IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 29, 2021, accepted July 17, 2021, date of publication July 26, 2021, date of current version August 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3099499

Novel Approaches to Realize the Reliability of Location Privacy Protocols in Monitoring Wireless Networks

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) by the Ministry of Education under Grant NRF-2018R1D1A1B07048338.

ABSTRACT Wireless sensor network (WSN) technology presents significant advantages for Internet of Things (IoT). Sensor-based IoT networks are designed to operate in unattended, harsh, and complex environments. However, WSNs are resource-constrained. Due to the operating environment settings, there exist great challenges in the privacy and reliability of WSN communications. To achieve secure and reliable communications, it is necessary to devise reliable routing protocols and provide a method to evaluate the performance of the protocols. To guarantee location privacy of source nodes, numerous source location privacy (SLP) routing protocols are presented in the literature. However, the existing literature fails to evaluate the SLP reliability of the protocols. This article achieves three main objectives. First, a new relay ring routing (ReRR) protocol is proposed to address some limitations of fake packet-based SLP routing protocols. The routing algorithm of ReRR is specifically designed to provide long-term SLP protection. Second, unlike previous articles that focus solely on measuring the magnitude of SLP protection using performance metrics such as safety period, capture ratio, attack success rate, and capture probability, this article proposes a novel approach to measure the SLP reliability of the protocols. In the third objective, we conduct a series of experiments to analyze the performance of ReRR and fake packet-based protocols. Using the proposed approach, the SLP reliability of the protocols is evaluated. Experiment results reveal that the proposed ReRR protocol exhibits advantageous performance features. It is observed that the fake packet-based routing protocols achieve strong SLP protection by integrating multiple routing techniques such as packet flooding and random distribution of fake packet traffic. However, the achieved SLP protection is short-term and less reliable. On the other hand, the proposed ReRR protocol employs an energy-efficient routing algorithm to guarantee reliability and long-term SLP protection. In addition, the ReRR protocol ensures improved network lifetime.

INDEX TERMS Source location privacy, wireless sensor network, routing protocol, reliability, energy efficiency.

I. INTRODUCTION

In recent years, wireless sensor network (WSN) technology has gained increasing popularity in ubiquitous support of sensing system services [1] and Internet of Things (IoT). WSNs attract worldwide attention in wide range of application domains including intelligent industrial monitoring, medical treatment, environmental monitoring, natural disaster prevention, smart home development, water quality controlling, and intelligent transportation systems [2]–[5]. Often, WSNs are battery-operated in unattended, harsh, and complex environments. Therefore, performance of WSNs is vulnerable to energy and environmental factors [3], [6]–[10]. Furthermore, WSNs are usually deployed in random areas with no protection. Consequently, the networks are vulnerable to traffic analysis attacks. In the attacks, adversaries focus on analyzing the network traffic to obtain critical information such as the location information of important sensor nodes [8], [11]–[15].

Therefore, it is important to ensure energy-efficient communications and location privacy protection in WSNs [13], [16]–[18]. Moreover, the dynamicity of WSNs is greater

The associate editor coordinating the review of this manuscript and approving it for publication was Laurence T. Yang.

as sensor nodes fail more often due to limited battery power and harsh application environments [19]. Thus, it is essential to guarantee reliability in WSNs and ensure reliable network operations [19]–[28].

In this study, we propose an energy-efficient and reliability-aware source location privacy (SLP) routing protocol to provide source node location privacy protection in monitoring WSNs. Similar to [23], we consider that to achieve reliable communications within WSNs, it is essential to design reliable routing protocols and provide a means to evaluate the reliability performance of the protocols. Subsequently, we propose a new approach to evaluate the SLP reliability of SLP routing protocols. To the best of our knowledge, this is the first study attempting to measure the SLP reliability. We quantify the ability of the SLP routing protocols to achieve SLP protection according to application-specific requirements. Thus, the main difference between this study and previous studies is that, previous studies focus solely on measuring the magnitude of the SLP protection using performance metrics such as safety period, capture ratio, attack success rate, and capture probability but fail to measure the SLP reliability. Moreover, many of the existing studies focus on connectivity-oriented and flow-oriented reliability in WSNs [19].

SLP protection is the process of minimizing the traceability and observability of a source node by an adversary in WSNs [12], [29]. SLP is a significant challenge in monitoring WSNs mainly because if a source location is easily exposed to the adversary, the security of the WSN can be compromised [12], [14], [15]. To address the challenge of SLP, numerous SLP routing protocols are presented in the literature [11], [12], [16], [30]–[36]. In this study, we propose the relay ring routing (ReRR) protocol. The ReRR protocol aims to outperform two existing protocols, the data dissemination routing (DissR) protocol [37] and the distributed fake source with phantom node (DistrR) protocol [38]. The proposed ReRR protocol outperforms the DissR and DistrR protocols in terms of long-term SLP protection, energy efficiency, network lifetime, and SLP reliability.

Exhaustive energy consumption of sensor nodes and unbalanced energy distribution can seriously affect the operation of WSNs, resulting in limitations such as limited network lifetime [1]–[5], [7], [39] and short-term SLP protection [30]. Therefore, to outperform the DissR and DistrR protocols, ReRR regulates the energy consumption of the sensor nodes by reducing the amount of packet traffic in the network. Hence, unlike the DissR and DistrR protocols that distribute large amounts of fake packet traffic or floods real and fake packets in particular regions of the network, ReRR generates a reduced amount of packet traffic. The routing algorithm of ReRR guarantees that only real packets are transmitted to the sink node.

To achieve high levels of SLP protection, ReRR employs a dynamic routing strategy that involves two routing techniques. The process of selecting a routing technique is based on the location of the source node with respect to the sink node location. ReRR creates random routing paths with high path diversity by computing parameters such as randomization factor and node offset angle. Furthermore, to realize the random routing paths, ReRR provides three candidate relay nodes for each source node packet forwarding instance and randomly selects one relay node during the route creation process. Multiple relay ring sections and relay regions are generated between a source node and relay nodes to ensure the location of any relay node is safeguarded. Thus, the location information of the source nodes is not easily leaked to the adversary even after the adversary locates a relay node. The strategic configuration of the relay ring sections and relay regions, and the dynamic route creation process guarantee that the routing paths for successive packets are unpredictable to the adversary. As a result, the adversary is obfuscated and the SLP is preserved.

A. MOTIVATION

This study is motivated by the discussions in [2], [4], [19], [21]–[23], [30]. In [30], it was shown that the DissR and DistrR protocols achieve short-term SLP protection and reduced network lifetime due to high energy consumption. Furthermore, it was shown that DissR incurs unbalanced energy distribution. The challenge of unbalanced energy distribution in WSNs was also highlighted in [2], [4]. Then, it was presented that when the challenge of unbalanced energy distribution is addressed, it can result in increased network lifetime and improved network reliability and feasibility. Therefore, this study proposes an energy-aware SLP routing protocol, namely, ReRR protocol. The ReRR protocol achieves reliable long-term SLP protection to outperform the DissR and DistrR protocols.

In [19], [21]–[23], reliability of WSNs was considered. It was presented that to ensure reliable network operations in WSNs, it is important to quantify the performance of such networks in terms of network reliability measures. Also, to provide services according to application-specific requirements. Subsequently, [19], [21]–[23] proposed new approaches to evaluate the reliability of WSNs. In [23], it was highlighted that to achieve reliable wireless communications within WSNs, it is essential to develop reliable routing protocols and provide a means to evaluate the reliability of different routing protocols. Therefore, in addition to devising the ReRR protocol, we propose a new approach to evaluate the SLP reliability of SLP routing protocols. This is the first study to consider approaches for realizing the SLP reliability.

B. CONTRIBUTIONS

The main contributions of this study can be summarized as follows.

- Identify the limitations of the DissR and DistrR protocols that are caused by various packet routing techniques. Explore the limitations that are caused by the distribution of fake packet traffic in particular regions of the WSN domain and flooding of real and fake packets.

- Develop the new ReRR protocol. Design the routing algorithm of ReRR to guarantee high path diversity, high levels of adversary obfuscation, and improved energy efficiency.
- Conduct a series of experiments to evaluate the performance of ReRR protocol and demonstrate the superiority of ReRR over DissR and DistrR protocols. Demonstrate that ReRR outperforms DissR and DistrR in terms of long-term SLP protection, energy efficiency, and network lifetime.
- Propose a new approach to measure the SLP reliability of SLP routing protocols. Then, using the proposed approach, evaluate the SLP reliability of the ReRR, DissR, and DistrR protocols. Also, exhibit that ReRR achieves improved SLP reliability to outperform DissR and DistrR.

C. PAPER ORGANIZATION

The remainder of this paper is organized as follows. Section II presents a review of the literature on routing protocols for SLP protection. Section III highlights some assumptions and details of the network and adversary models. Section IV provides a detailed description of the proposed ReRR protocol. Experimental analysis and simulation results are discussed in Section V. In Section VI, the paper is concluded.

II. RELATED WORK

The topic of SLP protection in WSNs has received a lot of attention in the literature since it was first introduced in 2004 [12]. Numerous SLP protocols have been proposed. Many of the protocols were discussed in [11], [12], [16], [30]–[36], [40]. Some of the recently proposed SLP protocols include the two-level phantom with a pursue ring protocol [12], unified single and multi-path routing protocol [13], dynamic multipath routing protocol [17], grid-based single phantom node protocol [34], data dissemination protocol [37], and the protocol based on anonymity cloud [41]. Other recently proposed SLP protocols include the cloud-based with multi-sinks protocol [14], protocol based on phantom nodes, rings, and fake paths [16], phantom walkabouts protocol [18], grid-based dual phantom node protocol [34], two-level phantom with a backbone route protocol [12], probabilistic routing protocol [42], and the circular trap protocol [43].

