IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 9, 2020, accepted April 16, 2020, date of publication April 22, 2020, date of current version May 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989434

Comprehensive Performance Analysis of Privacy Protection Protocols Utilizing Fake Packet Injection Techniques

LILIAN C. MUTALEMWA AND SEOKJOO SHIN, (Member, IEEE)
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 In many Internet of Things (IoT) systems and monitoring wireless sensor networks (WSNs), sensor nodes are expected to function for prolonged periods of time with no scope of recharging the sensor node batteries. Similarly, in safety-critical monitoring applications, the WSNs are expected to guarantee effective source location privacy (SLP) protection throughout the network lifetime. Fake packet-based SLP protocols are often energy-inefficient, they incur short network lifetime, and have high probability of packet collision events. Therefore, it is important to evaluate features such as the capability of the protocols to guarantee effective SLP protection for prolonged periods of time and reliable packet delivery. The existing studies show some deficit in the performance evaluation of the protocols. Consequently, this paper presents some investigations on the performance of the fake packet-based SLP protocols. Comprehensive performance analysis of four existing protocols is done under varied network parameters and configurations. Performance is observed under varied sensor node residual energy, source-sink distance, lifetime, source packet rate, network size, and node density. Analysis results establish that the protocols are capable of achieving high levels of SLP protection. However, the privacy protection is short-lived. Furthermore, the results show that long source-sink distance, long fake packet routes, short distance between fake packet sources and phantom nodes, and large amounts of fake packet traffic can improve the SLP protection while diminishing the packet delivery reliability, energy efficiency, and the network lifetime. The results also show that when the source packet rate is increased it influences some negative effects on the performance of the protocols. Moreover, it is observed that integrating fake packet routing and packet flooding techniques can impact some positive effects on the SLP protection and negative effects on the network lifetime. Based on the observations and analysis results, some recommendations are presented to improve the performance of the protocols.

INDEX TERMS Source location privacy protection, wireless sensor network, routing protocol, fake packet routing, packet delivery reliability.

I. INTRODUCTION

Internet of Things (IoT) technology has become a reality and its popularity is maturing. Wireless sensor network (WSN) technology is one of the important components of the IoT. Therefore, it is critical that the limitations of WSNs are considered during the designing of routing protocols for IoT systems [1]–[3]. The limitations of WSNs include limited power, memory, bandwidth, and processing capability [4]–[6]. When the WSNs are used in safety-critical and long-term monitoring applications such as monitoring of high value assets, the routing protocols are expected to warranty desirable features such as energy efficiency, low delay, reliable packet delivery, and high levels of source location privacy (SLP) protection. It is important to ensure energy efficiency and long network lifetime in the WSNs because the networks are often deployed in harsh and inaccessible environments. Hence, energy-efficient routing protocols enable the WSNs to achieve long unattended operation time [2].

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

SLP protection is defined as the process of minimizing the traceability and observability of a source node by an attacker in monitoring WSNs [4], [7]. In this study, we focus on investigating the performance of SLP routing protocols. Particularly, we focus on investigating a category of protocols which utilize fake source packet routing strategies. The protocols rely on obfuscating the adversaries by employing mimicking fake packet sources to imitate the real packet sources [8], [9]. The real and fake packet sources transmit packets in a synchronized manner. The main objective of the fake packet sources is to transmit fake packets which are capable of misleading the adversary into tracing back the fake packet routes while keeping the real packet routes secured. When the adversary is tricked into back tracing the fake packet routes, it is steered away from the location of the real source node and the SLP is protected [10]. The operations of the real and fake packet sources may be depicted as two teams in a tug-of-war game [10]. In the game, the two teams create a pull effect on a piece of rope. The team with a greater pull effect wins. Similarly, for the real and fake sources, the fake source nodes create a pull effect to pull the adversary away from the real source node. If the pull effect of the fake source node is greater, the fake source wins by keeping the adversary away from the location of the real source node. Subsequently, the SLP is protected.

There exists other categories of SLP protocols including the phantom routing, intermediate node routing, ring routing, angle routing, random walk routing, tree routing, data mule mechanism, directional communication mechanism, isolation mechanism, and the hiding mechanism [11], [12]. The main reason for choosing to investigate the protocols which utilize fake source packet routing techniques is that, the protocols are often criticized for their high communication cost including significantly high energy consumption and low packet delivery reliability [11]–[14]. Exhaustively high energy consumption may result in short-term SLP protection and reduced network lifetime. When the sensor nodes exhaust their energies at a fast rate, the protocols may preserve the SLP but only for a limited period of time. Thus, it is interesting to investigate the performance of the protocols under varied network parameters and configurations. More details about the motivation for this study are presented in section III.

Four fake packet-based SLP protocols are included in the investigations: the tree-based diversionary routing protocol (TDR) [15], data dissemination routing protocol (DDR) [16], distributed protocol with fake source and phantom source routing (FPR) [17], and the probabilistic source location privacy protection protocol (PRR) [18]. The four protocols were selected for investigations based on features and key differences in their routing strategies as shown in Fig. 1. The following differences are considered. (1) TDR employs fake packet sources far away from the sink node, in the diversionary routes. DDR employs fake packet sources away from the sink node, outside the blast ring. PRR employs fake packet sources in the near-sink regions. FPR employs fake packet sources at variable distances from the sink node, throughout the WSN domain. (2) In TDR and FPR the fake packet sources are not isolated from the real source nodes but in DDR and PRR the fake packet sources are isolated from the real source nodes. (3) TDR broadcasts a large number of fake packets in the network from multiple fake packet sources, employing numerous fake sources per real source node. DDR broadcast multiple fake packets from a single fake packet source, employing one fake source per real source node. PRR broadcasts one fake packet from a single fake packet source for a time period, employing one fake source per real source node for a time period. FPR broadcasts a variable number of fake packets from multiple fake packet sources which may be less than in TDR, employing multiple fake sources per real source node. (4) TDR broadcasts numerous fake packets per real source packet. DDR broadcast one fake packet per real source packet. PRR broadcasts one fake packet for a time period for each real source packet. FPR broadcasts multiple fake packets per real source packet which may be less than in TDR. Similar to other fake packet-based protocols, the TDR, DDR, PRR, and FPR protocols incur high energy consumption due to the distribution of fake packet traffic in the network [4], [11], [13], [14], [19]. Furthermore, the protocols incur unreliable packet delivery due to high probability of packet collision and packet loss events [4], [8].

We investigate the performance of TDR, DDR, PRR, and FPR protocols using important performance metrics: safety period, capture ratio, detection ratio, energy consumption, network lifetime, end-to-end delay, and packet delivery ratio. For comparative analysis, the traditional random intermediate node routing (RIN) protocol [20] is included in the analysis as a reference protocol.

Thus, the main contributions of this study can be summarized as follows. (1) Expose the underlying routing strategies of the fake packet-based SLP routing protocols and their influence on the privacy performance and packet delivery reliability. (2) Conduct a series of experiments to evaluate the SLP protection, energy consumption, network lifetime, end-to-end delay, and packet delivery ratio performance of the TDR, DDR, PRR, and FPR protocols under varied network configurations. (3) Contrast the performance of the TDR, DDR, PRR, and FPR protocols with the performance of the traditional RIN protocol through comprehensive experimental analysis. (4) Investigate the ability of the TDR, DDR, PRR, and FPR protocols to preserve the SLP in long-term monitoring networks and the effects of distributing fake packet traffic in various regions of the WSN domain. (5) Provide some recommendations to address the limitations of the TDR, DDR, PRR, and FPR protocols based on state-of-the-art techniques.

The remainder of this paper is organized as follows. Section II presents a review of the literature on SLP routing protocols utilizing fake packet routing strategies. Motivation for this study and the problem statement are highlighted in section III. Section IV conveys some assumptions and details of the network and adversary models. Experimental

analysis and simulation results are discussed in section V. Section VI presents some discussions and recommendations. In section VII, the paper is concluded.

II. PRIVACY PROTECTION PROTOCOLS WITH FAKE PACKET INJECTION TECHNIQUES

Various routing strategies have been proposed for SLP protection. Many of the strategies are described in [4], [11]–[13], [21]. In [22], it was established that baseline fake packet routing and probabilistic fake packet routing strategies can be used to preserve SLP in monitoring WSNs. Since then, the fake packet routing strategies have been adopted in numerous protocols. The key procedures in the operation of the fake packet-based protocols include the process of selecting a subset of the sensor nodes in the WSN to act as fake source nodes by imitating the real source nodes. The fake sources and real sources send packets concurrently to confuse the adversary. In this section, we explore the operational features of the protocols.

Fake packet routing strategies have been adopted in the cloud-based with multi-sinks protocol [23], dummy packet injection protocol [24], dynamic fake source-based protocol [10], tree-based diversionary routing protocol [15], hybrid online dynamic single path routing protocol [25], dummy uniform distribution protocol [26], and the data dissemination routing protocol [16]. The cloud-based with multi-sinks protocol is designed to preserve the SLP against adversaries with backtracking and hotspot-locating attacks. The protocol employs a routing strategy that changes the destination sink node randomly in each packet transmission. With a different destination sink node in each transmission, the routing paths become less predictable to the adversary. Many routing paths are created between the source nodes and the multiple sink nodes. Then, cloud-shaped fake hotspot regions and fake branches are created to broadcast fake packets and complicate the traffic pattern. As a result, the adversary is obfuscated by the fake traffic flow. The dummy packet injection protocol is designed to provide SLP protection against packet rate monitoring attacks combined with packet tracing attacks. In its operation, the protocol ensures that whenever a sensor node forwards a packet, its neighbor from a further group also sends a fake packet. The selection of the fake packet source nodes is based on the remaining energy of the sensor nodes. To improve the pull effect of the fake packet source on the adversary, the protocol broadcasts fake packets at a higher rate than the rate of the real packets. In the operation of the dynamic fake source-based protocol, no prior knowledge of the network is required. The protocol determines important parameters through online estimation to provide high levels of privacy protection.

