Received: 26 Aug 2023 | Revised: 23 Oct 2023 | Accepted: 06 Nov 2023 | Published: 29 Nov 2023
Volume 1(2) Pages 52-70 DOI: https://doi.org/10.56279/jicts.v1i2.50

JICTS
Journal of ICT Systems

Location Privacy Protection and Coverage Hole Effects in Event Monitoring Wireless Networks for Internet of Things Applications

Lilian C. Mutalemwa

Department of Mathematics and Information Communication Technology, The Open University of Tanzania, Tanzania

Corresponding author
Email: lilian.mutalemwa@out.ac.tz

Funding information

This study was supported by the Open University of Tanzania.

Keywords

Source location privacy
Wireless sensor network
Traffic analysis attacks
Coverage hole
Internet of Things

Abstract

Source-location privacy (SLP) protection improves security in event monitoring wireless sensor networks (WSNs) for Internet of Things (IoT) applications. However, due to constrained energy resources, WSNs incur coverage holes that affect the level of SLP protection. Existing studies have ineffectively analysed the effects of coverage holes on SLP protection. Noting the limitation, this study investigated the coverage hole effects. Performance of various SLP routing protocols was evaluated based on the sensor node utilization ratio, attack success rate, end-to-end delay, and packet delivery ratio. Then, considering the challenge of limited battery power in IoT sensors, the performance gains and limitations of the protocols were identified. Simulation results demonstrate that the data dissemination SLP routing protocol (DIRP) outperforms other protocols. However, the performance of DIRP is significantly affected by coverage holes. The results suggest that for DIRP to be viable in IoT applications, the integration of distributed energy resources should be considered.

1. Introduction

Sensor-based monitoring networks play a vital role in the Internet of Things (IoT) applications. The networks deploy sensor nodes that detect events and report sporadically to a sink node. The sink node collects data from the sensor nodes and reports it to the user [1, 2] . However, the sensor nodes are often resource-constrained, size-constrained, and lack physical protection [3, 4]. Sensor nodes are usually powered by energy-limited batteries and have constrained capabilities

for computing, storage, and communication [5]. Furthermore, when wireless sensor networks (WSNs) are deployed in remote and inaccessible areas, the sensor nodes are often randomly distributed in the sensing field of interest, resulting in unbalanced energy distribution [5]. Due to the unbalanced energy distribution, some of the sensor nodes expend their battery power quickly and coverage holes occur [5, 6]. Coverage hole is a disconnected region in a WSN where sensor nodes are unable to communicate due to sensor node power outage or node failure [6]. WSNs incur poor network connectivity and reduced quality of service (QoS) when coverage holes occur [7, 8].

This study investigated the effects of coverage holes on source location privacy (SLP) protection. The main objective of SLP protection is to improve security in monitoring WSNs by minimizing the observability of source nodes and hiding the location of source nodes from adversaries [9, 10]. Therefore, techniques such as SLP routing protocols are particularly important to provide SLP protection when WSNs are used in monitoring applications that require location privacy [11-13].

This study was inspired by Jan et al. [14], Roy et al. [15], Long at al. [16], and Mutalemwa and Shin [17]. Collectively, these authors did not investigate the effects of coverage holes. Long at al. [16] analysed the performance of the tree-based diversionary SLP routing protocol (TRRP) and phantom SLP routing protocol (PNRP). However, the authors did not evaluate the end-to-end delay (EED) and packet delivery ratio (PDR) of the protocols. Also, the attack success rate (ASR) was not effectively analysed. Roy et al. [15] presented the operational features of the SLP protocol with distributed fake and phantom sources (DFRP). However, the authors did not evaluate the performance of DFRP. Thus, Roy et al. [15] failed to analyse the ASR, EED, and PDR of DFRP. Jan et al. [14] evaluated the data dissemination routing protocol (DIRP), TRRP, and PNRP using various performance metrics. However, the authors failed to present detailed discussions on the performance of the protocols in terms of ASR, EED, and PDR. Mutalemwa and Shin [17] analysed DIRP, DFRP, relay node ring routing protocol (RRRP), and PNRP. Nevertheless, they failed to observe the ASR, EED, and PDR of the protocols. Therefore, to ensure a comprehensive performance analysis of the DIRP, DFRP, TRRP, and RRRP protocols, this study presents detailed investigations on the performance of the protocols.

In the investigations, the performance of DIRP, DFRP, TRRP, and RRRP protocols was measured in terms of SLP protection, EED, and PDR. The ASR metric was used to measure SLP protection. Different from the previous studies, this study analysed the ASR, EED, and PDR under varied network parameters. Also, the effects of unbalanced energy distribution and coverage holes were observed.

The main contributions of this study are highlighted as follows:

- Conduct experiments to evaluate the performance of DIRP, DFRP, TRRP, and RRRP protocols. Consider different network configurations to ensure comprehensive analysis.
- Investigate the effects of unbalanced energy distribution and coverage holes on the performance of DIRP, DFRP, TRRP, and RRRP protocols. Then, based on the observations, examine the feasibility of DIRP, DFRP, TRRP, and RRRP protocols for IoT applications.
- Outline the performance gains and limitations of DIRP, DFRP, TRRP, and RRRP protocols. Subsequently, considering the challenge of limited battery power in IoT sensors, present techniques to alleviate the coverage hole effects.

2. Related Work

SLP protection was first discussed by Ozturk et al. [18]. Since then, a lot of research has been done on SLP protocols [10, 12, 13, 19-35], with some works considering SLP protection for IoT applications. Other studies have proposed SLP protocols for cyber-physical systems [21, 23].

Table 1 summarizes the key differences between this study and the previous studies in [14-17] and highlights the significance of this study. The Table shows that ASR was partially considered by Long et al. [16] while Jan et al. [14], Roy et al. [15], and Mutalemwa and Shin [17] did not measure the ASR. In this study, ASR was measured under varied source-sink distance and node density. Also, ASR was measured at different packet generation rates and varied network size. Moreover, the ASR was observed when the adversary hearing range and mission duration was increased. In addition, ASR was observed when multiple source nodes were deployed. Table 1 provides additional information that the EED and PDR were partially considered by Jan et al. [14] while the other authors did not consider the EED or PDR metrics [15-17]. This study considers measurement of the EED under varied network parameters. Also, the PDR is measured under varied source packet rate and at different mission durations. EED and PDR are important parameters because they indicate the packet delivery reliability of the protocols.

Energy consumption (EC) and network lifetime (NL) of the protocols have been extensively studied [16, 17]. Therefore, this study focused on the measurement of node utilization ratio (NUR). The knowledge of NUR is useful during the analysis of coverage hole effects. On the contrary, NUR was not measured in [14-17].

3. Method

MATLAB network simulation tool was used to conduct experiments. Details of the network and adversary models are presented below.

3.1 Network Model for Simulations

The panda-hunter network model was used. The model was proposed by the seminal work of Ozturk et al. [18] and considered in many other studies [11, 16, 17, 22, 24, 41-44].

3.2 Adversary Model for Simulations

Table 1. Comparison with existing studies

Study	Protocols	Performance metrics					
		ASR	EED	PDR	EC	NL	NUR
[16]	TRRP, PNRP	Partial	No	No	Yes	Yes	No
[15]	DFRP	No	No	No	No	No	No
[14]	DIRP, TRRP, PNRP	No	Partial	Partial	Yes	Partial	No
[17]	DIRP, DFRP, RRRP, PNRP	No	No	No	Yes	Yes	No
This study	DIRP, DFRP, RRRP, TRRP, PNRP	Yes	Yes	Yes	No	No	Yes

A cautious traffic analyzing adversary model was adopted from [18, 45-48]. The main attack strategy of the adversary is hop-by-hop back tracing attack shown in Figure 1. In the figure, adversary is able to backtrack the packet routes. For example, adversary locating at the sink node can overhear communication from S_3. At IN_{13}, it overhears communications from S_{40} and at S_2, it overhears communications from SN_J. When it overhears communications between sensor nodes, it performs hop-by-hop back tracing attack until it reaches at the source node to capture the event/target.

