Achieving Reliability of Privacy-preserving Phantom Routing Protocols in Multi-hop Wireless Sensor Networks

Lilian C. Mutalemwa

The Open University of Tanzania, Dar es Salaam, Tanzania

https://doi.org/10.26636/jtit.2024.3.1703

Abstract — Due to the open nature of wireless channels and sensor node resource constraints, it is challenging to secure the communication in wireless sensor networks (WSNs) while simultaneously protecting the privacy of node location data. Therefore, a significant amount of research focusing on source location privacy (SLP) protocols has been conducted. The amount of research on SLP reliability, meanwhile, is insignificant. This study explores the operational features of various privacy-preserving phantom routing protocols and simulates WSNs with varied network configurations to investigate how different routing strategies affect SLP reliability. Safety period and capture ratio metrics are used to compute SLP reliability. Simulation results show that integration of phantom routing with fake packet distribution mechanisms adversely impacts SLP reliability. SLP reliability decreases also as the number of fake packet sources increases. Research proves that a protocol with many fake packet sources achieves SLP reliability for a mission duration of 940 rounds, while a protocol with no fake packet sources achieves SLP reliability for 1658 rounds.

Keywords — phantom routing, privacy preservation, reliability, source location privacy, wireless sensor network

1. Introduction

Wireless sensor networks (WSNs) employ multi-hop wireless communication mechanisms. Due to the open nature of wireless channels and limited resources available in sensor nodes, they also pose a number of challenges related to the application of WSNs [1]–[4]. For example, due to the absence of a secure infrastructure, it is challenging to preserve the locations privacy of critical sensor nodes, such as source nodes [2], [5], [6].

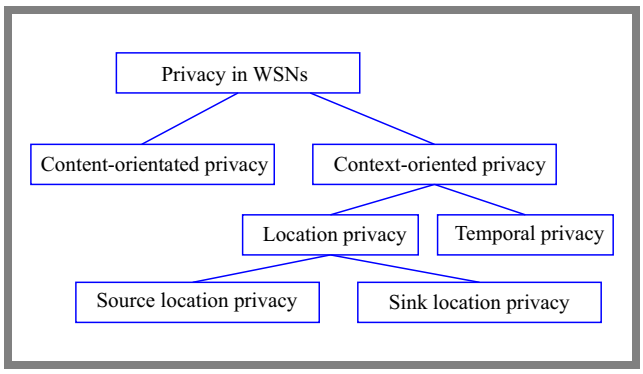

Fig. 1. Classification of privacy in WSNs.

To address this challenge, much research has been conducted on the topics of security and privacy in WSNs. This study focuses on source location privacy (SLP) in WSNs – an issue that is a specific aspect of context-oriented privacy [7]. As shown in Fig. 1, privacy in WSNs is classified into that of content-oriented and context-oriented categories. While content-oriented privacy ensures non-repudiation and confidentiality of data, context-oriented privacy is concerned with temporal and location privacy [8].

SLP is important when WSNs are deployed in safety-critical applications [3], [5], [9]. For example, in tactical military applications, SLP guarantees security and reduces the number of fatalities or victims on a battlefield. In healthcare, SLP mechanisms are employed in patient monitoring systems to ensure patient data are not disclosed to unauthorized users [5]. In wildlife monitoring, SLP techniques are employed to ensure that information on the location of endangered animal species is not exposed to illegal hunters [2], [3], [10]. SLP techniques are also important in underwater Internet of Things (UIoT) infrastructures, where WSNs are deployed for underwater exploration activities to ensure economic growth based the concept of Blue Economy [11], [12].

SLP routing protocols are used to provide SLP protection in WSNs [3], [9], [13]–[15]. In the existing literature, extensive projects on SLP routing protocols and their performance may be found. However, only a handful of papers focus on SLP reliability.

The study described in [16] reported that a lot of the existing literature focuses on analyzing connectivity-oriented and flow-oriented reliability. For example, the recent studies on reliability, as presented in [17]–[20], did not analyze SLP reliability. Although the authors of [20] studied privacy issues, their reliability evaluations focused mainly on data transmission reliability. SLP reliability was determined for the first time in [9].

To address this gap, this study analyzes SLP reliability and evaluates the energy efficiency of protocols, as inefficient use of energy in WSNs affects SLP reliability [9]. Moreover, to ensure higher operational efficiency of WSNs and SLP

protocols, it is important to balance energy distribution inside the WSN [21]–[23].

Three representative SLP protocols are considered: tree-based SLP protocol (TRP) [24], probabilistic SLP protocol (PRP) [25], and ring-based SLP protocol (RNP) [26]. The selection of TRP, PRP, and RNP protocols is based on the fact that TRP, PRP, and RNP employ phantom routing techniques. However, each protocol involves different routing strategies, as shown in Tab. 1. Therefore, it is interesting to observe the effects that each routing strategy has on privacy preservation and SLP reliability. Performance-related gains and limitations of each routing strategy are investigated as well.

The contribution of this study is summarized as follows:

- the paper explores operational features of various privacy-preserving phantom routing protocols and identifies the key similarities and differences in the routing strategies of TRP, PRP, and RNP,
- performance of TRP, PRP, and RNP is evaluated against an estimating adversary that uses the hidden Markov model,
- the impact of the routing strategies in TRP, PRP, and RNP on SLP reliability is investigated and energy efficiency for different network configurations is analyzed to identify the SLP protocol with superior performance features.

2. Related Work

Ozturk *et al.* introduced, in [27], a phantom routing strategy for SLP. Many other studies have explored phantom routing techniques for SLP, including those presented in [22], [26], [28]–[33]. Operational features of the phantom routing protocols are presented below.

The phantom routing protocol described in [32] is based on multiple sinks and a dynamic multipath routing strategy. It is designed to provide SLP protection for Internet of Things systems. The protocol generates a candidate area and selects phantom nodes to ensure the consumption of energy is more significant in the non-hotspot regions. Then, to increase dissemination randomness during the transmission, the protocol employs a packet segmentation technique to ensure the packets are segmented into many portions. The portions are transmitted through multiple dynamic paths. Furthermore, the protocol forms a closed-loop from the sink node to improve SLP protection.

