Computer Science and Information Systems 19(2):857–886 https://doi.org/10.2298/CSIS211009007R

Recent Advancements in Privacy-aware Protocols of Source Location Privacy in Wireless Sensor Networks: a Survey

Pradeep Kumar Roy[1], Asis Kumar Tripathy[2], Sunil Kumar Singh[3], and
Kuan-Ching Li[4,⋆]

[1] Department of Computer Science and Engineering
Indian Institute of Information Technology, Surat, India
pradeep.roy@iiitsurat.ac.in
[2] School of Information Technology and Engineering
Vellore Institute of Technology, Vellore, Tamil Nadu, India
asistripathy@gmail.com
[3] School of Computer Science and Engineering
VIT-AP University, Near Vijaywada, Andhra Pradesh, India
sksingh.cse@gmail.com
[4] Department of Computer Science and Information Engineering (CSIE),
Providence University, Taiwan
kuancli@gm.pu.edu.tw

Abstract. This review article summarises the protocols proposed in recent researches to secure location information in Wireless Sensor Networks (WSNs). Due to their lightweightness and easy to deploy properties, WSNs are widely used in numerous object tracking and monitoring applications. Due to such, source location privacy attracts the researchers and hence continuously enhances its improvement. Though, this privacy breach is not acceptable for WSNs, as it may reveal some critical information that is harmful. The SLP issue on WSN attracted researchers a lot, and hence a number of solutions are provided for it. However, an up-to-date survey does not exist for the same. To fill this gap, in this article, we summarize different approaches proposed in the last years to preserve location privacy. We first discuss the different privacy characteristics in WSNs, a detailed overview of the proposed protocols and their limitations, and discussions of solutions for the adversaries' capabilities in WSNs. Then the future research directions in this area are discussed. This review work may support researchers identifying the new research area in location privacy of wireless sensor networks.

Keywords: Wireless sensor networks, Source location privacy, Fake source, Phantom routing, Security,

1. Introduction

Wireless sensor networks (WSNs) are typically composed of sensor nodes with limited power, memory, computational capabilities, and communication resources. The sizes of these sensor nodes are tiny, with limited computing and processing resources, and are

[⋆] Corresponding author

cheaper than conventional sensors. However, WSNs provide potentially low-cost solutions to multiple issues in both civilian and military applications, along with target monitoring, battlefield surveillance, health care, environmental monitoring, traffic regulation, and wildfire detection[1,72]. In recent years, WSNs have attracted global attention, particularly with the proliferation of Micro-Electro-Mechanical Systems (MEMS) technology that helps a lot in the intelligent sensors development process [2]. These sensor nodes can sense, measure, and collect data from the environment and transmit the sensed information to the user based on routing techniques [3,73,71]. Researchers focused on the main characteristics of the WSNs, such as the sensors' energy conservation, their computational power, and the resource constraints. However, addressing the privacy issues in the WSNs are received very little attention [68]. Privacy in WSN refers to private information such as monitoring messages, object tracking messages, and others transmitted over the network. For example, a patient's blood pressure, sugar level, and various critical symptoms are usually essential concerns of privacy that need to be secured while transmitting this information to a faraway health centre or doctor's office using the WSNs. Privacy concerns may also arise beyond the information content and may include knowledge about context information that consists of a sensor's location starting information communication.

This paper focused on summarizing the recent works on monitoring and tracking applications with wireless sensor networks. The applications include the monitoring of doctors and patients movement in the hospital and wildlife tracking [4]. The sensor network is used for monitoring the objects and tracking their movements. Figure 1 shows the issue of SLP in object tracking, an adversary sitting near to base station and listing all incoming messages. Further, by following the route of the incoming message, they can reach the origin of the message to trap the object. The object might be a human being, a vehicle, or an animal. When the sensor nodes sense the object's presence, it passes the sensed information to the nearby one or more sinks [5]. Further, the collected data may be forwarded to the server or allows manual extraction to extract the information. Providing the confidentiality of the communication between nodes for message exchanging does not help to secure the source's location. SLP needs more than concealment of message exchange between the nodes in the network. Also, the confidentiality of a WSN message is part of another privacy policy called content privacy[5]. The main focus of content privacy is to provide the integrity, confidentiality, and availability of the message in WSNs. In contrast, SLP and sink location privacy are part of context privacy that aims to hide the contextual information in WSNs [6]. The SLP in WSN consisting three main components apart from the sensor node, including- Source, Sink, and Adversary. The sensitive information is originated from the source node in the network and is delivered to the base station using suitable network protocol in multiple packets. The number of packets depends upon the size of the information. Further, an adversary sitting near the base station starts following the route of incoming packets to find the origin of the message in the network.

