The Impact of Energy-Inefficient Communications on Location Privacy Protection in Monitoring Wireless Networks

Lilian C. Mutalemwa and Seokjoo Shin*
Department of Computer Engineering, Chosun University, Gwangju 61452, South Korea
Email: lilian.mutalemwa@gmail.com, *sjshin@chosun.ac.kr (corresponding author)

***Abstract*—Wireless sensor networks (WSNs) have gained increasing popularity in ubiquitous support of sensing system services. Often, WSNs are energy-constrained and they are deployed in harsh and unattended environments. Consequently, WSNs are vulnerable to energy and environmental factors. To ensure secure and reliable operations in safety-critical monitoring WSNs, it is important to guarantee energy-efficient communications, location privacy protection, and reliability. Fake packet-based source location privacy (SLP) protocols are known to be energy-inefficient. Therefore, in this study, we investigate the impact of energy-inefficient communications on the privacy performance of the fake packet-based SLP protocols. Experiment results show that the protocols achieve short-term and less reliable SLP protection.**

Keywords—source location privacy; wireless sensor network; routing protocol; energy efficiency; reliability.

I. INTRODUCTION

Wireless sensor networks (WSNs) are widely used in many applications including national security, asset monitoring, automation, intelligent transportation systems, and military surveillance [1], [2]. Often, WSNs operate in unattended environments and are mostly battery-powered, so their performances are vulnerable to energy and environmental factors [3], [4]. Furthermore, WSNs are usually deployed in random areas with no protection. Consequently, the networks are vulnerable to traffic analysis attacks. In monitoring WSNs, adversaries may focus on analyzing the network traffic to obtain critical information such as the location information of the source nodes [2], [5]. The source location reveals valuable information about the monitored asset. Thereafter, the asset can be easily attacked [6]. Therefore, it is important to ensure energy-efficient communications and source location privacy (SLP) protection in monitoring WSNs. Moreover, the dynamicity of WSNs is greater as sensor nodes fail more often due to the limited battery power and harsh application environments [7]. Thus, it is essential to guarantee reliability in WSNs to ensure reliable network operations [7]-[10].

Fake packet-based SLP protocols are capable of effectively protecting the SLP in monitoring WSNs [11]-[16]. However, the protocols have several limitations including high energy consumption and unbalanced energy distribution. Examples of fake packet-based SLP protocols include the data dissemination routing (DdnR) protocol [17] and distributed fake source with phantom node (DfpR) protocol [18]. The energy distribution of the DdnR protocol is unbalanced because it floods real and fake packet traffic in the near-sink regions. The DfpR protocol incurs high energy consumption because it distributes a large amount of fake packet traffic throughout the WSN domain.

In this study, we investigate the impact of energy-inefficient communications on the privacy performance of the DdnR and DfpR protocols. Similar to [19], [20], we assume that exhaustive energy consumption of the sensor nodes and unbalanced energy distribution can seriously affect the operation of WSNs, resulting in several limitations which include limited network lifetime. Therefore, we analyze the performance of the DdnR and DfpR protocols in terms of SLP protection, energy efficiency, and network lifetime. Moreover, similar to [8], [21], [22], we assume that it is essential to measure the reliability of the SLP protocols at any time. Therefore, using the SLP reliability parameter, we measure the degree to which the protocols can meet application-specific requirements. It is worth noting that this study is among the very first studies attempting to measure the SLP reliability.

Thus, the main contributions of this study are summarized as follows.

- Conduct a series of experiments to analyze the performance of the DdnR and DfpR protocols in terms of SLP protection, energy efficiency, network lifetime, and SLP reliability.
- Demonstrate through experimental analysis that due to energy-inefficient communications, the DdnR and DfpR protocols are less capable of achieving reliable long-term SLP protection or application-specific SLP protection requirements.