The tree-based diversionary routing protocol is designed to protect the SLP against adversaries with direction-oriented attack strategies. The protocol employs phantom nodes away from the source node. Then, it establishes a backbone route from sink node to the network border. Subsequently, it establishes many redundant diversionary routes as branch routes of the backbone route. Fake packets are distributed throughout the diversionary routes as the source nodes send packets to the sink node. In the hybrid online dynamic single path routing protocol, directed random walk strategy is used for fake source allocation. Packets are sent to inform sensor nodes of their source-sink distances. When the sink node receives an alert from a source node, it sends a choose packet to start the selection of the fake sources. Nodes choose a neighbor with the longest source-sink distance and send them a choose packet. When multiple candidate nodes exist, one node is chosen randomly as the fake source. Temporary fake sources are created along the random walk to pull the adversary away. The random walk ends when no neighbors are farther from the source node than the current node. Then, the node becomes a permanent fake source for packet routing.

The dummy uniform distribution protocol assumes a constant rate for transmitting both, real and fake packets. A node generates and sends fake packets when there are no real packets to send. A random number is generated by the nodes. If the random number is smaller than the constant rate and a real packet is present, the real packet is sent. Otherwise a fake packet is sent. The data dissemination routing protocol divides the WSN into four quadrants with the sink node at the center of the network domain. Also, a blast ring is generated with its center positioned at the sink node. Sensor nodes inside the blast ring employ a flooding mechanism for packet routing to ensure the sink node receives the same packet from multiple neighboring nodes. When a source node is located outside the blast ring, the sink node generates a fake source node for each real source node. Real packets and fake packets are sent to the sink node simultaneously. When the packets enter the blast ring region, blast nodes at the edge of the ring receive the packets and employ a flooding technique to forward the packets to the sink node.

Other protocols which adopt the fake packet routing strategies include the probabilistic source location privacy protection protocol [18], timed efficient privacy preservation protocol [27], fake network traffic-based protocol [28], bidirectional tree protocol [29], dummy adaptive distribution protocol [26], distributed fake source and phantom source protocol [17], controlled dummy adaptive distribution protocol [26], and the redundancy branch convergence-based privacy protocol [30]. To route packets, the probabilistic source location privacy protection protocol selects phantom nodes around the source node with careful consideration of the exposed areas. It also generates fake packet sources around the sink node. Real packets and fake packets are transmitted in the network simultaneously. The timed efficient privacy preservation protocol applies the timed data collection and universal re-encryption techniques to distribute real packets from the real source node and fake packets from fake packet sources. When a sensor node has upstream nodes, it periodically broadcasts data collection request to its upstream nodes. Every upstream node receives the request and returns an encryption text of real packet if it has real packets to send or an encryption text of fake packet if it does not have a

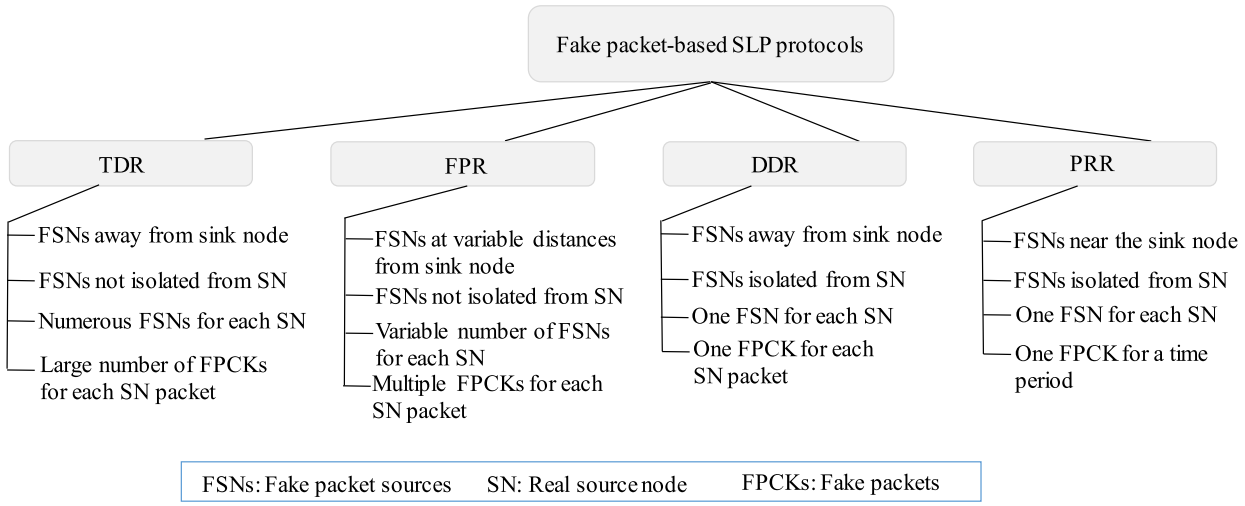


FIGURE 1. Features and routing strategies of the TDR, FPR, DDR, and PRR protocols.

real packet to send. After receiving the encryption text of the real packet, a sensor node re-encrypts and forwards the text to its downstream node. Subsequently, a filtering technique is applied at each sensor node to filter the fake packets from the upstream sensor nodes. The fake packets are filtered to ensure a controlled amount of fake packet traffic in the network.

In the bidirectional tree protocol, the end-to-end location privacy is protected by transmitting real packets along the shortest path from the source node to the sink node. To increase the complexity on the adversary tracing back attack, the protocol generates branch routes along the shortest path. Fake packets are transmitted along the branch routes. The direction of the fake packet transmission is from the leaf nodes to the stalk nodes to ensure the adversary is pulled away from the real packet routes. The dummy adaptive distribution protocol classifies the nodes in the network into fake nodes or real nodes. Nodes generate a random number and compare it to a threshold value which is equal to the transmission rate. Fake nodes generate fake packets if the random number is less than the threshold value. Once an event is detected, the detecting node becomes a real node and sends packets to the sink node. The transmission rate is designed to ensure the real nodes transmit at a higher rate than the fake nodes. In the operation of the distributed fake source and phantom source protocol, a source node floods a fake request packet into the network. Sensor nodes check their likelihood of becoming candidate fake sources based on the value of their residual energy and participation history. When a node is selected as a fake source, it starts sending fake packets to the sink node. Subsequently, the real source node selects a random phantom node. Then, the real source node sends packets to the sink node through the selected phantom node. The operation of the controlled dummy adaptive distribution protocol is based on the dummy adaptive distribution protocol explained above. To improve its performance, the controlled dummy adaptive distribution protocol guarantees that the real packets are transmitted at an increased transmission rate while reducing the transmission rate for the fake packets.

III. MOTIVATION AND PROBLEM STATEMENT

Many of the existing studies such as [4], [8], [11], [13], [14], [19], and [31] point out that fake packet-based routing protocols are capable of effectively protecting the SLP in monitoring networks. The studies also highlight some limitations of the protocols which result from the distribution of fake packet traffic in the network. The limitations include increased communication cost and network overhead. Also, the protocols incur unreliable packet delivery due to increased probability of packet collision and packet loss events. To mitigate the limitations while achieving high levels of SLP protection, the protocols employ unique features and strategies as described in section II.

Although many studies have analyzed the performance of the fake packet-based routing protocols, the evaluations are often not comprehensive. As a result, some factors are often overlooked. For example, the ability of the protocols to ensure effective SLP protection for prolonged periods of time or the ability of the protocols to provide reliable packet delivery under varied network conditions are often disregarded. It is therefore essential that comprehensive performance evaluation is conducted while considering various factors including the following. (1) The protocols are energy-inefficient with high probability of energy exhaustion in the sensor nodes. If large amounts of fake packets are broadcasted in a region of the WSN domain, sensor nodes may drain their energies at a fast rate and the SLP protection may become short-lived. (2) Broadcasting large amounts of fake packet traffic in the network may result in increased number of packet collision events to degrade the reliability of the protocols.

Thus, in this study, we conduct comprehensive performance evaluation of four representative fake packet-based protocols which employ different fake packet routing

strategies. We evaluate the performance of the tree-based diversionary routing protocol (TDR) [15], data dissemination routing protocol (DDR) [16], distributed protocol with fake source and phantom source routing (FPR) [17], and the probabilistic source location privacy protection protocol (PRR) [18]. The key features and routing strategies of the TDR, DDR, FPR, and PRR protocols are summarized in Fig. 1. To ensure comprehensive analysis, we investigate the performance of the protocols under varied network parameters and configurations. Performance is observed under varied sensor node residual energy, source-sink distance, network operation duration, network size, source packet rate, and node density. We include performance metrics such as safety period, capture ratio, detection ratio, energy consumption, network lifetime, end-to-end delay, and packet delivery ratio. Based on the observations from the investigations, we include some recommendations for improvements. For protocols with exhaustively high energy consumption, energy harvesting technologies are recommended to ensure effective long-term monitoring.

IV. MODELS

In this section, assumptions are highlighted and the network and adversary models are presented. The models are used for experimental analysis in the next section.

A. NETWORK MODEL

The network model similar to [7] is assumed. Sensor nodes are equipped with a wireless interface, limited resources and computational capabilities. All nodes are homogeneous and have the same communication range. The network is event-triggered. When a node senses an asset, it starts sending packets periodically to the sink node. Transmitted packets are encrypted and contain source node ID which only the sink node can infer as an asset location. Sensor nodes employ multi-hop communication for energy conservation. During the network deployment phase, the network initialization process is performed for localization of the sensor nodes.