SLP protocols may be classified into many categories including fake packet routing, tree-based routing, intermediate node routing, phantom node routing, angle-based routing, and ring routing. Fake packet-based protocols include the path extension protocol, dummy packet injection routing, protocol based on anonymity cloud, distributed fake source with phantom node routing, protocol based on phantom nodes, rings, and fake paths, fake network traffic-based routing, data dissemination routing, dynamic fake sources-based routing, hybrid online single path routing, and the probabilistic routing protocol [8], [12], [16], [30], [41], [42].

Tree-based routing protocols include the tree-based diversionary routing, bidirectional tree, dynamic bidirectional tree, and zigzag bidirectional tree routing [15]. Intermediate node-based protocols include the randomly selected intermediary node routing, strategic location-based routing, three-phase intermediate node routing with network mixing ring, sink toroidal region routing, and the all-direction random routing protocol [15], [35]. Phantom node-based routing protocols include the phantom single-path routing, phantom routing with locational angle, phantom walkabouts, two-level phantom with a backbone route protocol, pseudo normal distribution-based phantom routing protocol, greedy random walk routing, and the probabilistic routing protocol [11], [12], [18]. Angle-based routing protocols include the angle-based intermediate node routing, angle-strategic routing, angle-based dynamic routing, angle-proxy routing, constrained random routing, and the two-phantom angle-based routing [11], [29], [44].

Some of the SLP protocols employ multiple routing strategies. For example, in [16], phantom routing was integrated with ring routing and fake packet routing. In [15], [37], [38], [42], phantom routing was integrated with fake packet routing. Other protocols employ multiple sink nodes. For instance, the protocols in [14], [17], [45] employed multiple sink node routing strategies.

The study in [30] analyzed the performance of four fake packet-based protocols: the tree-based diversionary routing protocol [15], DissR [37], DistrR [38], and the probabilistic source location privacy protection protocol [42]. It was observed that the DissR and DistrR protocols were capable of achieving high levels of SLP protection to outperform the other protocols. However, the SLP protection of the DissR and DistrR protocols was short-term. Furthermore, the DissR and DistrR protocols incurred the highest energy consumption in the near-sink regions. As a result, DissR and DistrR achieved limited network lifetime. To address the challenges of DissR and DistrR protocols, this study develops the new ReRR protocol. The proposed ReRR outperforms DissR and DistrR in terms of long-term SLP protection, energy efficiency, and network lifetime. Moreover, ReRR achieves improved SLP reliability. The operational features of the DissR and DistrR protocols are presented below.

The DissR protocol assumes a four quadrants square grid WSN with the sink node at the center of the grid. When a source node wishes to send a packet to the sink node, the sink node generates a fake source and a phantom source depending on the location of the source node. A blast ring around the sink node contains nodes that are designed to flood packets inside the ring. When a blast node on the edge of the ring receives packets for forwarding, it starts flooding in a controlled manner. The protocol provides three levels of confusion to the adversary: fake node level, phantom node level, and the blast ring level. As a result, it achieves high levels of SLP protection. Limitations of DissR include exhaustive energy consumption inside the blast ring regions [12]. Furthermore, the

TABLE 1. Summary of the achievements in DissR, DistrR, and ReRR protocols.

Protocol	Level of SLP protection in short-term	Effective long-term SLP protection	Exhaustive energy consumption	Long network lifetime	Long-term SLP reliability
DissR [37]	Very high	No	Yes	No	No
DistrR [38]	Very high	No	Yes	No	No
Proposed ReRR	High	Yes	No	Yes	Yes

DissR protocol achieves short-term SLP protection due to the exhaustive energy consumption [30].

In the DistrR protocol, when a node wishes to transmit a packet to the sink node, it first floods a fake request packet into the network with a maximum hop count. Every node which receives the fake request packet checks their remaining energy levels and checks the number of times it has become a real source in the previous sessions. If a node has been a regular real source in the past, then it is disqualified from being a candidate fake source. If the energy level of the node is above a threshold value and it has not been a regular real source in recent sessions, then the node becomes a good candidate for fake source. The node computes a random number between 0 and 1. If the random number is greater than 0.5 then the node is selected as a fake source otherwise it ignores the request. When the node is selected as a fake source, it starts sending fake packets which are identical to real packets. Subsequently, the source node selects a random node located at a distance away to act as a phantom node. After a phantom node is selected, the source node sends packets to the sink node through the selected phantom node. The main limitation of DistrR is high energy consumption due to the distribution of fake packet traffic. Also, the protocol has reduced packet delivery reliability due to packet collisions which result from the simultaneous transmission of real and fake packets [12].

To insure improved performance in the proposed ReRR protocol, it is assumed that multi-hop data transfer technique leads to exhaustive energy consumption for sensor nodes in the near-sink regions. This is due to the fact that the sensor nodes in the near-sink regions have increased load of packet traffic, since the sink node is the destination node for the packet traffic. Thus, the sensor nodes in the near-sink regions have to burden the data forwarding for nodes in the away from sink node regions [2], [15], [29]. Furthermore, multi-hop data transfer technique results in non-uniform energy consumption across the network and the sensor nodes in the near-sink regions deplete their energy faster [2]. This phenomena results in short-term SLP protection and reduced network lifetime, especially in the DissR and DistrR protocols which distribute large amounts of packet traffic. Therefore, the main goal of ReRR is to reduce the energy consumption of the sensor nodes by reducing the amount of packet traffic in the WSN domain. To highlight the significance of the proposed ReRR protocol, Table 1 summarizes the achievements of DissR, DistrR, and ReRR protocols.

III. MODELS

In this section, the relevant features of the proposed network and adversary models are highlighted.

A. NETWORK MODEL

A WSN model similar to [29] is assumed. The WSN comprises a large number of homogeneous sensor nodes randomly deployed to continuously monitor a target field. The network is two-dimensional 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 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 powerful than the ordinary nodes. It has sufficient resources in terms of memory capacity, data transmission, and computational power. The source node is responsible for sensing the asset and forwarding the sensed data to the 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 modeled with a circular communication range centered at the node. 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. The k-nearest neighbor tracking approach [46] is employed to track the assets. 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 is performed for localization of the sensor nodes [35]. It is assumed that the sink node acquires its location information by using a 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. Thus, each node receives the beacon packet, stores the hop counter value with a sender

node ID, increments the hop counter by one, and rebroadcasts the beacon packet to its neighboring nodes. The hop counter number indicates the hop distance (d_S) between a sensor node and the sink node. If a sensor node receives multiple packets, it only stores the minimum hop count in its buffer and deletes other hop counter information. 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.

B. ADVERSARY MODEL

A cautious adversary similar to [29], [35] is assumed. The adversary is well-equipped with enough storage, energy, and 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 routes by moving hop-by-hop towards the source node, until it reaches at the location of 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 by the network administrator.

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 resume the packet listening 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. The hop-by-hop back tracing attack of the cautious adversary is illustrated in Fig. 1.

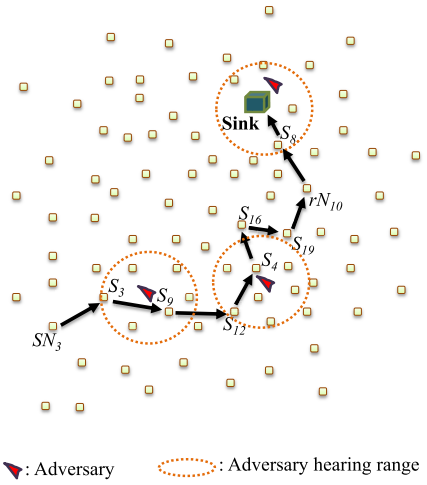

FIGURE 1. Illustration of hop-by-hop back tracing attack of the cautious adversary.

In the Fig.1, packets may be sent from the source node SN_3 to the sink node using a random route which passes through relay node rN_{10}. When the adversary is at the sink node, sensor node S_8 is within the adversary hearing range. When a packet arrives at the sink node from S_8, the adversary will move to the node S_8 without delay. Similarly, if the adversary is at S_4 and a packet arrives from S_{12}, the adversary will move to S_{12} without delay. At S_{12}, the adversary will wait for the next packet to arrive according to the waiting timer. If the timer expires, the adversary will roll back to S_4. Adversary will repeat the process until it arrives at the location of the source node to successfully capture the monitored asset.

IV. PROPOSED RELAY RING ROUTING (ReRR) PROTOCOL

Generally, SLP protection is achieved by injecting fake packet traffic in the network or increasing the randomness of the routing paths [14]. The proposed ReRR protocol considers the techniques to increase the randomness of the routing paths while the existing DissR and DistrR protocols employ fake packet injection techniques. Thus, the proposed ReRR protocol presents two main design goals to guarantee improved performance. The main design goals of ReRR are summarized as follows.