4. Experiments

In the experiments, the performance of DIRP, DFRP, RRRP, TRRP, and PNRP was measured. Similar to Adil et al. [49], this study assumed that efficient utilization of the resources in the resource-constrained WSNs increases the network effectiveness and QoS. Therefore, NUR should be considered when designing SLP protocols for the resource-constrained WSNs and IoT. NUR is a good indicator of how the protocols are able to balance the network traffic and energy consumption of the sensor nodes, so as to minimize the occurrence of coverage holes. This is mainly because unbalanced energy distribution has a negative effect on the reliability of the protocols in terms of network lifetime and privacy protection reliability [17].

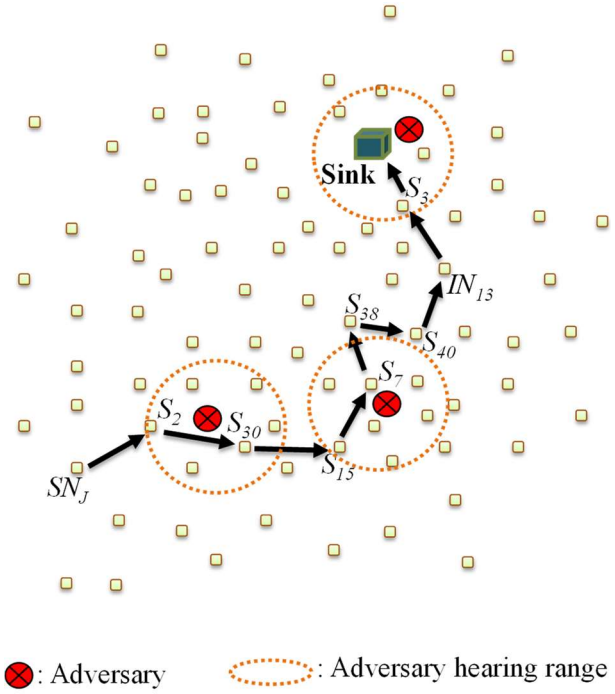


Figure 1. Back tracing attack of traffic analyzing adversary.

Furthermore, the occurrence of coverage hole presents negative effects on the QoS in WSNs and IoT [50]. In particular, coverage hole affects the packet delivery reliability in terms of EED and PDR. Therefore, in the analysis, the NUR, EED, and PDR were measured. Moreover, the ASR was measured to observe the SLP performance of the protocols. It was assumed that high NUR corresponds to high probability that sensor nodes end up exhausting their battery power and incur power outage. Thus, high NUR results in the presence of sensor nodes with power outage (SPO). Therefore, for each protocol, the number of SPO was observed. It is important to note that the PNRP is a traditional protocol. Hence, PNRP was included in the analysis as a baseline protocol, for comparative analysis.

The equations below were used to compute the NUR, SPO, ASR, PDR, and EED. Equation (1) was adopted from [36], (3) from [51], (4) from [52], [53], and (5) from [52], [53]. Description of the parameters used in the equations are presented in Table 2.

$$NUR = \frac{N_{PN}}{N_T} \quad (1)$$

$$SPO = N_{NBP} \quad (2)$$

$$ASR = \frac{N_{SA}}{N_{TA}} \quad (3)$$

$$PDR = \frac{P_{Rec}}{\sum_{i=1}^{n} P_{Trans_i}} \quad (4)$$

$$EED = \frac{\sum_{i=1}^{P_{Rec_i}} (T_{Rec_i} - T_{Trans_i})}{P_{Rec}} \quad (5)$$

4.1 Simulation Environment

The parameters used in the simulations are summarized in Table 3. MATLAB simulation environment was used to simulate the network. Similar to Mutalemwa and Shin [17], a network with a side length of 2000 m was simulated. Good network coverage was achieved when 3000 sensor nodes were randomly distributed.

5. Results and Discussions

Table 2. Parameters used for computation in (1), (2), (3), and (4)

Parameter	Description
N_{PN}	Number of sensor motes participating in data transmission for 300 rounds.
N_T	Total number of sensor motes.
N_{NBP}	Number of sensor motes with no battery power after a duration of packet transmission.
N_{SA}	Number of successful adversary attacks.
N_{TA}	Total number of attempts to attack by the traffic analyzing adversary.
P_{Rec}	Total number of data packets that are received by the sink node successfully.
P_{Trans}	Number of packets that were sent by the source nodes.
n	Number of source nodes.
T_{Rec}	The time that sinks node receives a data packet.
T_{Trans}	The time that a data packet is sent from a source node.

Table 3. Network simulation parameters

Parameter	Value
Network side length (m)	2000
Number of sensor nodes	3000
Number of sink nodes	1
Sensor node communication range (m)	40
Adversary hearing range (m)	40
Adversary waiting timer (source packets)	4
Initial location of the adversary	Near the sink node
Event monitoring technique	*k*-nearest neighbor tracking
Size of packet (bit)	1024
Packet generation rate (packet/second)	Varied between 1 and 4
Sensor mote initial energy (J)	0.5

5.1 Node Utilization Ratio

The technique to compute NUR by Han et al. [36] was used. High NUR corresponds to increased number of SPO and coverage hole which affects the level of SLP protection.

It was observed that the DIRP and TRRP protocols distribute different amount of traffic load in different regions of a WSN. Thus, both DIRP and TRRP incurred unbalanced energy distribution. Therefore, NUR was measured for hotspot regions (near the sink node) and non-hotspot regions (away from the sink node) as shown in Figure 2.

Figure 2 shows that NUR of the protocols increases with the source packet rate. This is caused by the increased packet traffic. Therefore, many packet routes are created to route the packets, and

the NUR increases. Furthermore, it was observed that when large amount of dummy traffic was generated or packet flooding mechanism was employed, the protocols created many routing paths. Consequently, NUR increased.

Figure 2 (a) shows that the NUR of DIRP and DFRP are significantly high. This is mainly because DIRP employs fake sources at a distance and floods packets in the hotspot regions. Also, it is shown that the NUR of DFRP is high and it increases rapidly. This is caused by the fact that DFRP employs many fake sources that distributes large amounts of dummy traffic which results in high NUR. On the other hand, the NUR of RRRP is low because it deploys fewer packets.

When the performance of TRRP was investigated, it was observed that TRRP deployed a small amount of packet traffic in the hotspot regions. Therefore, TRRP incurred low NUR in the hotspot regions. However, the routing algorithm of TRRP guaranteed that large amount of dummy traffic was distributed in non-hotspot regions. Therefore, TRRP incurred significantly high NUR in the non-hotspot regions.

When comparing the NUR of RRRP and TRRP in the hotspot regions, the NUR of RRRP was higher. The higher NUR of RRRP occurred because RRRP employs random relay nodes which are strategically positioned in the relay ring regions. It was observed that, due to the strategic position of the relay nodes, the routing paths of RRRP were longer than the routing paths of TRRP in the hotspot regions. When the routing paths were longer, the number of hops in the packet transmission increased. Consequently, the NUR of RRRP increased.