Conti et al. [7] provided an extensive survey on SLP; however, many latest protocols were proposed in recent years that need to be discussed. Li et al. [8] explained the types of privacy in WSN. Aivaloglou et al. [9] provide a survey in which only discussed half of the solutions that were already discussed in [8]. As shown in Table 1, the existing surveys were not up to date and lacked future research directions. To fill this gap, this article summarizes the solutions that the researchers proposed to date. For this survey, we have collected the research articles from the different libraries such as *Elsevier*, *IEEE*, *ACM*,

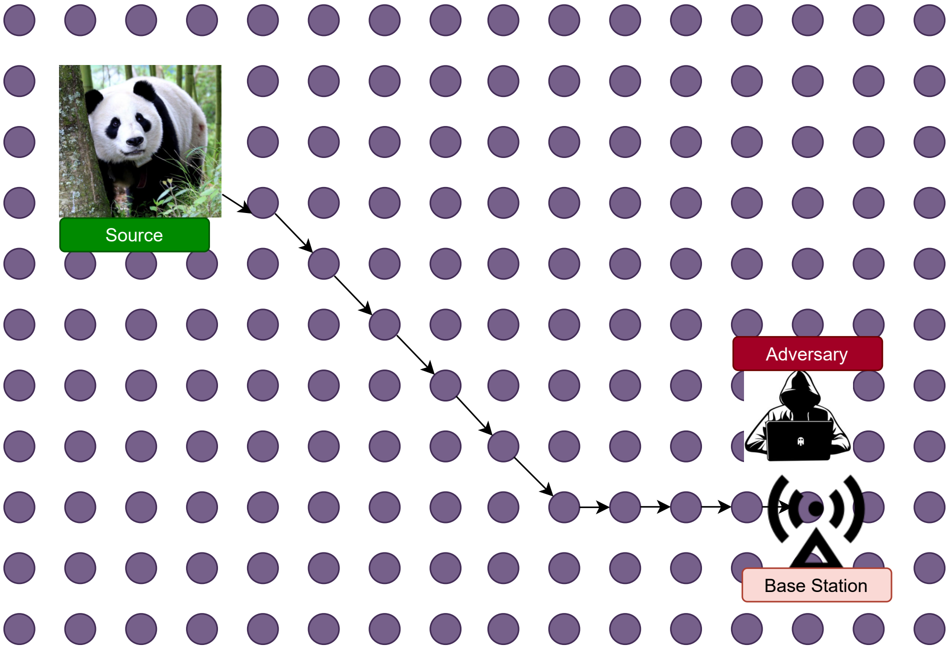

Fig. 1. Scenario of object tracking by following the incoming message to the base station

Springer, and *Scopus* using the keywords like: "source location privacy", "sink location privacy", "fake source", "phantom routing", and "privacy" published during year 2004 to April 2021. The collected articles were re-evaluated to check their belonging in the proposed aim and scope. Articles that were not fit was not added to this work. Our major contributions include the following:

1. Collected and organized high-quality research articles from various sources.
2. Discussed in brief, the privacy issues in WSNs.
3. Explored the different models and architectures that were used to provide the SLP in WSNs.
4. Briefly explains the existing models' limitations and provides future research directions.

The rest of the article is organized as follows: Section 2 discusses the background of location privacy. The solution to the SLP using fake source and phantom routing is shown in Section 3. In Section 4, the SLP challenges for WSN is discussed. The future research direction is detailed in Section 5. In Section 6, we conclude this work with limitations in the existing protocols.

2. Background

In recent year researcher put a lot of attention to preserve location privacy in WSNs [10]. In WSNs, privacy issues are mainly categorized in two parts: data privacy and context privacy, as shown in Fig. 2. This section focused on the different concepts proposed by the researchers for SLP and adversary capabilities. In data privacy, the security mechanism is mainly implemented to provide security to the packets transmitted in WSNs. In context privacy, the objective is to provide privacy to context, such as the location of the sensor nodes.

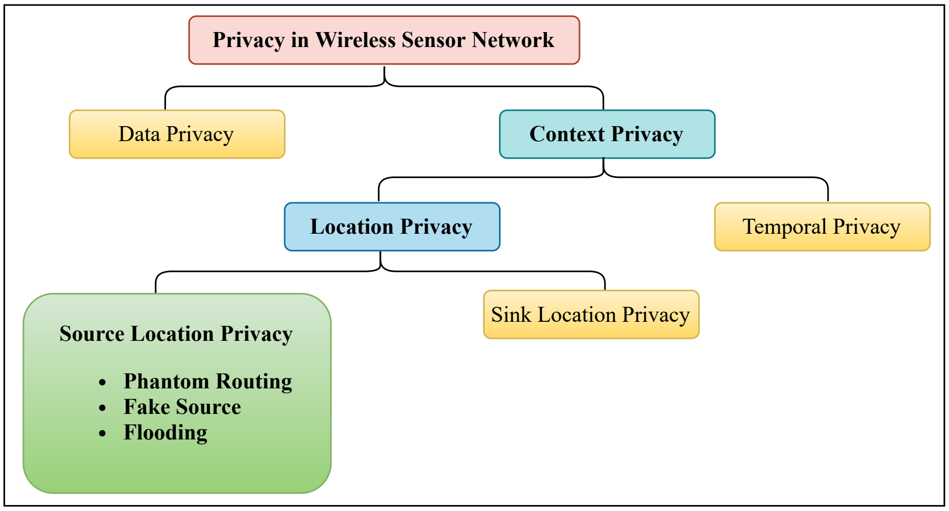

Fig. 2. Privacy issues in Wireless Sensor Networks

2.1. Adversary Model

The main goal of any privacy-preserving protocol is to create confusion in the backtracking route of an adversary. Hence, the adversary has to spend more time in the wrong direction. This will increase the source node's safety period. Researchers have made the following assumption about an adversary to proposed the privacy protocols in WSN.