Tab. 1. Summary of the key similarities and differences in the techniques of TRP, PRP, and RNP.

Routing technique	Protocol		
	TRP	PRP	RNP
Phantom routing	✓	✓	✓
Two-level phantom routing	×	×	✓
Fake packet distribution	✓	✓	×
Distributes fake packets in the vicinity of phantom node	✓	×	×
Distributes fake packet traffic in the sink node region	×	✓	×
Generates multiple sources of fake packets	✓	×	×
Isolates fake sources from real source nodes	×	✓	×
Long fake packet routing paths	✓	×	×

The protocol presented in [29] uses phantom nodes, rings, and fake paths. It is useful in networks that deploy multiple source or sink nodes. Fake packets are employed to mimic the behavior of real packets and perplex the adversary. The protocol transmits packets in four phases. In phase 1, the source node detects an event and generates real packets. The real packets are conveyed to the phantom node. In phase 2, the phantom node relays the real packets to the circular region. In phase 3, the real packets are conveyed clockwise in the circular region and arrive at the sink proxy node. The fourth phase involves the sink proxy node transmission process, where real packets are transmitted to the destination sink node.

The backbone-based protocol [26] relies on a routing technique to address the challenges faced by protocols that broadcast heavy traffic. The protocol introduces multiple levels of adversary confusion. It also employs a random backbone route between the sink node and the neighboring node of the phantom nodes, and packets are routed using a directed random-walk routing strategy.

It was highlighted in [28] that many of the existing phantom routing protocols are characterized by a high communication overhead and high energy consumption during the process of selecting the phantom node. Consequently, SLP protection and network lifetime are affected. To address this challenge, grid-based protocols [28] use powerful sink nodes to select phantom nodes. When the phantom nodes are selected by sink nodes, the energy of the ordinary sensor nodes is conserved.

The phantom walkabouts protocol described in [31] is a more general version of the phantom routing approach and presents phantom routes of variable lengths. It is different from the traditional phantom routing protocols, in which nodes have two sets of neighboring nodes. Here, the phantom walkabouts protocol divides each node's neighbors into four sets in different directions and creates a long random walk to generate a safeguarding distance between the phantom nodes and the real source node. As a result, the protocol achieves high levels of SLP protection and outperforms the baseline phantom routing protocol.

The phantom with angle protocol from [22] preserves the SLP and guarantees energy efficiency by regulating the traffic load in the network. The protocol locates phantom nodes at a safeguarded distance, away from the source nodes. Furthermore, it allocates multiple unique regions for phantom node selection. All the regions are assigned equal probability of selection. To ensure a new phantom node is selected for each successive packet, the protocol assigns a phantom selection factor.

This study evaluates SLP reliability of phantom routing protocols that were proposed in [24]–[26]. To route packets,

the TRP protocol proposed in [24] establishes a backbone route from the sink node to the boundaries of the network. Then, it establishes many redundant diversionary routes, serving as branch routes of the backbone route. Fake packets are distributed throughout the diversionary routes, while source nodes send packets to the sink node through the phantom nodes. To ensure strong SLP, TRP safeguards the location of phantom nodes located at a certain distance from the source nodes.

The PRP protocol [25] considers exposed regions and employs the directed random walk technique to ensure that selected phantom nodes are at a safe distance away from the source nodes. However, unlike in the case of TRP, PRP generates fake packet sources in the vicinity of the sink node and allows only one node to act as a fake source, for a fixed period of time. Also, PRP employs dynamic packet routes that vary based on source-sink distance and transmits both real and fake packets simultaneously. Real packets are routed through the selected phantom nodes. Fake packets are routed through rings and arcs facing different directions.

The RNP protocol presented in [26] does not broadcast fake packets. To ensure strong SLP, RNP relies on highly randomized packet routing paths that are less predictable to the adversaries. To achieve that goal, RNP constructs two levels of phantom nodes that provide strong adversary obfuscation effects.

3. Models

3.1. Network Model

Here, a WSN with numerous sensor nodes and a sink node is considered. The sink node is located at the center of the WSN. The sensor nodes are set to detect events. Once a sensor node detects an event within its sensing range, it becomes the source node and starts sending packets to the sink node using the multi-hop communication technique. If a sensor node fails to detect an event, it follows the sleeping pattern.

All sensor nodes are static and are characterized by the same memory capacity, initial energy, and computing ability. Neighboring sensor nodes are within each other's communication range and are able to communicate and exchange data. Figure 2 shows the structure of such a WSN. More details of this network model are presented in [8], [25].

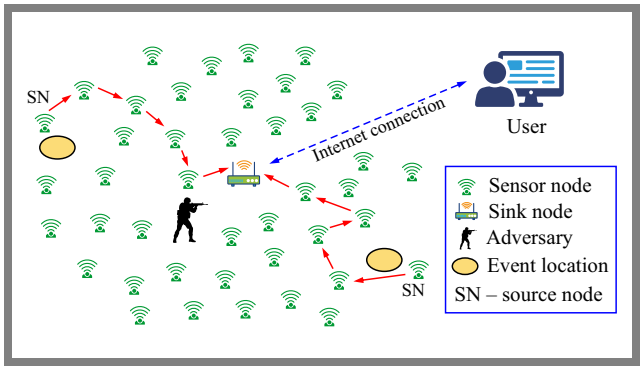

Fig. 2. Structure of the considered WSN.

3.2. Adversary Model

The adversary model uses an estimating adversary that eavesdrops on the communication between sensor nodes. It analyzes the packet traffic and checks the packet type by scanning the header of each packet. Thereafter, it employs the hidden Markov model (HMM) to estimate the likely state of the source nodes at a particular time.

The use of HMM is advantageous to the adversary because it helps make more precise estimations of the source state and predictions of the source location. Additional details of the adversary model are presented in [25].

