IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 12, 2019, accepted September 22, 2019, date of publication September 25, 2019,
date of current version October 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2943710

Regulating the Packet Transmission Cost of Source Location Privacy Routing Schemes in Event Monitoring Wireless Networks

LILIAN C. MUTALEMWA AND SEOKJOO SHIN
Department of Computer Engineering, Chosun University, Gwangju 61452, South Korea

Corresponding author: Seokjoo Shin (sjshin@chosun.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2018R1D1A1B07048338.

ABSTRACT Sensor nodes in wireless sensor networks (WSNs) are usually battery-operated and resource-constrained. The sensor nodes are often deployed in remote areas where the batteries cannot easily be recharged or replaced. Consequently, power becomes a limited resource in WSNs. Thus, energy consumption of the sensor nodes is among parameters of paramount importance. Subsequently, source location privacy (SLP) routing schemes must be energy-efficient and overall cost-effective. Angle-based routing schemes can cost-effectively protect the SLP. The goal of this study is to propose a new path node offset angle routing algorithm to improve the packet transmission cost of two existing SLP routing schemes. The proposed algorithm considers path node offset angles, arbitrary factors, and contrived regions to compute relatively short but greatly randomized routing paths. The routes offer a reduced number of packet forwarding events in the near-sink region and eventually diminish the packet transmission cost. Performance analysis results verify that the proposed path node offset angle routing algorithm effectively improves the packet transmission cost of the schemes and guarantees strong SLP protection throughout the WSN domain. Furthermore, the routing algorithm is capable of alleviating the energy-hole problem.

INDEX TERMS Source location privacy, wireless sensor network, offset angle, safety period, energy consumption, packet transmission cost.

I. INTRODUCTION

The process of minimizing the traceability and observability of a source node by an adversary in wireless sensor networks (WSNs) is denoted as source location privacy (SLP) protection. The design of the SLP routing schemes must consider one critical parameter, the energy consumption of sensor nodes. The sensor nodes usually run on battery power and are often deployed in remote and inaccessible areas where it is difficult to recharge or replace the batteries. For example, the Berkeley mote, which is powered by two AA batteries [1], can be used for monitoring applications in remote areas such as in ocean environments or in game reserves like the Serengeti national park. In such applications, the sensor nodes must be energy-efficient to allow for a long operational period of the nodes and long network lifetime. Many effective SLP routing schemes have a drawback of high energy consumption. For example, the schemes in [2]–[4] achieve strong SLP protection. However, the schemes incur very high packet transmission cost [5], [6]. In particular, the tree-based diversional routing scheme in [2] can have a total energy consumption of almost 20 times that of the traditional phantom routing scheme.

The recently proposed SLP routing schemes in [3] and [4] have high energy consumption especially for source nodes located near the sink node. The schemes use diversion and proxy nodes, respectively, to route packets originating from the near-sink regions. Due to the location of the diversion and proxy nodes, the routes become longer and introduce higher energy consumption. In many network configurations, the near-sink region has a greater load of packets to forward to the sink node which results into exhaustive energy consumption of the sensor nodes [2], [7]–[9]. In this study, we assume that exhaustive energy consumption in near-sink regions is

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman.

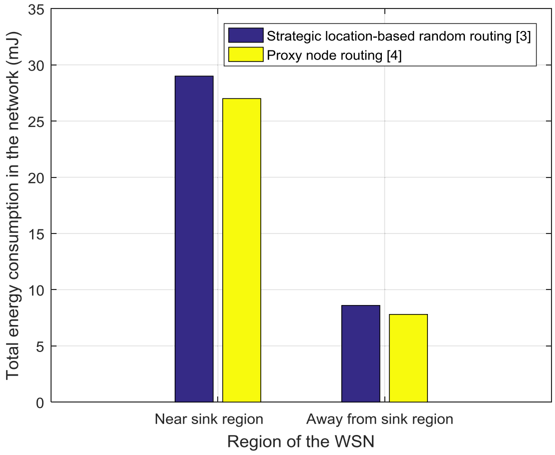


FIGURE 1. Energy consumption performance of the strategic location-based random routing [3] and proxy node routing [4].

a limitation for the schemes in [3] and [4]. Fig. 1 shows results of our recent analysis that shows the approximate energy consumption performance of the schemes in [3] and [4], when transmitting the same number of packets to the sink node. The Fig.1 shows that the schemes have significantly higher energy consumption in the near-sink region as compared to the regions away from the sink node. The high energy consumption in [3] is also pointed out in other recent studies including [10], [11]. The limitation of exhaustive energy consumption in the near-sink region may cause the sensor nodes around the sink node to deplete their power faster and become dead nodes. The limitation may further affect the network performance by triggering the energy-hole problem and shortening the network lifetime [1], [2], [7]–[9], [12], [13]. To address the performance issues of the schemes in [3] and [4], we design a new routing algorithm to provide strong SLP protection and minimize the energy consumption in the near-sink region. The routing algorithm also improves other packet transmission cost parameters such as packet delivery latency and delivery ratio.

A new path node offset angle routing algorithm is proposed. In the proposed algorithm, all ordinary sensor nodes compute and record their path node offset angles with respect to the sink node. When a source node in the near-sink region wishes to send packets to the sink node, the source node first determines its contrived region, randomly generates three candidate path nodes in three different forwarding regions, and computes a random value of an arbitrary factor. Based on the values of the computed arbitrary factor and the path node offset angles, a packet route is created through a randomly selected path node in one of the three forwarding regions. By using the proposed algorithm, successive packets are randomly routed in the network and the routing paths achieve high path diversity. The routing paths of the proposed algorithm are relatively shorter than the routing paths in [3] and [4]. However, the utilization of the path node offset angle and arbitrary factor parameters guarantee that the routes are highly randomized and provide similar levels of SLP protection for the source nodes in the near-sink region. Furthermore, the proposed algorithm offers cost-effective routing paths. Table 1 summarizes the limitations of the schemes in [3], [4] and the strategies for improvement in the proposed routing algorithm.

TABLE 1. Limitations of the existing schemes and strategies for improvement in proposed algorithm.

Limitations	Strategy for improvement in proposed routing algorithm
Both [3] and [4] use elongated routes which first divert to a diversionary [3] or proxy [4] node located outside the near-sink region.	Path nodes are located within the near-sink region to create relatively short routing paths.
Elongated routes increase the packet transmission cost including the energy consumption and packet delivery latency.	Relatively short routing paths effectively regulate the packet transmission cost.
Each source node has only two candidate diversionary or proxy nodes for the random route creation process.	Each source node has three candidate path nodes to guarantee highly dynamic route creation process with high path diversity.
Diversionary or proxy node selection process is based on the computation of a random bias number and a pre-defined threshold value.	Path node selection process is based on the computation of path node offset angles and arbitrary factors, and the location of contrived regions for vastly random routing paths.
A selected diversionary or proxy node has a small probability of near source node location.	Contrived regions are designed to guarantee selected path nodes are located far from the source node, to make the adversary tracing back process more complex and preserve strong SLP protection.

This study specifically addresses the limitations of the schemes in [3] and [4]. Thus, the objectives of the study are to: (1) modify the routing schemes in [3] and [4] by exploiting the proposed path node offset angle routing algorithm, (2) design the modified schemes to minimize the energy consumption for source nodes in the near-sink region and avert the energy-hole problem, and (3) evaluate the performance of the modified schemes to demonstrate their superiority over the existing schemes.

The remainder of this paper is organized as follows. In Section II, various related studies for protecting the source location privacy and cost-effective packet routing techniques are presented. In Section III, the assumptions, system design models and problem statement are introduced. In Section IV, the proposed path node offset angle routing algorithm is elaborated. Section V presents the experimental evaluation of the schemes as well as the analysis results. In Section VI, the paper is concluded.