B. ADVERSARY MODEL

The adversary model is adopted from [7]. Adversary is assumed to be equipped with spectrum analyzers and has sufficient resources such as adequate computation capabilities, memory, and unlimited power. The adversary is mobile, initially residing in the neighborhood of the sink node listening for arriving packets. The adversary is capable of localizing the immediate sender node when a packet is received at any node. That means, if a packet is received from a node which is located within the adversary detection range, the adversary will overhear the communication and move to the location of the immediate sender node. The back tracing attack on the packet routes is done by moving hop-by-hop towards the source node, until the adversary is co-located with the source node. The adversary is cautious. It has computational power to limit its waiting time at any immediate sender node. It also keeps a record of all the immediate sender nodes it has visited to avoid revisiting or getting trapped in a loop.

TABLE 1. Network simulation parameters.

Parameter	Value
Network area (m^2)	2000×2000
Number of nodes	2500
Sensor node communication range (m)	30
Adversary detection range (m)	30
Adversary waiting timer (source packets)	4
Adversary initial location	In the locality of the sink node
Target monitoring scheme	k-nearest neighbor tracking
Packet size (bit)	1024
Source rate (packet/second)	Varied between 1 and 6
Sensor node initial energy (J)	0.5

V. EXPERIMENTAL ANALYSIS

This section presents some investigations on the performance of the tree-based diversionary routing protocol (TDR), fake source with phantom source routing protocol (FPR), data dissemination protocol (DDR), and the probabilistic source location privacy protection protocol (PRR). For comparative analysis, the traditional random intermediate node routing protocol (RIN) is included in the analysis. The RIN protocol employs a simple routing algorithm which does not involve fake packet routing. When a source node has a packet to send to the sink node, the RIN protocol allows a random selection of an intermediate node which is located at a safe distance from the source node. Thereafter, the packet is sent to the sink node through the selected intermediate node [32].

A. SIMULATION ENVIRONMENT

MATLAB simulation tool was used to simulate a network of size 2000×2000 m^2, with 2500 randomly distributed sensor nodes. The sensor node communication range was set to 30 m to ensure multi-hop communications. Adversary detection range was set to 30 m, similar to the sensor node communication range to ensure the adversary performs hop-by-hop back tracing attack. The cautious adversary waiting timer was set to 4 source packets. Simulations were run for 500 iterations and average values were considered. The network simulation parameters are summarized in Table 1. The following performance metrics were used for analysis: safety period, capture ratio, detection ratio, energy consumption, network lifetime, end-to-end delay, and packet delivery ratio.

B. RESULTS AND DISCUSSIONS

The analysis results are discussed below. The safety period, capture ratio, and detection ratio metrics were used to measure the privacy performance of the protocols.

1) SAFETY PERIOD (SP)

Safety period is the time required for an adversary to perform back tracing attack and capture the monitored asset. It is used to measure the privacy performance of the protocols. Longer

safety periods provide stronger SLP protection [4], [15]. In this study, we measure the safety period by counting the number of hops during the adversary back tracing attack. To evaluate the SLP performance, equation (1) was assumed from [4], [15].

$$\max(SP) = \max(SLP_{Protection}) \quad (1)$$

Fig. 2 shows the privacy performance of the protocols. In the experiment scenarios for the results in Fig. 2 (a), the safety period was observed at various source-sink distances with a fixed source packet rate of 1 packet/second. It is shown in Fig. 2 (a) that the TDR, FPR and DDR protocols can achieve significantly longer safety period than the RIN protocol. In TDR, the long safety period is achieved by employing multiple routing strategies. The protocol employs phantom nodes which are located away from the source node. It creates long backbone routes which diverge to the network border regions. It generates diversionary routes as branches of the backbone routes and distributes large amounts of fake packet traffic in the diversionary routes. As a result, the protocol can effectively obfuscate the adversary and long safety period is achieved. Furthermore, the packet routes in TDR protocol are designed to ensure a back tracing adversary is encountered with multiple routes and multiple incoming packets, making it difficult for the adversary to predict the correct path to the real source node.

The FPR protocol distributes a considerable amount of fake packet traffic around the source node, simultaneously with the transmission of the real packets. As a result, the adversary is tackled with multiple packets and finds it difficult to identify the exact immediate sender node of the real packets. Therefore, the back tracing attack is made more complex and longer safety period is achieved. The results also show that the privacy performance of TDR and FPR improves when larger numbers of fake packet sources are employed in a region of the network. FPR employs a larger number of fake packet sources than TDR in the near-sink regions while TDR employs a larger number of fake packet sources than FPR in the near network border regions. Consequently, the FPR protocol achieves longer safety period than the TDR in the near-sink regions and TDR achieves longer safety period in the network border regions.

To analyze the performance of the DDR protocol, all the sensor nodes with source-sink distance less or equal to 20 hops were assumed to be located inside the blast ring. The DDR protocol is capable of achieving longer safety period than the TDR protocol inside the blast ring regions because it employs a probabilistic flooding mechanism. When the flooding mechanism is employed, multiple random nodes are selected to broadcast each packet. Thus, a packet may arrive at the sink node using multiple random routing paths. Furthermore, packets from a source node appear to arrive at the sink node from all possible angles. As a result, the tracing back attack becomes a complex and time consuming task. Moreover, the cautious adversary is restricted from revisiting the immediate sender nodes. To some extent, the restriction

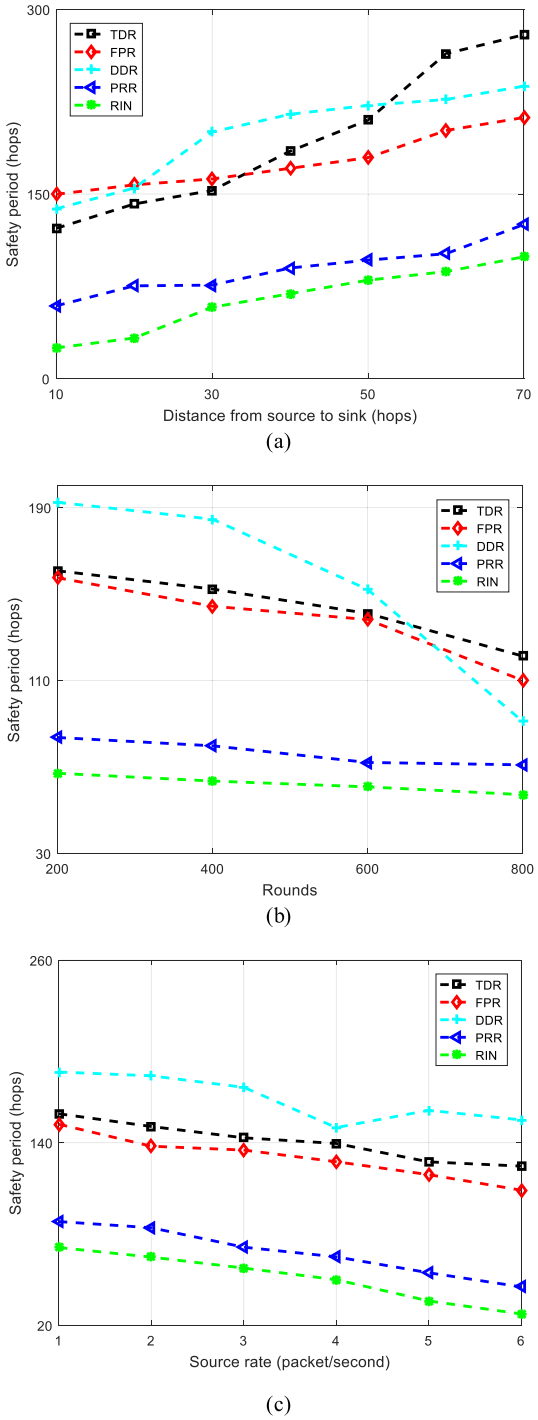


FIGURE 2. Privacy performance of the routing protocols. (a) Safety period against source-sink distance. (b) Safety period against rounds. (c) Safety period against source rate.

increases the complexity of the adversary back tracing attack when the flooding mechanism is used. It was also observed that the FPR protocol achieves slightly longer safety period than DDR, inside the blast ring. The main reason is that, in some scenarios, the fake packet sources in the FPR protocol were able to pull the adversary to a location further away from the real source nodes to prolong the safety period.

Outside the blast ring, the DDR achieves significantly longer safety period than the TDR and FPR protocols because the progress of the adversary back tracing attack is significantly hindered near the sink node regions. When source nodes are located outside the blast ring, the DDR creates two isolated routing paths. One path is used to route packets from the fake source node and the other path routes packets from the real source node. Both routes create a pull effect on the eavesdropping adversary. Furthermore, both real packets and fake packets are flooded inside the blast ring to prolong the safety period. However, for source nodes with source-sink distance greater than 52 hops, the TDR protocol achieves longer safety period than the other protocols. The main reason for the longer safety period is that, in that region, TDR broadcasts a considerable amount of fake packet traffic to pull the adversary away from the real source node. Also, TDR broadcasts fake packet traffic near the phantom node to increase the adversary obfuscation effect at the phantom node. On the other hand, DDR isolates the fake packets from the phantom node. Consequently, in DDR, the adversary has a higher probability of capturing the source node in a short time if it successfully captures the phantom node.