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

II. RELATED WORK

Since the problem of SLP was introduced in 2004, numerous protocols have been proposed to provide SLP protection [6], [12], [15], [23]-[28]. Many of the protocols were discussed in [6], [12], [15], [23]-[28]. Some of the

recently proposed SLP protocols include the two-level phantom with a pursue ring protocol [23], unified single and multi-path routing protocol [5], dynamic multipath routing protocol [29], grid-based single phantom node protocol [27], data dissemination protocol [17], and the protocol based on anonymity cloud [11]. Other recently proposed SLP protocols are the cloud-based with multi-sinks protocol [2], protocol based on phantom nodes, rings, and fake paths [24], phantom walkabouts protocol [30], grid-based dual phantom node protocol [27], two-level phantom with a backbone route protocol, probabilistic routing protocol [31], and the circular trap protocol [32].

There exist many fake packet-based SLP protocols including the data dissemination routing protocol [17], tree-based diversionary routing protocol [33], protocol based on phantom nodes, rings, and fake paths [24], protocol based on anonymity cloud [11], distributed fake source with phantom node protocol [18], and the probabilistic routing protocol [31]. Also, fake packet routing strategies were employed in the dummy adaptive distribution and controlled dummy adaptive distribution protocols [34]. In this study, we investigate the performance of the data dissemination routing protocol and distributed fake source with phantom node protocol. Therefore, we summarize the operational features of the data dissemination routing protocol and distributed fake source with phantom node protocol as follows.

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

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

III. MODELS

A. Network Model

The network model is adopted from [23]. The sensor nodes are equipped with a wireless interface and have limited resources and computational capabilities. The network is event-triggered, a node senses an asset then it sends packets periodically to the sink node. The sensor nodes employ multi-hop communication for energy conservation. During the network configuration phase, network initialization process is performed for localization of the sensor nodes. The *k*-nearest neighbor tracking approach [35] is employed to track the assets.

B. Adversary Model

The adversary model is adopted from [23]. The adversary is assumed to be more powerful than the sensor nodes in the network. It is equipped with spectrum analyzers and has sufficient resources such as adequate computation capabilities, memory, and unlimited power. The adversary is mobile, initially residing in the neighborhood of the sink node. It is capable of localizing an immediate sender node when a packet is received from a node within the adversary hearing range. It performs a hop-by-hop back tracing attack towards the source node, until it locates the source node.

IV. PERFORMANCE EVALUATIONS

A. Simulation environment

MATLAB simulation environment was used to evaluate the performance of the DdnR and DfpR protocols. For comparative analysis, the traditional phantom single-path routing (PspR) was included in the analysis [23]. A network of size 2000 × 2000 m^2 was simulated with 2500 randomly distributed sensor nodes. The network simulation parameters are summarized in Table I. Simulation was run for 500 iterations and average values were considered. Performance analysis was done using various performance metrics including safety period, attack success rate, energy ratio, network lifetime, and safety period reliability.

TABLE I: NETWORK SIMULATION PARAMETERS

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

The safety period and attack success rate were used to measure the level of SLP protection while energy ratio measured the energy efficiency and safety period reliability measured the SLP reliability.

B. Results and Discussions

1) Energy Efficiency

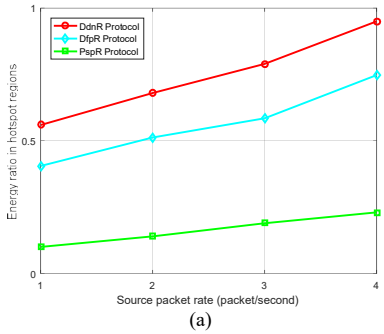
The energy consumption and energy efficiency of the protocols were investigated using the energy consumption model in [23], [33]. Equations (1) and (2) were used to compute the energy consumption of the sensor nodes. The details of the equations are presented in [23].