II. RELATED WORK

There exist numerous SLP routing schemes, many of which are described in [14]–[16]. The schemes can be grouped into five categories: fake source routing, phantom node routing, angle routing, tree-based routing, and intermediate node routing [15]. The use of angle-based routing for cost-effective packet routing was demonstrated in [17], [18]. In [17], the scheme uses the transmitting offset angles and constrained probability to prevent an adversary from tracing back to locate the source node. Each sending node determines a specific selection domain for the next-hop node according to the dangerous distance and the wireless communication range. Then, it analyzes the angles of the candidate nodes based on the direction of the nodes to the sink node. Lastly, the sending node calculates the selected weights of the candidate nodes according to their angles, and the selected weights are used to decide which node becomes the next-hop node. By randomly selecting the next-hop node under constrained angles, the scheme can ensure that relay nodes are relatively close to the sink node. When relay nodes are close to the sink node, the routing paths become relatively short to minimize the energy consumption of the scheme. In [18], the angle-based dynamic routing scheme uses location information of the nodes and calculates inclination angles formed between the nodes. The angles include the inclination angle between a sending node and a receiving node, and the inclination angle between a sending node and the sink node. Based on the angles, the scheme generates a set of candidate neighboring nodes. The candidate set changes at every packet forwarding event to form dynamic paths toward the sink node. The analysis results in [17], [18] revealed that the angle-based routing schemes were capable of protecting the privacy of source nodes with controlled packet transmission cost.

Other angle-based routing schemes were proposed in [19]–[21]. In [19], the phantom routing with the location angle scheme modified the phantom single-path routing scheme by introducing inclination angles of sensor nodes in the random-walk section of the phantom single-path routing. The scheme assigned different probabilities to the next-hop nodes in the random-walk area to optimize the routing paths for source location privacy protection. In [20], the two-phantom angle-based routing scheme considered a triplet for selecting the phantom nodes. A triplet was considered to be a group of three nodes formed on the basis of three parameters: distance from the sink node, location information, and the inclination angle between them. Phantom selection was performed for every packet forwarding instance to create dynamic routing paths for the packets. In [21], the angle-based intermediate node scheme allowed the source node to determine two types of angles: a maximum angle between the last intermediate node and the source node according to the sink node, and an actual angle between the last intermediate node and itself according to the sink node. Then, the source determined the number of intermediate nodes and generated the distances between the source node and the intermediate nodes. Based on the angles and distances, intermediate nodes were selected for packet routing.

Other effective techniques for regulating the packet transmission cost in WSNs and alleviating the energy-hole problem were discussed in [1], [7]–[9], [12], [13]. The techniques include the following strategies: (1) Provide effective routing protocols through power-aware routing, by providing multiple routing paths to balance the energy consumption, and selecting the optimal path from the available paths based on the cost of each path. (2) Allow sensor nodes to use different transmission power levels for energy-efficient data transmission. For example, the transmission power of a Berkeley mote can be made adjustable to regulate its transmission power according to the distance between the transmitter and the receiver node. The Berkeley motes have 100 transmission power levels [9]. Using lower transmission power in the near-sink region and higher transmission power in the regions farther away from the sink can effectively balance the energy consumption in the network. (3) Use mobile relays to share the load of sensor nodes around the sink node, the mobile relays only need to be within two hops from the sink. (5) Deploy sensor nodes with greater initial energy, or more sensor nodes in the regions which consume large amounts of energy. (5) Employ a mobile sink node to balance the energy consumption. With a mobile sink, nodes near the sink would change over time and share the load. Static sensor nodes only send their data when the sink is within their communication range. (6) Exploit the non-uniform clustering algorithms. Cluster-based networks can achieve higher energy efficiency than flat networks. Using an unequal cluster-radius can be effective at balancing the energy consumption. (7) Construct load-balancing networks.

III. MODELS AND PROBLEM STATEMENT

In this Section, the relevant features of the proposed network, adversary, and energy consumption models are introduced and assumptions are highlighted. The problem statement is also stated.

A. NETWORK MODEL

This study assumes a target field of a WSN comprising sensor nodes randomly deployed over a vast field to continuously monitor the ground. The target field is a two-dimensional flat area with the distance metric given in Euclidean distance. Three types of sensor nodes and sensor node functionalities exist in the network: sink node, source nodes, and ordinary (relay) nodes. The sink node is responsible for collecting data from other nodes and acts as a link between the WSN and the external world. The sink node is more capable than the other nodes. It has higher memory capacity and greater computational power. The source node is responsible for sensing the asset and forwarding the sensed data to sink node through multi-hop communication. Ordinary nodes are used to relay packets from the source node to the sink node. Communication from a node is typically modeled with a circular communication range centered at the node. All nodes are homogeneous and have the same communication range. Nodes in direct communication range with each other through single-hop communication are considered neighboring nodes and are able to exchange data.

The network is event-triggered, when a source node senses an asset, it starts sending packets periodically to the sink node.

When a node detects an asset in its monitoring area, it remains active until the asset moves out of its monitoring area. When the asset moves to a new location, it activates another sensor node to become a new source node. When no asset is detected, the nodes may follow a sleeping schedule. Transmitted packets are encrypted and contain source node ID that only the sink node can infer as an asset location. During the network deployment phase, the network initialization process similar to [3], [4], is performed for localization of the sensor nodes. It is assumed that the sink node acquires its location information by using Global Positioning System (GPS). Once the sink node is aware of its location, it can lead the network initialization process by broadcasting a beacon packet to other sensor nodes. Other sensor nodes use the beacon packet to approximate their location and rebroadcast the packet to the neighboring nodes. At the end of the network initialization process, each node in the network is aware of its location, location of its neighboring nodes and IDs, and the location of the sink node. The network employs the k-nearest neighbor tracking approach to track the assets.

B. ADVERSARY MODEL

A cautious adversary similar to [3], [4] is assumed. The adversary is well-equipped with powerful transceivers to enable detection of packet signals and traffic patterns. The adversary is mobile, initially residing in the vicinity of the sink node listening for arriving packets. When a packet is received at the sink node, the adversary will overhear and start back tracing the packet route by moving hop-by-hop towards the source node, until it reaches the source node. It captures and uses information such as message type, sequence number, and sender node ID. When the source node is found, the adversary can successfully locate the monitored asset. It can perform passive attacks and does not interfere with the proper functioning of the network. It does not perform attacks such as meddling with the data packets or destroying the sensor equipment, because these actions can be observed easily. The cautious adversary has computational power to limit its waiting time at any immediate sender node. It uses a waiting timer. If the timer expires, the adversary will roll back to its previous immediate sender node and restart the packet detection process at that node. Moreover, the cautious adversary has the ability to escape from getting trapped in a loop. It collects and stores the information of all the visited immediate sender nodes to avoid revisiting nodes which have already been visited. Fig. 2 shows an example hop-by-hop back tracing attack of the cautious adversary. Packets may be sent from a source node to the sink node using a random route which passes through the path node. When the adversary is at the sink node, sensor node N_3 is within the adversary packet detection range. When a packet arrives at the sink node from N_3, the adversary will move to node N_3 without delay. Similarly, if the adversary is at N_5 and a packet arrives from N_{11}, the adversary will move to N_{11} without delay. At N_{11}, the adversary will wait for the next packet according to the waiting timer. If the timer expires, the adversary will roll back to N_5. The adversary will repeat the same process until it reaches the source node to successfully locate the asset.

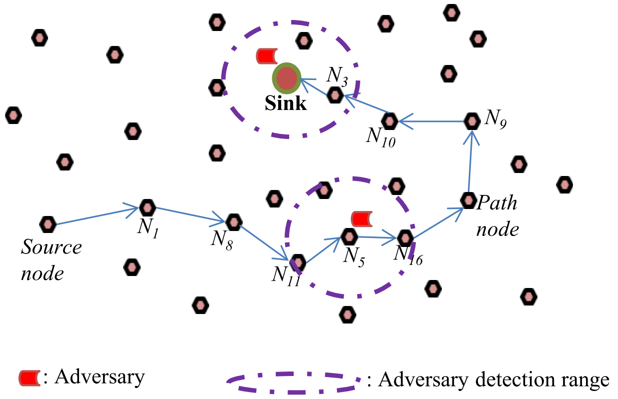


FIGURE 2. Example hop-by-hop back tracing attack of the cautious adversary.