The PRR protocol employs only one fake packet source at a time for each real source node. As a result, the obfuscation effect on the adversary is reduced and the safety period is only slightly longer than RIN. Furthermore, in PRR, the fake packet sources are located near the sink node, making the fake packet routes short and easy to predict by the adversary. After sometime of back tracing, the adversary can easily identify the fake packet sources and isolate the fake packet routes. If the fake packet routes are obvious, the adversary can focus the attack on the real packet routes and increase the probability of success in the back tracing attack. Consequently, the safety period is reduced. Moreover, in the PRR protocol, the fake packet sources are isolated from the real packet sources. These noticeable locations may make it easy for the adversary to predict the real packet routes and make the adversary back tracing attack a less complex task. As a result, the safety period is reduced.

In the RIN protocol, packets are routed from the source node to the sink node through a randomly selected intermediate node. However, packet routing between the intermediate nodes and sink node is done through less random routing paths. Consequently, the RIN protocol achieves significantly short safety period because it becomes easy for the adversary to back trace the less random routing paths. Furthermore, when the source node is near the sink node, there is a high probability of the selected intermediate node to be located near the sink node. If the intermediate node is located near the sink node, short routing paths are created. The short routing paths are less effective at obfuscating the adversary. Therefore, short safety period is achieved. For all the protocols, the safety period improves with the increase in source-sink distance because the adversary back tracing attack becomes more complex with longer routing paths. When the source node is located at a long distance from the sink node, the routing paths can be created with high path diversity and it becomes more challenging for the adversary to successively perform back tracing attacks. Hence, long safety period is achieved.

To evaluate the capability of the protocols to provide effective SLP protection for prolonged operational times, the safety period of the protocols was observed at different network operation durations. Analysis was done for source nodes at source-sink distance of 35 hops. The results are shown in Fig. 2 (b). The results show that the safety period of the PRR, and RIN protocols does not vary very much throughout the 800 rounds. For TDR, FPR and DDR, the protocols achieve reduced safety period when the number of rounds increases. The main reason for the reduced safety period in TDR is that, TDR relies on obfuscating the adversary by broadcasting a large amount of fake packet traffic in the diversionary routes. When the network has operated for many rounds, some of the sensor nodes drain their energies and become dead nodes. Therefore, the number of active sensor nodes in the regions of the diversionary routes is reduced and small number of fake packets is broadcasted. Subsequently, the adversary becomes less obfuscated and the safety period is reduced. The main reason for the reduced safety period in FPR is that, the number of candidate fake packet sources is highly dependent on the value of the sensor node residual energy. For a sensor node to become a candidate fake packet source, one of the criteria is that the value of the sensor node residual energy must be greater than a threshold value. In our analysis, a threshold value of 0.25 J was assumed. At 800 rounds, the residual energy of some of the sensor nodes was less than the threshold value. As a result, small numbers of fake packet sources were generated. Subsequently, the amount of fake packet traffic was reduced, the adversary became less obfuscated, and the safety period was reduced.

For DDR, the protocol depends highly on flooding mechanism to obfuscate the adversary. When the source nodes are outside the blast ring, DDR ensures both real packets and fake packets are flooded inside the blast ring. As a result, a significant amount of sensor nodes energy is consumed to transmit a single packet. Consequently, the sensor nodes drain their energies at a fast rate. At 800 rounds, a significant number of sensor nodes inside the blast ring have exhausted their battery power. Therefore, a reduced number of sensor nodes can participate in the flooding mechanism. Hence, the adversary becomes less obfuscated and the safety period is reduced. The safety period of the PRR protocol does not vary very much during the 800 rounds because PRR broadcasts one fake packet for a time period. Therefore, the sensor nodes drain their energies at a slow rate. Hence, a great number of sensor nodes take part to route packets and obfuscate the adversary for prolonged periods of time. Similar to PRR, the safety period of the RIN protocol does not vary during the 800 rounds because the routing strategy of RIN ensures that the sensor nodes drain their energies at a slow rate. Therefore, sensor nodes can participate to route packets and

obfuscate the adversary for prolonged periods of time. However, the safety period of RIN is significantly short.

In the experiment scenarios for the results in Fig. 2 (c), the safety period was observed under varied source rate. The source rate was varied between 1 and 6 packet/second. The source nodes were randomly positioned at source-sink distance of 35 hops. It is shown in Fig. 2 (c) that all the protocols achieve reduced safety period as the source rate increases. The main reason for the reduced safety period is that, as more packets are generated in the network, the packet traffic is increased and the probability that the adversary captures successive packets is also increased. At higher data rates, the cautious adversary is capable of capturing enough number of successive packets to allow it to make a successful back tracing attack within a short period of time. For DDR protocol, it was observed that the safety period was significantly reduced when the adversary was able to locate the initial blast ring node which received packets from the phantom node. In Fig. 2 (c), such scenario was observed at the source rate of 4 packet/second. The main reason for the sharp reduction in safety period once the initial blast ring node was located is that, the routing paths for the real packets and fake packets are isolated. Therefore, DDR does not distribute fake packets near the phantom nodes. Consequently, the adversary obfuscation effect between the phantom nodes and source nodes is reduced. Thus, it becomes easy for the adversary to successfully locate the source nodes and the safety period is reduced. For RIN protocol, at high data rates, the adversary is capable of locating the source nodes within a significantly short period of time due to the easily predictable routing paths.

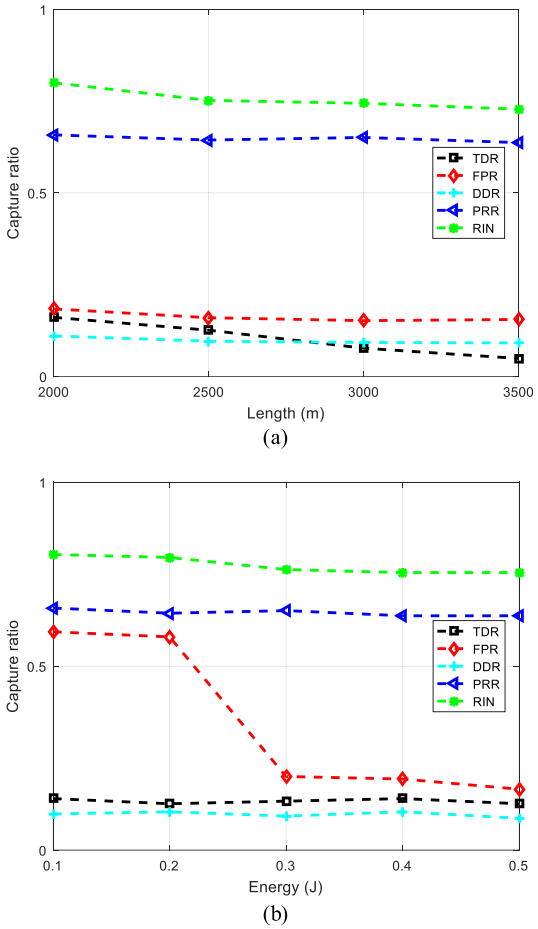


FIGURE 3. Privacy performance of the protocols. (a) Capture ratio against network size. (b) Capture ratio against energy of sensor node.

2) CAPTURE RATIO (CR)

Capture ratio is the ratio between the number of experiments where the adversary ends in locating the source node and the total number of experiments. To locate the source node, an adversary must back trace the packet routes and reach at the location of the source node. That means, the adversary must co-locate with the source node. To compute the CR, equation (2) was assumed [33].

$$CR = \frac{Number\ of\ experiment\ sending\ with\ located\ source}{Total\ number\ of\ experiments} \tag{2}$$

The capture ratio and safety period parameters have an inversely proportional relationship. When the SP of a protocol is maximized, the CR is minimized, as shown in equation (3).

$$\max\,(SP) = min\,(CR) \tag{3}$$

Fig. 3 shows the privacy performance of the protocols using the capture ratio metric. In the experiment scenarios for the results in Fig. 3 (a), CR was observed against varied network size. The parameter ''Length'' represents the side length of the network. The source nodes were randomly positioned at a source-sink distance of 40 hops. The results show that the CR for DDR, PRR, FPR, and RIN does not vary very much when the network size is varied. The main reason is that, if the source-sink distance is fixed, the change in network size causes insignificant effect on the location configuration of the fake packet sources in PRR and FPR or intermediate nodes in RIN. Therefore, the configurations of the routing paths remain the same and the CR does not vary significantly. For DDR, when the radius of the blast ring is kept constant, the change in the network size causes insignificant effect on the packet routing algorithm and the CR remains unchanged. However, for TDR, the increase in network size causes a reduction in CR. This is mainly due to the fact that, TDR locates the fake packet sources in the diversionary routes, towards the network border regions. If the intermediate node is kept at a constant location in the network, the length of the diversionary routes increases with the increase in network size. As a result, the ability of the protocol to obfuscation the adversary is increased. When the adversary is tricked into tracing back the fake packets which are transmitted in the long diversionary routes, it is steered far away from the real source node and the CR is reduced.

In the experiment scenarios for the results in Fig. 3 (b), CR was observed against the residual energy of the sensor

nodes. For analysis, we observed the residual energy of 90% of the sensor nodes which were located within 6 hops from the source nodes. The source nodes were located at source-sink distance of 40 hops. The results in Fig. 3 (b) show that, the CR for the TDR, DDR, PRR, and RIN protocols does not vary very much when the residual energy of the sensor nodes is varied. However, for the FPR protocol, the CR was high when the residual energy of the sensor nodes was below the threshold value of 0.25 J. The reason for the increased CR below 0.25 J is that, FPR uses the residual energy as one of the criteria for the selection of candidate fake packet sources. When the residual energy of some of the sensor nodes was below the threshold value, smaller numbers of fake packet sources were selected. Consequently, reduced amounts of fake packet traffic were broadcasted and the adversary was less obfuscated. Hence, the adversary was able to improve its attack success rate and high CR was achieved. When the residual energy of the sensor nodes was above the threshold value of 0.25 J, increased numbers of sensor nodes were able to meet the conditions for becoming candidate fake packet sources. Subsequently, large amounts of fake packet traffic were broadcasted in the network. As a result, the adversary became effectively obfuscated and the CR was reduced.