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

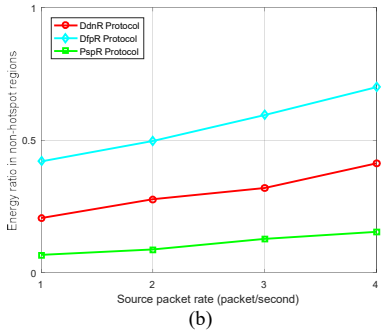
$$E_{rec} = lE_{loss} \quad (2)$$

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

Since the energy distribution of the DdnR protocol is unbalanced, the ER was computed for the near-sink regions (hotspot regions) and the away from sink node regions (non-hotspot regions) as shown in Fig. 1. All sensor nodes with source-sink distance < 25 hops were considered to be located in in the hotspot regions. Fig. 1 shows the ER of the protocols at varied source packet rate. It shows that the DdnR and DfpR protocols have significantly higher ER than the traditional PspR protocol. This means that compared to the PspR, the DdnR and DfpR are less energy-efficient. Fig. 1 (a) shows that DdnR has the highest ER in the hotspot regions. This is mainly because DdnR floods real and fake packet traffic in the hotspot regions. The DfpR protocol incurs high ER because it distributes a large amount of fake packet traffic. On the other hand, Fig. 1 (b) shows that DdnR has lower ER than DfpR in the non-hotspot regions. This confirms that the energy distribution of the DdnR protocol is unbalanced. Therefore, the impact of the energy-inefficient communications in DdnR and DfpR on the SLP protection and network lifetime were investigated and results are presented in Fig. 2 and Fig. 3.



(a)



(b)

Fig. 1. Energy efficiency of the protocols. (a) Energy ratio in hotspot regions. (b) Energy ratio in non-hotspot regions.

It is also shown in both Fig. 1 (a) and Fig. 1 (b) that the ER of all the protocols tends to increase with the increase in source packet rate. This is mainly because when the packet rate is increased, more packets are generated per second and higher amount of energy is consumed to transmit the packets. As a result, the ER is increased. Thus, the energy efficiency of the protocols is significantly reduced when the source packet rate is high.

2) Safety Period

The privacy performance of the protocols was analyzed using the safety period (SP) metric. SP is defined as the time required for an adversary to back trace the packet routes and successfully locate the source node [23], [33]. We measure the safety period by counting the number of hops during the adversary back tracing attack. Longer SP provides high levels of SLP protection as shown in equation (3).

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

Fig. 2 shows the SP of the protocols at different mission durations (rounds). It is shown that the DdnR and DfpR protocols achieve significantly longer SP than the traditional PspR protocol. Also, it is shown that the SP of the DdnR and DfpR protocols tends to decrease as the number of rounds is increased. The SP decreases because the protocols are not energy-efficient. For DdnR, when both real and fake packets are flooded, a significant amount of sensor nodes energy is consumed to transmit a single packet. Consequently, the sensor nodes drain their energies at a fast rate. At 900 rounds, a significant number of sensor nodes inside the blast ring have exhausted their battery power. Therefore, a reduced number of

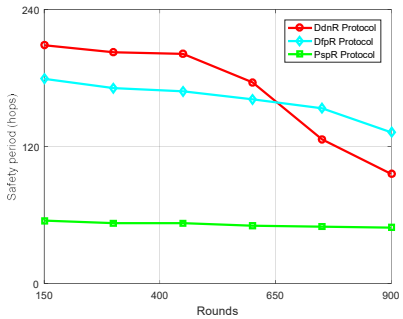


Fig. 2. Privacy performance of the protocols.

sensor nodes can participate in the flooding mechanism. As a result, the adversary becomes less obfuscated and the SP is reduced. For DfpR, since a considerable amount of fake packet traffic is distributed in the network, many of the sensor nodes deplete their energies at a fast rate. When the number of rounds is increased, the residual energy of the sensor nodes become less than the threshold value. As a result, small numbers of fake packet sources are generated. Subsequently, the amount of fake packet traffic is reduced, the adversary becomes less obfuscated, and the SP is reduced.