- An adversary is resource-rich as they have more storage and a more range of tracing power.
- An adversary is passive. They monitor the flow of traffic without making any detectable change.
- An adversary has a sectional antenna, through which they can predict the direction of incoming messages. Hence, they start backtracking the packets from the sink to reach the source.
- An adversary may store the visited node ID that helps avoid entering the loop if any loop is present or not visiting the same node again.
- An adversary knows the sink node location and silently stays there and waits for a message.

Table 1. List of the existing surveys on privacy models in WSN

Source	**Major Focus**	**Topic discussed**	**Remarks**
Conti et al. [7]	Source location privacy	overview of the solutions that provide source location privacy within a WSN	challenges are not provided, survey is very old.
Li et al. [8]	privacy-preserving techniques for WSNs	mainly discussed two privacy techniques data-oriented and context-oriented	more than 1 decade old and source location privacy not covered
Rios et al. [11]	Location privacy	analyse whether traditional communication systems are comfortable to the requirements of location privacy in sensor networks	Only communication related issues are discussed and survey is very old.
Jiang et al. [12]	Privacy models	mainly concern on privacy models to see their comparability and suitability analysis for different scenarios.	Only 5 years papers are considered in this survey.
Gupta and Prince [13]	Source location privacy	mainly deals on SLP but in random walk model.	Only random walk model related works are included with limited papers.
Jiang et al. [14]	Location privacy protection	This survey is classified into three categories i) source node's location privacy protection ii) sink nodes' location privacy protection, and iii) location privacy protection for both source and sink nodes	survey is good but it is mainly based on location privacy.
Our Survey	Source location privacy	source location privacy with adversary model discussed in detail.	Only focused on source location privacy.

- When a message arrives at the sink node, it predicts the direction of that incoming message with the help of section antenna and moves towards that node.
- After moving, the adversary wait for the next message for a fixed amount of time, called the observation period. If any message arrives during that time, then move again else return to the previous node location.
- The above procedure is continued until the adversary reaches the source node.

2.2. Network Model

The main issue with the WSNs is the network lifetime. Due to the limited battery power of the sensor devices, the network lifetime is one of the main research issues. To save the sensor node's energy and increase the network lifetime, a network may split into some clusters or grids [15]. Such a network is helpful to save the energy of the sensor node in large WSNs. However, the researcher proposed the solutions concerning the flat networks where all the sensor nodes are active and homogeneous. The nodes have the same battery power, processing capabilities, and storage capacity. In the network, nodes are deployed randomly to monitor the object and transmit it to the sink node using a multi-hop communication technique. An adversary is there to breach the privacy of the network. It is assumed that the adversary has more battery power, processing capabilities, and storage capacity as compared to the normal sensor nodes [5,70]. They may introduce some malicious nodes in the network, and hence they find out the locations of the source or sink node [16].

There are several works that have been done to preserve the source location privacy using the different approaches [17,18,19]. Among all the different techniques, the most effective technique is the fake source. Researchers have been proved that the protocol based on the fake source is more efficient to achieve better SLP. To the best of our knowledge, there is no updated review article published in the recent year that summarizes current researches. Hence, it is necessary to collect and summarize the research progress, highlight the limitations, and provide future research directions. The updated review may help new researchers in the domain to identify the gaps in ongoing research and proposed new frameworks.

2.3. Inclusion-Exclusion Method

As shown in Figure 3 and 4, the research on SLP was started in year 2004, then it continues. The total number of articles downloaded from the various digital libraries with the help of search keywords is 924. Many articles found duplicates and even not uses the sensor concepts, which was removed and left with 612 articles. The further manual screening was done from our side and excluded 473 articles, as they used the WSN concepts but not for preserving the SLP and hence did not fit our objective. From the remaining 139 articles, the non-English, or without proper simulation details, discusses only security issues but not privacy; not included adversary details are excluded and left with 82 articles.

3. Privacy Protocols with Fake Source and Phantom Routing

The privacy issues in WSN was first introduced by Ozturk et al. [17] with the help of the panda hunter game. They used four different concepts to preserve the SLP of the sensor

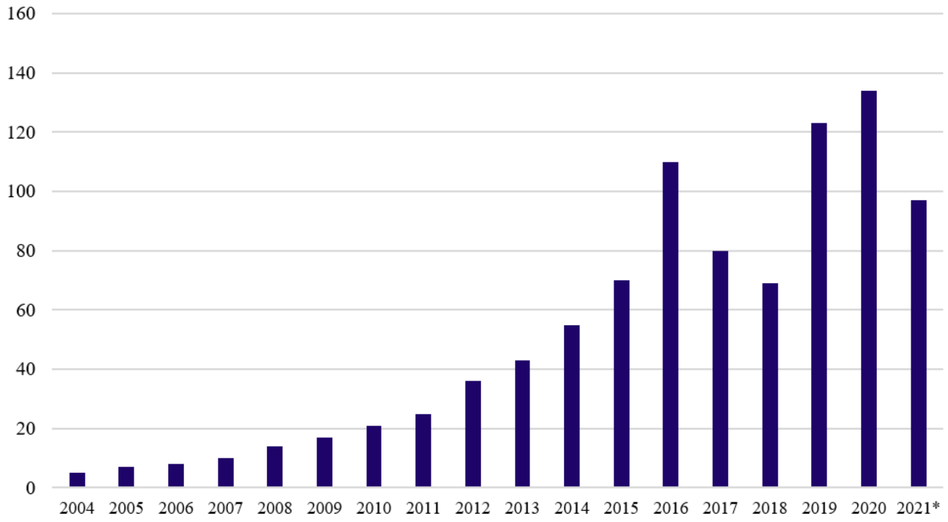

Fig. 3. Number of articles published for SLP in WSNs

node (i) Baseline flooding technique, (ii) Probabilistic flooding technique, (iii) Flooding with fake messages, and (iv) Phantom flooding.