3) DETECTION RATIO (DR)

Detection ratio is the ratio between the number of packets detected by the adversary and the total number of packets sent by the source node during the back tracing attack. To compute the DR, equation (4) was assumed.

At all times, the adversary uses its spectrum analyzer to eavesdrop on the communication and detect the packets which are transmitted between the sensor nodes. Since the adversary detection range is assumed to be equal to the sensor node communication range, a packet is detected when it is received from an immediate sender node which is located 1 hop away from the adversary location.

$$DR = \frac{Number\ of\ detected\ packets}{Total\ number\ of\ packets\ sent\ by\ source\ node} \quad (4)$$

To successfully locate the real source nodes, the adversary must detect a sufficient number of successive packets from the source nodes and make significant progress in the back tracing attack. However, when the routing paths have high path diversity, the number of detected packets is significantly reduced. Consequently, the DR is reduced and safety period is increased. Therefore, minimum DR corresponds to maximum SP as shown in equation (5). Thus, when the DR is close to 0, the safety period is prolonged and the level of SLP protection is improved. However, when the DR is close to 1, the safety period is minimized and the level of SLP protection is reduced.

$$\min(DR) = \max(SP) \quad (5)$$

Fig. 4 shows the privacy performance of the protocols using the detection ratio metric. In the experiment scenarios for the results in Fig. 4 (a), DR was computed for source nodes at different source-sink distances. 400 packets were sent from each source node. The source rate was fixed at 1 packet/second. The results show that the DR for the TDR, FPR, PRR and RIN protocols tend to decrease when the source-sink distance is increased. The main reason for the decrease in DR is that, the routing paths become more diverse when the distance between the source nodes and sink node increases. As a result, the routing paths become more obfuscating to the adversary and the DR is reduced. The results also show that FPR achieves lower DR than TDR when the source-sink distance is below 34 hops. This is mainly due to the fact that FPR employs larger amounts of fake packet traffic in the near-sink regions to achieve higher levels of adversary obfuscation and lower DR.

To analyze the DR of the DDR protocol, all source nodes with source-sink distance less or equal to 30 hops were assumed to be located inside the blast ring. It is shown in Fig. 4 (a) that the adversary was able to achieve high DR when the source nodes were located inside the blast ring. This is mainly due to the flooding of the packets inside the blast ring. When the adversary is initially located at the sink node, it is capable of detecting a significant number of packets from the source nodes to increase its DR. For the source nodes outside the blast ring, the DR is significantly reduced. The main reason for the reduced DR is that, outside the blast ring, the DDR protocol creates two isolated routing paths. One path is used to route packets from the fake source node and the other path routes packets from the real source node. Furthermore, both fake packets and real packets are flooded when they arrive inside the blast ring. As a result, the fake packets and real packets are transmitted to the sink node with equal probability. Therefore, the eavesdropping adversary has a reduced chance of detecting the real packets and the DR is reduced. Unlike the TDR and FPR protocols, the DDR protocol can achieve long SP despite the high DR. The main reason for the high DR and long SP is that, the adversary is flooded with many packets from multiple immediate sender nodes. Given that probabilistic flooding is used, the adversary is encountered with a complex back tracing task and long SP is achieved. Hence, the obfuscation ability of the DDR protocol is high despite the high DR.

In the experiment scenarios for the results in Fig. 4 (b), DR was computed under varied node density. The source nodes were assumed at source-sink distance of 40 hops. The number of sensor nodes in the network was varied between 2500 and 4000. The source rate was fixed at 1 packet/second. The results show that, at source-sink distance of 40 hops, the DR for the TDR, DDR, PRR and RIN protocols does not vary very much when the number of sensor nodes in the network is increased. However, the DR for the FPR protocol tends to decrease when the number of nodes is increased. The main reason for the reduced DR is that, FPR randomly selects candidate fake packet sources from the neighborhood regions of the source node. When the number of sensor nodes increases, it increases the probability of a higher number of candidate fake packet sources. When a large number of fake

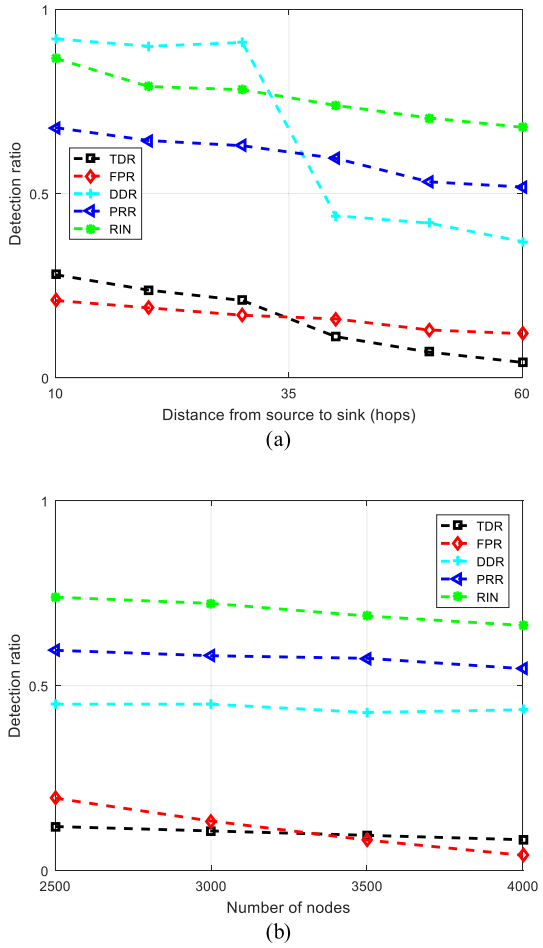


FIGURE 4. Privacy performance of the protocols. (a) Detection ratio against source-sink distance. (b) Detection ratio against node density.

packet sources is selected, large amounts of fake packet traffic can be broadcasted to obfuscate the adversary. Consequently, the DR is reduced. For the DDR protocol, when the number of nodes is increased, the DR remains unchanged because both fake packets and real packets are flooded with equal probability.

4) ENERGY CONSUMPTION

Energy consumption is the energy consumed by the sensor nodes for transmitting and receiving packets. Packet transmission and reception are the most energy consuming tasks for the sensor nodes [34]. Thus, the energy consumption or energy efficiency of a protocol may be indicated by the number of packets which are being transmitted in the network [35]. Therefore, the fake packet-based protocols are prone to low energy efficiency because they transmit large amounts of packet traffic.

Equations (6) and (7) were used to compute the energy consumption of the sensor nodes. The energy consumption model was adopted from [15], [34]. To transmit an l-bit packet to a transmission distance D, transmission energy, E_{trans}, and receive energy, E_{rec}, follow equations (6) and (7), respectively. The model assumes that the energy consumption for packet transmission is an exponential function of d. E_{loss} is the transmitting circuit loss. The model uses both, the free space (D^2 power loss) and the multi-path fading (d^4 power loss) channel models. If the transmission distance is less than the threshold distance d_0, the power amplifier loss is based on the free-space model. Otherwise, if the transmission distance is equal or greater than the threshold d_0, the multi-path attenuation model is used. The threshold distance, d_0, is computed according to equation (8). E_{fs} and E_{amp} are the energies required by power amplification in the two power loss models. Table 2 shows the energy consumption model parameters [15], [34].

$$E_{trans} = \begin{cases} lE_{loss} + lE_{fs}d^2, & if\ d < d_0 \\ lE_{loss} + lE_{amp}d^4, & otherwise \end{cases} \tag{6}$$

$$E_{rec} = lE_{loss} \tag{7}$$

$$d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}} \tag{8}$$

Fig. 5 shows the energy consumption performance of the protocols. In the experiment scenarios for the results in Fig. 5 (a), 25 source nodes were assumed at different source-sink distances. 1000 packets were sent from each source node to the sink node and the energy consumption per sensor node was computed. For the DDR protocol, the boundary of the blast ring was assumed at 400 m from the sink node. The results in Fig. 5 (a) show that the TDR protocol has the highest energy consumption near the network border regions while the DDR protocol has the highest energy consumption in the near-sink regions. Also, the FPR incurs significantly high energy consumption. The main reason for such kind of distribution in the energy consumption is that, the TDR broadcasts large amounts of fake packet traffic in the diversionary routes, towards the network border. In the near-sink regions, TDR employs a backbone route to route real packets. It does not broadcast any fake packets in the near-sink regions. On the other hand, the DDR protocol employs packet flooding mechanism in the near-sink regions which causes significantly high energy consumption. Moreover, both real packets and fake packets are flooded when the source nodes are located outside the blast ring. Outside the blast ring region, the energy consumption of DDR is significantly reduced because the protocol employs only one fake packet for each real packet.

The FPR protocol distributes a significant amount of fake packet traffic throughout the network domain, depending on the location of the source node. The fake packets are routed towards the sink node. Hence, higher energy consumption in the near-sink regions. The PRR protocol employs one fake packet source for a period of time. As a result, it broadcasts significantly lower amounts of packet traffic than the FPR. Furthermore, the fake packets are broadcasted in the near-sink regions. Hence, PRR incurs considerably lower energy consumption than FPR. The RIN protocol has the lowest energy consumption because it does not involve the transmission of fake packet traffic. Only real packets are transmitted between

TABLE 2. Energy consumption model parameters.