4. Performance Evaluation

4.1. Simulation Environment

With the use of Matlab simulation software, a WSN was simulated with randomly distributed sensor nodes. The network configuration was adopted from [34]. Table 2 shows a summary of the network simulation parameters.

4.2. Performance Metrics

The performance of TRP, PRP, and RNP protocols was evaluated in terms of energy efficiency, SLP protection, and SLP reliability. The baseline phantom single-path protocol (PHP) [35] was used as a reference solution, for comparison purposes. The following metrics were used to analyze the performance:

- the energy ratio (ER) metric was used to measure energy efficiency,
- node utilization ratio (NUR) and sensor node residual energy metrics were used to evaluate energy distribution in the WSN,
- safety period (SP) and capture ratio (CR) metrics were used to determine the level of SLP preservation,
- safety period reliability (SPR) and capture ratio reliability (CRR) metrics were used to assess SLP reliability.

Tab. 2. Parameters used for network simulations.

Parameter	Value
Network side length	2000 m
Number of sensor nodes	3000
Number of sink nodes	1
Sensor node communication range	40 m
Adversary hearing range	40 m
Adversary attack strategy	Traffic analysing with HMM
Packet size	1024 bits
Source packet rate	Varied between 1 and 4 packet/s
Sensor node initial energy	0.5 J

ER, NUR, SP, SPR, CR, and CRR were computed using the following equations:

$$ER = \frac{E_{600}}{E_t}\,, \tag{1}$$

where E_{600} is the energy used in 600 rounds and E_t is total energy.

$$NUR = \frac{SN_{600}}{N_{sn}}\,, \tag{2}$$

where SN_{600} defines the number of sensor nodes participating in data transmission for 600 rounds and N_{sn} stands for total number of sensor nodes.

$$SP = N_{hops}\,, \tag{3}$$

where N_{hops} is the number of hops during the adversary backtracing attack.

$$CR = \frac{N_e}{T_e}\,, \tag{4}$$

Here, N_e is the number of experiments where the adversary ends in locating the source node while T_e is the total number of experiments.

$$SPR = \begin{cases} 1 & \text{if } e^{\Delta_{SP}} \geqslant 1 \\ 0 & \text{otherwise} \end{cases}\,, \tag{5}$$

$$CRR = \begin{cases} 1 & \text{if } e^{\Delta_{CR}} \geqslant 1 \\ 0 & \text{otherwise} \end{cases}\,. \tag{6}$$

The relationship between ER and energy efficiency is that high ER correlates with low energy efficiency. Also, the relationship between SP, CR, and SLP preservation is that long SP corresponds to high levels of SLP preservation, while low CR corresponds to high levels of SLP preservation [36]. In Eq. (5), Δ_{SP} is the difference between the achieved SP and the application-specific required SP. When $e^{\Delta_{SP}} \geqslant 1$, SPR becomes 1 to indicate that SLP reliability is guaranteed. Otherwise, SPR becomes 0 to indicate that SLP reliability is not guaranteed [9]. Same principles apply to compute CRR, as shown in Eq. (6).

5. Results and Discussions

5.1. Energy Efficiency

Energy efficiency determines the reliability of routing protocols in WSNs [21], [37]–[42]. The ER metric was used to measure energy efficiency. The relationship between ER and energy efficiency is that high ER correlates with low energy efficiency. The energy consumption model presented in [2], [9], [21], [25], [43]–[45] was used.

Figure 3 shows the ER of specific protocols at varied source packet rates. It shows that the ER of TRP is significantly higher than the ER of PRP and RNP. The baseline PHP incurs the lowest ER. TRP and PRP distribute fake packet traffic that increases the energy consumption and ER. Moreover, TRP generates multiple fake packet sources. In the transmission of every real packet, TRP distributes many fake packets, resulting in an increased ER.

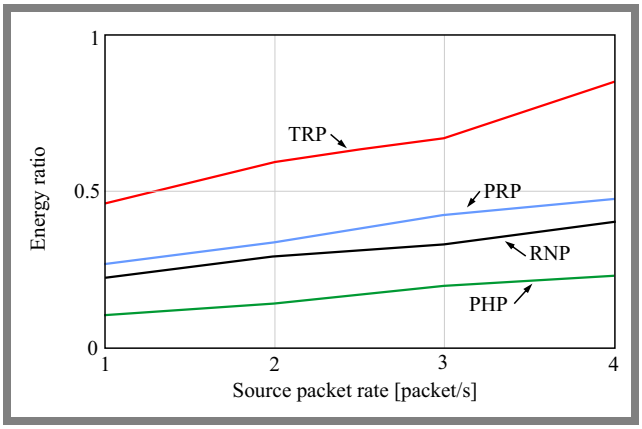

Fig. 3. Energy efficiency of the protocols.

PRP generates a single fake packet source at a time. Therefore, the ER of PRP is significantly lower than the ER of TRP. RNP does not distribute fake packet traffic. As a result, the ER in RNP is lower than in TRP and PRP. However, despite the fact that RNP does not distribute fake packet traffic, the ER of RNP is close to the ER of PRP. This is because RNP employs a two-level phantom routing strategy which creates long routing paths. Long routing paths increase the ER.

The results shown in Fig. 3 suggest that the energy efficiency of TRP is significantly lower. Thus, PRP and RNP outperform TRP in terms of energy efficiency.

5.2. Energy Distribution

The use of multi-hop packet routing technique results in unbalanced energy distribution (ED) in the WSN domain [46], [47]. Unbalanced ED affects the operation of WSNs and results in short-term SLP protection [3]. In systems requiring reliable data transmission or in which as many sensor nodes as possible are required to operate simultaneously, unbalanced ED results in a system failure [48].

To effectively measure the ED of TRP, PRP, and RNP, NUR and residual sensor node energy levels were analyzed. NUR increases along with an increase in randomness and length of the routing paths [32]. Additionally, NUR increases with the grooving number of routing paths and the amount of packet traffic. The relationship between NUR and ED is that if different regions in the WSN incur different levels of NUR, the ED is affected as well. Thus, an area with a high NUR depletes the sensor node's residual energy at a fast rate and uneven distribution of sensor node energy occurs.