In the Baseline flooding technique, all intermediate sensor node only transfer the message once. Whenever a sensor node receives a message from its neighbour, it checks first whether it is receiving the first time or not, if the first time, then forward, else discard the message. In *probabilistic flooding technique*, only the subset of sensor nodes will participate instead of all the sensor nodes. In this way, the network lifetime was improved. Each node forwards the packet with the dependency of forwarding probability p. The model's drawback was that the networks might be disconnected if the messages were lost while they were in the transit phase. The third approach to preserve the SLP was flooding with fake messages. To mislead the adversary, some fake sources were created on the network to flood the fake messages. Fake messages are similar to real ones. An adversary receives a fake message they cannot differentiate. As a result, they may lead to fake sources instead of the real source node. In the phantom flooding approach, the message delivers to the base station in two phases. First, the message passes up to h hops using either a random walk or directed random walk. Second, flooding technique is used to deliver it to the sink node as shown in Fig. 5.

Two grid-based SLP schemes, namely single phantom node SLP scheme (SPS) and dual phantom node SLP protection scheme (DPS) was proposed [20]. Here, the sink node helps the source node select the phantom node candidate set (PNCS). The source node randomly selects the fake source node from the PNCS. A location privacy mechanism based on fake source nodes was described to keep the source location secret from the global adversary [21,65,67]. Here, the adversary can see the entire network traffic in an energy-efficient manner. A two hierarchy shadow routing was proposed to checkmate the adversary [22]. The adversary gets two levels of obstruction during the enforcement of the traffic analysis attack. The two protocols, namely Two-level phantom with a pursue

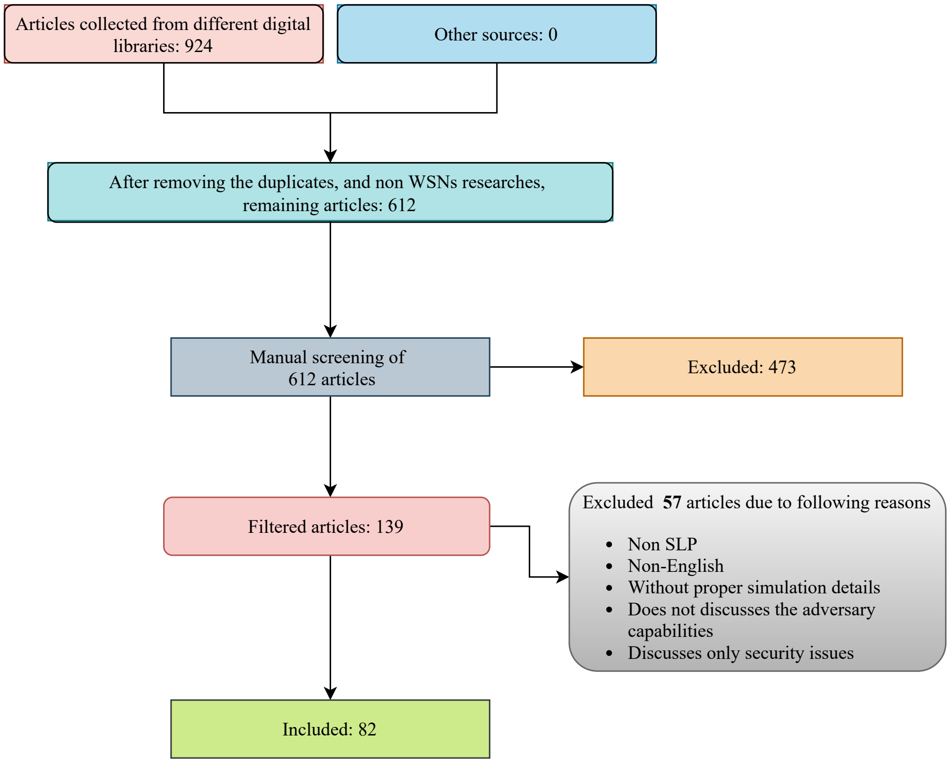
Articles collected from different digital libraries: 924
Other sources: 0
After removing the duplicates, and non WSNs researches, remaining articles: 612
Manual screening of 612 articles
Excluded: 473
Filtered articles: 139
Excluded **57** articles due to following reasons
Non SLP
Non-English
Without proper simulation details
Does not discusses the adversary capabilities
Discusses only security issues
Included: 82

Fig. 4. Process of including and excluding the research articles

ring protocol (PhaP) and Two-level phantom with a backbone route protocol (PhaT), are described, which overcomes the drawbacks of the fake source routing schemes.