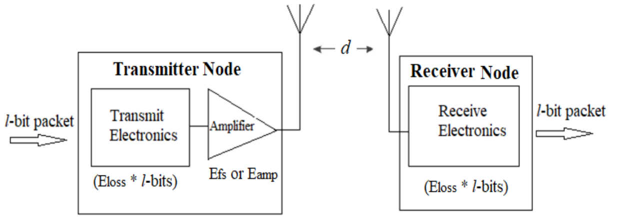


FIGURE 3. Energy consumption parameters for transmitting and receiving l-bit packet between two nodes of a WSN.

C. ENERGY CONSUMPTION MODEL

Energy consumption of the sensor nodes in WSNs is primarily due to three processes: sensing, computation, and communication [22]. Communication by the nodes consumes the most energy as compared to the other processes. Thus, this study considers only the energy consumption due to the communication process. The energy consumption model assumes that nodes expend energy while transmitting and receiving packets. The transmit and receive energy consumption models are characterized by the distance, d, and size of the packets, l, as shown in Fig. 3 and in the energy consumption model equations (1) and (2), as adopted from [3] and [4]. The model is also assumed in [2], [5], [7], [12], [22]. Transmitting a packet to a greater distance d or a larger packet containing a large number of bits causes higher energy consumption. According to the model, energy consumption for packet transmission is an exponential function of d. In the equations (1) and (2), E_{trans} is the transmission energy, and E_{rec} is reception energy. The energy model considers a free-space model (d^2 power loss) for d less than the threshold d_0, and multi-path attenuation model (d^4 power loss) for d greater or equal to d_0. The threshold distance, d_0, is designed to follow equation (3). E_{loss} represents the transmitting circuit loss, which depends on factors such as modulation and digital coding techniques. E_{fs} and E_{amp} are the energy required by power amplification in the two power

TABLE 2. Energy consumption model parameters.

Parameter	Description	Value
Initial energy (J)	Initial energy of a sensor node	0.5
d_o (m)	Threshold distance for the channel models	87
E_{loss} (nJ/bit)	Transmitting circuit energy loss	50
E_{amp} (pJ/bit/m^4)	The energy required by power amplification in the free-space model	0.0013
E_{fs} (pJ/bit/m^2)	The energy required by power amplification in the multi-path attenuation model	10
l (bit)	Size of the transmitted packet	1024

loss models. Table 2 shows the energy model parameters.

$$E_{trans}(l,d) = \begin{cases} lE_{loss} + lE_{fs}d^2, & if\ d < d_0 \\ lE_{loss} + lE_{amp}d^4, & otherwise \end{cases} \tag{1}$$

$$E_{rec}(l) = lE_{loss} \tag{2}$$

$$d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}} \tag{3}$$

D. PROBLEM STATEMENT

The primary focus of this study is to design a new path node offset angle SLP routing algorithm with the main objective of minimizing the packet transmission cost for the schemes in [3] and [4]. To achieve the objective, two tasks are performed: design the new routing algorithm to maximize the SLP protection, and minimize the energy consumption.

To characterize the performance of the proposed and existing schemes, the following performance metrics are used:

1) Safety period (*SP*): the same as in [2], [3], [5], safety period can be defined in three ways: (1) the time required for an adversary to back trace and capture the asset, (2) the number of packets successfully delivered to the sink node before the adversary reaches the source node, or, (3) the maximum time an asset will be at a given location before it moves to a new location. This study assumes the first definition. Longer safety period provides stronger SLP protection.
   To maximize the safety period, the following expression is assumed

$$\max\,(SP) = \max\,(SLP_{Protection})$$

2) Energy consumption (*E*): The energy consumption model assumes the sensor nodes consume most of their energy while transmitting and receiving packets, as shown in equations (1) and (2). The proposed routing algorithm employs relatively short but highly randomized routing paths, with fewer packet transmission and reception events (hops). If each hop involves consumption of E_{trans} and E_{rec}, the total energy consumption, E, for delivering a packet at the sink node can be computed as

$$E = \sum_{i=1}^{h} \left(E_{trans_i} + E_{rec}\right) \tag{4}$$

To minimize the energy consumption, the following expression is assumed

$$\min(E) = \min(h)$$

where h is the number of hops.

IV. PROPOSED PATH NODE OFFSET ANGLE ROUTING ALGORITHM

The proposed routing algorithm aims to provide a high degree of source location privacy protection while improving the packet transmission cost of strategic location-based random routing [3] and proxy node routing [4] schemes. Hereafter, we refer to the strategic location-based random routing scheme as “*Strat-R*”and the proxy node routing scheme as “*Proxy-R*.” The proposed path node offset angle routing algorithm is adopted into both schemes, *Strat-R* and *Proxy-R*, to produce modified schemes, namely “*Angle-Strat*” and “*Angle-Proxy*”, respectively. The key difference between the proposed *Angle-Strat* and *Angle-Proxy* schemes is the structure of the WSN domains. *Angle-Strat* locates the sink node at the center of the network with a circular near-sink region while *Angle-Proxy* locates the sink node toward the network edge with a square near-sink region.

A. OVERVIEW OF THE PROPOSED PATH NODE OFFSET ANGLE ROUTING ALGORITHM

The algorithm divides the sensor domain into two regions: the near-sink region and the region away from sink. The near-sink region is further divided into four quadrants as shown in Fig. 4. The sink node is located at the center of the near-sink region. An *X-Y* coordinate is generated at the sink node location as shown in the Fig. 4. Using this configuration, five parameters are introduced. The parameters are identified as:

- *Path node*: the relay node in the network domain randomly generated and then selected by the source node during route creation process. A routing path of any

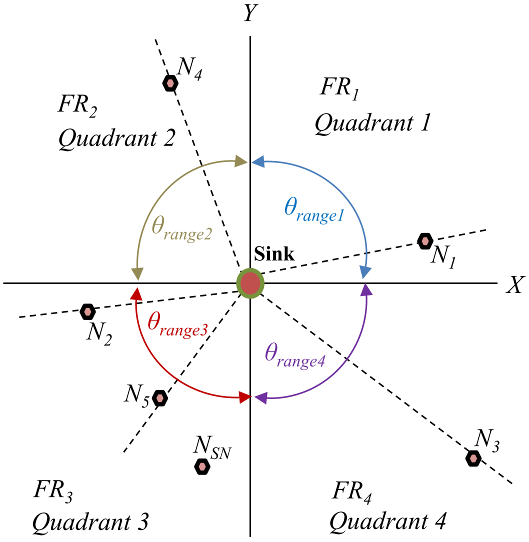


FIGURE 4. **Configuration of the near-sink region in the proposed path node offset angle routing algorithm.**

packet from a source node must pass through a randomly selected path node.

- *Contrived region*: the quadrant where the source node is located. It is the restricted region around the source node where the path node cannot be located. Locating the path node outside the contrived region ensures an increased complexity for the adversary during the back tracing attack, to maximize the SLP protection. It also ensures stronger SLP protection than that of the traditional schemes such as the shortest path routing [23], phantom single-path routing [24], and the randomly selected intermediate node routing [25] schemes. For every source node, one out of the four quadrants is a contrived region.
- *Forwarding regions (FR)*: the three regions (quadrants) in the near-sink region where path nodes are located. A source node identifies the quadrant of its location as its contrived region. The other three quadrants become forwarding regions.
- *Path node offset angle* (θ) : the angle formed between the X-axis and the imaginary line connecting the path node and the sink node.
- *Arbitrary factor* (A_F): the route creation factor. A_F is computed by a source node during the path node selection process. A_F is designed to ensure exposure of the path node location information to the adversary is minimized by randomizing the path node location for each successive packet.

Before any packet transmission is done in the network, it is assumed that the network initialization process is performed by a network planner to determine the network architecture according to Fig. 7, 8, 9 and 10. The network initialization process is explained in detail in [26]. The process involves the localization process for each sensor node. At the end of the initialization process, all nodes are localized and become aware of their locations as well as the location of their neighboring nodes and the sink node. Furthermore, the process enables the sensor nodes to realize the location of their contrived region and forwarding regions. After the network initialization process is complete, the offset angle computation process is performed.