Figure 2 (a) and Figure 2 (b) indicate that the NUR varies in the hotspot and non-hotspot regions, especially for the DIRP and TRRP protocols. This confirms that DIRP and TRRP have unbalanced energy distribution. For DFRP, high NUR is incurred in both hotspot and non-hotspot regions. High NUR corresponds to an increased number of SPO and coverage hole, which affects the level of

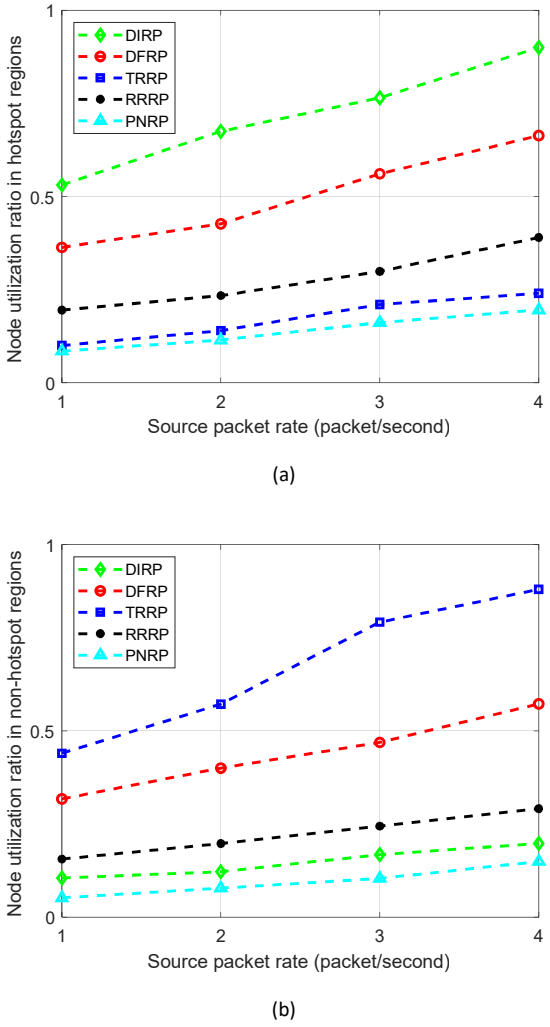


Figure 2. (a) NUR in the hotspot regions. (b) NUR in the non-hotspot regions.

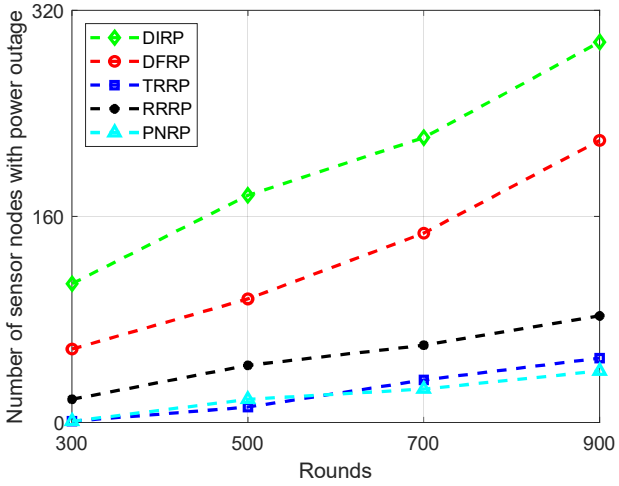
SLP protection. Therefore, the observations in Figure 2(a) and Figure 2(b) suggest that SPO and coverage holes are likely to occur in DIRP, TRRP, and DFRP before they occur in RRRP. For DIRP, SPO and coverage hole are likely to occur first in the hotspot regions. In the case of TRRP, SPO and coverage hole are likely to occur first in the non-hotspot regions. Also, the results suggest that the SLP performance of DIRP, TRRP, and DFRP is more likely to be affected by coverage holes.

5.2 Sensor Nodes with Power Outage

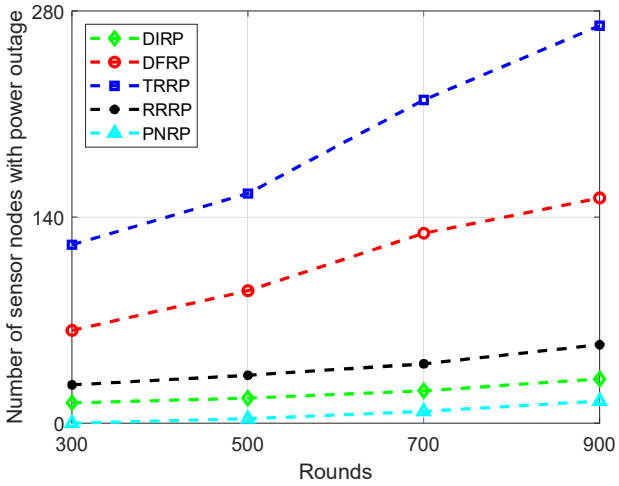
When the mission duration for a WSN is prolonged, high NUR causes large number of SPO

and coverage holes which affects the effectiveness and reliability of WSNs [49]. Mutalemwa and Shin [17] presented that performance of SLP protocols is significantly affected when large number of SPO occurs. In this study, experiments were done to observe the number of SPO in DIRP, DFRP, RRRP, and TRRP.

Figure 3(a) shows that, in hotspot regions, DIRP incurs the largest number of SPO, followed by DFRP. These results coincide with the results in Figure 2 (a) which show that DIRP incurs the highest NUR, followed by DFRP. These observations confirm that high NUR corresponds to large number of SPO in the network. Conversely, Figure 3(b) shows that, in non-hotspot regions, TRRP presents the largest number of SPO, followed by DFRP. These results coincide with the observations in Figure 2 (b) which show that, in non-hotspot regions, TRRP incurs the highest NUR, followed by the DFRP.



(a)



(b)

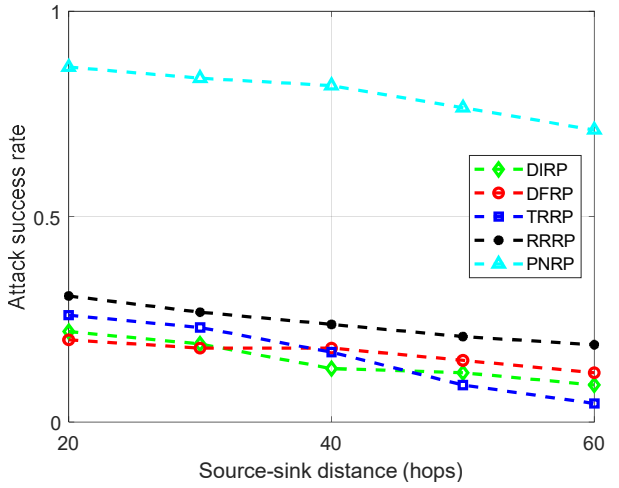
Figure 3. (a) Number of SPO in the hotspot regions. (b) Number of SPO in the non-hotspot regions.

5.3 Attack Success Rate

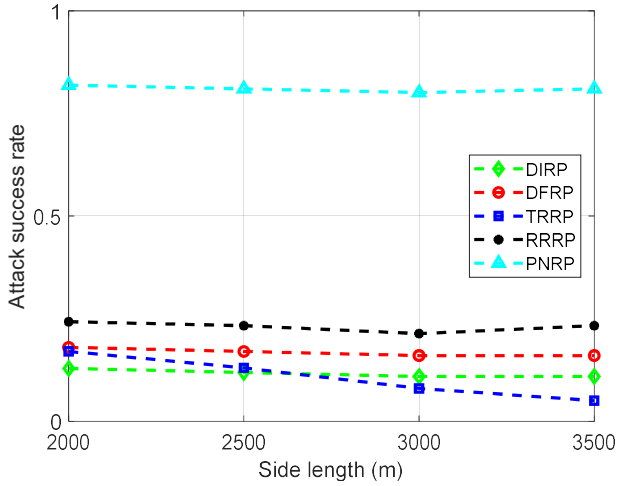
SLP protection was measured using the ASR metric. The technique to compute ASR was adopted from Mutalemwa and Shin [51]. Low ASR indicates strong SLP protection.