To improve the source node's safety period [6] modified the fake source routing technique and suggested a new protocol called phantom routing. In the fake source routing, the fake source node's position is very important because if the fake source node is situated between the real source and the base station, then an adversary may reach the real source while backtracking the messages. In Fig. 6 there are few fake source are shown, among these fake sources the choice of *f1* is not good whereas *f2, f3, f4, f5, f6* are better choice. Among these locations, if a fake source is situated too far from the real source or too near to the real source node, it is not effective to preserve the source node's location privacy. Hence, in the given Fig. 6, *f2, f3, f4* are the best location for the fake source.

3.1. Phantom Routing

Both techniques *baseline flooding* and *single-path routing* are not much effective individually. The path from the source to the base station is fixed in both. As a result, the source node can be easily traced back by an adversary. However, the combination of these two protocols, called "Phantom routing," was a better choice. The outcomes of phantom

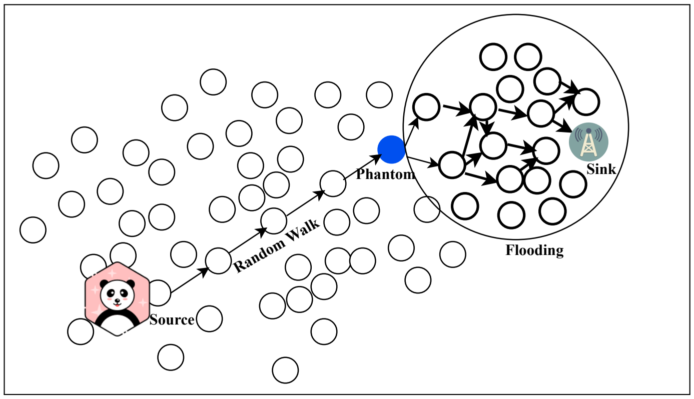

Fig. 5. Phantom routing for source location privacy

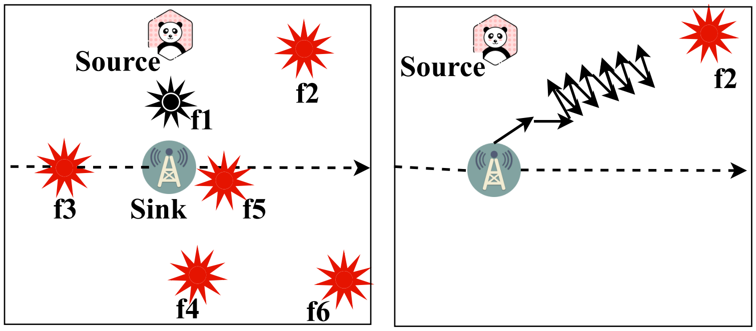

Fig. 6. Different location of fake source and message pulling direction

routing protocols confirmed that it is comparatively better in terms of safety than earlier proposed protocols.

In [23] authors focused on the weak points of the model developed by [17]. They said that if the location of the fake source node is fixed, then there is a high chance that an adversary will record the location and decrease the node's safety period. If the number of fake sources increases and the location of that fake source changes dynamically, it increases the source node's safety period. A more number of fake sources lead to more energy consumption, hence, will degrade network lifetime . To overcome this problem author proposed a protocol called *Cyclic Entrapment Method* (CEM). In CEM, between the source node and base station, a cycle is formed with fake messages as shown in Fig. 7. When an adversary starts backtracking from the base station node, they are trapped into the fake cycle. As a result, the source node's safety period is increased. The safety period depends on the number of loops activated between the source and base station nodes. If there are more loops, then the safety period is high.

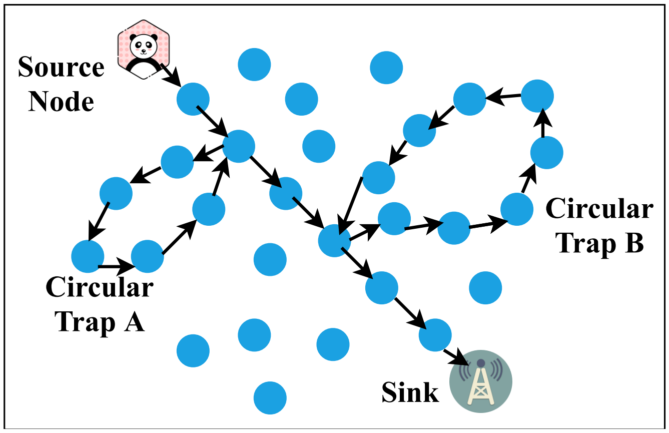

Fig. 7. Cyclic entrapment method

Shao et al. [24] proposed a model called *FitProbRate* that provides privacy to the source node from an adversary that can see the flow of the whole network at any time. In their model, each node forwarded a dummy packet in an interval. The interval may be fixed or probabilistic. Due to the probabilistic flooding technique, they claimed that it increased the source node's network lifetime and privacy. Wang et al. [25] mainly focused on the drawbacks of the phantom single path routing technique. They said that increasing the path length can't improve the safety period in the phantom single path routing technique—the proposed phantom routing with location angle (PRLA). PRLA works in two phases. First, using the inclination angle, selected the phantom node. Instead of choosing the fixed path for the random walk, the sensor node neighbours are divided into two different sets called *nearer* and *further* neighbour. As can be seen from Fig. 8, four phantom nodes are present, and all of them are in the range of the random walk. The message transmitting rate of the source node is to keep high compared to the message tracing rate to secure the source node location. Also, if the phantom node is just opposite the source node, there was a very low probability of an adversary going there. Hence, the selection of such an area for the phantom node may be wasted, as shown in Fig. 9. The definition of a wasted path: The area of coverage that does not increase the privacy of the source node, called the wasted path. If the path having a minimum distance from the sink node to the phantom node crosses through the covered area, the transmitting period is more than the safety period.