3) Attack Success Rate

The privacy performance of the protocols was also analyzed using the attack success rate (ASR) metric. ASR is the measure of the rate of source node traceability when an eavesdropping adversary is back tracing against a SLP routing protocol. It is computed by counting the number of successful adversary attempts [6], [23]. Low ASR corresponds to high levels of SLP protection as shown in equation (4).

$$\min\ (ASR) = \max\ (SLP_{Protection}) \tag{4}$$

Fig. 3 (a) shows the ASR of the protocols under varied adversary hearing range. The adversary hearing range was varied between 30 and 90 m. It is shown that for all the protocols, the ASR increases with the increase in adversary hearing range. This is mainly due to the fact that the adversary becomes more powerful when it has a longer hearing range. The traffic analysis attacks become less complex when the adversary can hear a packet sent from a sensor node which is more than 1 hop away. Furthermore, Fig. 3 (a) shows that the ASR of DdnR increases at a fast rate compared to the ASR of DfpR. The main reason for the increased ASR in DdnR is that DdnR isolates the real and fake source nodes and it does not distribute fake packets near the phantom nodes. Consequently, the adversary obfuscation effect between the phantom nodes and source nodes is reduced. Also, the location information of the source nodes is easily leaked to the adversary after the adversary locates a phantom node. Thus, it becomes easy for the adversary to capture successive packets and improve its ASR.

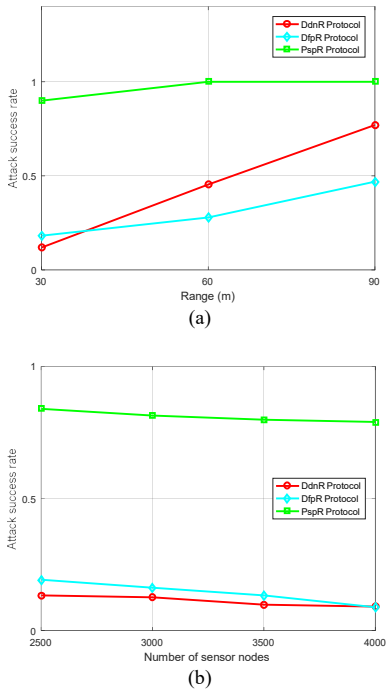


Fig. 3. Privacy performance of the protocols. (a) ASR against varied adversary hearing range. (b) ASR against varied number of sensor nodes.

Fig. 3 (b) shows the ASR of the protocols under varied number of sensor nodes. It is shown that the ASR for the DfpR tends to decrease when the number of nodes is increased. This is due to the fact that when the number of sensor nodes is increased, it increases the probability of a higher number of candidate fake packet sources. When a large number of fake packet sources is generated, large amounts of fake packet traffic are broadcasted to obfuscate the adversary. Consequently, the ASR is reduced.

4) Network Lifetime

To investigate the impact of low energy efficiency of the DdnR and DfpR protocols on the network lifetime, the network lifetime of the protocols was observed under varied source packet rate as shown in Fig. 4. The network lifetime model was adopted from [33]. The model assumes that the network lifetime is maximized when the energy consumption of the sensor node with maximum energy consumption is minimized as shown in equation (5). Thus, the the network lifetime is maximized when the ER in hotspot regions is minimized. In the equation (5), NL is the network lifetime and NE_i is the energy consumption of node i.

$$\max\ (NL) = \min \max_{0 < i \le k} (NE_i) \tag{5}$$

Therefore, network lifetime is denoted as the period between the start of the network operation and the first sensor node power outage.

Fig. 4 shows that the DdnR and DfpR protocols achieve significantly reduced network lifetime compared to the PspR protocol. The main reason for the reduced network lifetime is that both DdnR and DfpR incur high ER and low energy efficiency. Furthermore, it is shown that the network lifetime is affected by the source packet rate. When the packet rate is increased, more packets are generated per second, the sensor nodes consume more energy per unit time, the ER is increased, and the network lifetime is reduced.