Parameter	Description	Value
E_{loss} (nJ/bit)	Transmitting circuit energy loss	50
E_{amp} (pJ/bit/m^4)	Energy for power amplification in the free-space model	0.0013
E_{fs} (pJ/bit/m^2)	Energy for power amplification in the multi-path attenuation model	10
d_o (m)	Threshold distance for the channel models	87
l (bit)	Size of the packets	1024

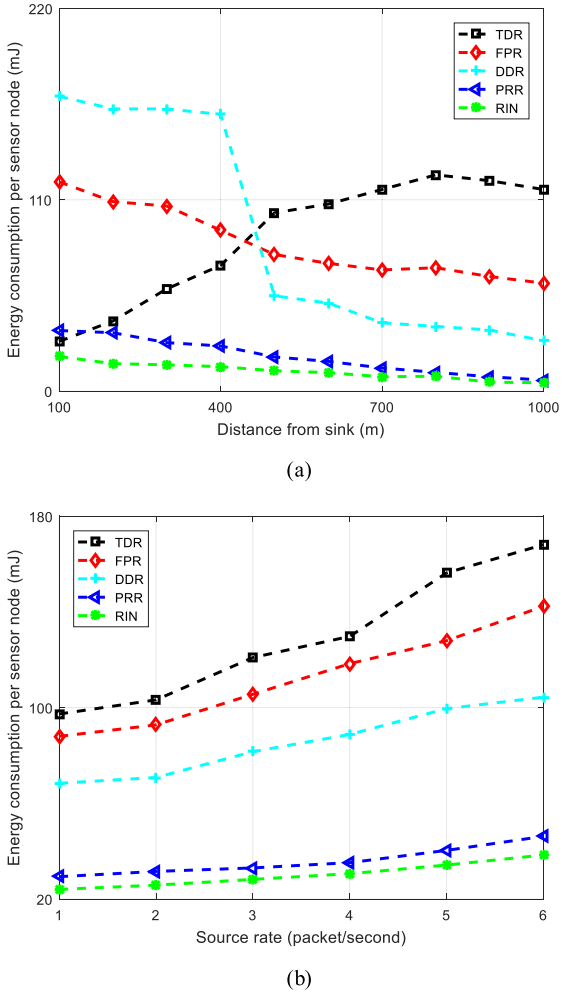


FIGURE 5. Energy consumption of the protocols. (a) Energy consumption against source-sink distance. (b) Energy consumption against source rate.

the sensor nodes. As a result, the sensor nodes consume less energy. Comparing the results in Fig. 2 (a) and Fig. 5 (a), it is shown that the ability of the TDR and FPR protocols to achieve strong SLP protection is highly influenced by the amount of fake packet traffic. As a result, the energy cost of TDR and FPR protocols is high.

In the experiment scenarios for the results in Fig. 5 (b), energy consumption per sensor node was observed for sensor nodes located at 500 m from the sink node. The energy consumption was measured against varied source rate. The source rate was varied between 1 and 6 packet/second. The results in Fig. 5 (b) show that the energy consumption of the protocols tend to increase when the source rate is increased. The main reason for the increase in the energy consumption is that, when more packets are generated per second, the packet traffic in the network is increased. As a result, the sensor nodes spend more energy to transmit the packets in the network. For the TDR and FPR protocols, the energy consumption increases at a fast rate because of the presence of large amounts of fake packet traffic in the network. With the large amounts of fake packet traffic, the number of packet collision and packet retransmission events is increased. Consequently, the energy consumption is increased. In DDR, packet collision and packet retransmission events occur due to the flooding of real packets and fake packets. Subsequently, the energy consumption of DDR increases at a faster rate than in PRR and RIN protocols. The energy consumption for the PRR and RIN protocols increases at a slow rate. This is due to the fact that, at 500 m from the sink node, PRR and RIN employ routing strategies with smaller amounts of packet traffic than in the TDR and FPR protocols. Therefore, fewer events of packet retransmission occur and the sensor nodes spend less energy.

5) NETWORK LIFETIME

To investigate the network lifetime performance, we adopt the network lifetime model from [15]. The model assumes that there is no direct relationship between the network lifetime and the total energy consumption of the network. However, there is a direct relationship between the network lifetime and the total energy consumption of the sensor nodes in the near-sink regions. The main reason for the assumption is that, the sensor nodes in the near-sink regions forward their own packets and act as relay nodes for the sensor nodes which are located away from the sink node. As a result, the sensor nodes incur exhaustive energy consumption [3], [34]. A phenomenon called energy hole can happen when the sensor nodes in the near-sink regions exhaust their energies. Subsequently, a ring of dead nodes may form around the sink node and the network lifetime may be affected. Therefore, the network lifetime is maximized when the energy consumption of the sensor node with maximum energy consumption is minimized, as shown in equation (9) from [15], [30]. In the equation, NL is the network lifetime and NE_i is the energy

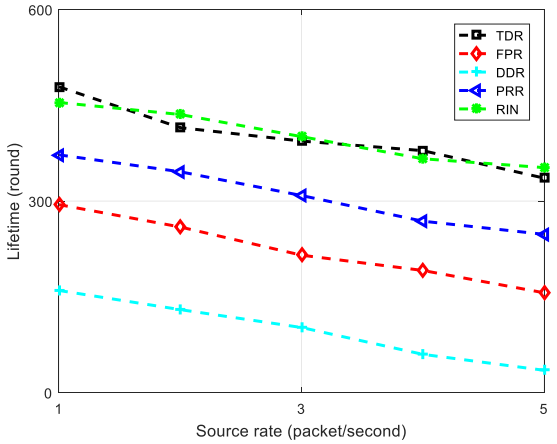


FIGURE 6. Network lifetime of the protocols under varied source rate.

consumption of node i.

$$\max(NL) = \min_{0<i\leq k} \max (NE_i) \tag{9}$$

Based on the model, we define the network lifetime as the period between the start of the network operation and the first sensor node power outage.

To analyze the network lifetime of the protocols, all the sensor nodes with source-sink distance less or equal to 20 hops were assumed to be located in the near-sink region. The source nodes were randomly distributed at various source-sink distances. 2000 packets were sent from each source node. The network lifetime was observed under varied source rate. Fig. 6 shows the results of the network lifetime analysis. It shows that the TDR and RIN protocols achieve long network lifetime. Also, it is shown that the TDR and RIN protocols have comparable network lifetime performance. The TDR achieves long network lifetime because it employs shortest routing paths in the near-sink regions. Furthermore, TDR broadcasts small amounts of packet traffic in the near-sink regions to minimize the sensor node energy consumption. RIN protocol achieves long network lifetime because it employs relatively short routing paths between the intermediate nodes and sink node. Similar to TDR, the RIN protocol distributes relatively small amounts of packet traffic in the near-sink regions to minimize the sensor node energy consumption.

The FPR and PRR protocols employ both, real packets and fake packets in the near-sink regions. Hence, more energy is consumed by the sensor nodes and the network lifetime is reduced. Moreover, the FPR employs larger amounts of fake packet traffic than the PRR. Consequently, the FPR achieves reduced network lifetime. The DDR achieves significantly short network lifetime because it employs packet flooding mechanism to route fake packets and real packets in the near-sink regions. When packet flooding is used, a large number of sensor nodes participate in transmitting each packet. As a result, the sensor nodes drain their energies at a fast rate and the network lifetime is affected.

The results also show that the network lifetime of the protocols tend to decrease when the source rate is increased. The main reason for the reduced network lifetime at higher source rates is that, more packet traffic is broadcasted in the network per unit time when the source rate is high. Therefore, the sensor nodes consume more energy per unit time and the network lifetime is reduced.

6) PACKET DELIVERY RATIO (PDR)

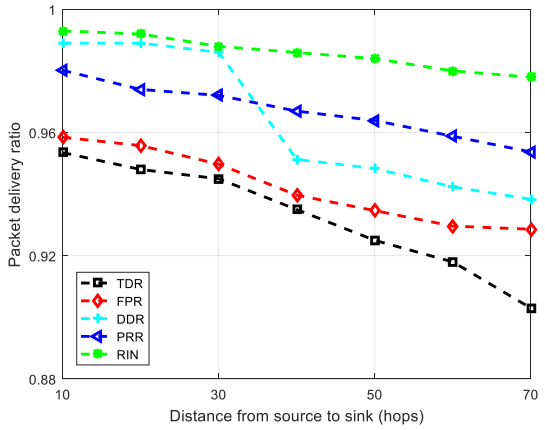
Packet delivery ratio is the ratio between the total number of packets successfully delivered at the destination sink node and the number of packets transmitted by the source nodes. Equation (10) was used to compute the PDR [4]. In the equation, P_{Rec} is the total number of data packets successfully received by the destination sink node. P_{Trans} is the number of packets transmitted by the source nodes. n is the number of source nodes.

$$PDR = \frac{P_{Rec}}{\sum_{i=1}^{n} P_{Trans_i}} \tag{10}$$

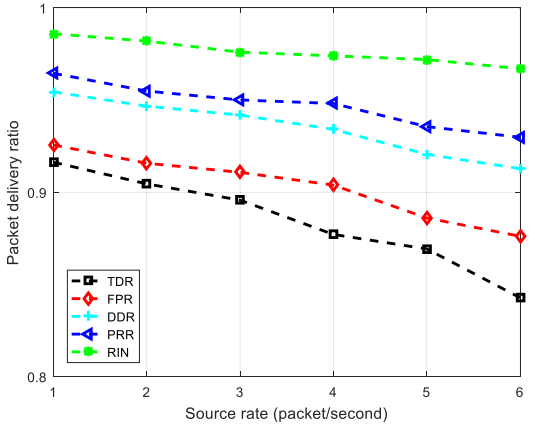
Fig. 7 shows the PDR performance of the protocols. In the experiment scenarios for the results in Fig. 7 (a), 20 source nodes were assumed at various source-sink distances. Each source node transmitted 100 packets to the sink node. The source packets were generated at a rate of 1 packet/second. The results in Fig. 7 (a) show that the PDR of the protocols tends to decrease when the source-sink distance is increased. The main reason for the reduced PDR is that, the routing paths become longer when the source-sink distance is increased. As a result, the probability of packet loss events increases and the PDR is reduced. The TDR and FPR protocols achieve significantly low PDR for source nodes which are located at long distances from the sink node due to the distribution of large amounts of fake packet traffic. The probability of packet collision and packet loss events increases when large amounts of fake packet traffic is distributed in the network.