In the experiments, NUR and ED were observed in different regions of the WSN: hotspot (HT) regions where the hop distance between a sensor node and the sink node was $\leqslant 20$ hops, and non-hotspot (NHT) regions where the hop distance was > 20.

Figure 4 shows that with the exception of TRP, all the other protocols achieve higher NUR in HT regions due to the increased amount of packet traffic. The unbalanced packet traffic causes unbalanced ED. The NUR of TRP in NHT is

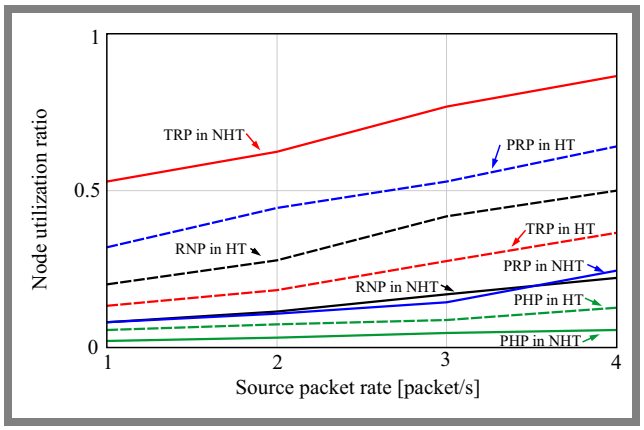

Fig. 4. Node utilization ratio of the protocols.

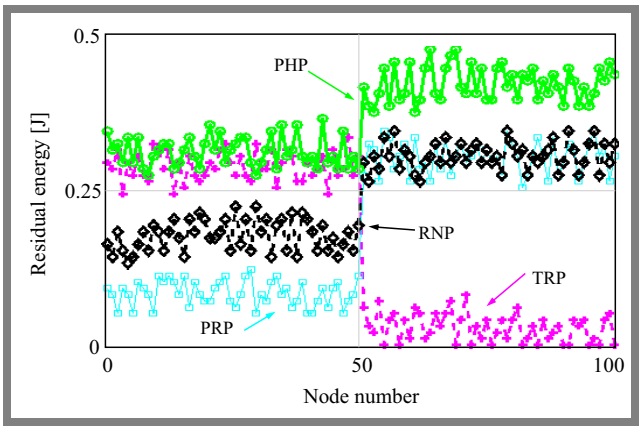

Fig. 5. Energy distribution of the protocols under consideration.

very high, because TRP generates multiple fake packet sources in NHT regions and for every real source node packet TRP distributes many fake packets. Consequently, many routing paths are created to route packet traffic in NHT regions and a high NUR value is incurred.

It is also shown in Fig. 4 that the NUR of PRP is significantly higher in HT regions. This is because PRP distributes fake packet traffic only in HT regions. Therefore, PRP creates a large number of routing paths in HT regions, which results in high NUR.

RNP creates few routing paths in the regions. As a result, in HT regions, the NUR of RNP is lower than the NUR of PRP. On the other hand, in HT regions, RNP creates longer routing paths and incurs higher NUR than TRP. In NHT regions, the NUR of RNP and PRP is comparable, because RNP and PRP employ similar routing techniques for source nodes in NHT regions. The results of experiments conducted indicate that RNP achieves an improved ED, outperforming TRP and PRP.

Figure 5 shows the residual energy of 100 randomly selected sensor nodes at the mission duration of 900 rounds. Sensor nodes number 1 to 50 were located in HT regions, while sensor nodes number 51 to 100 were located in NHT regions.

It is shown in Fig. 5 that for TRP, the residual energy of many sensor nodes in HT regions is above 0.25 J. However, in NHT regions, many of the sensor nodes have depleted their energy. These results confirm that TRP suffers from exhaustive energy consumption in NHT regions. Thus, TRP incurs unbalanced ED.

On the other hand, there is a smaller difference in the residual energy of RNP for HT and NHT regions. The results confirm that RNP outperforms TRP and PRP in terms of ED.

5.3. Safety Period

Figure 6 shows that TRP achieves the longest safety period (SP), while PRP achieves the shortest SP. The results indicate that the privacy preservation in TRP is the strongest. Figure 7 shows the SP of the protocols, as the number of sensor nodes increases. In the experiments, the source nodes were assumed to be at a source-sink distance of 30 hops. The packet rate was fixed at 1 packet/s. This shows that the SP of RNP increases more rapidly than the SP of the remaining protocols.

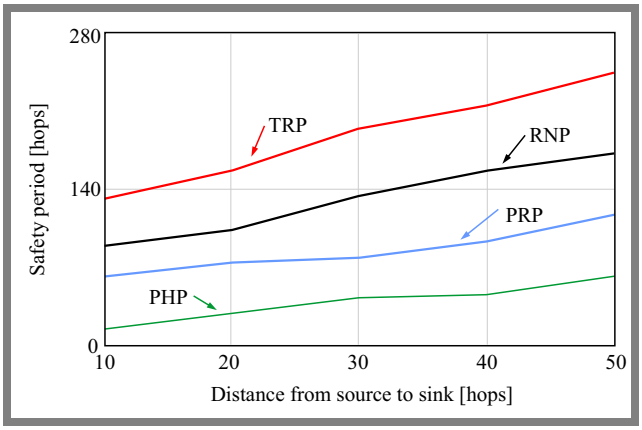

Fig. 6. Privacy preservation of the protocols while varying distance from source to sink.