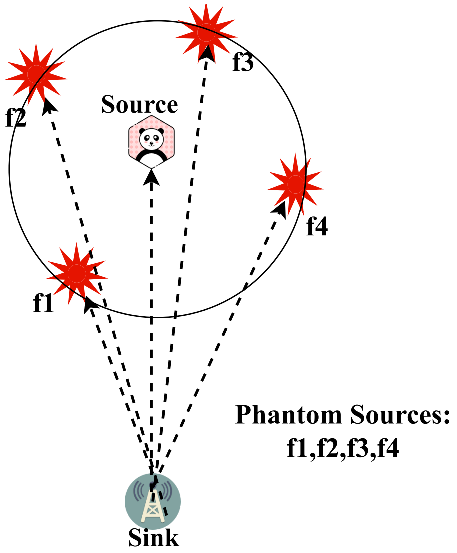

Fig. 8. Possible routes of the messages

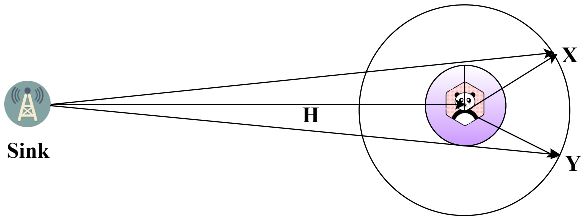

Fig. 9. The ratio of waste path

Doomun et al. [26] proposed a model called Source and Destination seclusion using Clouds (SECLOUD), which can hide the source node from the adversary. They used the concept of the fake source and fake base station. The source and base station nodes are hidden with the help cloud formed with a group of sensor nodes having similar configurations. The source node chose the cloud's size; if the size of the cloud was bigger, the safety period of the source node was high and vice versa. Also, formed some fake source cloud and the base station cloud and were also similarly communicated with each other that the real source and real base station node is communicated. The source node's privacy increases if it intersects the communication line of the fake source cloud and real source cloud with each other at any point. Their model achieves privacy level comparatively better than the random walk technique regarding message overhead, anonymity, and unlike-ability. Recently a similar concept was used to protect the location of source [27].

Wang et al. [28] proposed a protocol called Weighted Random Stride (WRS) routing . In this technique, two parameters, the stride and the forwarding angle, were used (Fig. 10). The forwarding angle is between the estimated forwarding route and the line joining the forwarding node and the base station node. The main aim of their work was to fix up some pre-route from the source node to the base station node. The source node can choose any pre-set routes to send a message to the base station. So, an adversary is forced to stay on one of these routes to backtrace the source node's location, which helps to increase the safety period of the node. The application demand led to the development of data centre sensor networks. Shao et al. [29] proposed a protocol called Data-Centric Sensor networks (DCS) Security and Privacy Support. They named the sensor data based on event type or geographic location as a contrast to sensor nodes. To address DCS security issues, they proposed another protocol called a privacy-enhanced DCS (pDCS) network that offers different data privacy levels based on different cryptography keys. They also proposed query optimization techniques based on Euclidean Steiner Tree [30], and Keyed Bloom Filter [31] to minimize the query overhead while providing query privacy.

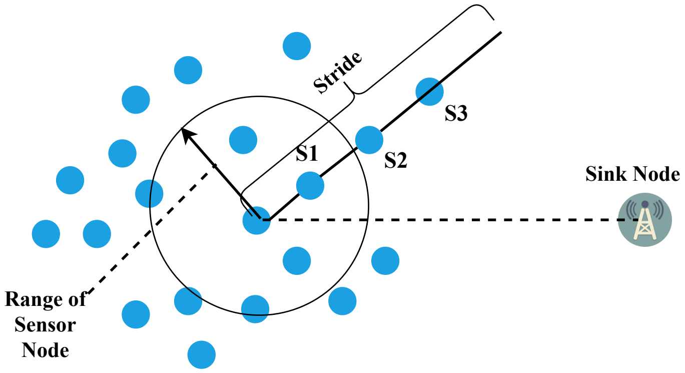

Fig. 10. Weighted random stride routing scheme

Alomair et al. [32] proposed a model that can guarantee the event indistinguishability by achieving Event Indistinguishability (EI) and interval indistinguishability (II). In EI, an adversary is unable to distinguish between the real event message and the fake message. In II, the adversary cannot distinguish between the first, the middle, or the end of the interval. The EI-based approach provides anonymity under EI and quantifies its information leakage. Their proposed technique was helpful to preserve the souce anonymity in the wireless sensor networks. When a source node is located far away from the base station node, there is a high latency in the message delivery rate. Kokalj et al. [33] referred to this latency as the publishing route latency. They argue that the FitProbRate protocol [24] does not work well for the networks where the source node is just one hop away from the base station. The actual latency of the publishing route depends on the rate of reporting of events.