The PRR protocol achieves higher PDR than the TDR and FPR protocols because it broadcasts only one fake packet for each real packet transmission. Furthermore, the fake packet sources in PRR are isolated from the real source nodes. As a result, less packet collision and packet loss events occur. To analyze the PDR of the DDR protocol, the boundary of the blast ring was configured at source-sink distance of 30 hops. The results show that the DDR protocol is capable of achieving high PDR inside the blast ring due to packet flooding. However, the PDR is reduced when the source nodes are located outside the blast ring. The reduced PDR is mainly due to the increased probability of packet collision events which occur when both real and fake packets are flooded inside the blast ring. The RIN protocol achieves significantly high PDR because it incurs reduced number of packet loss events.

In the experiment scenarios for the results in Fig. 7 (b), the PDR performance was observed for the source nodes located at source-sink distance of 35 hops. The source rate was varied between 1 and 6 packet/second. The results show that the PDR tends to decrease when the source rate is increased. The reduction in PDR is due to the fact that more packets are generated in the network when the source rate is high.



(a)



(b)

FIGURE 7. Packet delivery ratio (PDR) of the routing protocols. (a) PDR against varied source-sink distance. (b) PDR against varied source rate.

Consequently, the probability of packet collision and packet loss events is increased and the PDR is reduced. The PDR of the TDR and FPR protocols decreases at a fast rate due to the high probability of packet collision events. For DDR, at source-sink distance of 35 hops, the fake packets and real packets have equal probability of transmission through packet flooding. Therefore, the probability of packet collision is high and the PDR is reduced. The PRR protocol has a low probability of packet collision events. As a result, the PDR decreases at a slower rate than in TDR and FPR protocols. The PDR of the RIN protocol decreases at a much slower rate than in TDR and FPR because RIN employs less random routing paths with small amounts of packet traffic. As a result, the increase in packet rates causes less impact on the PDR performance.

7) END-TO-END DELAY (EED)

End-to-end delay is the time taken for a packet to be transmitted across the network from a source node to the destination sink node. Equation (11) was used to compute the EED [4]. T_{Rec} is the time when a data packet is received by the sink node. T_{Trans} is the time when a data packet is transmitted by a source node. P_{Rec} is the total number of data packets received at the destination sink node.

$$EED = \frac{\sum_{i=1}^{P_{Rec_i}} (T_{Rec_i} - T_{Trans_i})}{P_{Rec}} \tag{11}$$

Fig. 8 shows the EED performance of the protocols. In the experiment scenarios for the results in Fig. 8 (a), 20 source nodes were assumed at various source-sink distances. Each source node transmitted 100 packets to the sink node. The source packets were generated at a rate of 1 packet/second. It is shown in the Fig. 8 (a) that the EED tends to increase when the source-sink distance is increased. This is mainly due to the fact that increased number of packet forwarding instances (hops) occur when the distance between the source node and sink node is long. Some EED is incurred at each hop. Consequently, the EED increases with the increase in hop distance. The EED for TDR and FPR is relatively long because of the occurrence of packet collision events. When many packet collision and packet loss events occur, the instances of packet retransmission events increaese. Subsequently, the EED is increased. The DDR and PRR protocols employ small amounts of fake packet traffic to ensure fewer events of packet collision and retransmission. As a result, the EED is not significantly long. The PRR achives slightly shorter EED than DDR because it isolates the fake packet routes from the real packet routes to reduce the packet collison events and improve the EED. The routing paths of the RIN protocol are less random. Moreover, the RIN protocol transmits only real packets to ensure reduced number packet loss and retransmission events. Hence, relatively short EED is achieved by the RIN protocol.

In the experiment scenarios for the results in Fig. 8 (b), the EED performance was observed for source nodes with source-sink distance of 40 hops. The source rate was varied between 1 and 6 packet/second. It is shown in Fig. 8 (b) that the EED tends to increase when the source rate is increased. This is due to the fact that the probability of packet collision, packet loss, and packet retransmission events is increased when more packets are generated per second. The EED is significantly affected when many packet retransmission events occur. The EED of TDR and FPR protocols increases at a fast rate due to the presence of large amounts of fake packet traffic. The large amounts of fake packet traffic triggers increased number of packet collision events. Hence, increased number packet retransmission events occur when the source rate is high.

VI. DISCUSSIONS

Table 3 provides a summary of the findings from the performance analysis. The SLP protection, energy consumption, and network lifetime performance are summarized. Packet delivery reliability is included in the summary. The packet delivery reliability is measured by the PDR. High PDR corresponds to high delivery reliability while low PDR corresponds to low reliability.

Comparing the performance of the TDR, DDR, PRR and FPR protocols with the performance of the traditional RIN

TABLE 3. Summary of the results.

Protocol	SLP Protection	Energy Consumption	Network Lifetime	Delivery Reliability
TDR [15]	Significantly higher than RIN in near network border regions due to distribution of large amount of fake packet traffic in diversionary routes.	Significantly higher than RIN due to distribution of large amount of fake packet traffic in diversionary routes.	Comparable with RIN due to minimized energy consumption in the near-sink regions.	Significantly lower than RIN due to packet collision events.
DDR [16]	Significantly higher than RIN due to flooding of fake and real packets inside the blast ring.	Significantly higher than RIN due to packet flooding inside the blast ring.	Significantly shorter than RIN due to flooding of fake and real packets inside the blast ring.	Lower than RIN due to packet collision events when source node is outside of the blast ring.
FPR [17]	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Shorter than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly lower than RIN due to packet collision events.
PRR [18]	Slightly higher than RIN due to distribution of small amount of fake packet traffic.	Slightly higher than RIN due to distribution of fake packet traffic in the near-sink regions.	Shorter than RIN due to distribution of fake packet traffic in the near-sink regions.	Slightly lower than RIN due to packet collision events.
RIN [20]	Low.	Low.	Long.	High.

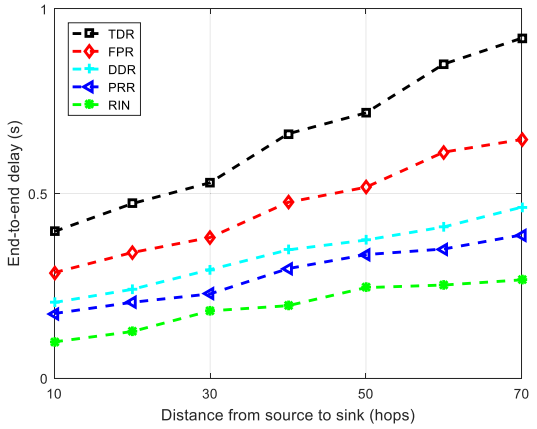


FIGURE 8. End-to-end delay (EED) of the routing protocols. (a) EED under varied source-sink distance. (b) EED under varied source rate.

protocol, it is presented in the Table 3 that the TDR, DDR, PRR and FPR protocols achieve improved SLP protection. However, the protocols incur costs in energy consumption, network lifetime, and delivery reliability. The TDR protocol shows some interesting performance features for energy consumption and network lifetime. The protocol is capable of achieving long network lifetime despite the high energy cost. It guarantees long network lifetime by consuming most of the energy in the near network border regions. In the near-sink regions, it employs short routing paths to minimize the energy consumption. Minimizing the energy consumption in the near-sink regions is particularly useful in improving the network lifetime. On the other hand, the DDR protocol disregards the idea of minimizing the energy consumption in the near-sink regions. As a result, the network lifetime of DDR is shortened. Another interesting observation was made from the performance analysis of the TDR, FPR, and DDR protocols. It was observed that, although the TDR, FPR, and DDR protocols can guarantee effective SLP protection, the privacy protection may be brief.

Based on the analysis results and observations, we present some recommendations to address the limitations of the protocols. To minimize the communication cost while achieving high levels of adversary obfuscation, the DDR, TDR, PRR, and FPR protocols can integrate node offset angle routing strategies in their routing algorithms. The effectiveness of the node offset angle routing algorithms was demonstrated in [4], [34], and [36]. To improve the privacy performance of the PRR protocol, the real packet routes and fake packet routes must be homogenous. When the routes are homogenous, the adversary becomes more obfuscated and high levels of SLP protection can be achieved. Furthermore, a more strategic location of the fake packet sources is required in the PRR protocol. Currently, the fake packet sources are isolated from both, real source nodes and phantom nodes. To improve the privacy performance, the location of the fake packet sources must provide some adversary obfuscation effect near the phantom nodes. On the other hand, the TDR protocol does not isolate the fake packet sources from the phantom nodes. As a result, TDR is capable of providing effective adversary obfuscation even when the phantom node has been captured by the adversary. Some of the existing studies have presented a few techniques which may be useful in addressing the limitations of the protocols. The DDR and FPR protocols can adopt the routing techniques in [30], [37] to address the

limitation of exhaustively high energy consumption in the near-sink regions. Also, some of the limitations of the TDR and PRR protocols were recently addressed in [4].