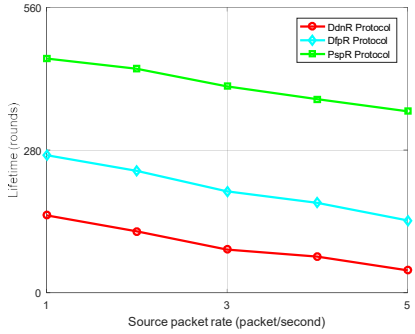


Fig. 4. Network lifetime of the protocols.

5) Safety Period Reliability

The analysis results in Fig. 2 and Fig. 3 show the magnitude of SLP protection. Although the DdnR and DfpR protocols are capable of achieving high levels of SLP protection, they may not be reliable in long-term monitoring due to their low energy efficiency and reduced network lifetime. Therefore, it is important to investigate the SLP reliability of the protocols. Moreover, since there are many factors influencing the functioning of WSNs, it is essential to measure the ability of the DdnR and DfpR protocols at any time [21], [22]. Also, it is important to quantify the degree to which the performance of the protocols can meet the application-specific requirements [8].

According to [7]-[9], a reliability index for a WSN should quantitatively assess the ability of the network to perform its intended function. Although SP and ASR measure the magnitude of the SLP protection, they do not take into consideration the application-specific requirements for achieving the intended SLP protection. Thus, the SP and ASR metrics fail to measure the SLP reliability or to reflect whether or not the SLP protection can be maintained for a given period of time, such as a specified mission duration. Therefore, in this study, we analyze the SLP reliability of the SLP protocols by measuring the safety period reliability (R_η) using equations (6), (7), (8).

In the equations, η represents the SP. Two main values of η are considered, the achieved η (η_{ach}) and the application-specific required η (η_{req}). The η_{ach} is the magnitude of η which is achieved by the protocols, as shown in Fig. 2. The η_{req} is according to the application-specific requirements. For example, some applications such as monitoring of endangered animals may specify a minimum η_{req} as 140 hops, throughout the mission duration. Meaning that throughout the mission duration, the protocols must guarantee that the achieved SP is greater than or equal to 140 hops.

In the equation (6), the R_η is computed. When $e^{\Delta_\eta} \geq 1$, the R_η becomes 1 to indicate that the η_{req} is achieved and SLP reliability is guaranteed. Otherwise, the R_η becomes 0 to indicate that the η_{req} is not achieved and the SLP reliability is not guaranteed.

$$R_\eta = \begin{cases} 1, & if\ e^{\Delta_\eta} \geq 1 \\ 0, & otherwise. \end{cases} \quad (6)$$

where Δ_η is the difference between the η_{ach} and η_{req}. The Δ_η is computed using equation (7).

$$\Delta_\eta = \frac{\eta_{ach} - \eta_{req}}{\eta_{ave}} \quad (7)$$

where η_{ave} is the average of the η_{ach} and η_{req}. The η_{ave} is computed using equation (8).

$$\eta_{ave} = \frac{\eta_{ach} + \eta_{req}}{2} \quad (8)$$

Therefore, we define the R_η as the probability that the achieved η is greater than or equal to the minimum required η.

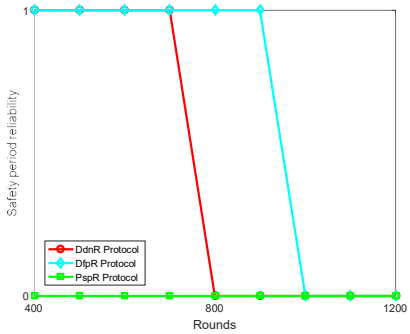


Fig. 5. Safety period reliability of the protocols.

In the experiments, R_η was observed for the mission duration of 1200 rounds. It was assumed that the η_{req} was 140 hops. Fig. 5 shows the R_η of the DdnR, DfpR, and PspR protocols. It is shown that the DdnR and DfpR protocols are capable of achieveing R_η but only for a limited number of rounds. Beyond 900 rounds, both DdnR and DfpR do not provide R_η. The observations in Fig. 5 confirm that due to the energy-inefficient communications, the DdnR and DfpR protocols are less capable of providing long-term SLP reliability. On the other hand, the PspR employs a simple routing algorithm which is energy-efficient. However, when the η_{req} is long, the PspR is not capable of guaranteeing the η_{req} or SLP reliability.