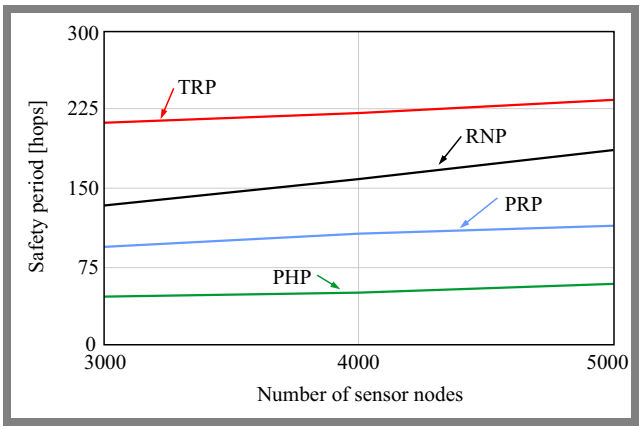

Fig. 7. Privacy preservation of the protocols for different number of sensor nodes.

The rapid increase in SP of RNP is caused by the fact that when the number of nodes in the network is growing, the number of neighboring nodes and candidate phantom nodes increases as well. Consequently, a larger set of phantom nodes is generated and the path diversity increases. Also, RNP employs a bias random number to ensure a dynamic phantom node selection process. The use of the bias random number guarantees that for each successive packet, the second level phantom node is selected from different regions of the WSN domain.

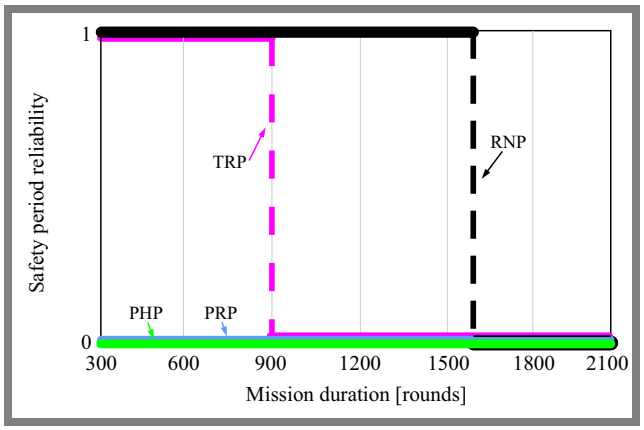

Fig. 8. Safety period reliability of the protocols.

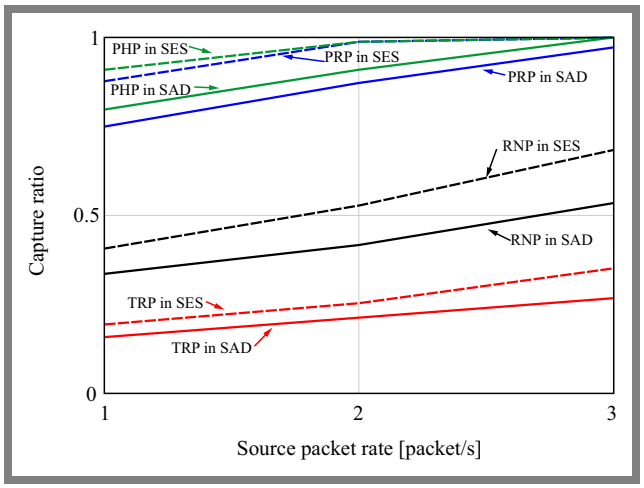

Fig. 9. Capture ratio of the protocols.

Moreover, RNP selects a new phantom node for each source node packet transmission. Therefore, when a larger set of phantom nodes is available, the path diversity and adversary obfuscation effects become more significant, resulting in longer SP.

5.4. Safety Period Reliability

Experiments were performed to observe safety period reliability (SPR) for a mission duration of 2100 rounds. Source nodes were located at a source-sink distance of 40 hops. The source packet generation rate was 1 packet/s. Similarly to [9], the minimum required SP was assumed to be 140 hops.

Figure 8 shows that PHP and PRP do not ensure SPR. This is because PHP and PRP are not able to achieve the required SP. On the other hand, TRP and RNP ensure SPR because they are able to achieve the required SP. However, the SPR of TRP is of the short-term variety. TRP is not capable of ensuring SPR beyond 950 rounds, because it is energy inefficient, as shown in Fig. 3. Only RNP is capable of providing SPR at 1500 rounds.

The results shown in Fig. 8 suggest that RNP provides long-term SPR to outperform TRP. RNP achieves better performance, as it is more energy efficient and achieves better ED than TRP.

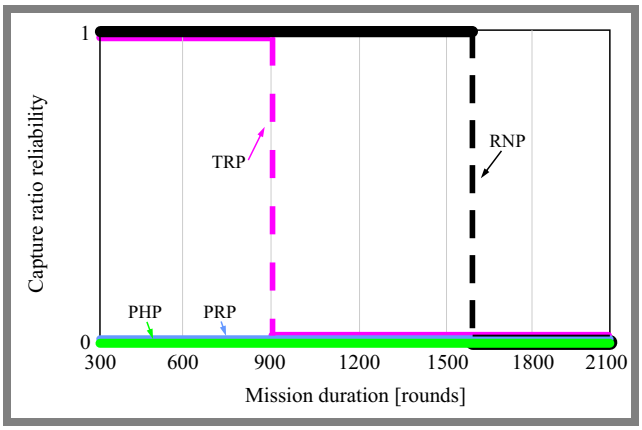

Fig. 10. CRR reliability of the protocols.

5.5. Capture Ratio

Figure 9 shows the capture ratio (CR) when the number and location of source nodes is varying. In the experiments, two scenarios were considered: “scenario east of the sink node” (SES) and “scenario all directions” (SAD). Four source nodes were deployed. In SES, the source nodes were randomly distributed on the east side of the sink node, at a source-sink distance of 25 hops. The distance between the source nodes was between 3 and 6 hops. In SAD, one source node was positioned at a source-sink distance of 25 hops, on the north side of the sink node.

Similarly, one source node was deployed east, west, and south of the sink node. Source packet generation rate was 1 packet/s. It is shown in Fig. 9 that for all the protocols, CR in SES is higher than in SAD. This is because in SES, the generated source packet traffic is concentrated on one side of the network domain. Therefore, the adversary performs a more focused attack and improves its CR. On the other hand, when the source nodes are distributed in SAD, the packet traffic arrives at the sink node from all directions. Consequently, the traffic analyzing attack becomes more complex and CR is reduced.