Figure 4 shows the ASR for DIRP, DFRP, RRRP, TRRP, and PNRP protocols. Figure 4 (a) shows the ASR at different source-sink distances. It is shown in Figure 4 (a) that the ASR is considerably lower for DIRP, DFRP, RRRP, and TRRP than the ASR for the traditional PNRP protocol. Thus, the level of SLP protection in DIRP, DFRP, RRRP and TRRP is significantly high. The ASR decreased when the distance between source node and sink node was increased. The cause for this observation was that path diversity increased at longer source-sink distances. When the path diversity was high, the routing paths became more obfuscating to the adversary and the ASR was hindered. For example, at 40 hops, the DIRP protocol created long and isolated routing paths. Then, it flooded real and dummy traffic. Therefore, the adversary was effectively obfuscated and low ASR was achieved. When the source-sink distance was short, DIRP flooded only real packets. As a result, the adversary obfuscation effect was reduced and the level of ASR increased.

Figure 4(b) shows the ASR when the network size was varied. It is shown in Figure 4 (b) that the ASR for DIRP, DFRP, RRRP, and PNRP did not vary significantly when the side length was changed. This was mainly because the configuration of the routing paths and the level of



(a)

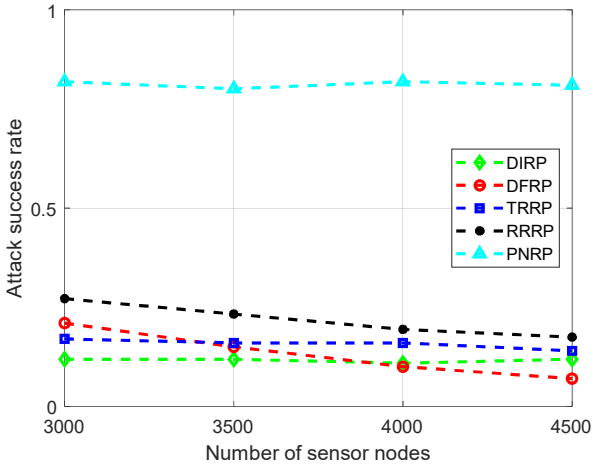


(b)

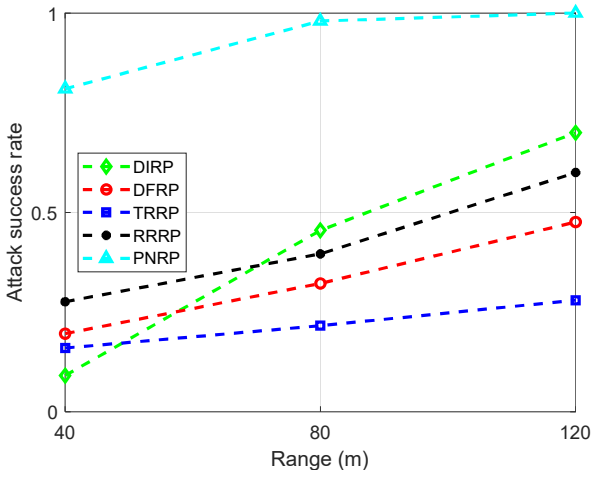
Figure 4. (a) ASR at different source-sink distances. (b) ASR for different network sizes.

adversary obfuscation remained the same. Consequently, ASR incurred an insignificant change. On the other hand, for TRRP, the configuration of the routing paths and the level of adversary obfuscation changed significantly. As a result, the ASR of TRRP was significantly reduced at longer network side lengths. Thus, the TRRP protocol provides higher levels of SLP protection when the network size is increased.

Figure 5(a) shows that the ASR for DIRP and TRRP incurred insignificant change when the node density was increased. However, for DFRP and RRRP, the ASR decreased. Furthermore, during the experiments, it was interesting to measure the ASR at different adversary hearing range because it was observed that the adversary became more powerful when its hearing range was long. Figure 5(b) shows that, at the hearing range of 120 m, the adversary was able to eavesdrop on the communication of the sensor nodes at a longer distance. Results from Figure



(a)



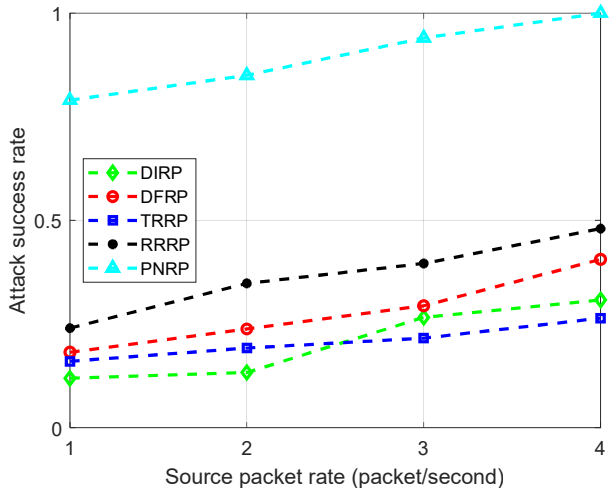
(b)

Figure 5. (a) ASR against varied nodes density. (b) ASR when adversary hearing range was varied.

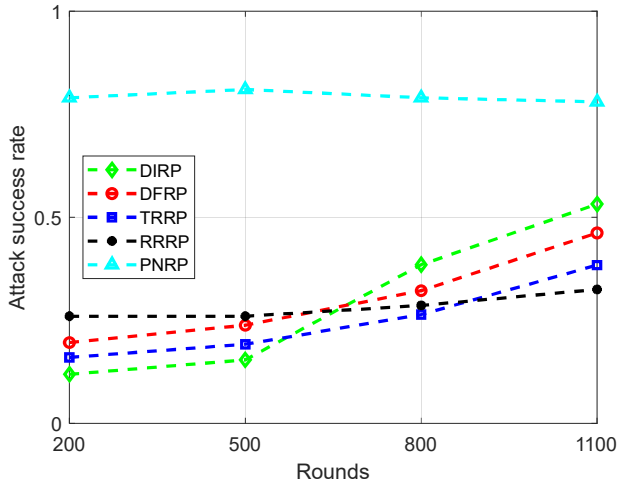
5(b) indicate that the ASR for all the protocols increased when the adversary hearing range was increased. Thus, with a longer hearing range, the adversary became more powerful and it improved its ASR. At the adversary hearing range of 80 m, the ASR for the baseline PNRP was almost 100%. Figure 5(b) also shows that the ASR for DIRP increased rapidly. The fast increase was due to the fact that the routing algorithm of DIRP provided weak adversary obfuscating effect at the phantom nodes. The increase in the ASR for DFRP was slow because, unlike DIRP, DFRP provided strong adversary obfuscating effect at the phantom nodes. Also, the increase in the ASR for RRRP was slower than for DIRP because RRRP guaranteed high path diversity, which increased the obfuscation of the adversary and hindered the ASR. The ASR for TRRP increased at a slow rate because TRRP generated many fake hotspots in the diversionary routes and near the phantom nodes. The diversionary routes were diverted to the network border regions. Consequently, the obfuscation of the adversary increased and the ASR was hindered.

The ASR for DIRP, DFRP, RRRP, TRRP, and PNRP increased when the packet rate was increased, as shown in Figure 6 (a). This was because more packets were generated and the adversary captured an increased number of successive packets to allow more successful back tracing attacks, thereby increasing the ASR. In addition, Figure 6 (a) shows that the ASR for DIRP incurred a significant change. The main reason for the variation was that, in some scenarios, the adversary could locate the phantom node. When that happened, the ASR increased because DIRP does not obfuscate the adversary effectively at the phantom node.

Figure 6 (b) shows the ASR at different mission durations (rounds). It was observed that the ASR for DIRP, DFRP, and TRRP increased. On the other hand, the ASR for RRRP and PNRP incurred less significant change. This was because DIRP, DFRP, and TRRP incurred high NUR (Figure 2).