V. Conclusion and Future Work

This paper presents some investigations on the drawbacks of energy-inefficient communications in fake packet-based SLP protocols. Performance of two fake packet-based SLP protocols is investigated. To achieve high levels of SLP protection, the protocols distribute large amounts of fake packet traffic throughout the WSN domain or in particular regions of the network. However, the distribution of large amounts of fake packet traffic result in limitations such as reduced energy efficiency and limited network lifetime. When the fake packet traffic is flooded in particular regions of the WSN domain, the protocols incur unbalanced energy distribution. It is demonstrated through a series of experiments that due to energy-inefficient communications, fake packet-based SLP protocols achieve short-term and less reliable SLP protection. As part of our future work, we will investigate the packet delivery reliability of the protocols in various network configurations.

Acknowledgment

This research is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07048338).

References

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

[2] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, March 2019.

[3] X. Fu, Y. Yang, and O. Postolache, "Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 168–181, March 2021.

[4] F. Wang, et al, "To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in wsns," *IEEE Access*, vol. 7, pp. 55983–56015, May 2019.

[5] 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, February 2020.

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

[7] 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, March 2020.

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

[9] W. Sun, et al, "End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial wsns," *IEEE Transactions On Automation Science And Engineering*, vol. 15, no. 3, pp. 1127–1137, July 2018.

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

[11] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 100–114, 2020.

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

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

[14] M. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 409–416.

[15] Z. Hong, R. Wang, S. Ji, and R. Beyah, "Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1337–1350, May 2019.

[16] A. Thomason, M. Leeke, M. Bradbury, and A. Jhumka, "Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, July 2013, pp. 667–674.

[17] N. Jan, A. Al-Bayatti, N. Alalwan, and A. Alzahrani, "An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP)," *Sensors*, vol. 19, no. 9, p. 2050, 2019.

[18] P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, "Source location privacy using fake source and phantom routing (FSAPR) technique in wireless sensor networks," *Procedia Comput. Sci.*, vol. 57, pp. 936–941, 2014.

[19] M. Adil, et al, "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163209–163224, September 2020.

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

[21] H. Feng and J. Dong, "Reliability analysis for wsn based on a modular k-out-of-n system," *Journal of Systems Engineering and Electronics*, vol. 28, no. 2, pp. 407–412, April 2017.

[22] L. Xing, "Reliability in internet of things: current status and future perspectives," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6704–6721, August 2020.

[23] L. C. Mutalemwa, and S. Shin, "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks," *Energies*, vol. 13, p. 292, 2020.

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

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

[26] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity against global adversary in WSNs using dummy packet injections: A survey," *Electronics*, vol. 7, no. 10, p. 250, 2018.

[27] 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, p. 2074, May 2019.

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

[29] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in wsns intended for iiot," *IEEE Transactions On Industrial Informatics*, vol. 16, no. 8, pp. 5527– 5538, August 2020.

[30] C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks," *Concurrency Computat Pract Exper.*, vol. 31, e5304. 2019.

[31] H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, "A probabilistic source location privacy protection scheme in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 68, 5917–5927, 2019.

[32] Y. Wang, L. Liu, and W. Gao, "An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks," *Symmetry*, vol. 11, p. 632, 2019.

[33] 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.

[34] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity in WSNs against global adversary utilizing low transmission rates with delay constraints," *Sensors*, vol. 16, p. 957, 2016.

[35] Y. Liu, J.-S. Fu, and Z. Zhang, "K-nearest neighbors tracking in wireless sensor networks with coverage holes," *Pers. Ubiquitous Comput.*, vol. 20, no. 3, pp. 431–446, June 2016.