- Reduce the energy consumption of the sensor nodes by reducing the amount of packet traffic in the network. It was shown in [30] that exhaustive energy consumption of the sensor nodes can result in short-term SLP protection. Furthermore, packet transmission and reception are the most energy consuming tasks for the sensor nodes [29], [30]. Therefore, unlike the DissR and DistrR protocols which distribute large amounts of packet traffic in the network, ReRR aims to distribute a reduced amount of packet traffic to ensure long-term SLP protection.
- Create random routing paths with high path diversity by employing a randomization factor (R_F) and node offset angle (θ) parameters. To achieve the random routing paths, provide three candidate relay nodes (rNs) for each source node (SN) and randomly select one rN based on the values of R_F and θ. The routing algorithm of ReRR guarantees that a new rN is selected for each successive packet routing to ensure the routing paths are unpredictable to the adversary. Hence, ReRR ensures adversary obfuscation to achieve high levels of SLP protection.

The ReRR protocol operates in two phases as shown in algorithm 1. Phase 1 involves the processes for network configuration while phase 2 includes the mechanisms for packet routing. The network initialization is done according to the process explained in section III (A). The sink node is located at coordinates (0, 0). Distance between any two points in the network is calculated using the Euclidian distance equation as shown in equation (1). The equation shows the parameters for calculating the distance between point V at (x_V, y_V) and

TABLE 2. Section boundary angle for each *SB*.

SB	SB_1	SB_2	SB_3	SB_4
θ_{SB}	$\pi/4$	$3\pi/4$	$5\pi/4$	$7\pi/4$

Algorithm 1 Algorithm for ReRR Protocol

Phase 1: Network configuration
1: network initialization
2: generate X–Y coordinate
3: each node compute θ according to Fig. 2
4: generate *SBs* according to Fig. 3 and Table 2
5: generate R_{ring} according to Fig. 3
6: assign nodes into R_{ring} according to Table 3
7: assign nodes into sections of R_{ring} according to Table 4
8: assign d_T
9: assign nodes into *RRs* according to Table 5

Phase 2: Packet routing
10: sensor node detect asset, becomes *SN*
11: generate R_F
12: **if** $(d_S \geq d_T)$ **then**
13: select *rN* according to RS1 in Table 6
14: **else**
15: select *rN* according to RS2 in Table 7
16: **end if**
17: route packet from *SN* to sink node through selected *rN*

point W at (x_W, y_W).

$$d_{VW} = \sqrt{(x_V - x_W)^2 + (y_V - y_W)^2} \tag{1}$$

After the network initialization process is complete, an X–Y coordinate is generated, centered at the sink node. The θ for all sensor nodes is computed. The θ is an inclination angle formed between the X-axis and the imaginary line connecting the sink node and the node that is computing the θ. As an example, in Fig. 2, to compute the θ for node Z at (x_Z, y_Z), distances d_{SZ} and d_{ZA} are considered. Then, θ_Z is computed according to equation (2).

$$\theta_Z = sin^{-1}\left(\frac{d_{ZA}}{d_{SZ}}\right) \tag{2}$$

The network configuration for the proposed ReRR protocol is shown in Fig. 3. The network is divided into four network sections. Each section is separated from other sections by using the section boundaries (*SBs*) as shown in Fig. 3. The *SBs* are used to ensure the *rNs* and *SNs* are located in different network sections. This guarantees that the location of any *rN* is safeguarded at a safe distance away from the *SNs*. The location of the *SBs* is determined by the value of section boundary angle (θ_{SB}). The θ_{SB} is the inclination angle formed between a *SB* and the X-axis. Table 2 shows the θ_{SB} for each *SB*. A relay node ring (R_{ring}) is generated according to Fig. 3.

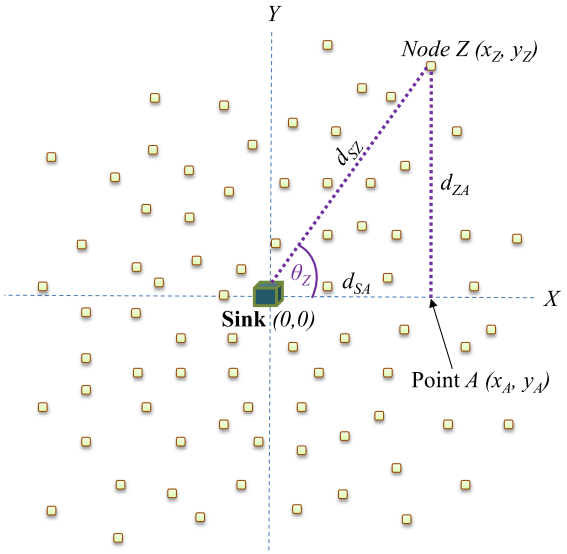

FIGURE 2. Computation of node offset angle.

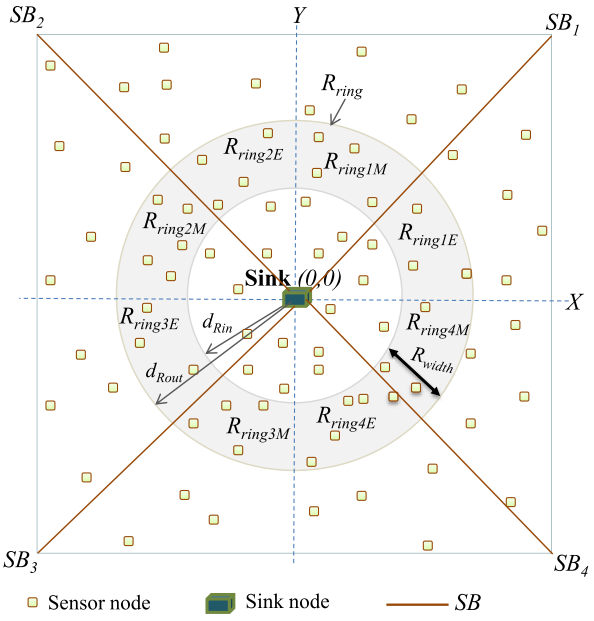

FIGURE 3. Network configuration for the proposed ReRR protocol.

R_{width} is the width of the R_{ring} while d_{Rin} is the distance between the sink node and the inner boundary of the R_{ring} and d_{Rout} is the distance between the sink node and the outer boundary of the R_{ring}.

The R_{ring} has four unique sections according to θ of the sensor nodes, as shown in Table 3. Thus, the R_{ring} is divided

TABLE 3. Assignment of sensor nodes into R_{ring}.

θ	$0° \leq \theta < \pi/2$	$\pi/2 \leq \theta < \pi$	$\pi \leq \theta < 3\pi/2$	$3\pi/2 \leq \theta < 2\pi$
Section of R_{ring}	R_{ring1}	R_{ring2}	R_{ring3}	R_{ring4}

TABLE 4. Assignment of sensor nodes into sections of R_{ring}.

Node location	R_{ring1}		R_{ring2}		R_{ring3}		R_{ring4}	
θ	$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$	$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
Section of R_{ring}	R_{ring1E}	R_{ring1M}	R_{ring2E}	R_{ring2M}	R_{ring3E}	R_{ring3M}	R_{ring4E}	R_{ring4M}

TABLE 5. Assignment of sensor nodes into *RRs*.

θ	$0° \leq \theta < \theta_{SB1}$	$\theta_{SB1} \leq \theta < \pi/2$	$\pi/2 \leq \theta < \theta_{SB2}$	$\theta_{SB2} \leq \theta < \pi$	$\pi \leq \theta < \theta_{SB3}$	$\theta_{SB3} \leq \theta < 6\pi/4$	$6\pi/4 \leq \theta < \theta_{SB4}$	$\theta_{SB4} \leq \theta < 2\pi$
RR	RR_1	RR_2	RR_3	RR_4	RR_5	RR_6	RR_7	RR_8

TABLE 6. RS1 for selection of *rN* from sections of R_{ring} according to *SN* location, θ, and R_F.

X* and *Y* coordinates, and θ of *SN		$X \geq 0$ and $Y \geq 0$		$X < 0$ and $Y \geq 0$		$X < 0$ and $Y < 0$		$X \geq 0$ and $Y < 0$	
		$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$	$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
***Selection of rN* from R_{ring}**	$R_F < 4$	R_{ring2E}	R_{ring2M}	R_{ring3E}	R_{ring3M}	R_{ring4E}	R_{ring4M}	R_{ring1E}	R_{ring1M}
	$4 \leq R_F \leq 6$	R_{ring3E}	R_{ring3M}	R_{ring4E}	R_{ring4M}	R_{ring1E}	R_{ring1M}	R_{ring2E}	R_{ring2M}
	$R_F > 6$	R_{ring4E}	R_{ring4M}	R_{ring1E}	R_{ring1M}	R_{ring2E}	R_{ring2M}	R_{ring3E}	R_{ring3M}

TABLE 7. RS2 for selection of *rN* from *RRs* according to *SN* location, θ, and R_F.