Figure 9 also shows the differences in the level of CR in SES and SAD. For TRP, the difference is small. This is because TRP distributes fake packet traffic between long diversionary routes. Therefore, it is able to effectively obfuscate the adversary in both SES and SAD. Furthermore, TRP distributes fake packet traffic in the vicinity of the phantom nodes. Therefore, even when the adversary is able to locate the phantom nodes, the success of its attack is hindered and CR improves at a slow rate.

The difference in the level of CR in SES and SAD for PRP is high, because unlike TRP, PRP employs short fake packet routes and it does not distribute fake packet traffic in the vicinity of the phantom nodes. Therefore, when the adversary performs a more focused attack in SES, it is able to improve CR.

The difference in the level of CR in SES and SAD for RNP is lower than for PRP, because RNP is characterized by high path diversity. The use of a dynamic two-level phantom node selection process ensures that packets arrive at the sink node through highly randomized packet routes, both in SES and

Tab. 3. Summary of the observations.

Routing strategy	Impact on the performance of the protocols
Two-level phantom routing	– Increases the path diversity and adversary obfuscation effect in RNP to improve SLP preservation
Fake packet distribution	– Increases the adversary obfuscation effect in TRP to improve SLP preservation – Reduces energy efficiency, which results in short-term SLP protection and reduced SLP reliability
Distributes fake packet traffic in the vicinity of phantom node	– Increases the adversary obfuscation effect in TRP and improves SLP preservation – Reduces energy efficiency, which results in short-term SLP protection and reduced SLP reliability
Distributes fake packet traffic in the vicinity of sink node	– Reduces energy efficiency – Insignificant effect on SLP preservation for PRP
Generates multiple fake packet sources at a time period	– Increases the adversary obfuscation effect in TRP to improve SLP preservation – Reduces energy efficiency, which results in short-term SLP protection and reduced SLP reliability – Unbalanced energy distribution in TRP
Isolates fake source nodes from real source nodes	– Reduces SLP preservation in PRP
Long fake packet routes	– Increases the adversary obfuscation effect in TRP to improve SLP preservation – Reduces energy efficiency, which results in short-term SLP reliability

in SAD. Therefore, the adversary obfuscation effect remains high, even in SES. The routing paths of the baseline PHP are less random. Therefore, CR is significantly higher when the adversary performs a more focused attack in SES.

In addition, Fig. 9 shows that CR in SES and SAD increases at higher source packet rates. This is because at higher data rates the adversary captures an increased number of packets and makes, within a short period of time, significant progress in its attacks. Consequently, CR increases. In particular, when the packet rate is high in SES, the region where the source nodes are located becomes an obvious hotspot region. Therefore, the attack becomes less complex and the adversary improves its CR. In SES, at the rate of 2 packets/s, CR for both PRP and PHP is 100%.

5.6. Capture Ratio Reliability

In the experiments aiming to compute capture ratio reliability (CRR), the value of the parameter was measured for a mission duration of 2100 rounds. A single source node was deployed. The maximum required CR equaled 0.35. Figure 10 shows that PHP and PRP do not ensure the CRR. This is because PHP and PRP are not capable of achieving a CR below 0.35.

On the other hand, TRP and RNP ensure CRR, because they are able to achieve the required CR. However, the CRR of TRP is of the short-term variety, because TRP is energy inefficient and it causes the sensor nodes to deplete their battery power at a fast rate. These results indicate that RNP outperforms TRP and PRP in terms of long-term CRR.

Table 3 summarizes the observations from the experiments. Based on the observations, it is established that RNP offer superior performance. RNP achieves long-term SLP reliability, outperforming TRP and PRP protocols.

6. Conclusion

There are key similarities and differences in the routing strategies of privacy-preserving phantom routing protocols, namely TRP, PRP, and RNP. The routing strategies exert different impacts on SLP reliability, energy distribution, and energy efficiency of the protocols under investigation. Protocols that integrate phantom and fake packet routing strategies improve SLP performance. However, distribution of fake packet traffic degrades the performance of the protocols in terms of SLP reliability and energy efficiency.

The TRP protocol is based on phantom and fake packet routing strategies that achieve short-term SLP reliability. The PRP protocol is more energy efficient than TRP, but it achieves low levels of SLP protection and reliability. On the other hand, RNP is based on a ring distribution of phantom nodes and evades the broadcasting of fake packets. As a result, RNP achieves improved SLP reliability, outperforming TRP and PRP protocols.

As part of future work, SLP protocols for underwater sensor networks (USNs) will be investigated, as previous studies have shown that SLP preservation still remains a challenge in USNs. Studies focusing on SLP are necessary due to the fact that USNs and UIoT systems have become rather powerful and may potentially support various applications, such as maritime security, natural disaster prediction and control, oil and gas exploration, and marine life observation.

References

[1] K.P.R. Krishna and R. Thirumuru, "Energy Efficient and Multi-hop Routing for Constrained Wireless Sensor Networks", *Sustainable Computing: Informatics and Systems*, vol. 38, art. no. 100866, 2023 (https://doi.org/10.1016/j.suscom.2023.100866).

[2] M. Rathee *et al.*, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks", *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 170–182, 2021 (https://doi.org/10.1109/TEM.2019.2953889).

[3] N. Wang, J. Fu, J. Li, and B.K. Bhargava, "Source-location Privacy Protection Based on Anonymity Cloud in Wireless Sensor Networks", *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 100–114, 2020 (https://doi.org/10.1109/TIFS.2019.2919388).

[4] A. Chmielowiec, L. Klich, and W. Woś, "Energy Efficient ECC Authenticated Key Exchange Protocol for Star Topology Wireless Sensor Networks", *Journal of Telecommunication and Information Technology*, vol. 1, pp. 1–10, 2024 (https://doi.org/10.26636/jtit.2024.1.1389).