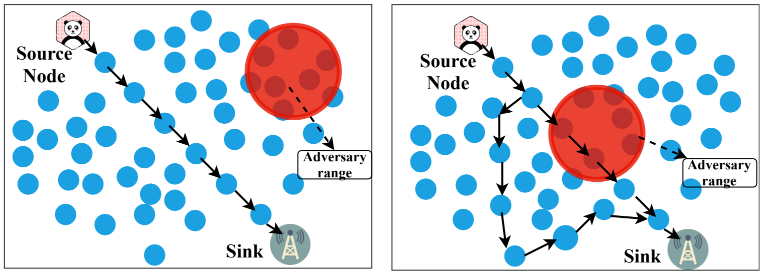

Fig. 11. Method to chose different path when an adversary is present

Rios et al. [34] proposed Context-Aware Location Privacy (CALP) protocol for SLP. Earlier proposed protocols have some disadvantages, such as in most of the techniques, the data packets were routed to the base station blindly without any prior knowledge of an adversary. Hence, it cost more energy consumption of the network that leads to network lifetime decreases. To overcome this issue, they used the advantages of sensor nodes, as the sensor node check whether any mobile agent is present in their communication range or not. Based on the adversary's availability, the process of data delivery to the base station is changed. The CALP algorithm's working principle can be seen from Fig. 11 where the network adapts the routing path to bypass an adversary moving in the locality of the shortest path.

Jiang et al. [14] described the importance of securing location information. The intruders can get the location information from the packets exchanged between the source and destination. They have done an extensive survey to classify the source location privacy, sink location privacy for securing the location information. Additionally, network performance, packet delay, energy efficiency, and network safety is analyzed. Mehta et al. [38] proposed a protocol that could hide the source location from the global adversary. A real sender can be hidden from an adversary by using multiple proxy source nodes [39]. The multiple source branch can be achieved by using the random walk model. The multiple proxy nodes are selected randomly from the list of neighbour nodes by the source node. This scheme prevents adversaries from getting the location information from the real source nodes. Besides, branch interference is created around the base station by increasing the routing branches.

Multiple sinks are used in this scheme to protect the source node from the adversaries [40]. Dynamically multiple paths are generated to confuse the adversaries. A high volume

Table 2. An overview of the research work for SLP in terms of different metrics

Protocol	**Accuracy**	**Power Uses**	**Delay**	**Privacy**
Fake source [6]	There is no impact on accuracy and data arrival	High	No	Misguide from real source
Dummy injection to protect real source [18]	There is no impact on accuracy and data arrival	High	Yes	Dummy packet disturb the traffic pattern
Flooding to protect the data source [36]	Baseline Flooding: Yes, Probabilistic Flooding:No Guarantee of data arrival	High	Baseline Flooding: NO, Probabilistic Flooding: Not guarantee packet comes with shortest route	Baseline Flooding: Less, Probabilistic Flooding: High
Random Delay [37]	There is no impact on accuracy and data arrival	Normal	Yes	Yes
Random Walk [5]	Phantom: Yes, Grow: Depends on intersection of random walk	Average	For Phantom: depends on no, of hops, GROW: depends on randomness path	Yes, Misguide from the real route
Random packet sending time [19]	There is no impact on accuracy and data arrival	Normal	Yes	Create ambiguity between two hops
Packet transmission rate	There is no impact on accuracy and data arrival	Normal	Yes	Hide traffic pattern with transmission control

of the number of packets can be transmitted through multiple paths towards multiple sink nodes. The scheme focuses on local adversaries based on the transmission loop of the actual and forgery packets. The sociality among the sensor nodes can be discontinued in this scheme.

Path Extension Method (PEM) proposed by Tan et al. [41] to preserve the privacy of the source node from the adversary. They used fake source concept to mislead the adversary from the real route. The fake source node is chosen and wherein the network they were placed as described in [6,28]. Fake sources are generated after the network is deployed and activated by receiving a message generated by the source node, increasing the sensor node lifetime. Once the fake sources receive a real message from the source node, they start creating a fake tree in the backbone with fake messages as shown in Fig. 12. The author compares their work with the other existing work based on fake source nodes such as [6,17], and found that the safety period of PEM is comparatively better than the existing work. Also, the delay is less, and the network lifetime is more.

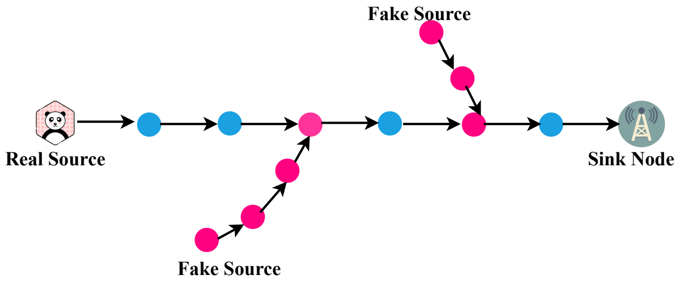

Fig. 12. The working model of path extension method

Angle-based Dynamic Routing Scheme (ADRS) proposed for SLP in [42]. When a sensor node becomes the source node, before broadcasting their message to all their neighbours' nodes, send a Request to Send (RTS) message. After getting the Clear to Send (CTS) from the neighbour sensor node, measure the angle ϕ between the neighbour node and the distance concerning the base station node. Based on these measurements, the next node was selected for the communication. A cloud-based source location privacy scheme is proposed with multiple sinks in place [43]. Due to the availability of multiple sinks, the destination of each packet changes randomly for each transaction. The routing paths are varied for each packet with the help of intermediate nodes. A directed random walk model is adopted to hide the source nodes' direction information from the adversaries. Roy et al. [5] used fake source and phantom routing concept for SLP. The source node sent the message to the phantom source using random walk. The phantom source flooded the message in the network to deliver it to the base station. Their model consumes more energy for flooding operations.