X* and *Y* coordinates, and θ of *SN		$X \geq 0$ and $Y \geq 0$		$X < 0$ and $Y \geq 0$		$X < 0$ and $Y < 0$		$X \geq 0$ and $Y < 0$	
		$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$	$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
Selection of rN* from *RRs	$R_F < 4$	RR_3	RR_4	RR_5	RR_6	RR_7	RR_8	RR_1	RR_2
	$4 \leq R_F \leq 6$	RR_5	RR_6	RR_7	RR_8	RR_1	RR_2	RR_3	RR_4
	$R_F > 6$	RR_7	RR_8	RR_1	RR_2	RR_3	RR_4	RR_5	RR_6

into R_{ring1}, R_{ring2}, R_{ring3}, and R_{ring4}. Each section of the R_{ring} is further divided into two sections according to the θ of the sensor nodes, as shown in Table 4 and Fig. 3. For example, in R_{ring1}, if θ of a node is $< \theta_{SB1}$, the sensor node is assigned into R_{ring1E}. Otherwise, node is assigned into R_{ring1M}. The structure of the network configuration and node assignment ensure that during packet routing, any *rN* will be located at least one R_{ring} section away from the *SNs*. The aim is to guarantee that the *SN* location information is not easily leaked to the adversary even after the adversary locates the *rNs*. A threshold hop distance (d_T) is defined. All sensor nodes with $d_S \geq d_T$ are assigned into relay regions (*RR*) based on their θ, as shown in Table 5. The d_S is computed by each sensor node during the network initialization process. The algorithm of ReRR protocol is summarized in algorithm 1.

To create highly random routing paths and provide high path diversity, the ReRR protocol involves two routing strategies: routing strategy 1 (RS1) and routing strategy 2 (RS2). The choice of a routing strategy for each *SN* is highly dependent on the values of distances d_S and d_T. For each *SN*, if $d_S \geq d_T$, RS1 is employed. Otherwise, RS2 is employed. The *rN* selection process for RS1 is summarized in Table 6 while RS2 is summarized in Table 7. Both RS1 and RS2 generate three candidate *rNs* for each *SN* and one of the *rNs* is selected based on the value of R_F. R_F is a random number in the range [1, 9]. It is generated by the *SN* after the *SN* detects an asset. The use of R_F ensures a high probability that a different *rN* is selected for each successive packet and the routing paths are unpredictable to the adversary.

The location of *SNs* with respect to the sink node location and θ are also considered during the *rN* selection process in RS1 and RS2. As an example, if *SN* has $d_S \geq d_T$, then RS1 in Table 6 is employed. If the *SN* has *X*-coordinate ≥ 0, *Y*-coordinate ≥ 0, $\theta < \theta_{SB1}$, and $R_F < 4$, then a *rN* is selected from R_{ring2E}. On the other hand, if the same *SN* generates $R_F > 6$, then a *rN* is selected from R_{ring4E}. When *SN*

TABLE 8. Key differences in the routing strategies of DissR, DistrR, and ReRR protocols.

Protocol	Routing strategy	
	If *SN* has $d_S < d_T$	If *SN* has $d_S \geq d_T$
DissR	• Real packets from the source node are flooded inside the blast ring.	• Real packets and fake packets are distributed in the WSN domain. • Real packets and fake packets are flooded inside the blast ring.
DistrR	• Real packets and large amount of fake packets are distributed in the WSN domain.	• Real packets and large amount of fake packets are distributed in the WSN domain.
Proposed ReRR	• Real packets are transmitted to the sink node through *rNs*, using RS2.	• Real packets are transmitted to the sink node through *rNs*, using RS1.

has $d_S < d_T$, the RS2 in Table 7 is employed. If the *SN* has X-coordinate < 0, Y-coordinate < 0, $\theta \geq \theta_{SB3}$, and $4 \leq R_F \leq 6$, then a *rN* is selected from RR_2. On the other hand, if the same *SN* generates $R_F > 6$, then a *rN* is selected from RR_4. After a *rN* is selected, packet routing between the *SN* and *rN* and between the *rN* and the sink node is done by using the directed random-walk routing strategy.

The directed random-walk routing strategy operates as follows. Once a sensor node has a packet to forward, it starts the process of next-hop node selection. The forwarding node computes a set of one-hop neighboring nodes with a shorter hop distance to the destination node than the forwarding node itself. Then, it randomly selects one neighboring node from the set as the next-hop node. The next-hop node becomes the forwarding node and forwards the packet. At the *SN*, the destination node is the selected *rN*. At the *rN*, the destination node is the sink node. To ensure the routing paths for successive packets are diversified, ReRR generates three candidate *rNs* for each *SN* packet forwarding instance and randomly selects a *rN* based on the value of the R_F and θ. Moreover, a new R_F is generated for each *SN* packet forwarding instance.

The key differences in the routing strategies of the proposed ReRR protocol and the existing DissR and DistrR protocols are summarized in Table 8. For the DissR protocol, we assume all sensor nodes with $d_S < d_T$ are located inside the blast ring.

Some investigations were done to observe the relationship between the size of R_{ring} and the level of SLP protection. Then, we determined an effective R_{ring} size. We assume that an effective R_{ring} size ensures effective number of sensor nodes in the R_{ring} to enable high path diversity and high levels of SLP protection.

Path diversity signifies the presence of route variation where successive packets from a *SN* follow different routing paths that are created between the *SN* and sink node [34], [47], [48]. Hence, in ReRR, path diversity denotes the existence of many alternative paths between a *SN* and sink node based on the randomly selected *rNs*. We measure the path diversity by counting the number of alternative packet routes that are created between a *SN* and sink node.

Path diversity enables successive packets from a *SN* to follow different routes to the sink node. This has a positive effect on the level of SLP protection by making it more difficult for the adversary to predict the routes for successive packets. Therefore, high path diversity corresponds to high levels of SLP protection. For instance, for a successful back tracing attack, an adversary needs to intercept many packets. If the packets use diversified routing paths, it takes longer for the adversary to detect a great number of packets to intercept. Therefore, the adversary obfuscation effect is increased, the back tracing attack of the adversary becomes complex, and the level of SLP protection is improved.

It is observed that the size of the R_{ring} can be altered to vary the number of sensor nodes inside the R_{ring}. Subsequently, high path diversity and high levels of SLP can be achieved when a large number of sensor nodes is available inside the R_{ring}. This is mainly because when a large number of sensor nodes is available, it generates a larger set of *rNs* for each *SN*. As a result, a greater number of routing paths can be created to improve the path diversity.

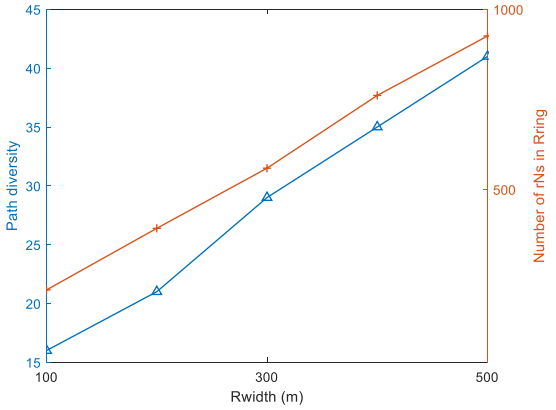

FIGURE 4. Achievable path diversity and number of *rNs* for different R_{width} size.

Fig. 4 shows the average values for path diversity and number of sensor nodes in the R_{ring} for different R_{width} sizes. To obtain the observations in the Fig. 4, 2500 sensor nodes were randomly distributed in a target field with side length of 2000 m and d_{Rin} of 300 m. The ds of the *SNs* was 35 hops and d_T was set to 25 hops. It is depicted in Fig. 4 that a greater number of sensor nodes become available in the R_{ring} and high path diversity is achieved when the size of R_{width} is increased.

In addition, similar to [34], it is observed that path diversity improves with the diversity of the *rNs* in terms of location and randomness. This is due to the fact that the *rNs* in the ReRR protocol appear randomly across the R_{ring} regions. Also, the

diversity of the *rNs* in terms of location and randomness tend to increase when the R_{width} is increased.

Although the level of SLP protection improves with the increase in R_{width}, it is important to note that the R_{width} must be regulated to control the communication overhead. When R_{width} is significantly long, the packet routes become longer. Consequently, more energy may be spent to deliver the packets, longer delay may be incurred, and the probability of packet loss events may be increased. Therefore, the network planner must configure the R_{width} according to the application-specific requirements. In this study, it is assumed that the level of SLP protection at $R_{width} = 400$ m is effectively adequate. Also, it is assumed that the communication overhead at $R_{width} = 400$ m is acceptable.

V. EXPERIMENTAL EVALUATION

This section presents some investigations on the performance of DissR, DistrR, and the proposed ReRR protocol. Various performance metrics were used to evaluate the performance of the protocols. First, the safety period and capture ratio were used to measure the level of SLP protection. Then, the energy consumption, energy efficiency, and network lifetime were analyzed. Also, investigations were done to analyze the SLP reliability of the protocols. Thus, a new approach was proposed to measure the safety period reliability and capture ratio reliability of the protocols.

For comparative analysis, the traditional phantom single-path routing (PhanR) protocol was included in the evaluations. In the PhanR protocol, packets are sent from the source nodes to the sink node through less random routing paths. Also, the routing paths are relatively short. Consequently, the adversary is not effectively obfuscated and PhanR achieves low levels of SLP protection [12].

A. SIMULATION ENVIRONMENT

Using MATLAB simulation environment, a network of size 2000×2000 m^2 was simulated with 2500 randomly distributed sensor nodes. The d_{Rin} was 300 m and R_{width} was 400 m. The d_T was set to 25 hops. The sensor node communication range was set to 30 m to ensure multi-hop communications between the source nodes and sink node. Adversary hearing 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. To ensure accuracy of the simulation results, simulations were run for 500 iterations and average values were considered. The network simulation parameters are summarized in Table 9. The simulation results are discussed below.

TABLE 9. Network simulation parameters.