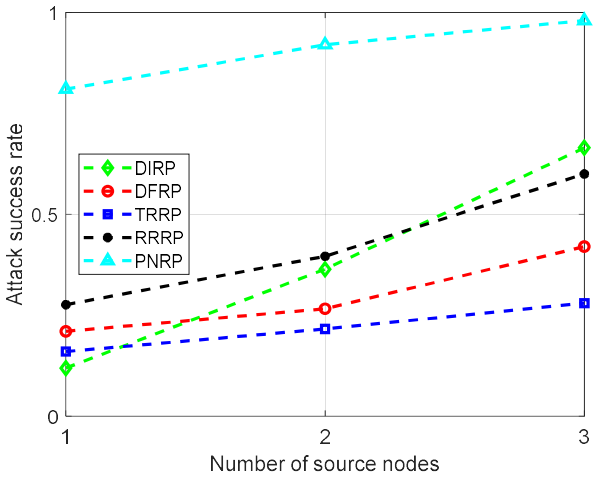
(a)



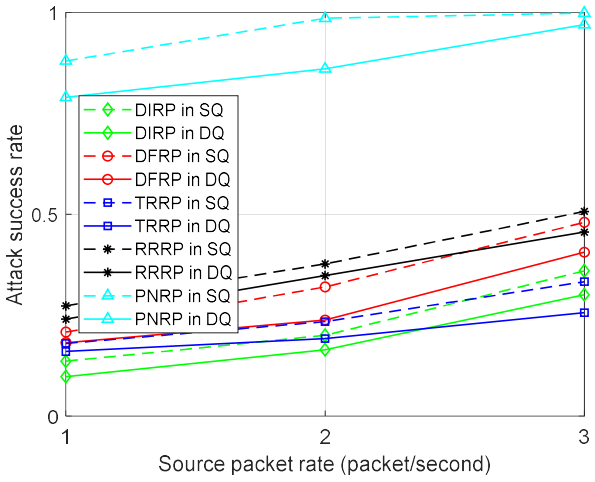
(b)

Figure 6. (a) ASR at different packet generation rates. (b) ASR at different number of rounds.

Also, DIRP, DFRP, and TRRP incurred large number of SPO (Figure 3). At 1100 rounds, DIRP, DFRP, and TRRP incurred large number of SPO. Therefore, the effectiveness of DIRP, DFRP, and TRRP was significantly reduced and the ASR increased. The ASR in RRRP and PNRP incurred less significant change because RRRP and PNRP have reduced NUR (Figure 2). Also, RRRP and PNRP incurred a reduced number of SPO (Figure



(a)



(b)

Figure 7. (a) ASR when the number of source nodes per event is varied. (b) ASR at different source packet rates for scenarios SQ and DQ.

3). Figure 6(b) shows that, at 1100 rounds, RRRP ensured the lowest ASR. Thus, at 1100 rounds, RRRP outperformed the other protocols in terms of SLP protection because it had low NUR and fewer SPO.

Figure 6(b) indicates that DIRP, DFPR, and TRRP can provide strong SLP protection. However, the SLP protection of DIRP, DFPR, and TRRP is short-term due to a large number of SPO. The presence of a large number of SPO indicates the occurrence of coverage holes. These results suggest that the privacy performance of DIRP, DFPR, and TRRP is affected by coverage holes. Furthermore, it is shown that, although RRRP provides lower levels of SLP protection when compared with DIRP, DFPR, and TRRP, RRRP outperforms DIRP, DFPR, and TRRP in terms of long-term SLP protection.

Based on the observations in Figure 6(b), it can be suggested that, when it is possible to supplement the sensor nodes with energy resources to ensure fewer number of SPO, DIRP is a better option. This is mainly because DIRP is capable of achieving very low ASR if the number of SPO is controlled. However, if energy of the sensor nodes is a limited resource, RRRP is a better option. This is because RRRP provides long-term SLP protection and maintains acceptable ASR.

It was observed that DIRP was capable of achieving the best performance when the number of SPO was controlled. However, one challenge remains open: DIRP provides weak obfuscation effect at the location of the phantom nodes. As a result, it is easy for the adversary to improve its ASR after it discovers the location of the phantom nodes. The challenge was more obvious in the experimental results depicted by Figure 5(b) and Figure 6(a).

In another experiment, the number of source nodes per event was varied and the ASR was observed. Figure 7(a) shows that the ASR of DIRP, DFRP, RRRP, TRRP, and PNRP increased. The increase in ASR was mainly because, when the number of source nodes was increased, the amount of packet traffic around the event location was also increased. Therefore, the event location became an obvious hotspot region, which enabled the adversary to improve its ASR.

In addition, an increased number of source nodes resulted in an increase in the packet traffic and the NUR. As shown in the discussions above, higher NUR increases the number of SPO. When large

number of SPO occurs, the ASR increases. Figure 7(a) shows that the ASR for DIRP increased more significantly. The increase was because DIRP located the real source node far away from the fake source nodes. Therefore, increased number of source nodes and packet traffic made the event location more obvious to the adversary. The results in Figure 7 (a) suggest that, to provide strong SLP protection, it is important to regulate the number of source nodes per event.

More experiments were done to observe the ASR when multiple events occurred at different locations. Two events were computed at different locations in the WSN domain. A single source node was deployed per event. As shown in Figure 8, the network was partitioned into four quadrants: Q_1, Q_2, Q_3, and Q_4. For the experiment results in Figure 7(b), two scenarios were considered: when source nodes were positioned in the same quadrant (SQ) and when source nodes were located in different quadrants (DQ). In Figure 8, source nodes SN_E and SN_L are located in Q_1. Source node SN_H is located in Q_2 while SN_I is in Q_4. Figure 7(b) shows the average ASR for DIRP, DFRP, RRRP, TRRP, and PNRP for scenario SQ and DQ. Similar observations were made in Figure 6(a). Furthermore, Figure 7(b) shows that, for all the protocols, the ASR was higher in scenario SQ. This is due to the fact that in scenario SQ, the real packet traffic was concentrated in one region of the network. As a result, the region became an obvious hotspot region and the adversary improved its ASR by focusing its back tracing attack in one region.

In the scenario DQ, the ASR for DIRP was slightly lower because, when probabilistic flooding was employed, the packets arrived at the sink node from opposite sides. Therefore, the adversary was obfuscated more effectively and lower ASR was achieved in the DQ scenario. In DFRP and TRRP, the ASR in scenario SQ was higher because when multiple sources were located in the same quadrant and the source packet rate was increased, the effects

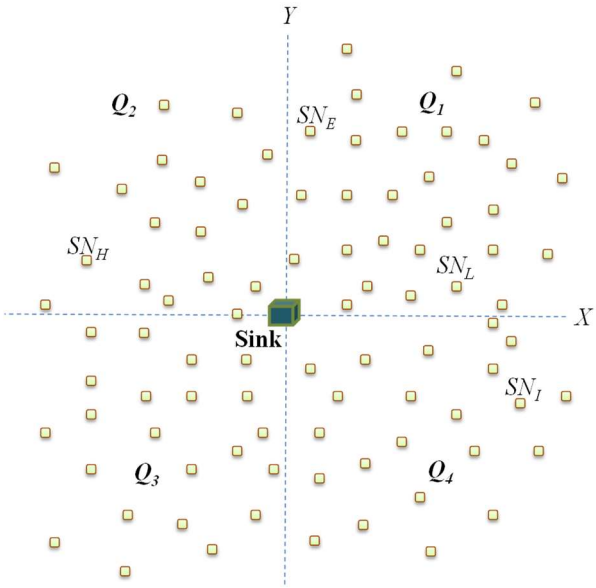
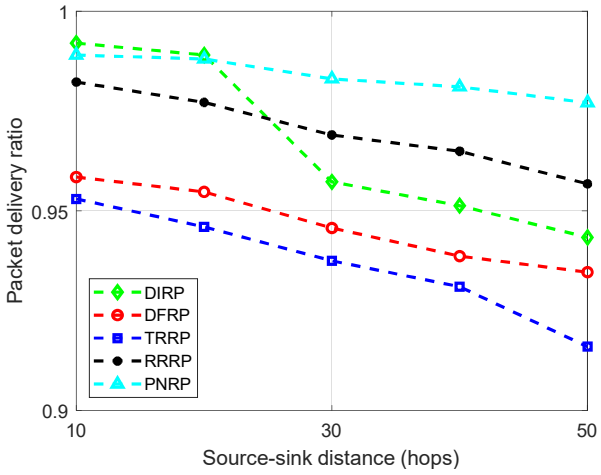


Figure 8. Division of the WSN domain.

