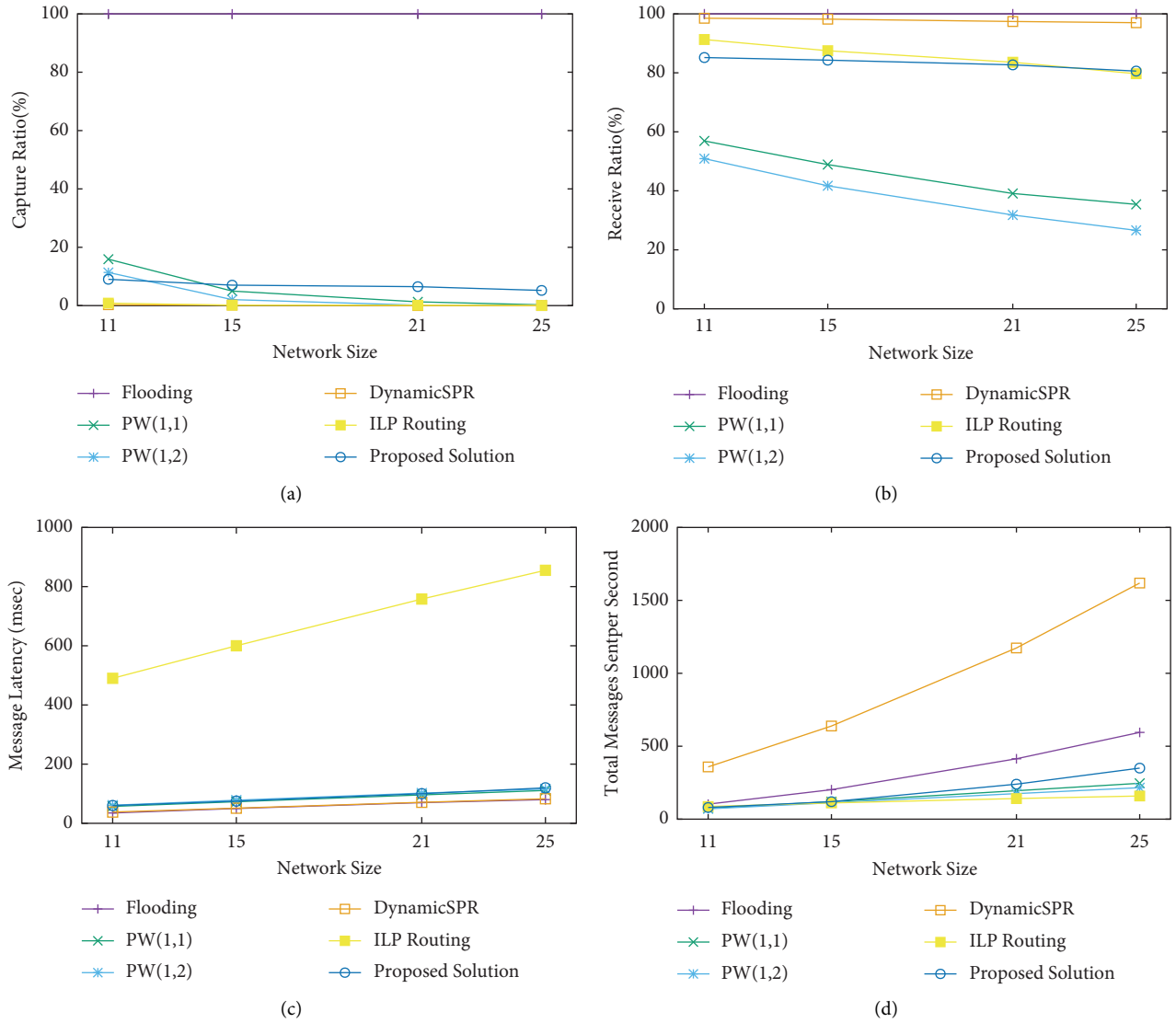

Figure 10: Comparing our proposed technique with other routing protocols. (a) Capture ratio. (b) Receive ratio. (c) Latency. (d) Messages sent.

the source locates in the centre and the sink is in the corner of the network, the parameters vary to fit the specific network environment.

7. Conclusion

In this paper we have focused on bounding the overhead issue and proposed a novel SLP-routing protocol by choosing a number of nodes that will be silent. We first formalized silent nodes selection (SiNS) problem and showed that SiNS is NP-complete. Then, a novel routing protocol was proposed for solving the SLP problem and demonstrated their efficiency through extensive simulation. Our results showed that a high level of SLP is achieved under certain parameterization. In future work it would be desirable to develop new heuristics to address the SLP problem for different network configurations. It would also be informative to consider alternative attacker models.

Data Availability

The code used to generate these results can be found at https://github.com/Chen-Gu/slp, and the data presented in this paper can be found at [32].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by Anhui Science and Technology Key Special Program under Grant no. 201903a05020016, in part by the National Natural Science Foundation of China (NSFC) under Grant no. U1836102, in part by Anhui Provincial Natural Science Foundation under Grant no. 2008085MF196, and in part by the Fundamental

Research Funds for the Central Universities under Grant no. JZ2022HGQA0166.