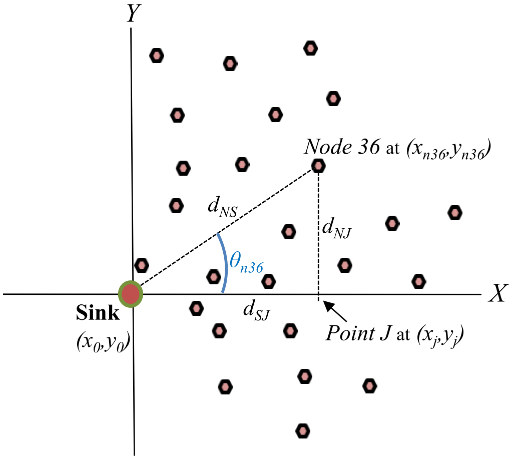


FIGURE 5. **Offset angle computation process.**

The offset angle computation process is executed using the coordinate information of the sink node and other sensor nodes, and the distance between the sensor nodes. The process begins by generating two imaginary lines: one connection line from the computing node (sensor node which is currently computing its offset angle) to the sink node, and one connection line from the computing node to the X-axis (perpendicular to X-axis). For example in Fig. 5, assuming *Node 36* at (x_{n36}, y_{n36}) is the computing node, and the perpendicular line connects to the X-axis at point J at (x_j, y_j), the distances d_{NS}, d_{SJ} and d_{NJ} can be determined using the Euclidean distance equation. Distance d_{NJ} can be computed as

$$d_{N,J} = \sqrt{\left(x_{n36} - x_j\right)^2 + \left(y_{n36} - y_j\right)^2} \tag{5}$$

Once the distances are known, the offset angle for the computing node is determined. From Fig. 5, the offset angle for *Node 36* (θ_{n36}) is computed as

$$\sin\left(\theta_{n36}\right) = \frac{d_{NJ}}{d_{NS}} \tag{6}$$

The offset angles are computed according to quadrants. For example, in Fig. 4, sensor nodes N_1, N_4, N_2 and N_5, and N_3 compute their offset angles in ranges θ_{range1}, θ_{range2}, θ_{range3}, and θ_{range4}, respectively. The offset angle for each sensor node is a fixed value and it is appended to the sensor node parameters together with other features such as the node ID.

Upon asset detection, a source node randomly generates a set of three candidate path nodes, one path node in each forwarding region. It records the values of the offset angle for each candidate path node. Then it computes an arbitrary factor, A_F, according to equation (7). K is a pre-defined constant number 0.9. R_F is a generated random factor with

TABLE 3. Determination of A_F value.

R_F	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A_F	0.81	0.75	0.69	0.64	0.6	0.56	0.52	0.5	0.47

values distributed from 0.1 to 0.9. Nine different values of A_F are possible as shown in Table 3. The source node computes a random value of A_F to use in the path node selection process.

$$A_F = \frac{K}{1 + R_F} \tag{7}$$

Using the value of A_F, one path node is selected from the set of candidate path nodes according to the path node selection process summarized in Table 4. The path node selection algorithm is shown in algorithm 1. Randomly selecting one path node from the three different forwarding regions provides packet routes which appear as if they originate from a broader range of source node locations, making the routes less predictable to the adversary. For example, in Fig. 4, assuming N_{SN} is the source node, then FR_3 becomes the contrived region and N_1, N_3, and N_4 may be candidate path nodes. N_1 may be selected as the random path node for route creation.

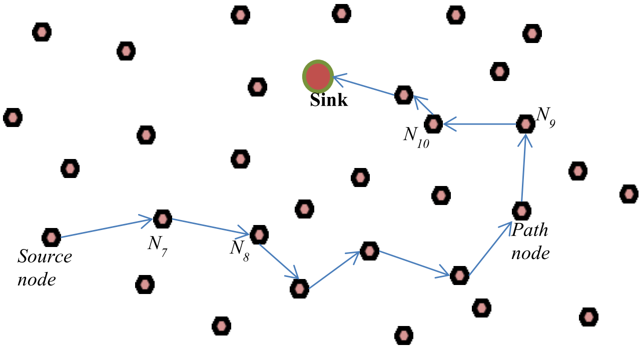


FIGURE 6. Random-walk routing strategy of the proposed routing schemes.

After the path node selection process, the source node randomly sends the packets to the selected path node using a random-walk routing strategy. Upon reception of the packets, the path node randomly forwards the packet to the destination sink node using random-walk routing. The random-walk routing strategy involves a next-hop selection process at every packet forwarding instance. In the process, the sending node determines a group of neighboring nodes with a shorter hop distance to the destination node than the sending node itself. One neighboring node from the group is randomly selected as the next-hop node. At the source node, the destination node is the selected path node. At the path node, the destination node is the sink node. Fig. 6 shows the random-walk routing strategy between the source node and path node, and between the path node and the sink node. For example, in Fig. 6, if a packet is from the source node to the sink node through the path node, nodes N_7 and N_8 are the next-hop nodes for the source node and N_7, respectively, while nodes N_9 and N_{10} are the next-hop nodes for the path node and N_9, respectively.

Algorithm 1 Path Node Selection Algorithm

```
Network initialization
Offset angle computation
Sensor node detects asset, becomes the sourceNode
sourceNode determines its contrivedRegion ($CR$)
sourceNode generates a set of candidate pathNodes
sourceNode computes $A_F$
if($CR ==$ forwardingRegion 1) do
    if ($A_F < 0.55$) then
        Select pathNode with $\theta$ within $\theta_{range2}$
    else if ($0.55 < A_F < 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range3}$
    else if ( $A_F > 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range4}$
    end
else if($CR ==$ forwardingRegion 2) do
    if ($A_F < 0.55$) then
        Select pathNode with $\theta$ within $\theta_{range3}$
    else if ($0.55 < A_F < 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range4}$
    else if ( $A_F > 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range1}$
    end
else if($CR ==$ forwarding Region 3) do
    if ($A_F < 0.55$) then
        Select pathNode with $\theta$ within $\theta_{range4}$
    else if ($0.55 < A_F < 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range1}$
    else if ($A_F > 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range2}$
    end
else if($CR ==$ forwardingRegion 4) do
    if ($A_F < 0.55$) then
        Select pathNode with $\theta$ within $\theta_{range1}$
    else if ($0.55 < A_F < 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range2}$
    else if ( $A_F > 0.65$) then
        Select pathNode with $\theta$ within $\theta_{range3}$
    end
end
```

To guarantee minimized exposure of the path node location information to the adversary, the proposed algorithm uses the A_F parameter to ensure a new path node is randomly selected from a different forwarding region, for each successive packet forwarding event. If successive packets arrive at the sink node from a wide range of directions, the adversary becomes highly confused, makes insignificant progress towards the path nodes and the vulnerability of the path nodes is very much reduced.

B. OVERVIEW OF THE PROPOSED ANGLE-STRAT ROUTING SCHEME

The *Angle-Strat* routing scheme adopts the path node offset angle routing algorithm to route packets for source nodes

TABLE 4. Path node selection process based on the path node offset angle, A_F, and contrived region parameters.

Source node location	Contrived region	θ_{range} identification for path node selection		
		$A_F < 0.55$	$0.55 < A_F < 0.65$	$A_F > 0.65$
Quadrant 1	FR_1	θ_{range2}	θ_{range3}	θ_{range4}
Quadrant 2	FR_2	θ_{range3}	θ_{range4}	θ_{range1}
Quadrant 3	FR_3	θ_{range4}	θ_{range1}	θ_{range2}
Quadrant 4	FR_4	θ_{range1}	θ_{range2}	θ_{range3}

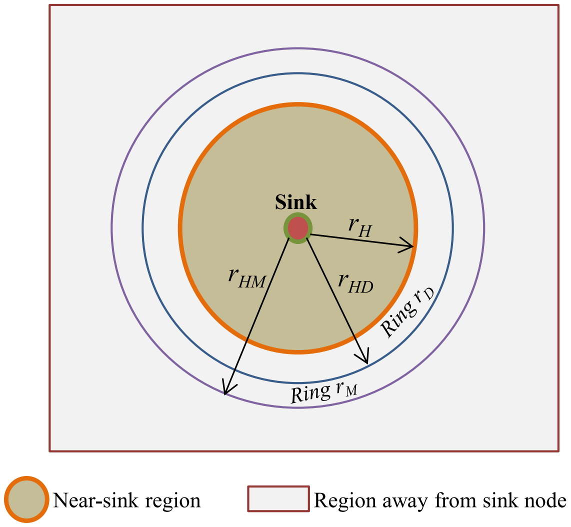


FIGURE 7. Distribution of the WSN regions for Strat-R scheme.