The performance of the FPR protocol can also be improved by improving the algorithm for selecting candidate fake packet sources. Currently, a simple technique is used where the sensor node residual energy is used as one of the criteria for selecting the candidate fake packet sources. The technique is not very effective since it results in reduced performance when the residual energy of the sensor nodes is below a threshold value. Instead, a criterion such as hop count can be used. As an example, together with the other criteria, a sensor node may become a candidate fake source depending on the value of its hop count to the sink node. If a sensor node meets the other criteria and has longer hop distance to the sink node than the source node itself, it becomes a candidate fake source, otherwise it ignores the fake source request. In such scenarios, the selection of the candidate fake sources becomes less dependent on the sensor node energy. Subsequently, effective number of fake packet sources may be guaranteed for longer durations. An improved algorithm for selecting candidate fake packet sources was proposed in [23]. The performance of FPR protocol can also be improved by using energy harvesting wireless sensor networks (EHWSNs) schemes. Using the techniques discussed in [3], EHWSNs may be utilized to improve the availability of effective candidate fake packet sources by ensuring the residual energy of the sensor nodes is maintained above the threshold values.

The TDR, DDR, and FPR protocols incur considerably high energy consumption. Consequently, the privacy protection of the protocols is short-lived. Therefore, TDR, DDR, and FPR protocols may not be practical in monitoring systems which require effective SLP protection for prolonged time periods. Thus, to enable long-term monitoring, the TDR, DDR, and FPR protocols may require additional network and hardware configurations to manage the energy of the sensor nodes. The work in [3], [6], [38]–[41] presented some of the techniques for sensor node energy management in energy hungry WSNs. EHWSNs can be used to replenish the energy of the sensor nodes to ensure effective long-term monitoring. A trust-based routing protocol was proposed in [41] to ensure security of data and maximized use of available energy in EHWSNs. Some state-of-the-art energy management techniques were presented in [3], [6], [39], and [40]. An on-board recharging circuit to harvest energy from any unregulated energy source was discussed in [6]. In [39], rechargeable WSNs used the sensor nodes to harvest energy from both, solar and the radio frequency transmissions of their neighbors. However, it is important to note that the EHWSNs may not be infinitely supplemented with energy because energy harvesting requires additional hardware cost.

VII. CONCLUSION AND FUTURE WORK

This paper presents some investigations on the performance of fake packet-based SLP protocols. Four protocols are analyzed and their performance is compared with the performance of a traditional SLP protocol. Experimental evaluation of the SLP protection, energy consumption, network lifetime, end-to-end delay, and packet delivery ratio performance is done. Various experiment scenarios are assumed with varied network parameters and configurations. The analysis results support some interesting conclusions. (1) The level of SLP protection for the protocols is strongly influenced by the amount of the fake packet traffic in the network. (2) Integrating fake packet routing and packet flooding techniques can improve the privacy performance of a protocol. However, high energy cost is incurred and the network lifetime is shortened. (3) Using a threshold value of the sensor node residual energy as a criterion for selecting candidate fake packet sources may result in short-term SLP protection. (4) In many scenarios, the protocols maintain high levels of adversary obfuscation when the fake packet sources are not isolated from the phantom nodes. However, such configurations often result in reduced packet delivery reliability due to increased number of packet collision events. (5) Increasing the source packet rate can impact some negative effects on the privacy performance of the protocols. (6) Long source-sink distances allow for improved adversary obfuscation effects and strong SLP protection. (7) The protocols have high probability of packet collision and packet loss events which may result in reduced packet delivery reliability. (8) The energy consumption, network lifetime, end-to-end delay, and packet delivery ratio performance of the protocols can be affected when the source packet rate is increased.

Based on the observations from the experimental evaluations, some recommendations are presented to address the limitations of the protocols. As part of future work, we will propose some new algorithms for performance improvement. Specifically, we will propose an improved algorithm for the selection of candidate fake packet sources in the FPR protocol.

REFERENCES

[1] F. Wang, W. Liu, T. Wang, M. Zhao, M. Xie, H. Song, X. Li, and A. Liu, "To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in WSNs," *IEEE Access*, vol. 7, pp. 55983–56015, 2019.

[2] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "I-SEP: An improved routing protocol for heterogeneous WSN for IoT-based environmental monitoring," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 710–717, Jan. 2020.

[3] X. Liu, A. Liu, T. Wang, K. Ota, M. Dong, Y. Liu, and Z. Cai, "Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks," *J. Parallel Distrib. Comput.*, vol. 135, pp. 140–155, Jan. 2020.

[4] 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, Jan. 2020.

[5] I. Khan and D. Singh, "Energy-balance node-selection algorithm for heterogeneous wireless sensor networks," *ETRI J.*, vol. 40, no. 5, pp. 604–612, Oct. 2018.

[6] S. Misra, S. K. Roy, A. Roy, M. S. Obaidat, and A. Jha, "MEGAN: Multipurpose energy-efficient, adaptable, and low-cost wireless sensor node for the Internet of Things," *IEEE Syst. J.*, vol. 14, no. 1, pp. 144–151, Mar. 2020.

[7] L. 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.
[8] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 100–114, 2020.
[9] A. Jhumka, M. Bradbury, and M. Leeke, "Fake source-based source location privacy in wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 27, no. 12, pp. 2999–3020, Aug. 2015.
[10] M. Bradbury, M. Leeke, and A. Jhumka, "A dynamic fake source algorithm for source location privacy in wireless sensor networks," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 2015, pp. 531–538.
[11] 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.
[12] 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.
[13] L. C. Mutalemwa and S. Shin, "Routing protocols 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.
[14] M. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 409–416.
[15] J. Long, M. Dong, K. Ota, and A. Liu, "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," *IEEE Access*, vol. 2, pp. 633–651, 2014.
[16] N. Jan, A. Al-Bayatti, N. Alalwan, and A. Alzahrani, "An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP)," *Sensors*, vol. 19, no. 9, p. 2050, 2019.
[17] P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, "Source location privacy using fake source and phantom routing (FSAPR) technique in wireless sensor networks," *Procedia Comput. Sci.*, vol. 57, pp. 936–941, 2015.
[18] 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.
[19] Z. Hong, R. Wang, S. Ji, and R. Beyah, "Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1337–1350, May 2019.
[20] 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.
[21] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity against global adversary in WSNs using dummy packet injections: A survey," *Electronics*, vol. 7, no. 10, p. 250, 2018.
[22] Y. Chen, W. Xu, W. Trappe, and Y. Zhang, "Enhancing source-location privacy in sensor network routing," in *Proc. 25th ICDCS*, Jun. 2005, pp. 599–608.
[23] 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 Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, Mar. 2019.
[24] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proc. Int. Conf. Inf. Sci. Appl. (ICISA)*, Apr. 2010, pp. 1–6.
[25] M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 115, pp. 67–81, May 2018.
[26] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity in WSNs against global adversary utilizing low transmission rates with delay constraints," *Sensors*, vol. 16, no. 7, p. 957, 2016.
[27] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: Timed efficient source privacy preservation scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–6.
[28] S. Kokalj-Filipovic, F. Le Fessant, and P. Spasojevic, "The quality of source location protection in globally attacked sensor networks," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PERCOM Workshops)*, Mar. 2011, pp. 44–49.
[29] H. Chen and W. Lou, "From nowhere to somewhere: Protecting end-to-end location privacy in wireless sensor networks," in *Proc. Int. Perform. Comput. Commun. Conf.*, Dec. 2010, pp. 1–8.
[30] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, p. 724, 2017.
[31] A. Thomason, M. Leeke, M. Bradbury, and A. Jhumka, "Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 667–674.
[32] Y. Li, L. Lightfoot, and J. Ren, "Routing-based source-location privacy protection in wireless sensor networks," in *Proc. IEEE Int. Conf. Electro/Inf. Technol.*, Jun. 2009, pp. 29–34.
[33] C. Gu, M. Bradbury, A. Jhumka, and M. Leeke, "Assessing the performance of phantom routing on source location privacy in wireless sensor networks," in *Proc. IEEE 21st Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Nov. 2015, pp. 99–108.
[34] L. C. Mutalemwa and S. Shin, "Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks," *IEEE Access*, vol. 7, pp. 140169–140181, 2019.
[35] A. Jhumka, M. Bradbury, and M. Leeke, "Towards understanding source location privacy in wireless sensor networks through fake sources," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 760–768.
[36] 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, 2017.
[37] 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, 2019, pp. 1–16.
[38] F. Engmann, F. A. Katsriku, J.-D. Abdulai, K. S. Adu-Manu, and F. K. Banaseka, "Prolonging the lifetime of wireless sensor networks: A review of current techniques," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, Aug. 2018.
[39] T. He, K.-W. Chin, S. Soh, and C. Yang, "On optimizing max min rate in rechargeable wireless sensor networks with energy sharing," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 1, pp. 107–120, Jan. 2020.
[40] A. Boukerche, Q. Wu, and P. Sun, "Efficient green protocols for sustainable wireless sensor networks," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 1, pp. 61–80, Jan. 2020.
[41] J. Tang, A. Liu, J. Zhang, N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, p. 751, 2018.

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 security and privacy in the IoT and monitoring networks, and WSN protocol design and performance evaluation.

SEOKJOO SHIN (Member, IEEE) received the B.Eng. degree in electronics engineering from Korea Aerospace University, South Korea, and 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 as a Visiting Researcher at Georgia Tech, USA. His research interests include wireless communication systems, the IoT, AI related to networking, and network security and privacy.