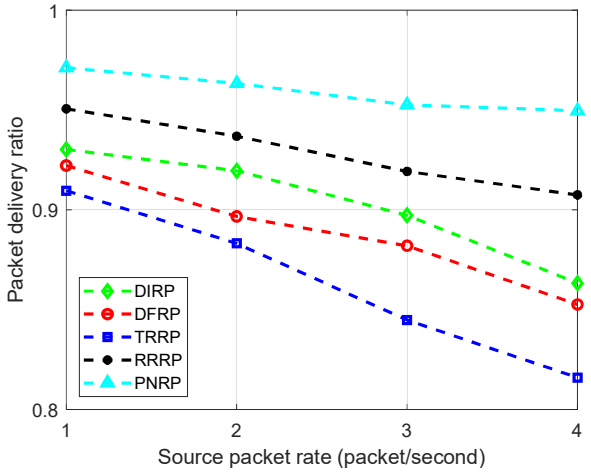
of unbalanced energy distribution and high NUR became more impactful. TRRP maintained low ASR. For RRRP protocol, the ASR in scenario DQ was lower than in scenario SQ.

5.4 Packet Delivery Ratio

The technique to compute PDR was adopted from Khan et al. [52] and Fotue et al. [53]. Figure 9(a) shows that, as the source-sink distance was increased, the PDR decreased. In scenarios where the transmission distance was long, the packet loss events increased, hence decreasing the PDR. It was also observed that DFRP and TRRP achieved significantly lower PDR than the traditional PNRP protocol because DFRP and TRRP experienced many packets collision events which resulted in packet loss. For the same reason, there was a faster decrease in PDR of DFRP and TRRP as shown in Figure 9(b). Furthermore, Figure 9(a) shows a significant change in the PDR of DIRP between 20 and 30 hops. The significant change in PDR of DIRP was because DIRP used the flooding mechanism inside the blast ring which ensured high PDR. In regions not covered by the blast ring, the



(a)



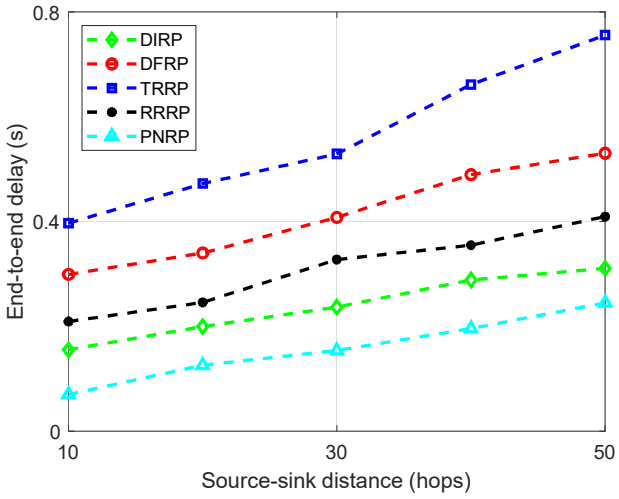
(b)

Figure 9. (a) PDR at different distances between source and sink nodes. (b) PDR against varied packet generation rate.

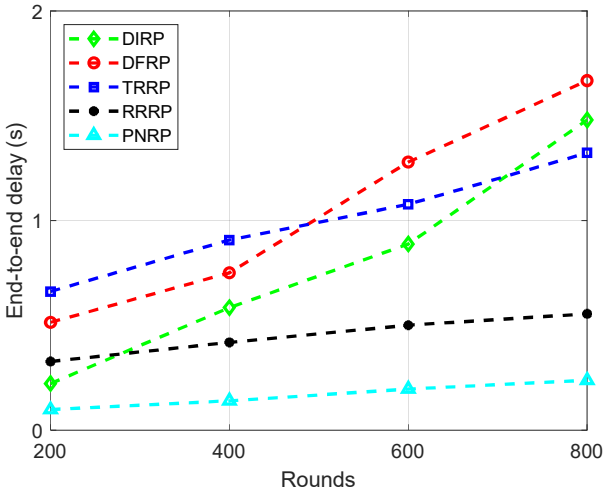
PDR was reduced. The PDR of RRRP was significantly higher than the PDR of DFRP, and TRRP mainly because RRRP incurred fewer events of packet loss.

As it is shown in Figures 2 and 3, NUR and the number of SPO increased when packets were generated at a high rate. The presence of SPO results in poor network connectivity and reduced PDR, as shown in Figure 9(b). As the source packet rate was increased, DIRP, DFRP and TRRP incurred large number of SPO and reduced PDR. However, DIRP could provide higher PDR than DFRP and TRRP because it employed packet flooding mechanism. The RRRP achieved higher PDR than DIRP and DFRP because it incurred fewer number of SPO and fewer packet loss events.

5.5 End-to-End Delay.



(a)



(b)

Figure 10. (a) EED at different source-sink distances. (b) EED at different number of rounds.

To measure the EED, the equations by Khan et al. [52] and Fotue et al. [53] were considered. Figure 10 shows the experiment results. Figure 10 (a) shows that the EED increased when the distance from source to sink nodes increased. The EED for TRRP and DFRP was relatively long. DIRP achieved lower EED than DFRP and TRRP. RRRP achieved longer EED than DIRP because RRRP created long and dynamic routing paths which resulted in long EED. The EED was also measured at different durations (rounds). Figure 10(b) shows that the EED increased when the number of rounds was high. The increase in the EED of DIRP, DFRP, and TRRP was high because DIRP, DFRP, and TRRP had high NUR and incurred large number of SPO. At a packet generation rate of 4 packet/second, the NUR and number of SPO increased significantly. Consequently, coverage holes occurred, the network experienced poor connectivity, and the EED increased.

6. Summary

QoS requirements in mission-critical event monitoring applications include security, coverage and connectivity [54]. Furthermore, coverage and connectivity are good performance indicators in WSNs [7, 50]. Table 4 summarizes the observations from section 5. It also outlines the limitations of the protocols and highlights the reasons for the limitations. It was observed that the performance of DIRP, DFRP, and TRRP was affected by high NUR, large number of SPO, and coverage holes. The observations in Table 4 suggest that DIRP is a better protocol for IoT applications because it can perform significantly better if the challenge of SPO is addressed.

7. Recommendations

There are various techniques to supplement energy resources and control the number of SPO in WSNs [20], [55-59]. Xiong et al. [20] presented that distributed energy resources (DERs) are becoming increasingly popular in IoT to address the challenges of limited energy resource. New technologies and lower costs promote the deployment of DERs [20, 60, 61]. Solar-powered DERs provide flexible energy management to prolong the network lifetime, reduce the number of SPO, and effectively preserve the SLP [20]. Therefore, DERs may be considered to improve the viability of the protocols for IoT applications, especially the DIRP protocol. Moreover, energy-harvesting WSNs (EH-WSNs) may be considered to improve the performance of SLP protocols for IoT applications. Artificial Intelligence-based EH-WSNs present mechanisms to address SPO challenges for IoT applications [62].

8. Conclusion

SLP is crucial when sensor-based IoT networks are deployed for monitoring applications that require privacy protection. This study presents a comprehensive performance analysis of SLP protocols. In the analysis, the challenges of limited energy resource in IoT sensors, unbalanced energy distribution, and coverage hole were explored. Experiment results reveal that the DIRP protocol achieves good performance to outperform the DFRP, TRRP, RRRP, and PNRP protocols in terms of ASR, EED, and PDR. However, to achieve the good performance, DIRP tradeoffs the efficiency in power consumption. Thus, DIRP is energy inefficient. Also, DIRP is prone to coverage hole effects. The results suggest that DIRP may present better performance if the integration of DERs is considered.