Parameter	Value
Network area (m^2)	2000×2000
Number of nodes	2500
Number of sink nodes	1
d_{Rin} (m)	300
R_{width} (m)	400
d_T (hops)	25
Sensor node communication range (m)	30
Adversary hearing range (m)	30
Adversary waiting timer (source packets)	4
Adversary initial location	In the vicinity of sink node
Target monitoring scheme	*k*-nearest neighbor tracking
Packet size (bit)	1024
Source packet rate (packet/second)	1
Sensor node initial energy (J)	0.5

B. SLP PROTECTION

1) SAFETY PERIOD

Safety period (SP) is the time required for an adversary to back trace the packet routes and successfully locate the source node. As shown in equation (3), longer SP corresponds to high levels of SLP protection [15], [30]. Similar to [30], we measure the SP by counting the number of hops during the adversary back tracing attack.

$$\max(SP) = \max(SLP_{Protection}) \tag{3}$$

The SP of the protocols was computed to observe the ability of the protocols to provide effective long-term SLP protection. Therefore, the SP was observed at different mission durations (rounds). In the experiments, source nodes were located at a source-sink distance of 35 hops. The results are shown in Fig. 5. The results show that the DissR, DistrR, and ReRR protocols achieve significantly longer SP than the traditional PhanR protocol. Furthermore, the results show that the SP of the ReRR protocol remains high throughout the 900 rounds. On the other hand, the SP of the DissR and DistrR protocols tend to decrease as the number of rounds is increased. Thus, the results indicate that the ReRR protocol is able to achieve effective long-term SLP protection to outperform the DissR and DistrR protocols.

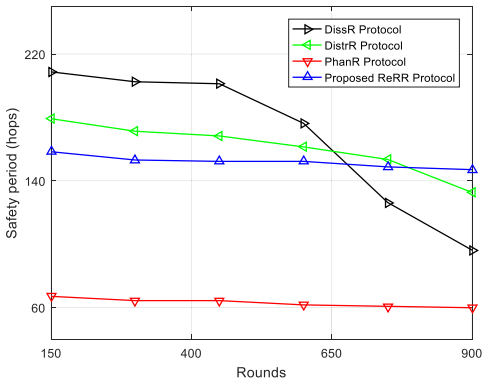

FIGURE 5. Privacy performance of the protocols.

When the number of rounds is low, the DissR protocol is capable of obfuscating the adversary to achieve longer SP than the other protocols because it employs a probabilistic flooding mechanism. It floods both real and fake packets. Therefore, multiple random nodes are selected to broadcast

each packet so that the packets arrive at the sink node using multiple random routing paths. As a result, the tracing back attack becomes a complex and time consuming task and longer SP is achieved. Moreover, the cautious adversary is restricted from revisiting the immediate sender nodes. To some extent, the restriction increases the complexity of the adversary back tracing attack when the flooding mechanism is used.

Although the flooding mechanism of DissR helps to improve the SP, it causes short-term SLP protection. As shown in Fig. 5, the SP of DissR protocol is significantly reduced at 900 rounds. When both real and fake packets are flooded, a significant amount of sensor nodes energy is consumed to transmit a single packet. Consequently, the sensor nodes drain their energy at a fast rate. At 900 rounds, a significant number of sensor nodes inside the blast ring have exhausted their battery power. Therefore, fewer sensor nodes are able to participate in the flooding mechanism. As a result, the adversary becomes less obfuscated and the SP is reduced.

The DistrR protocol distributes a considerable amount of fake packet traffic around the source node, simultaneously with the transmission of real packets. Consequently, the adversary is tackled with multiple packets and finds it difficult to identify the exact immediate sender node of the real packets. Also, the adversary is tricked into back tracing the fake packet routes. As a result, adversary is steered away from the location of the real source node. Therefore, the adversary is obfuscated, the back tracing attack is made more complex, and long SP is achieved. However, similar to DissR, the SP of DistrR is significantly reduced at 900 rounds. The main reason for the reduced SP in DistrR is that, the number of candidate fake packet sources is highly dependent on the amount 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 experiments, a threshold value of 0.2 J was assumed. Since DistrR distributes a considerable amount of fake packet traffic in the network, many of the sensor nodes deplete their residual energy. When the number of rounds was increased, the residual energy of some of the sensor nodes became 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 SP was reduced.

To achieve significantly longer SP than the traditional PhanR protocol, the ReRR protocol creates random routing paths with high path diversity by employing the R_F and θ parameters during the route creation process. Also, to ensure high path diversity, ReRR generates three candidate *rNs* for each source node packet forwarding instance and randomly selects a *rN* based on the value of the R_F and θ. Therefore, it guarantees that the routing paths for successive packets are unpredictable to the adversary. Moreover, ReRR ensures the *rNs* and source nodes are located at least one R_{ring} section or *RR* away from each other. This ensures that the location of any *rN* is safeguarded at a safe distance away from the source nodes. As a result, the location information of the source nodes is not easily leaked to the adversary even after the adversary locates a *rN*. The adversary back tracing attack is made more complex. Hence, ReRR achieves significantly longer SP than the PhanR protocol.

To achieve long-term SLP protection, ReRR considers three aspects. (i) Packet transmission and reception are the most energy consuming tasks for the sensor nodes [29], [30]. (ii) Exhaustive energy consumption of the sensor nodes can result in short-term SLP protection [30]. (iii) DissR and DistrR protocols transmit large amounts of packet traffic in the network, resulting in high energy consumption and short-term SLP protection. Therefore, ReRR transmits a reduced amount of packet traffic in the network. Fig. 5 shows that beyond 850 rounds the ReRR protocol achieves long SP to outperform the other protocols.

2) CAPTURE RATIO

Capture ratio (CR) 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. Thus, the adversary must co-locate with the source node. To compute CR, equation (4) was assumed [30], [49].

$$CR = \frac{Number\ of\ experiments\ with\ located\ source}{Total\ number\ of\ experiments} \quad (4)$$

The CR and SP parameters have an inversely proportional relationship as shown in equation (5). When the SP of a protocol is maximized, the CR is minimized [30].

$$\max\,(SP) = \min\,(CR) \quad (5)$$

It is shown in Fig. 5 that below 600 rounds, the DissR and DistrR protocols are able to achieve significantly long SP to outperform the ReRR protocol. Therefore, in such conditions, it was interesting to investigate how the SLP performance of the protocols is affected when some of the network parameters are varied. Hence, the CR of the protocols was observed under varied sensor node residual energy, adversary hearing range, and number of sensor nodes.

The SLP performance of the DistrR protocol is affected by the amount of sensor node residual energy [30]. Therefore, we observed the CR of the protocols against varied sensor node residual energy. In the experiments, the threshold value for residual energy was 0.2 J. We observed the residual energy of 90% of the sensor nodes that were located within 6 hops from the source nodes. The source nodes were located at a source-sink distance of 35 hops. The results are shown in Fig. 6 (a). The results show that the ReRR protocol is able to achieve significantly lower levels of CR than the PhanR protocol. Furthermore, when the residual energy of the sensor nodes is below the threshold value, the ReRR protocol achieves significantly lower levels of CR than the DistrR protocol. The CR of the DistrR protocol is high

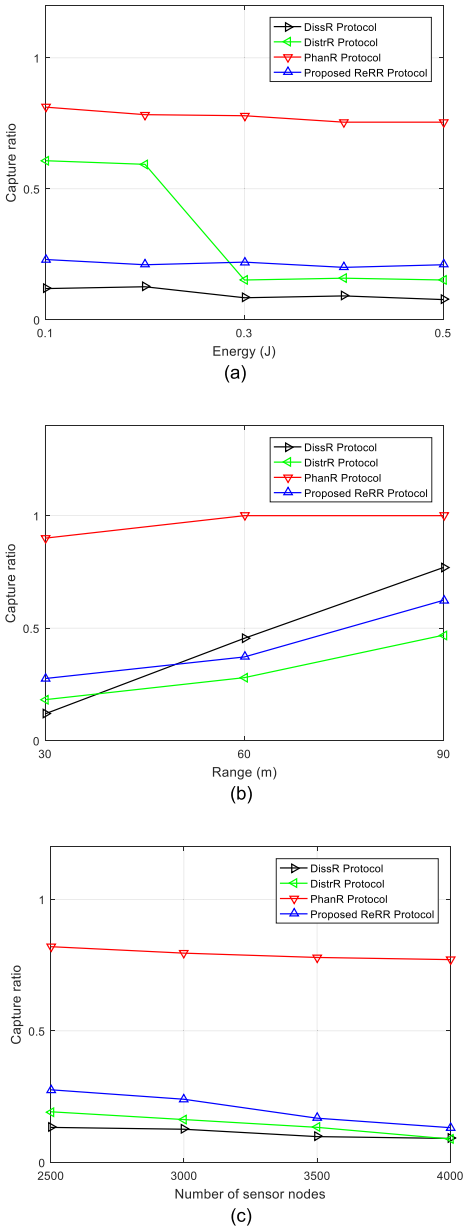

FIGURE 6. Privacy performance of the protocols. (a) Capture ratio against energy of sensor node. (b) Capture ratio against adversary hearing range. (c) Capture ratio against number of sensor nodes.

below the threshold value mainly because smaller numbers of fake packet sources were generated. Consequently, reduced amount of fake packet traffic was broadcasted and the adversary became less obfuscated. Therefore, the adversary was able to improve its attack success rate and high CR was achieved. Fig. 6 (a) also shows that DissR achieves lower CR than the other protocols. Moreover, the CR of DissR remains unchanged when the residual energy of the sensor nodes is varied.