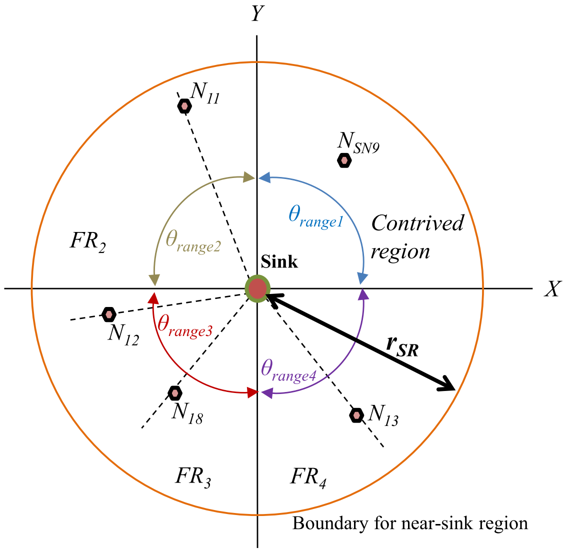


FIGURE 8. Configuration of near-sink region in the proposed Angle-Strat routing scheme.

located in the near-sink region. For the regions away from the sink, the routing strategy is similar to the *Strat-R* scheme. It is assumed that *Strat-R* is adequately cost-effective for the source nodes that are distant from the sink region. Fig. 7 shows the distribution of the network regions in the *Strat-R* scheme. The scheme divides the sensor domain into two regions: the near-sink region and region away from the sink. For *Strat-R*, nodes in the near-sink region route their packets through diversion nodes, while nodes in regions away from the sink route their packets through the mediate nodes. Diversion nodes are located in ring r_D, where the width of $r_D = r_{HD} - r_H$. Mediate nodes are located in ring r_M, where $r_M = r_{HM} - r_{HD}$.

In the *Angle-Strat* scheme, the near-sink region has a circular structure and is defined by the radius r_{SR} as shown in Fig. 8. For a smooth modification of *Strat-R* into the *Angle-Strat* scheme, the radius r_{SR} is assumed to be equal to the radius r_H. i.e., $r_{SR} = r_H$. All nodes which are located within distance r_{SR} from the sink node are considered as nodes in the near-sink region and adopt the path node offset angle routing algorithm. When a source node detects an asset, it computes the path node selection process according to Table 4 and algorithm 1. Fig. 8 also shows the forwarding regions, the *X-Y* coordinate generated at the sink node, the path node offset angle ranges, example candidate path nodes, and the boundary of the near-sink region in the proposed *Angle-Strat* routing scheme. If node N_{SN9} is assumed as a source node, quadrant 1 becomes the contrived region and N_{11}, N_{13} and N_{18} may be generated as candidate path nodes. Consequently, N_{11}, N_{13} or N_{18} may be selected for route creation process.

C. OVERVIEW OF THE PROPOSED ANGLE-PROXY ROUTING SCHEME

Similar to *Angle-Strat*, the *Angle-Proxy* model adopts the path node offset angle routing algorithm to route packets for source nodes located in the near-sink region. Fig. 9 shows the distribution of the network regions in the *Proxy-R* scheme. The scheme divides the WSN domain into four quadrants as shown in the Figure. The sink node is positioned at the center of Quadrant1. The proxy nodes are strategically located in proxy regions $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ in Quadrants 2, 3 and 4, respectively. During packet routing, a source node randomly selects a proxy region of a quadrant other than its own. Packets are routed through the selected proxy nodes. Source nodes in the near-sink region route their packets through proxy regions $Proxy_{R2}$ or $Proxy_{R4}$.

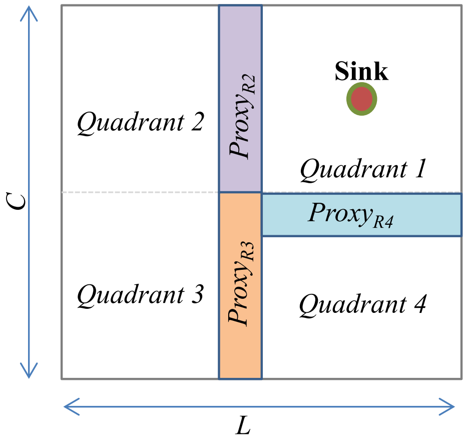


FIGURE 9. Distribution of the WSN regions for Proxy-R scheme.

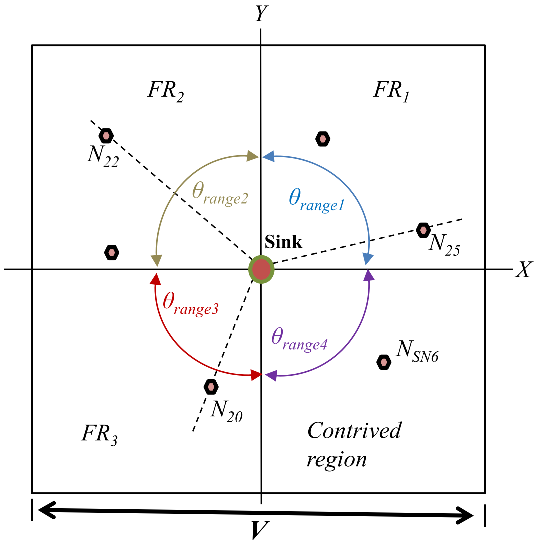


FIGURE 10. Configuration of the near-sink region in the Angle-Proxy routing scheme.

The *Angle-Proxy* scheme considers the Quadrant 1 region shown in Fig. 9 as the near-sink region. The scheme further divides the region into four quadrants as shown in Fig. 10. V is the width of the near-sink region. The sink node is located at the center of the region. All nodes which are located within width V are considered as nodes in the near-sink region and adopt the path node offset angle routing algorithm. When a source node detects an asset, it computes the path node selection process according to Table 4 and algorithm 1. After the path node is selected, packets are routed from the source node to the path node through random-walk routing as illustrated in Fig. 6. Similarly, the path node forwards the packets to the sink node through random-walk routing strategy.