[5] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020 (https://doi.org/10.1109/COMST.2019.2953364).

[6] N. Hrovatin, A. Tošić, M. Mrissa, and J. Vičič, "A General Purpose Data and Query Privacy Preserving Protocol for Wireless Sensor Networks", *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4883–4898, 2023 (https://doi.org/10.1109/TIFS.2023.3300524).

[7] G. Han *et al.*, "CPSLP: A Cloud-based Scheme for Protecting Source Location Privacy in Wireless Sensor Networks Using Multi-sinks", *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2739–2750, 2019 (https://doi.org/10.1109/TVT.2019.2891127).

[8] N. Jan and S. Khan, "Energy-efficient Source Location Privacy Protection for Network Lifetime Maximization against Local Eavesdropper in Wireless Sensor Network (EeSP)", *Emerging Telecommunications Technologies*, vol. 33, no. 2, art. no. 3703, 2022 (https://doi.org/10.1002/ett.3703).

[9] L.C. Mutalemwa and S. Shin, "Novel Approaches to Realize the Reliability of Location Privacy Protocols in Monitoring Wireless Networks", *IEEE Access*, vol. 9, pp. 104820–104836, 2021 (https://doi.org/10.1109/ACCESS.2021.3099499).

[10] L.C. Mutalemwa, "On the Use of Wireless Technologies for Wildlife Monitoring: Wireless Sensor Network Routing Protocols", *Tanzania Journal of Engineering and Technology*, vol. 42, no. 2, pp. 113–133, 2023 (https://doi.org/10.52339/tjet.v42i2.837).

[11] G. Han, R. Xia, H. Wang, and A. Li, "Source Location Privacy Protection Algorithm Based on Polyhedral Phantom Routing in Underwater Acoustic Sensor Networks", *IEEE Internet of Things Journal*, pp. 8459–8472, 2023 (https://doi.org/10.1109/JIOT.2023.3318567).

[12] S.A.H. Mohsan, A. Mazinani, N.Q.H. Othman, and H. Amjad, "Towards the Internet of Underwater Things: A Comprehensive Survey", *Earth Science Informatics*, vol. 15, no. 2, pp. 735–764, 2022 (https://doi.org/10.1007/s12145-021-00762-8).

[13] M. Singh and M.P. Singh, "Congestion Avoidance with Source Location Privacy Using Octopus-based Dynamic Routing Protocol in WSN", *Wireless Networks*, vol. 29, pp. 729–748, 2023 (https://doi.org/10.1007/s11276-022-03165-9).

[14] G. Kumar *et al.*, "Dynamic Routing Approach for Enhancing Source Location Privacy in Wireless Sensor Networks", *Wireless Networks*, vol. 29, pp. 2591–607, 2023 (https://doi.org/10.1007/s11276-023-03322-8).

[15] 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, 2020 (https://doi.org/10.1109/ACCESS.2020.2972354).

[16] S. Chakraborty, N.K. Goyal, S. Mahapatra, and S. Soh, "Minimal Path-based Reliability Model for Wireless Sensor Networks with Multistate Nodes", *IEEE Transactions on Reliability*, vol. 69, no. 1, pp. 382–400, 2020 (https://doi.org/10.1109/TR.2019.2954894).

[17] P. Mishra *et al.*, "Reliability Evaluation of a Wireless Sensor Network in Terms of Network Delay and Transmission Probability for IoT Applications", *Contemporary Mathematics*, pp. 309–325, 2024 (https://doi.org/10.37256/cm.5120242906).

[18] F. Dan *et al.*, "An Accuracy-aware Energy-efficient Multipath Routing Algorithm for WSNs", *Sensor*s, vol. 24, no. 1, art. no. 285, 2024 (https://doi.org/10.3390/s24010285).

[19] N. Sonnappa and K. Muniyegowda, "Privacy-aware Secured Discrete Framework in Wireless Sensor Network", *International Journal of Electrical and Computer Engineering*, vol. 14, no. 1, pp. 75–85, 2024 (https://doi.org/10.11591/ijece.v14i1.pp75-85).

[20] X. Xu, J. Tang, and H. Xiang, "Data Transmission Reliability Analysis of Wireless Sensor Networks for Social Network Optimization", *Journal of Sensors*, vol. 2022, art. no. 3842722, 2022 (https://doi.org/10.1155/2022/3842722).

[21] A.M. Alabdali, N. Gharaei, and A.A. Mashat, "A Framework for Energy-efficient Clustering with Utilizing Wireless Energy Balancer", IEEE Access, vol. 9, pp. 117823–117831, 2021 (https://doi.org/10.1109/ACCESS.2021.3107230).

[22] L.C. Mutalemwa and S. Shin, "Energy Balancing and Source Node Privacy Protection in Event Monitoring Wireless Networks", *2021 International Conference on Information Networking (ICOIN)*, Jeju Island, South Korea, 2021 (https://doi.org/10.1109/ICOIN50884.2021.9333901).

[23] C.-M. Yu *et al.*, "BRATRA: Balanced Routing Algorithm with Transmission Range Adjustment for Energy Efficiency and Utilization Balance in WSNs", *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1096–1111, 2023 (https://doi.org/10.1109/JIOT.2022.3206316).

[24] J. Long, M. Dong, K. Ota, and A. Liu, "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-based Diversionary Routing in Wireless Sensor Networks", *IEEE Access*, vol. 2, pp. 633–651, 2014 (https://doi.org/10.1109/ACCESS.2014.2332817).

[25] H. Wang *et al.*, "A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks", *IEEE Transaction on Vehicular Technology*, vol. 68, no. 6, pp. 5917–5927, 2019 (https://doi.org/10.1109/TVT.2019.2909505).

[26] 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, art. no. 292, 2020 (https://doi.org/10.3390/en13020292).

[27] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location Privacy in Energy-constrained Sensor Network Routing", *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 88–93, 2004 (https://doi.org/10.1145/1029102.1029117).