The observations in Fig. 6 (a) suggest that when short-term SLP protection is considered, DissR is capable of achieving higher levels of SLP to outperform DistrR and ReRR even when the residual energy of the sensor nodes is varied. On the other hand, ReRR is capable of achieving higher levels of SLP to outperform DistrR when the residual energy of the sensor nodes is below the threshold value. However, DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.

In the experiments for the results in Fig. 6 (b), CR was observed under varied adversary hearing range. The adversary hearing range was varied between 30 and 90 m. The results show that for all the protocols, the CR increases with the increase in adversary hearing range. This is mainly due to the fact that the adversary becomes more powerful when it has a longer hearing range. The traffic analysis attacks become less complex when the adversary can hear a packet sent from a sensor node which is more than 1 hop distance away.

Fig. 6 (b) also shows that when the adversary hearing range is increased, the ReRR protocol is capable of achieving reduced CR to outperform the DissR protocol. The CR of ReRR increases at a slower rate than the CR of DissR mainly because ReRR ensures high path diversity by generating multiple candidate *rNs* for each source node packet forwarding instance. Moreover, the *rNs* and source nodes are located at least one R_{ring} section or *RR* away from each other to ensure the location of any *rN* is safeguarded at a safe distance away from the source nodes. As a result, the routing paths for successive packets are less predictable to the adversary and the location information of the source nodes is not easily leaked to the adversary. On the other hand, DissR isolates the real and fake source nodes and it does not distribute fake packets near the phantom nodes. Consequently, the adversary obfuscation effect between the phantom nodes and source nodes is reduced. Also, the location information of the source nodes is easily leaked to the adversary after the adversary locates a phantom node. Therefore, it becomes easy for the adversary to successfully locate the source nodes and the CR is increased.

Fig. 6 (b) also shows that although the CR of DistrR increases with the increase in adversary hearing range, DistrR maintains a low CR to outperform ReRR. DistrR is able to maintain low CR because it employs a different fake packet distribution strategy. Unlike DissR, DistrR does not isolate the real and fake source nodes. Furthermore, DistrR distributes fake packets near the phantom nodes. As a result, the adversary obfuscation effect is increased and low CR is maintained.

The observations in Fig. 6 (b) suggest that when short-term SLP protection is considered, DistrR is capable of achieving high levels of SLP to outperform DissR and ReRR even when the adversary hearing range is increased. On the other hand, ReRR is capable of achieving high levels of SLP to outperform DissR when the adversary hearing range is increased. However, both DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.

In the experiments for the results in Fig. 6 (c), CR was observed under varied number of sensor nodes. The number of sensor nodes in the network was varied between 2500 and 4000. Fig. 6 (c) shows that the CR for ReRR

TABLE 10. Energy consumption model parameters.

Parameter	Description	Value
E_I (J)	Initial energy of a sensor node	0.5
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

and DistrR tend to decrease when the number of nodes is increased. In ReRR, CR decreases mainly because the number of *rNs* increases with the increase in number of sensor nodes. When a large number of *rNs* is available, the path diversity can be improved to ensure the routing paths are unpredictable to the adversary and CR is reduced. Furthermore, the number of next-hop neighboring nodes at the source node can be increased with the increase in number of sensor nodes. Consequently, different next-hop node can be selected during the packet forwarding process to improve the path diversity.

As an example, if a source node has j next-hop neighboring nodes with shorter hop distance to *rN*, the probability that the source node will select a particular next-hop neighboring node during the directed random-walk is $1/j$. If *rN* has h next-hop neighboring nodes with shorter hop distance to the sink node, the probability that *rN* will select a particular next-hop neighboring node during the directed random-walk is $1/h$. Also, if u sensor nodes are available as *rNs*, the probability that a node will select a particular sensor node as a *rN* is $1/u$. Thus, there can be up to $j \times h \times u$ random routes between a source node and the sink node. Therefore, when the number of sensor nodes is increased, it results in improved path diversity and reduced CR. Similarly, in DistrR, when the number of sensor nodes is increased, it increases the probability of a higher number of candidate fake packet sources. When a large number of fake packet sources is generated, large amount of fake packet traffic is broadcasted to obfuscate the adversary. Consequently, the CR is reduced.

Fig. 6 (c) also shows that the CR of DissR does not vary very much when the number of sensor nodes is increased. This is due to the fact that DissR employs a probabilistic flooding mechanism and both fake and real packets are flooded with equal probability. When the number of sensor nodes is 4000, the CR of ReRR is approaching the CR of DissR.

The observations in Fig. 6 (c) suggest that when short-term SLP protection is considered, DistrR and DissR are capable of achieving high levels of SLP to outperform ReRR. Furthermore, the SLP protection of DistrR and ReRR improves with the increase in number of sensor nodes. Moreover, when the number of sensor nodes is increased, the level of SLP protection in ReRR tends to approach the level of SLP protection in DissR. However, DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.

C. ENERGY CONSUMPTION AND NETWORK LIFETIME

1) 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 [29], [30]. Therefore, energy consumption and energy efficiency of a protocol may be indicated by the amount of packet traffic that is transmitted in the network [50].

The energy consumption of the sensor nodes was computed using equations (6) and (7), based on the energy consumption model in [2], [14], [15], [29], [30], [39], [51]–[55]. 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 energy consumption for packet transmission is an exponential function of d. The model uses both, the free space (d^2 power loss) and the multi-path fading (d^4 power loss) channel models, depending on the distance between the transmitter and receiver. Power control can be used to invert the loss by appropriately setting the power amplifier. Thus, if the transmission distance is less than the threshold distance d_0, the power amplifier loss is based on the free-space model. Otherwise, the multi-path attenuation model is used. The d_0 is computed according to equation (8). E_{loss} is the transmitting circuit loss. E_{fs} and E_{amp} are the energy required by power amplification in the two power loss models. The energy parameter E_{loss} depends on factors such as modulation, coding, and filtering [2], [29], [55]. When the number of bits is increased, it increases the amount of energy dissipated in the electronics of the radio. Table 10 shows the energy consumption model parameters.

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

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

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

Fig. 7 shows the energy consumption of the protocols. In the experiments, source nodes were assumed at

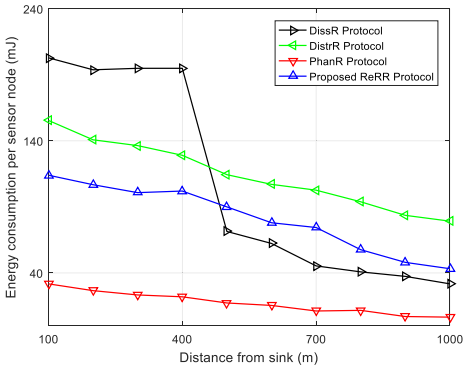

FIGURE 7. Energy consumption of the protocols.

different source-sink distances. Packets were sent from each source node to the sink node and the energy consumption per sensor node was computed. For the DissR protocol, the boundary of the blast ring was assumed at 400 m from the sink node. The results in Fig. 7 show that in the near-sink regions, the ReRR protocol incurs lower energy consumption than the DissR and DistrR protocols. ReRR incurs low energy consumption mainly because it distributes a reduced amount of packet traffic in the near-sink regions. In the case of DissR, both real and fake packets are flooded when the source nodes are located outside the blast ring. Therefore, DissR incurs the highest energy consumption in the near-sink regions. The DistrR protocol generates a significant amount of fake packet traffic throughout the network domain, depending on the location of the source nodes and phantom nodes. Based on the distribution of the fake packet traffic, DistrR is able to trick the adversary into back tracing the fake packet routes. Therefore, the adversary is steered away from the location of the real source nodes. Although this process ensures high levels of SLP protection in DistrR, it has a negative effect on the energy consumption performance. Consequently, DistrR incurs high energy consumption.

Fig. 7 also shows that the DissR protocol achieves unbalanced energy distribution. It shows that DissR incurs significantly lower energy consumption in the regions away from the sink node. The unbalanced energy distribution in DissR is due to the fact that the packet flooding mechanism is employed inside the blast ring regions. Outside the blast ring, the energy consumption of DissR is significantly reduced because the protocol distributes only one fake packet for each real packet.

In the energy-constrained WSNs, unbalanced energy distribution can seriously affect the operation of the network, resulting in inefficient energy consumption and limited network lifetime [1], [5], [7], [30]. Investigations on the energy efficiency and network lifetime are presented below.

2) ENERGY EFFICIENCY

To measure the energy efficiency of the protocols, we used the energy ratio parameter. We define the energy ratio (ER) as the ratio of the energy that is used in 600 rounds to the total energy. High ER corresponds to low energy efficiency.

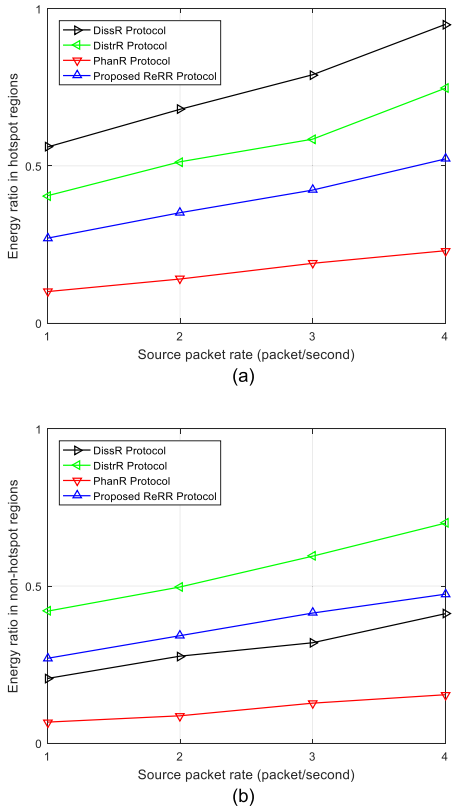

FIGURE 8. Energy efficiency of the protocols. (a) Energy ratio in hotspot regions. (b) Energy ratio in non-hotspot regions.