V. EXPERIMENTAL EVALUATION

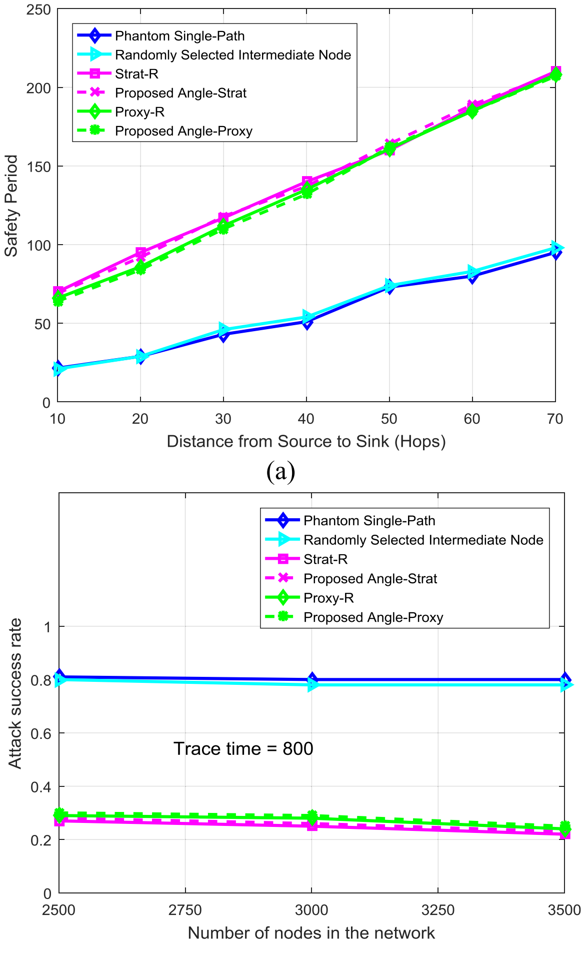
A. SIMULATION ENVIRONMENT

A square grid network layout of size 2000 × 2000 m^2 was simulated using the MATLAB simulation environment. For good coverage in the network, 2500 sensor nodes were randomly distributed throughout the network domain. Performance analysis of the proposed *Angle-Strat* and *Angle-Proxy* schemes was done. A total of six schemes were included in the analysis: the *Strat-R*, *Proxy-R*, *Angle-Strat*, *Angle-Proxy*, randomly selected intermediate node routing, and the phantom single-path routing schemes. The phantom single-path routing and randomly selected intermediate node routing schemes were included in the analysis as representative schemes for the traditional SLP routing schemes, for comparative analysis. The network model is explained in Section III. The following configurations were done. For *Strat-R*, $r_H = 400\ m$, $r_D = 200\ m$ and $r_M = 200\ m$, following the distribution shown in Fig. 7. For *Proxy-R*, $L = 2000\ m$ and $C = 2000\ m$. The length and width of the proxy regions were as follows: the lengths of $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ were $0.5C$, $0.5C$, and $0.5L$, respectively. The widths of $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ were $0.2L$, $0.2L$, and $0.2C$, respectively. The configuration of the *Proxy-R* network followed the distribution of the regions shown in Fig. 9. For *Angle-Strat*, $r_{SR} = r_H = 400\ m$, according to the distribution in Fig. 7 and Fig. 8. For *Angle-Proxy*, $V = 1000\ m$, according to the distribution in Fig. 10.

TABLE 5. Simulation environment parameters.

Parameter	Value
Network area (m^2)	2000 × 2000
Number of nodes	2500
r_H (m)	400
r_D (m)	200
r_M (m)	200
r_{SR} (m)	400
V (m)	1000
L (m)	2000
C (m)	2000
Sensor node sensing range (m)	30
Adversary detection range (m)	30
Adversary waiting timer (source packets)	4
Target monitoring scheme	k-nearest neighbor tracking

A cautious adversary was implemented with a waiting timer of four source packets. The adversary initiated the hop-by-hop back tracing attack at the sink node location. The network simulation parameters are summarized in Table 5. The simulation was run for 500 iterations and average values were considered. Evaluation of the schemes was done using five performance metrics: safety period, attack success rate, energy consumption, packet delivery latency, and packet delivery ratio. Safety period and attack success rate metrics measured the privacy performance of the schemes while energy consumption, packet delivery latency, and packet delivery ratio metrics measured the packet transmission cost.



(a)

(b)

FIGURE 11. Privacy performance of the routing schemes.(a) Safety period at various distances between source and sink node. (b) Attack success rate for different node density.

B. RESULTS AND DISCUSSIONS

Figure 11 (a) shows the four schemes: *Strat-R*, *Proxy-R*, the proposed *Angle-Strat*, and *Angle-Proxy* have somewhat comparable privacy performance. In the near-sink region, *Strat-R* offers slightly longer safety period than the *Proxy-R* because the use of strategically positioned diversion nodes provides a marginal increase in path diversity. Despite the relatively short packet routes, the proposed schemes are able to achieve a high degree of privacy protection similar to the other schemes because they employ path node offset angle routing strategy. The schemes use contrived regions to ensure that the path nodes are located away from the source nodes to obfuscate the adversary when it tries to back-trace the packet routes. Furthermore, the use of A_F ensures that successive packets use path nodes selected from a diverse range of path node offset angles to guarantee the packet routes are equally obfuscating to the adversary as compared to *Strat-R*, and *Proxy-R* schemes. For example, from Fig. 12, if packets from source node 1 are routed using the proposed *Angle-Strat* or *Angle- Proxy* schemes, path node 2 (*PN2*) with $\theta = \theta_2$ may be selected when θ selection falls under θ_{range1}. *PN 3* with $\theta = \theta_3$ or *PN 1* with $\theta = \theta_1$ may be selected when the θ selection falls under θ_{range2} or θ_{range4}, respectively. For the next packet, the source node 1 may generate other path nodes such as *PN 4*, *PN 7*, and *PN 8*, and one *PN* is randomly selected for the packet routing. Similarly, for source node 2, the source node may generate path nodes such as *PN 5*, *PN 6*, and *PN 9*, and one *PN* is randomly selected.

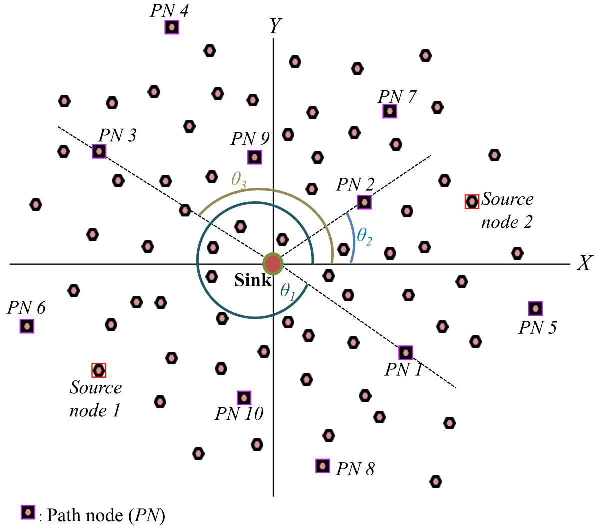


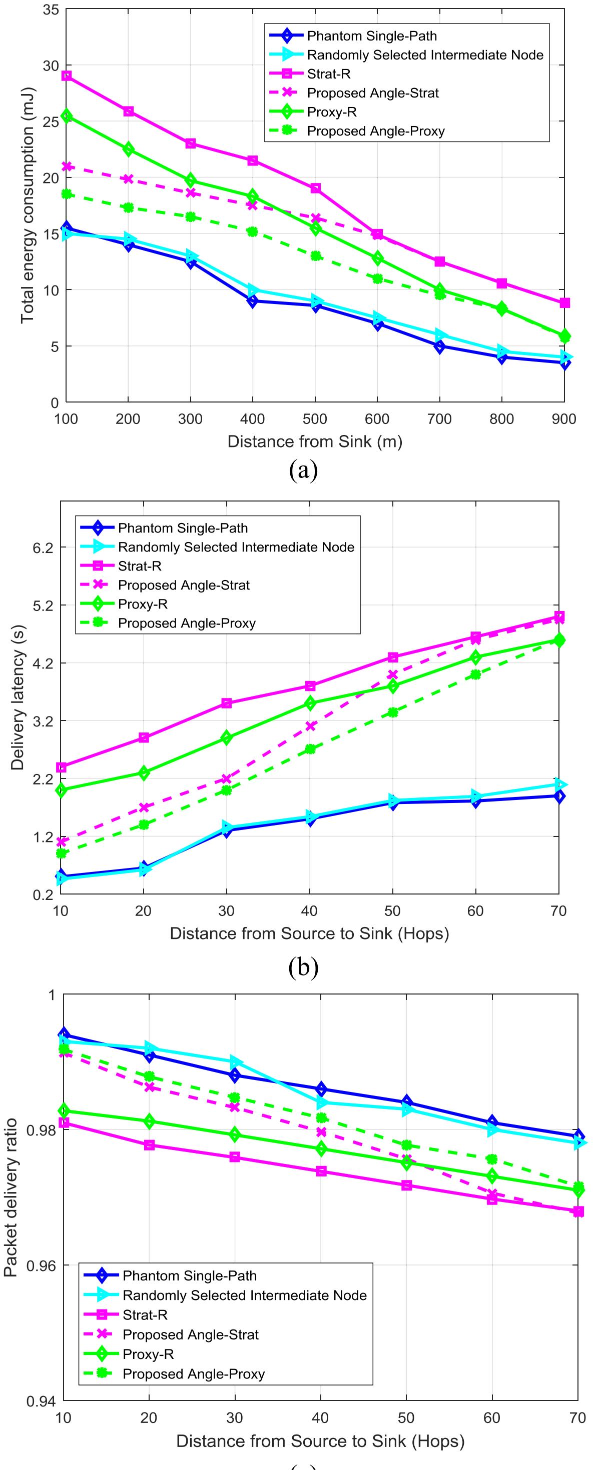
FIGURE 12. Example path node selection in the proposed routing schemes for the near-sink regions.