References

[1] G. Han, H. Wang, J. A. Ansere, J. Jiang, and Y. Peng, "SSLP: A Stratification-based source location privacy scheme in Underwater Acoustic sensor networks," *IEEE Network*, vol. 34, no. 4, pp. 188–195, 2020.

[2] L. C. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through Proxy node routing," *Sensors*, vol. 19, no. 5, p. 1037, 2019.

[3] 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, 2020.

[4] L. C. Mutalemwa and S. Shin, "Novel Approaches to realize the Reliability of location privacy protocols in monitoring wireless networks," *IEEE Access*, vol. 9, pp. 104820–104836, 2021.

[5] Z. W. Hussien, D. S. Qawasmeh, and M. Shurman, "MSCLP: Multi-sinks cluster-based location privacy protection scheme in WSNs for IoT," in *Proceedings of the 2020 32nd International Conference on Microelectronics (ICM)*, pp. 1–4, IEEE, Aqaba, Jordan, December 2020.

[6] M. Bradbury, A. Jhumka, and C. Maple, "A spatial source location privacy-Aware duty Cycle for Internet of Things sensor networks," *ACM Transactions on Internet Technology*, vol. 2, no. 1, pp. 1–32, 2021.

[7] V. Dyo, S. A. Ellwood, D. W. Macdonald et al., "WILDSENSING: design and deployment of a sustainable sensor network for wildlife monitoring," *ACM Transactions on Sensor Networks*, vol. 8, no. 4, pp. 1–33, 2012.

[8] K. Chou, "Wildlife Crime Technology Project," 2017, https://www.worldwildlife.org/projects/wildlife-crime-technology-project.

[9] H. Wang, G. Han, Y. Zhang, and L. Xie, "A Push-based Probabilistic method for source location privacy protection in Underwater Acoustic sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 770–782, 2022.

[10] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 599–608, IEEE, Columbus, OH, USA, June 2005.

[11] M. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proceedings of the IEEE Trustcom/BigDataSE/ICESS*, pp. 409–416, IEEE, Sydney, Australia, August 2017.

[12] C. Ozturk, Y. Zhang, W. Trappe, and M. Ott, "Source-location privacy for networks of energy-constrained sensors," in *Proceedings of the IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems*, pp. 68–72, IEEE, Vienna, Austria, May 2004.

[13] A. Jhumka and M. Bradbury, "Deconstructing source location privacy-aware routing protocols," in *Proceedings of the ACM Symposium on Applied Computing*, pp. 431–436, ACM, Marrakech, Morocco, April 2017.

[14] C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts in wireless sensor networks," in *Proceedings of the ACM Symposium on Applied Computing*, pp. 609–616, ACM, Marrakech, Morocco, April 2017.

[15] 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.

[16] L. C. Mutalemwa and S. Shin, "Secure routing protocols for source node privacy protection in Multi-hop communication wireless networks," *Energies*, vol. 13, no. 2, p. 292, 2020.

[17] R. Manjula, T. Koduru, and R. Datta, "Protecting source location privacy in IoT-Enabled wireless sensor networks: the case of multiple Assets," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10807–10820, 2022.

[18] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the ACM workshop on Security of ad hoc and sensor networks*, pp. 88–93, ACM, Washington DC USA, October 2004.

[19] 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.

[20] G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A k-means cluster-based location privacy protection scheme in WSNs for IoT," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 84–90, 2018.

[21] N. Wang, J. Fu, J. Zeng, and B. K. Bhargava, "Source-location privacy full protection in wireless sensor networks," *Information Sciences*, vol. 444, pp. 105–121, 2018.

[22] H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, "A Probabilistic source location privacy protection scheme in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5917–5927, 2019.

[23] 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, 2020.

[24] Y. He, G. Han, M. Xu, and M. Martinez-Garcia, "A pseudopacket scheduling Algorithm for protecting source location privacy in the Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9999–10009, 2022.

[25] J. Kirton, M. Bradbury, and A. Jhumka, "Source location privacy-Aware data Aggregation scheduling for wireless sensor networks," in *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 2200–2205, IEEE, Atlanta, GA, USA, July 2017.

[26] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 689–697, 2018.

[27] R. Manjula and R. Datta, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs," *Pervasive and Mobile Computing*, vol. 44, pp. 58–73, 2018.

[28] 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.

[29] C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 20, Article ID e5304, 2019.

[30] C. Gu, M. Bradbury, J. Kirton, and A. Jhumka, "A decision theoretic framework for selecting source location privacy

aware routing protocols in wireless sensor networks," *Future Generation Computer Systems*, vol. 87, pp. 514–526, 2018.

[31] A. Jhumka, M. Leeke, and S. Shrestha, "On the use of fake sources for source location privacy: trade-Offs between energy and privacy," *The Computer Journal*, vol. 54, no. 6, pp. 860–874, 2011.

[32] C. Gu, *Dataset for: Silence is Golden: Source Location Privacy for Wireless Sensor Networks Based on Silent Nodes*, 2021.