Based on Fig. 7, the protocols incur significantly higher energy consumption in the near-sink regions (hotspot regions) than in the away from sink node regions (non-hotspot regions). Therefore, the ER was computed for hotspot regions and non-hotspot regions as shown in Fig. 8. If the *ds* of a sensor node was <25 hops, the sensor node was considered to be located in hotspot regions. Otherwise, sensor node was in non-hotspot regions.

Fig. 8 shows the ER of the protocols at varied source packet rate. It shows that the ER of all the protocols tend to increase with the increase in source packet rate. Fig. 8 (a) shows that in the hotspot regions, the ReRR protocol incurs lower ER than the DissR and DistrR protocols while Fig. 8 (b) shows that the ReRR protocol has lower ER than the DistrR protocol in the non-hotspot regions. Furthermore, Fig. 8 shows that the ER of the ReRR protocol increases at a slower rate that the ER of the DissR and DistrR protocols. In the hotspot regions, the ER of DissR increases at a fast rate mainly because DissR floods a large amount of packet traffic. Therefore, when the packet rate is increased, more packets are generated per second and the ER is increased. Similarly, the ER of DistrR increases at a fast rate mainly because DistrR distributes large amounts of fake packet traffic throughout the WSN domain.

It was shown in [15], [30], [56] that high energy consumption of the sensor nodes in the hotspot regions can have a significant impact on the network lifetime. To maximize

the network lifetime, the energy consumption and ER of the sensor nodes in the hotspot regions must be minimized [30]. Investigations on the network lifetime of the protocols are presented below.

3) NETWORK LIFETIME

Network lifetime is the period between the start of the network operation and the first sensor node power outage [15], [30], [56].

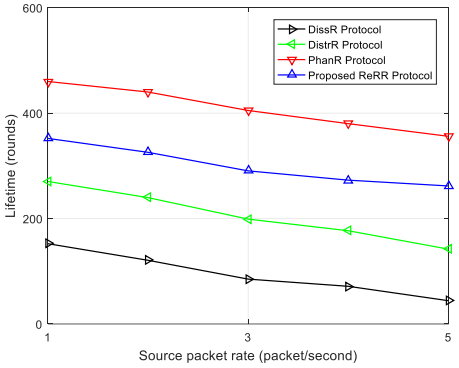

FIGURE 9. Network lifetime of the protocols.

The network lifetime was observed under varied source packet rate. Fig. 9 shows the results of the network lifetime analysis. The results show that the ReRR protocol achieves significantly long network lifetime to outperform the DissR and DistrR protocols. ReRR achieves significantly long network lifetime because it guarantees reduced ER in the hotspot regions. On the other hand, the DissR and DistrR protocols achieve limited network lifetime mainly due to the high ER in the hotspot regions as shown in Fig. 8 (a). The results also show that the network lifetime is affected by the source packet rate. When the packet rate is increased, more packets are generated per second, the ER is increased, and the network lifetime is reduced. At the source packet rate of 5 packets/second, the network lifetime of DissR is significantly reduced because DissR floods a large amount of packet traffic in the hotspot regions. Hence, high packet rate increases the ER and reduces the network lifetime.

D. SLP RELIABILITY

The investigations and analysis results in section V (B) have shown the SLP protection capability of the protocols in terms of SP and CR. Although some of the protocols are capable of achieving high levels of SLP protection, they may not be reliable in long-term monitoring due to their high energy consumption, high ER, and reduced network lifetime. Therefore, it is important to investigate the SLP reliability of the protocols. Moreover, since there are many factors influencing the functioning of WSNs, it is essential to obtain its working ability at any time [57], [58]. Also, it is important to quantify the degree to which the performance can meet the application-specific requirements [21].

According to [19], [21], [22], a reliability index for a WSN should quantitatively assess the ability of the network to perform its intended function. Although the SP and CR parameters are able to measure the magnitude of the SLP protection, they do not take into consideration the application-specific requirements for achieving the intended SLP protection. Thus, the SP and CR metrics fail to reflect whether or not the SLP protection can be maintained for a given period of time, such as a specified mission duration. Therefore, we propose a new approach to analyze the SLP reliability of the SLP protocols using equations (9), (10), (11).

In the equations, γ represents the SLP metric which is being analyzed. For example, γ may represent SP or CR. Two main values of γ are considered, the achieved γ (γ_{Ach}) and the application-specific required γ (γ_{Req}). The γ_{Ach} is the magnitude of γ that is achieved by the protocols, as shown section V (B). The γ_{Req} is according to the application-specific requirements. For example, some applications such as monitoring of endangered animals may specify a minimum γ_{Req} in terms of SP as 140 hops, throughout the mission duration. Meaning that throughout the mission duration, the protocols must guarantee that the achieved SP is greater than or equal to 140 hops.

In the equation (9), the γ realiability (R_γ) is computed. When $e^{\Delta_\gamma} \geq 1$, the R_γ becomes 1 to indicate that the γ_{Req} is achieved and SLP reliability is guaranteed. Otherwise, the R_γ becomes 0 to indicate that the γ_{Req} is not achieved and the SLP reliability is not guaranteed.

$$R_\gamma = \begin{cases} 1, & if\ e^{\Delta_\gamma} \geq 1 \\ 0, & otherwise. \end{cases} \tag{9}$$

where Δ_γ is the difference between the γ_{Ach} and γ_{Req}. Equation (10) is used to compute the Δ_γ.

$$\Delta_\gamma = \frac{\gamma_{Ach} - \gamma_{Req}}{\gamma_{Ave}} \tag{10}$$

where γ_{Ave} is the average of the γ_{Ach} and γ_{Req}. Equation (11) is used to compute the γ_{Ave}.

$$\gamma_{Ave} = \frac{\gamma_{Ach} + \gamma_{Req}}{2} \tag{11}$$

Therefore, we define the SLP reliability as the probability that the achieved level of SLP protection is greater than or equal to the minimum required level of SLP protection. In this study, we measure the SLP reliability in terms of safety period reliability (R_{SP}) and capture ratio reliability (R_{CR}). The R_{SP} and R_{CR} of the protocols are investigated below.

1) SAFETY PERIOD RELIABILITY

Safety period reliability (R_{SP}) is the probability that the achieved SP is greater than or equal to the minimum required SP. Based on equations (9), (10), (11), the R_{SP} was computed using equation (12).

$$R_{SP} = \begin{cases} 1, & if\ e^{\Delta_{SP}} \geq 1 \\ 0, & otherwise. \end{cases} \tag{12}$$

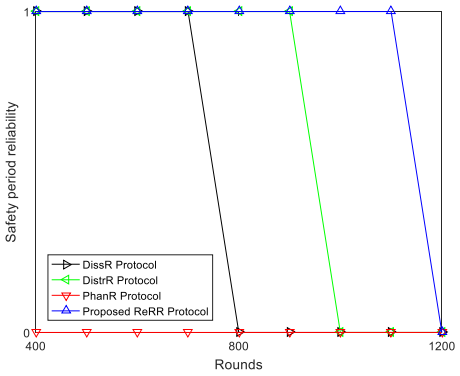

FIGURE 10. Safety period reliability of the protocols.

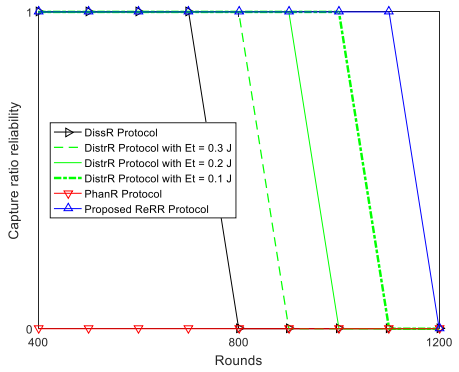

FIGURE 11. Capture ratio reliability of the protocols.

In the experiments, R_{SP} was observed for the mission duration of 1200 rounds. It was assumed that the minimum required SP was 140 hops. Fig. 10 shows the R_{SP} of the DissR, DistrR, PhanR, and ReRR protocols. It is shown that the DissR and DistrR protocols are able to achieve R_{SP} but only for few rounds. Beyond 900 rounds, both DissR and DistrR do not provide R_{SP}. The proposed ReRR protocol is capable of providing R_{SP} for more than 1000 rounds mainly because ReRR has lower ER and higher energy efficiency than DissR and DistrR. The traditional PhanR protocol does not provide the required R_{SP} mainly because it employs a simple routing algorithm that is not effective at obfuscating the adversary. The achieved SP of PhanR was below the required SP.