Table 4. Summary of the observations

Protocol	Limitation	Causes of the limitation
DIRP	• Very high NUR in hotspot regions. • Large number of SPO in hotspot regions. • ASR increases rapidly in long mission durations. • Short-term SLP protection. • Reduced PDR when source nodes are not inside the flooding regions. • EED increases at an accelerated rate when the mission duration is prolonged.	• Flooding of real and dummy packet traffic in the blast ring. • Large number of SPO in hotspot regions. • Floods only real packet traffic when packet generating node is near the sink but floods both real and dummy traffic when the node is away from sink node. • Large number of SPO in hotspot regions which result in poor connectivity between source node and sink.
DFRP	• Very high NUR in hotspot regions and high NUR in non-hotspot regions. • Large number of SPO in hotspot and non-hotspot regions. • ASR increases rapidly in long mission durations. • Short-term SLP protection. • Reduced PDR at high source packet rate. • EED increases rapidly when the mission duration is prolonged.	• Broadcasts large amount of dummy traffic. • Large number of SPO in hotspot and non-hotspot regions. • Many events of packet retransmissions due to collisions and loss of packets. • Large number of SPO in hotspot and non-hotspot regions which result in poor connectivity between source node and sink.
TRRP	• Very high NUR in non-hotspot regions. • Large number of SPO in non-hotspot regions. • ASR increases at an accelerated rate in long mission durations. • Short-term SLP protection. • Reduced PDR. • EED increases when the mission duration is prolonged.	• Distribution of a significant amount of dummy traffic in non-hotspot regions. • Large number of SPO in non-hotspot regions. • Broadcasts a significant amount of packet traffic which result in packet collision, loss, and retransmissions. • Large number of SPO in non-hotspot regions which result in poor connectivity between source node and sink.
RRRP	• In many scenarios, ASR is higher than in DIRP, DFRP, and TRRP.	• Does not distribute dummy traffic therefore adversary is less obfuscated.
PNRP	• High ASR.	• PNRP is a traditional protocol that provides weak SLP protection.

ACKNOWLEDGEMENT

Special thanks to the Open University of Tanzania for providing the facilities to conduct this study.

CONTRIBUTIONS

Lilian C. Mutalemwa	[ORCID: 0000-0003-4342-5562]	Conceived the idea, carried out the simulations, analysed the results, and wrote the manuscript.

REFERENCES

[1] Pokhrel, S. R. S., Garg, V. S., Sharma, A. K., Choi, J., *An efficient clustering framework for massive sensor networking in industrial internet of things*, IEEE Trans. Ind. Inf., **17**(7): p. 4917–4924, 2021.

[2] Li, D., Yu, W., Xu, H., Zhang, L., *Low reliable and low latency communications for mission critical distributed industrial internet of things*, IEEE Commun. Lett., **25** (1): p. 313–317, 2021.

[3] Wang, M., Zhu, L., Yang, L. T., Lin, M., Deng, X., Yi, L., *Offloading-assisted energy-balanced IoT edge node relocation for confident information coverage*, IEEE Internet Things J., **6**(3): p. 4482–4490, 2019.

[4] Zhang, Q., Zhang, K., *Protecting location privacy in iot wireless sensor networks through addresses anonymity*, Security and Communication Networks, **2022:** p. 1–12, 2022.

[5] Deng, X., Xu, M., Yang, L. T., Lin, M., Yi, L., Wang, M., *Energy balanced dispatch of mobile edge nodes for confident information coverage hole repairing in IoT*, IEEE Internet Things J., **6**(3): p. 4782–4790, 2019.

[6] Sharma, P., Singh, R. P., *Energy-efficient deterministic approach for coverage hole detection in wireless underground sensor network: Mathematical model and simulation*, Computers, **11**(6): p. 86, 2022.

[7] Philco, L. O., Marrone, L., Estupiñan, E., *MiA-CODER: A multi-intelligent agent-enabled reinforcement learning for accurate coverage hole detection and recovery in unequal cluster-tree-based QoSensing WSN*, Applied Sciences, **11**(23): p. 11134, 2021.

[8] Bhat, S. J., Santhosh, K. V., *A localization and deployment model for wireless sensor networks using arithmetic optimization algorithm*, Peer-to-Peer Netw. Appl., **15**(3): p. 1473–1485, 2022.

[9] Wang, N., Fu, J., Li, J., Bhargava, B. K., *Source-location privacy protection based on anonymity cloud in wireless sensor networks*, IEEE Trans. Inform. Forensic Secur., **15**: p. 100–114, 2020.

[10] Mutalemwa, L. C, Shin, S., *Secure routing protocols for source node privacy protection in multi-hop communication wireless networks*, Energies, **13**(2): p. 292, 2020.

[11] Gu, C., Bradbury, M., Jhumka, A., *Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks*, Concurrency Computat Pract Exper, **31**(20): 2019.

[12] Shukla, A., Singh, D., Sajwan, M., Kumar, M., Kumari, D., Kumar, A., Panth, M., *SLP-RRFPR: A source location privacy protection scheme based on random ring and limited hop fake packet routing for wireless sensor networks*, Multimed Tools Appl, **81**(8): p. 11145–11185, 2022.

[13] Gutiérrez-Soto, C., Galdames, P., Faúndez, C., Durán-Faúndez, C., *Location-query-privacy and safety cloaking schemes for continuous location-based services*, Mobile Information Systems, **2022**: p. 1–22, 2022.

[14] Jan, N., Al-Bayatti, A., Alalwan, N., Alzahrani, A., *An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP)*, Sensors, **19**(9): p. 2050, 2019.

[15] Roy, P. K., Singh, J. P., Kumar, P., Singh, M. P., *Source location privacy using fake source and phantom routing (FSAPR) Technique in Wireless Sensor Networks*, Procedia Computer Science, **57**: p. 936–941, 2015.

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

[17] Mutalemwa, L. C., Shin, S., *Novel approaches to realize the reliability of location privacy protocols in monitoring wireless networks*, IEEE Access, **9**: p. 104820–104836, 2021.

[18] Ozturk, C., Zhang, Y., Trappe, W., *Source-location privacy in energy-constrained sensor network routing*, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004, p. 88–93.