The process of generating a set of candidate path nodes at different path node offset angles improves the path diversity and randomness of the routing paths. As a result, it becomes a complex task for the adversary to capture successive packets. Adversary can make significant progress in the back tracing attack only if it captures a sufficient number of successive packets. In the proposed schemes, the adversary attack progress is very much hindered.

The phantom single-path routing and randomly selected intermediate node routing schemes offer the lowest privacy level because they use fixed routes between the phantom/ intermediate nodes and the sink node. The fixed routes can easily be traced by adversaries. Moreover, the schemes have a higher probability of the phantom or intermediate nodes for successive packets to be located very near the sink node, when a source node is located in the near-sink region. Continuously selecting a phantom or intermediate node which is located very near the sink node causes weak privacy protection, since it will take a short time for an adversary to successfully back-trace the routes to the nodes. Figure 11 (b) shows the attack success rate of the schemes at a trace time of 800 source packets for different node density. In this study, trace time refers to the time spent by the adversary since it initiated the back tracing attack at the sink node. Attack success rate measures the rate of source traceability when using a routing algorithm against the backtracking adversary. It is calculated by counting the number of successful attempts of an attacker.

The higher the safety period and privacy level for a scheme, the lower the attack success rate. The proposed *Angle-Strat* and *Angle-Proxy* schemes are capable of achieving low attack success rate of the adversary. The attack success rate for the schemes decreases with the increase in the node density which suggests that the schemes are practical for networks which require scalability. The Fig.11 (b) shows similar privacy performance between the *Strat-R*, *Proxy-R*, *Angle-Strat*, and *Angle-Proxy* schemes.

Figure 13 shows the cost performance of the routing schemes for delivering the same number of packets to the sink node. The energy consumption per packet delivery was computed using the energy consumption model explained in Section III. In the energy consumption analysis, 24 experiment scenarios were assumed, each scenario with a different source node location. 12 scenarios were run for source nodes in the near-sink regions and 12 scenarios in the regions away from sink node. For the near-sink region scenarios, three scenarios were run in each quadrant. In each scenario, 1000 packets were transmitted from a source node to the sink node using the six analyzed schemes. After all the packets were delivered at the sink node, for each scenario, the average energy consumption per sensor node was observed at different node locations. Figure 13 (a) shows the average total energy consumption per sensor node at various sensor node locations. The Fig. 13 (a) shows that the sensor nodes using the proposed *Angle-Strat* and *Angle-Proxy* schemes have lower energy consumption near the sink region. The schemes achieve lower energy consumption by using routing paths which are shorter than the routes of *Strat-R* and *Proxy-R* as demonstrated in Fig. 14. While *Strat-R* and *Proxy-R* use longer routes to obfuscate the adversary for source nodes in the near-sink region, the proposed schemes apply relatively short routing paths. Shorter routing paths incur fewer packet forwarding events in the near-sink region. With fewer packet forwarding events, the sensor nodes consume less transmit and receive energy. The proposed schemes achieve strong SLP protection while being more energy-efficient in the near-sink region. For example, in Fig. 13 (a), at a distance of 200 m from the sink node where it is assumed to be in the near-sink region, the total energy consumption of sensor nodes when using routing schemes *Strat-R*, *Angle-Strat*, *Proxy-R,* and *Angle-Proxy* are 25.9 mJ, 19.6 mJ, 22.5 mJ, and 17.1 mJ, respectively.



(a)

(b)

(c)

FIGURE 13. Packet transmission cost of the routing schemes. (a) Energy consumption. (b) Packet delivery latency. (c) Packet delivery ratio.

The graphs for *Strat-R* and *Angle-Strat* converge at 600 m from the sink node while the graphs for *Proxy-R* and *Angle-Proxy* converge at 700 m from the sink node. This structure of the graphs illustrates that the modified schemes consume lower energy in the near-sink regions due to the adoption of the path node offset angle routing algorithm. Beyond the near-sink region, the schemes assume the same routing strategies as their contender schemes. Hence, the same energy consumption performance is experienced. Despite the near-sink region boundary being at 400 m for both *Strat-R* and *Angle-Strat*, the region between 400 m and 600 m in the *Strat-R* scheme has higher energy consumption, because this region has more packet forwarding events through the diversion nodes. In the *Angle-Strat* scheme, the diversion node region is not defined, instead, nodes in the region are used simply as relay nodes with fewer packet forwarding events. Similarly, despite the near-sink region boundary being at 500 m for both

Proxy-R and *Angle-Proxy*, the region between 500 m and 700 m in the *Proxy-R* scheme has more packet forwarding events through the proxy nodes. This work embraces the conclusion that the reduced energy consumption in the near-sink region can have a positive impact on the performance of the network, including improved network lifetime and an alleviated energy-hole problem. Comparing the energy consumption of the proposed schemes and that of the traditional phantom single-path or randomly selected intermediate node routing, the proposed schemes incur an acceptable increase in energy cost.

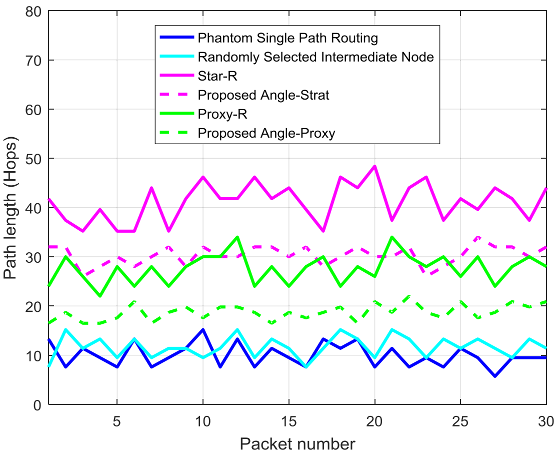


FIGURE 14. Path length of the routing schemes.

Figure 14 further demonstrates the relatively short and energy-efficient routing paths of the proposed schemes. The Fig. 14 shows the length of the routing paths for 30 successive packets sent from a source node in the near-sink region. For example, the path length of the *Strat-R*, *Angle-Strat*, *Proxy-R*, *Angle-Proxy*, phantom single-path routing, and randomly selected intermediate node routing schemes for delivering packet number 18 to the sink node are, 46 hops, 30 hops, 24 hops, 17 hops, 11 hops, and 15 hops, respectively. Assuming each hop involves consumption of E_{trans} at the transmitting node and E_{rec} at the receiving node, the total energy consumption E_{tot} for delivering one packet at the sink node can be approximated as $E_{tot} = E_{trans} * N_{hop} + E_{rec} * N_{hop}$. It is evident that the proposed schemes will incur lower energy cost per packet transmission compared to their contender schemes. Similarly, the short routing paths will results in improved packet delivery latency and delivery ratio.