2) CAPTURE RATIO RELIABILITY

Capture ratio reliability (R_{CR}) is the probability that the achieved CR is less than or equal to the maximum required CR. Based on equations (9), (10), (11), the R_{CR} was computed using equation (13).

$$R_{CR} = \begin{cases} 1, & if\ e^{\Delta_{CR}} \geq 1 \\ 0, & otherwise. \end{cases} \tag{13}$$

In the experiments, R_{CR} was observed for the mission duration of 1200 rounds. It was assumed that the maximum required CR was 0.3. Fig. 11 shows the R_{CR} of the DissR, DistrR, PhanR, and ReRR protocols. It is shown that, similar to the R_{SP} performance, the ReRR protocol provides R_{CR} for longer durations to outperform the DissR and DistrR protocols. The proposed ReRR protocol is capable of providing R_{CR} for more than 1000 rounds mainly because ReRR has lower ER and higher energy efficiency than DissR and DistrR. Furthermore, as it was shown in Fig. 6 that the CR of DistrR can be affected by the amount of sensor node residual energy and the threshold value for residual energy, it was interesting to observe the R_{CR} of DistrR when the threshold value for residual energy (Et) is varied. Therefore, the Et was varied between 0.1 and 0.3 J. It is shown in Fig. 11 that DistrR provides R_{CR} for longer durations when the Et is reduced.

E. LIMITATIONS AND OPEN ISSUES

Although the proposed ReRR protocol achieves reduced energy consumption in the near-sink regions to outperform the DissR and DistrR protocols, ReRR has significantly higher energy consumption than the traditional PhanR protocol. To ensure a more flexible energy management, techniques such as integration of distributed energy resources (DERs) [16] may be considered. Thus, DERs may be integrated with the ReRR protocol. The integration of DERs into ReRR protocol remains an open issue and it will be considered in our future work. Furthermore, due to the location configuration of the relay regions, ReRR may incur long end-to-end delays and reduced packet delivery reliability. Therefore, in our future work, we will analyze the performance of ReRR in terms of end-to-end delay, packet delivery ratio, and delivery reliability.

VI. CONCLUSION

One of the main challenges in designing and developing WSNs and SLP routing protocols is satisfying their strict reliability requirements. Therefore, this article considers the techniques for achieving reliable SLP protection in monitoring WSNs. Limitations of two fake packet-based SLP protocols are identified. A new ReRR protocol is proposed to address the limitations of the fake packet-based protocols. To achieve high levels of SLP protection, the ReRR protocol provides multiple candidate relay nodes for each source node and randomly selects one relay node based on the value of the randomization factor and node offset angles. Furthermore, ReRR generates multiple relay ring sections and relay regions between source nodes and relay nodes. As a result, the location of any relay node is safeguarded. The configuration of ReRR guarantees that the location information of the source nodes is not leaked to the adversary even after the adversary locates a relay node. Moreover, the routing paths for successive packets have high path diversity. Therefore, the adversary is effectively obfuscated and strong SLP protection is achieved.

It is observed that exhaustive energy consumption of the sensor nodes and unbalance energy distribution result in less reliable SLP protection. Therefore, unlike the fake packet-based protocols, ReRR ensures improved energy efficiency and reliable SLP protection. Analysis results demonstrate

the superiority of the ReRR protocol. Moreover, a novel approach is presented to measure the SLP reliability of the protocols. It is demonstrated through experimental evaluation that the proposed ReRR protocol is capable of satisfying the reliability requirements to outperform the fake packet-based protocols. Finally, the limitations of ReRR protocol are highlighted as open issues for further research.

REFERENCES

[1] J. Zhang, J. Tang, and F. Wang, "Cooperative relay selection for load balancing with mobility in hierarchical WSNs: A multi-armed bandit approach," *IEEE Access*, vol. 8, pp. 18110–18122, Jan. 2020.

[2] O. J. Pandey and R. M. Hegde, "Low-latency and energy-balanced data transmission over cognitive small world WSN," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7719–7733, Aug. 2018.

[3] X. Liu and J. Wu, "A method for energy balance and data transmission optimal routing in wireless sensor networks," *Sensors*, vol. 19, no. 13, p. 3017, Jul. 2019.

[4] M. Adil, R. Khan, J. Ali, B. H. Roh, Q. T. Ta, and M. A. Almaiah, "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163209–163224, Aug. 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] X. Fu, Y. Yang, and O. Postolache, "Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 168–181, Jan. 2021.

[7] L. Tang, Z. Lu, and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks," *Appl. Sci.*, vol. 10, no. 5, p. 1885, Mar. 2020.

[8] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in WSNs based on path extension," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 461–471, Oct. 2014.

[9] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.

[10] 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, May 2019.

[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] 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.

[13] M. Kamarei, A. Patooghy, A. Alsharif, and V. Hakami, "SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy," *IEEE Access*, vol. 8, pp. 33818–33829, Feb. 2020.

[14] 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.

[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, Jul. 2014.

[16] Z. Xiong, H. Wang, L. Zhang, T. Fan, and J. Shen, "A ring-based routing scheme for distributed energy resources management in IIoT," *IEEE Access*, vol. 8, pp. 167490–167503, Sep. 2020.

[17] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5527–5538, Aug. 2020.

[18] C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 20, p. e5304, Oct. 2019.

[19] S. Chakraborty, N. K. Goyal, S. Mahapatra, and S. Soh, "Minimal path-based reliability model for wireless sensor networks with multistate nodes," *IEEE Trans. Rel.*, vol. 69, no. 1, pp. 382–400, Mar. 2020.

[20] S. Lata, S. Mehfuz, S. Urooj, and F. Alrowais, "Fuzzy clustering algorithm for enhancing reliability and network lifetime of wireless sensor networks," *IEEE Access*, vol. 8, pp. 66013–66024, Apr. 2020.

[21] S. Xiang and J. Yang, "Reliability evaluation and reliability-based optimal design for wireless sensor networks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1752–1763, Jun. 2020.

[22] W. Sun, X. Yuan, J. Wang, Q. Li, L. Chen, and D. Mu, "End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial WSNs," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 3, pp. 1127–1137, Jul. 2018.

[23] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. L. Sun, "Reliability-oriented single-path routing protocols in wireless sensor networks," *IEEE Sensors J.*, vol. 14, no. 11, pp. 4059–4068, Nov. 2014.

[24] I. Al-Anbagi, M. Erol-Kantarci, and H. T. Mouftah, "A survey on cross-layer quality-of-service approaches in WSNs for delay and reliability-aware applications," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 525–552, 1st Quart., 2016.

[25] Y. Duan, W. Li, X. Fu, Y. Luo, and L. Yang, "A methodology for reliability of WSN based on software defined network in adaptive industrial environment," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 1, pp. 74–82, Jan. 2018.

[26] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.

[27] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: A survey," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1243–1256, Nov. 2012.

[28] J. Long, M. Dong, K. Ota, A. Liu, and S. Hai, "Reliability guaranteed efficient data gathering in wireless sensor networks," *IEEE Access*, vol. 3, pp. 430–444, May 2015.

[29] 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.

[30] L. C. Mutalemwa and S. Shin, "Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques," *IEEE Access*, vol. 8, pp. 76935–76950, Apr. 2020.

[31] 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, 2018.

[32] 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.

[33] 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, Oct. 2018.

[34] Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, "SPS and DPS: Two new grid-based source location privacy protection schemes in wireless sensor networks," *Sensors*, vol. 19, no. 9, p. 2074, May 2019.

[35] 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.

[36] M. Bradbury, M. Leeke, and A. Jhumka, "Hybrid online protocols for source location privacy in wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 115, pp. 67–81, May 2018.

[37] 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, May 2019.

[38] P. K. Roy, J. P. Singh, P. Kumar, and M. P. Singh, "Source location privacy using fake source and phantom routing (FSAPR) technique in wireless sensor networks," *Procedia Comput. Sci.*, vol. 57, pp. 936–941, Jan. 2015.

[39] 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.

[40] 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.

[41] 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.

[42] 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.
[43] Y. Wang, L. Liu, and W. Gao, "An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks," *Symmetry*, vol. 11, no. 5, p. 632, May 2019.
[44] 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.
[45] N. Wang and J. Zeng, "All-direction random routing for source-location privacy protecting against parasitic sensor networks," *Sensors*, vol. 17, no. 3, p. 614, Mar. 2017.
[46] Y. Liu, J.-S. Fu, and Z. Zhang, "K-nearest neighbors tracking in wireless sensor networks with coverage holes," *Pers. Ubiquitous Comput.*, vol. 20, no. 3, pp. 431–446, Jun. 2016.
[47] 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.
[48] R. A. Shaikh, H. Jameel, B. J. D'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, Feb. 2010.
[49] 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.
[50] 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.
[51] 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.
[52] 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.
[53] 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.
[54] 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.
[55] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.
[56] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, p. 724, Mar. 2017.
[57] H. Feng and J. Dong, "Reliability analysis for WSN based on a modular k-out-of-n system," *J. Syst. Eng. Electron.*, vol. 28, no. 2, pp. 407–412, Apr. 2017.
[58] L. Xing, "Reliability in Internet of Things: Current status and future perspectives," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6704–6721, Aug. 2020.

LILIAN C. MUTALEMWA received the B.Eng. degree in telecommunications engineering from the University of Essex, U.K., in 2008, and the M.Sc. degree in mobile and satellite communications from the University of Surrey, 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 WSN protocol design and performance evaluation, the IoT, and 5G networks.

SEOKJOO SHIN (Member, IEEE) 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. He spent 2009, as a Visiting Researcher with Georgia Tech, USA. His research interests include wireless communication systems and network security and privacy.