[28] 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, art. no. 2074, 2019 (https://doi.org/10.3390/s19092074).

[29] Z. Xiong *et al.*, "A Ring-based Routing Scheme for Distributed Energy Resources Management in IIoT", *IEEE Access*, vol. 8, pp. 167490–167503, 2020 (https://doi.org/10.1109/ACCESS.2020.3023260).

[30] T. Hussain *et al.*, "Improving Source Location Privacy in Social Internet of Things Using a Hybrid Phantom Routing Technique", *Computers & Security*, vol. 123, art. no. 102917, 2022 (https://doi.org/10.1016/j.cose.2022.102917).

[31] C. Gu, M. Bradbury, and A. Jhumka, "Phantom Walkabouts: A Customisable Source Location Privacy Aware Routing Protocol for Wireless Sensor Networks", *Concurrency and Computation, Practice and Experience*, vol. 31, no. 20, 2019 (https://doi.org/10.1002/cpe.5304).

[32] G. Han *et al.*, "A Dynamic Multipath Scheme for Protecting Source-location Privacy Using Multiple Sinks in WSNs Intended for IIoT", *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5527–5538, 2020 (https://doi.org/10.1109/TII.2019.2953937).

[33] 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, art. no. 2050, 2019, DOI: (https://doi.org/10.3390/s19092050).

[34] L. Mutalemwa, "Location Privacy Protection and Coverage Hole Effects in Event Monitoring Wireless Networks for Internet of Things Applications", *Journal of ICT Systems*, vol. 1, no. 2, pp. 52–70, 2023 (https://doi.org/10.56279/jicts.v1i2.50).

[35] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-location Privacy in Sensor Network Routing", *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, Columbus, USA, 2005 (https://doi.org/10.1109/ICDCS.2005.31).

[36] C. Gu, M. Bradbury, J. Kirton, and A. Jhumka, "A Decision Theoretic Framework for Selecting Source Location Privacy Aware Routing Protocols in Wireless Sensor Networks", *Future Generation Computer Systems*, vol. 87, pp. 514–526, 2018 (https://doi.org/10.1016/j.future.2018.01.046).

[37] W.-K. Yun and S.-J. Yoo, "Q-Learning-based Data-aggregation-aware Energy-efficient Routing Protocol for Wireless Sensor Networks", *IEEE Access*, vol. 9, pp. 10737–10750, 2021 (https://doi.org/10.1109/ACCESS.2021.3051360).

[38] N.R. Patel, S. Kumar, and S.K. Singh, "Energy and Collision Aware WSN Routing Protocol for Sustainable and Intelligent IoT Applications", *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25282–25292, 2021 (https://doi.org/10.1109/JSEN.2021.3076192).

[39] D. Thomas, R. Shankaran, M.A. Orgun, and S.C. Mukhopadhyay, "SEC 2: A Secure and Energy Efficient Barrier Coverage Scheduling for WSN-Based IoT Applications", *IEEE Transactions on Green Communications Networking*, vol. 5, no. 2, pp. 622–634, 2021 (https://doi.org/10.1109/TGCN.2021.3067606).

[40] Y. Liu *et al.*, "An Improved Energy-efficient Routing Protocol for Wireless Sensor Networks", *Sensors*, vol. 19, no. 20, art. no. 4579, 2019 (https://doi.org/10.3390/s19204579).

[41] G. Sudha and C. Tharini, "Trust-based Clustering and Best Route Selection Strategy for Energy Efficient Wireless Sensor Networks", *Automatika*, vol. 64, no. 3, pp. 634–641, 2023 (https://doi.org/10.1080/00051144.2023.2208462).

[42] V. Narayan, A.K. Daniel, and P. Chaturvedi, "E-FEERP: Enhanced Fuzzy Based Energy Efficient Routing Protocol for Wireless Sensor Network", *Wireless Personal Communications*, vol. 131, pp. 371–398, 2023 (https://doi.org/10.1007/s11277-023-10434-z).

[43] T.M. Behera *et al.*, "CH Selection via Adaptive Threshold Design Aligned on Network Energy", *IEEE Sensors Journal*, vol. 21, no. 6, pp. 8491–8500, 2021 (https://doi.org/10.1109/JSEN.2021.3051451).

[44] S. K. Chaurasiya *et al.*, "An Energy-efficient Hybrid Clustering Technique (EEHCT) for IoT-Based Multilevel Heterogeneous Wireless Sensor Networks", *IEEE Access*, vol. 11, pp. 25941–25958, 2023 (https://doi.org/10.1109/ACCESS.2023.3254594).

[45] Z. Qu *et al.*, "An Energy-efficient Dynamic Clustering Protocol for Event Monitoring in Large-scale WSN", *IEEE Sensors Journal*, vol. 21, no. 20, pp. 23614–23625, 2021 (https://doi.org/10.1109/JSEN.2021.3103384).

[46] Q. We *et al.*, "A Cluster-based Energy Optimization Algorithm in Wireless Sensor Networks with Mobile Sink", *Sensors*, vol. 21, no. 7, art. no. 2523, 2021 (https://doi.org/10.3390/s21072523).

[47] T. Shafique *et al.*, "A Review of Energy Hole Mitigating Techniques in Multi-hop Many to One Communication and its Significance in IoT Oriented Smart City Infrastructure", *IEEE Access*, vol. 11, pp. 121340–121367, 2023 (https://doi.org/10.1109/ACCESS.2023.3327311).

[48] X. Liu and J. Wu, "A Method for Energy Balance and Data Transmission Optimal Routing in Wireless Sensor Networks", *Sensors*, vol. 19, no. 13, art. no. 3017, 2019 (https://doi.org/10.3390/s19133017).

Lilian C. Mutalemwa, Ph.D.
Faculty of Science, Technology and Environmental Studies
https://orcid.org/0000-0003-4342-5562
E-mail: lilian.mutalemwa@out.ac.tz
The Open University of Tanzania, Dar es Salaam, Tanzania
https://out.ac.tz