The experimental evaluation of the schemes included the analysis of packet delivery latency and delivery ratio. In this study, packet delivery latency is defined as, the time required to transmit a packet of data from a source node to the sink node. It is highly dependent on the length of the routing paths. Longer routing paths incur higher delivery latency. Delivery ratio is the ratio of the number of packets successfully delivered at the sink node to the total number of packets sent from a source node. The experiment scenarios included source nodes at different source-sink distances. 100 packets were sent from each source node to the sink node and average values for delivery latency and delivery ratio were found. Figure 13 (b) (c) show that the *Angle-Strat* and *Angle-Proxy* have better packet delivery latency and delivery ratio than their contenders *Strat-R* and *Proxy-R*. *Strat-R* and *Proxy-R* achieve high privacy protection by ensuring longer routing paths hence high delivery latency. The short routing paths of the proposed *Angle-Strat* and *Angle-Proxy* schemes ensure fewer packet forwarding events to minimize the delivery latency for the near-sink regions. Beyond the near-sink region, the graphs for *Strat-R* and *Angle-Strat*, and for *Proxy-R* and *Angle-Proxy*, converge. The convergence is due to similar performance since the path node offset angle routing algorithm is adopted only in the near-sink regions. These results can be a clear indication that the *Angle-Strat* and *Angle-Proxy* schemes are capable of controlling the packet transmission costs in the network, and can be considered when parameters such as delivery latency and reliable packet transmission are important. From these findings, this work can conclude that the proposed *Angle-Proxy* scheme is a more cost-effective SLP scheme and practical for WSNs which locate the sink node towards the network edge while the proposed *Angle-Strat* is more practical for WSNs which locate the sink node at the center of the WSN domain. Furthermore, the schemes can be more appropriate for network scenarios where network reliability is required and the energy-hole problem is undesirable.

A possible limitation of the proposed routing schemes may happen when a source node is located near the X-axis or Y-axis and it randomly selects a path node which is located adjacent to the axis. In such scenarios, the location information about the source node may be exposed to the adversary. However, this limitation is minimized by using the A_F parameter which guarantees high path diversity. A_F is designed to ensure a high probability that, path nodes for successive packets are selected from different forwarding regions. If successive packets are routed randomly in different regions of the network, it becomes difficult for the adversary to capture the packets. Hence, it makes no significant progress towards the source node. Based on the value of A_F, successive packets from the same source node are guaranteed to use completely different routes to sustain strong SLP protection. When considering the storage cost of the proposed algorithm, there is a slight increase in the required memory size of the sensor nodes compared to the *Strat-R* and *Proxy-R* schemes. The proposed algorithm requires an additional one byte memory for each sensor node to store the offset angle information. We assume that the additional memory space is acceptable for event monitoring WSNs.

VI. CONCLUSION AND FUTURE WORK

It is typical for individuals and organizations to use WSN technology to secure and monitor assets of great value. When the WSNs are deployed in remote areas, it becomes difficult to recharge or replace the batteries in the sensor nodes. It is then essential that network designers offer energy-efficient source location privacy routing schemes. Realizing the need, this study has proposed a new path node offset angle routing algorithm. The study has also demonstrated the adoption of the algorithm to modify and improve the packet transmission cost of two existing schemes. The modified schemes effectively utilize routing paths which are relatively short but vastly diverse. The tactical use of path node offset angles, contrived regions, and arbitrary factors during the path node selection process guarantees cost-effective routing paths. The modified schemes are well-suited for systems which require strong source location privacy protection with controlled packet transmission cost. Moreover, the schemes are capable of alleviating the energy-hole problem in WSNs. As part of future work, techniques to regulate the packet transmission cost in the regions away from the sink node will be considered. In addition, the feasibility of the schemes in various event-driven and resource-constrained application scenarios will be investigated.

REFERENCES

[1] Y. Yang, M. I. Fonoage, and M. Cardei, "Improving network lifetime with mobile wireless sensor networks," *Comput. Commun.*, vol. 33, no. 4, pp. 409–419, 2010.

[2] 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, Jul. 2014.

[3] L. C. Mutalemwa and S. Shin, "Strategic location-based random routing for source location privacy in wireless sensor networks," *Sensors*, vol. 18, no. 7, p. 2291, 2018.

[4] 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.

[5] R. Manjula and D. Raja, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in wsns," *Pervasive Mobile Comput.*, vol. 44, pp. 58–73, Feb. 2018.

[6] H. Wang, G. Han, L. Zhou, J. A. Ansere, and W. Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT," *Comput. Netw.*, vol. 148, pp. 142–150, Jan. 2019.

[7] A. Liu, X. Jin, G. Cui, and Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," *Inf. Sci.*, vol. 230, pp. 197–226, May 2013.

[8] A. Liu, X. Wu, Z. Chen, and W. Gui, "Research on the energy hole problem based on unequal cluster-radius for wireless sensor networks," *Comput. Commun.*, vol. 33, no. 3, pp. 302–321, 2010.

[9] A. Liu, D. Zhang, P. Zhang, G. Cui, and Z. Chen, "On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 255–273, 2014.

[10] H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, "A probabilistic source location privacy protection scheme in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5917–5927, Jun. 2019.

[11] N. Jan and S. Khan, *Energy-Efficient Source Location Privacy Protection for Network Lifetime Maximization Against Local Eavesdropper in Wireless Sensor Network (EeSP)*. Hoboken, NJ, USA: Wiley, Aug. 2019.

[12] R. Yarinezhada and A. Sarabib, "Reducing delay and energy consumption in wireless sensor networks by making virtual grid infrastructure and using mobile sink," *Int. J. Electron. Commun.*, vol. 84, pp. 144–152, Feb. 2018.

[13] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 788–800, Apr. 2016.

[14] J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 125, pp. 93–114, Jan. 2019.

[15] L. C. Mutalemwa and S. Shin, "Routing schemes for source location privacy in wireless sensor networks: A survey," *J. Korean Inst. Commun. Inf. Sci.*, vol. 43, no. 9, pp. 1429–1445, Sep. 2018.

[16] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.

[17] W. Chen, M. Zhang, G. Hu, X. Tang, and A. K. Sangaiah, "Constrained random routing mechanism for source privacy protection in WSNs," *IEEE Access*, vol. 5, pp. 23171–23181, Nov. 2017.

[18] P. Spachos, D. Toumpakaris, and D. Hatzinakos, "Angle-based dynamic routing scheme for source location privacy in wireless sensor networks," in *Proc. 79th IEEE Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–5.

[19] W.-P. Wang, L. Chen, and J.-X. Wang, "A source-location privacy protocol in WSN based on locational angle," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1630–1634.

[20] S. Gupta, P. Kumar, J. P. Singh, and M. P. Singh, "Privacy preservation of source location using phantom nodes," in *Information Technology: New Generations*, vol. 448. Cham, Switzerland: Springer, 2016, pp. 247–256.

[21] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[22] N. Alaouil, J. P. Cances, and V. Meghdadi, "Energy consumption in wireless sensor networks for network coding structure and ARQ protocol," in *Proc. 1st Int. Conf. Electr. Inf. Technol. (ICEIT)*, Mar. 2015, pp. 317–321.

[23] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proc. 2nd ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, Oct. 2004, pp. 88–93.

[24] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. 25th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2005, pp. 599–608.

[25] J. Ren, Y. Li, and T. Li, "Routing-based source-location privacy in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[26] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, Apr. 2006, Art. no. 829835.

LILIAN C. MUTALEMWA received the B.Eng. degree in telecommunications engineering from the University of Essex, Colchester, U.K., in 2008, and the M.Sc. degree in mobile and satellite communications from the University of Surrey, Guildford, U.K., in 2010. She is currently pursuing the Ph.D. degree with the Department of Computer Engineering, Chosun University, Gwangju, South Korea. Since 2012, she has been with The Open University of Tanzania, Tanzania, where she is also an Assistant Lecturer with the Department of Information and Communication Technology. Her current research interests include wireless networks, WSN protocol design and performance evaluation, and communication systems engineering.

SEOKJOO SHIN received the M.S. and Ph.D. degrees from the Department of Information and Communications, Gwangju Institute of Science and Technology (GIST), South Korea, in 1999 and 2002, respectively. He joined the Mobile Telecommunication Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), South Korea, in 2002. In 2003, he joined the Faculty of Engineering, Chosun University, where he is currently a Full Professor with the Department of Computer Engineering. In 2009, he was a Visiting Researcher with Georgia Tech, USA. His research interests include wireless communication systems, and network security and privacy.