[19] Mutalemwa, L., Shin, S., *Strategic location-based random routing for source location privacy in wireless sensor networks*, Sensors, **18**(7): p. 2291, 2018.
[20] Xiong, Z., Wang, H., Zhang, L., Fan, T., Shen, J., *A ring-based routing scheme for distributed energy resources management in IIoT*, IEEE Access, **8**: p. 167490–167503, 2020.
[21] Hong, Z., Wang, R., Ji, S., Beyah, R., A*ttacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems*, IEEE Trans. Inform. Forensic Secur., **14**(5): p. 1337–1350, 2019.
[22] Wang, Q., Zhan, J., Ouyang, X., Ren, Y., *SPS and DPS: Two new grid-based source location privacy protection schemes in wireless sensor networks*, Sensors, **19**(9): p. 2074, 2019.
[23] Roy, P. K., Singh, S. K., *Privacy preserving monitoring protocol for cyber–physical system*, Computers and Electrical Engineering, **102**: p. 108232, 2022.
[24] Jiang, J., Han, G., Wang, H., Guizani, M., *A survey on location privacy protection in Wireless Sensor Networks*, Journal of Network and Computer Applications, **125**: p. 93–114, 2019.
[25] Mutalemwa, L. C., Shin, S., *Routing schemes for source location privacy in wireless sensor networks: A survey*, *kics*, **43**(9): p. 1429–1445, 2018.
[26] Conti, M., Willemsen, J., Crispo, B., *Providing source location privacy in wireless sensor networks: A survey*, IEEE Commun. Surv. Tutorials, **15**(3): p. 1238–1280, 2013.
[27] Bushnag, A., Abuzneid, A., Mahmood, A., *Source anonymity against global adversary in wsns using dummy packet injections: A survey*, Electronics, **7**(10): p. 250, 2018.
[28] Bradbury, M., Jhumka, A., Leeke, M., *Hybrid online protocols for source location privacy in wireless sensor networks*, Journal of Parallel and Distributed Computing, **115**: p. 67–81, 2018.
[29] Ma,D., Kong, D., Chen, X., Zhang, L., Yuan, M., *Robot location privacy protection based on Q-learning particle swarm optimization algorithm in mobile crowdsensing*, Front. Neurorobot., **16**: p. 981390, 2022.
[30] Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., Zhang, J., *Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing*, IEEE Trans. Ind. Inf., **18**(9): p. 6290–6299, 2022.
[31] Chinnu, C. M., Gayathri, K. M., Reeja S. R., *Hybrid optimization enabled routing protocol for enhancing source location privacy in wireless sensor networks*, IJCNA, **10**(1): p. 51, 2023.
[32] Kumar, G., Rathore, R. S., Thakur, K., Almadhor, A., Biabani, S. A. A., Chander, S., *Dynamic routing approach for enhancing source location privacy in wireless sensor networks*, Wireless Netw., **29**: p. 2591–2607, 2023.
[33] Alkanjr, B., Mahgoub, I., *Location privacy-preserving scheme in iobt networks using deception-based techniques*, Sensors, **23**(6): p. 3142, 2023.
[34] Tian, X., Du, X., Wang, L., Zhao, L., Han, D., *LSLPR: A layering and source-location-privacy-based routing protocol for underwater acoustic sensor networks*, IEEE Sensors J., **23**(19): p. 23676–23691, 2023.
[35] Mutalemwa, L., *On the use of wireless technologies for wildlife monitoring: Wireless sensor network routing protocols*, TJET, **42**(2): p. 113–133, 2023.
[36] Han, G., Wang, H., Miao, X., Liu, L., Jiang, J., Peng, Y., *A dynamic multipath scheme for protecting source-location privacy using multiple sinks in wsns intended for IIoT*, IEEE Trans. Ind. Inf., **16**(8): p. 5527–5538, 2020.
[37] Wang, H., Wu, L., Zhao, Q., Wei, Y., Jiang, H., *Energy balanced source location privacy scheme using multibranch path in WSNs for IoT*, Wireless Communications and Mobile Computing, **2021**: p. 1–12, 2021.
[38] Shukla, A., Singh, D., Sajwan, Verma, M., A., Kumar, A., *A source location privacy preservation scheme in WSN-assisted IoT network by randomized ring and confounding transmission*, Wireless Netw., **28**(2): p. 827–852, 2022.
[39] Hussain, T., Yang, B., Rahman, H. U., Iqbal, A., Ali, F., Shah, B., *Improving source location privacy in social internet of things using a hybrid phantom routing technique*, Computers & Security, **123**: p. 102917, 2022.

[40] Han, G., Wang, H., Guizani, M., Chan, S., Zhang, W., *KCLP: A k-means cluster-based location privacy protection scheme in WSNs for IoT*, IEEE Wireless Commun., **25**(6): p. 84–90, 2018.
[41] Jan, N., Khan, S., *Energy-efficient source location privacy protection for network lifetime maximization against local eavesdropper in wireless sensor network (EeSP)*, Trans Emerging Tel Tech., **33**(2): 2022.
[42] Wang, H., Han, G., Zhang, W., Guizani, M., Chan, S., *A probabilistic source location privacy protection scheme in wireless sensor networks*, IEEE Trans. Veh. Technol., **68**(6): p. 5917–5927, 2019.
[43] Li, Y., Ren, J., Wu, J., *Quantitative measurement and design of source-location privacy schemes for wireless sensor networks*, IEEE Trans. Parallel Distrib. Syst., **23**(7): p. 1302–1311, 2012.
[44] Mutalemwa, L. C., Shin, S., *Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques*, IEEE Access, **8**: p. 76935–76950, 2020.
[45] Chen, H., Lou, W., *From nowhere to somewhere: Protecting end-to-end location privacy in wireless sensor networks*, International Performance Computing and Communications Conference, 2010, p. 1–8.
[46] Wang, Y., Liu, L., Gao, W., *An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks*, Symmetry, **11**(5): p. 632, 2019.
[47] Mutalemwa, L., Shin, S., *Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing*, Sensors, **19**(5): p. 1037, 2019.
[48] Kamat, P., Zhang, Y., Trappe, W., Ozturk, C., *Enhancing source-location privacy in sensor network routing*, 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), 2005, pp. 599–608.
[49] Adil, M., Khan, R., Ali, J., Roh, B.-H., Ta, Q. T. H., Almaiah, M. A., *An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment*, IEEE Access, **8**: p. 163209–163224, 2020.
[50] Han, B., Ran, Li, F., Yan, J., L., Shen, H., Li, A., *A novel adaptive cluster based routing protocol for energy-harvesting wireless sensor networks*, Sensors, **22**(4): p. 1564, 2022.
[51] Mutalemwa, L. C., Shin, S., *Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks*, IEEE Access, **7**: p. 140169–140181, 2019.
[52] Khan, M. F., Felemban, E. A., Qaisar, S., Ali, S., *Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs)*, 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, 2013, p. 324–329.
[53] Fotue, D., Labiod, H., Engel, T., *Controlled data collection of mini-sinks for maximizing packet delivery ratio and throughput using multiple paths in wireless sensor networks*, 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), 2012, p. 758–764.
[54] Thomas, D., Shankaran, R., Orgun, M. A., Mukhopadhyay, S. C., *SEC ^{2}: A secure and energy efficient barrier coverage scheduling for wsn-based iot applications*, IEEE Trans. on Green Commun. Netw., **5**(2): p. 622–634, 2021.
[55] Al-Tous, H., Barhumi, I., *Differential Game for resource allocation in energy harvesting wireless sensor networks*, IEEE Trans. on Green Commun. Netw., **4**(4): p. 1165–1173, 2020.
[56] Hou, L., Tan, S., Zhang, Z., Bergmann, N. W., *Thermal energy harvesting wsns node for temperature monitoring in IIoT*, IEEE Access, **6**: p. 35243–35249, 2018.
[57] Diez, P. L., Gabilondo, I., Alarcon, E., Moll, F., *Mechanical energy harvesting taxonomy for industrial environments: Application to the railway industry*, IEEE Trans. Intell. Transport. Syst., **21**(7): p. 2696–2706, 2020.
[58] Li, N., Xiao, M., Rasmussen, L. K., Hu, X., Leung, V. C. M., *On resource allocation of cooperative multiple access strategy in energy-efficient industrial internet of things*, IEEE Trans. Ind. Inf., **17**(2): p. 1069–1078, 2021.

[59] Song, C., Lu, P., Shen, S., *Highly efficient omnidirectional integrated multiband wireless energy harvesters for compact sensor nodes of internet-of-things*, IEEE Trans. Ind. Electron., **68**(9): p. 8128–8140, 2021.
[60] Alharbi, W., Bhattacharya, K., *Flexibility provisions from a fast charging facility equipped with DERs for wind integrated grids*, IEEE Trans. Sustain. Energy, **10**(3): p. 1006–1014, 2019.
[61] Valinejad, J., Marzband, M., Korkali, M., Xu, Y., Al-Sumaiti, A. S., *Coalition formation of microgrids with distributed energy resources and energy storage in energy market*, Journal of Modern Power Systems and Clean Energy, **8**(5): p. 906–918, 2020.
[62] Al-Tous, H., Barhumi, I., *Reinforcement learning framework for delay sensitive energy harvesting wireless sensor networks*, IEEE Sensors J., **21**(5): p. 7103–7113.