Zhou et al. [44] proposed an anonymous routing protocol for preserving location information (ARPLP) by using the proxy source nodes. The proxy node is randomly selected from the list of neighbours to create confusion for the hackers to get the location information of the actual source node. The real source node randomly sends the packets to the neighbours until the packet reaches the proxy node. The routing branches are increased to disturb the adversary from getting the real path towards the source node. This scheme preserves the source/sink location information of the wireless multimedia sensor networks [45]. It uses multipath routing to hide the location information and the event occurrence of the source node. The cross-layer design among the application and routing layers is used to protect the source locations. Han et al. [46] proposed a model using the cloud and multi sink technology. The destination of every packet changes randomly for each transmission. The routing path for each packet changes automatically due to the presence of multiple sinks and intermediate nodes. Fake messages are added to the WSN to create a fake hotspot in the network. The important packets travel in multiple paths, which creates confusion for the hotspot locating adversaries.

Kumar et al. [19] proposed a new concept to secure the location of the source node in WSN. In their proposal, the base station node selected three nodes located on a fixed angle position that formed a triplet. Among these triplets, if a node becomes the source node, the other two-node act as a phantom node for that source node. Their work was extended by [36]. The authors used two phantom nodes to preserve the source node's privacy. The selection of the phantom node is based on the triplets. The triplets are a group of three nodes in the network based on a position concerning the sink node and the distance from the sink. Whenever the source node wants to send a packet to the base station, two phantom nodes are created and based on these. The packet is forwarded to the sink node via a phantom node. Since the phantom node's position and location are dynamic, it is very hard for an adversary to trace back the location of the source node.

Bai and Zhu [47] proposed an SLP scheme using a random annular region. The annular region was developed based on the coordinates of the actual and intermediate nodes. The relay node and source node are selected in one direction, but the phantom node was selected in the random annular region. The packets can be transmitted from the source towards the sink by strategically positioned mediate nodes [48]. The mediate nodes are selected based on the locality information. Multiple paths are used to transmit the packets towards the sink node, which creates confusion for the sink node to trace out the real sending node. An SLP scheme based on the anonymity cloud is proposed by Wang et al. [27]. The source node initially sends a lightweight message to its neighbours to create an anonymity cloud in its periphery. The set of nodes present in the cloud must have the same frequency range. The small message travel range forms the anonymity cloud. The duplicate nodes present in the borders of the cloud independently send the short messages. The real message can be recovered at the sink node when it receives at least *t* shares. The adversary uses the hidden Markov model to find the source node. So a probabilistic SLP model was proposed to identify the adversaries easily. The fake source nodes are used to mimic the behaviour of the actual source nodes. These specific nodes are used to diversify the routing path among the source and sink nodes. Deciding the next-hop node is dependent on the calculated weight of the nodes [49].

Bradbury et al. [50] proposed a hybrid model called DynamicSPR, which preserves the privacy of the source node. They used a random walk technique for fake source allocations in the network, which helped reduce energy consumption and improve the privacy of the source node. Wang et al. [51] proposed a model using the fake source technique, namely SLP full protection (SPFP). Their model able to defend the smart adversary also means the adversary who has access to both the global and local view of the network. To address the issue of energy consumption in WSN, authors [52]proposed Energy Balanced Branch Tree (EBBT) in SLP. Their model uses fake sources and works in three phases: firstly, the source node is sent to an intermediate node randomly, then with minimum hop routing, the shortest path between the intermediate node and the base station is identified. Finally, a tree-shaped structure helps to achieve the privacy of the source node. Mamoun et al. [53] proposed clustering-based approach for SLP. They used dynamic shortest path and dynamic tree and their combinations to achieve the best privacy for the source. Chen et al. [54] suggested a protection scheme based on sector phantom routing scheme for SLP. Both the phantom source and random routing strategies were used in their approach. Tang et al. [55] suggested a theoretical model for analysing information leakage. Arvarsi et al. [56] did a survey of existing SLP protocols and calculated the number of sensor nodes needed to deploy to achieve the SLP, ensuring the connectivity of the WSN.

Alzaabi et al. [57] have presented a new location privacy protection algorithm based on phantom technique. This is energy-aware privacy preservation named phantom++. They have used a layering in-depth scheme to enhance the security in phantom++. The major problem with this scheme is validation because the authors have not presented any simulation results and analysis. To increase the source location privacy, fake packets and multi-path techniques are applied. An Adaptive Trust Sector-Based Authenticated System (ATSAS) is developed for SLP by Arivarasi, and Ramesh [58]. In their work, message authentication is done by honey encryption, and for security, packet encryption is used. This scheme provides better security in SLP, but it is complex due to multiple encryptions. Zhou et al. have designed a pseudospiral-based routing protocol for WSN to protect the node location as well as the location of base station [59]. To achieve this, they use a new two-phase location attack for two important types of nodes (including a base station and a source node). Mutalemwa and Shin extended their previous work to increase the reliability of the messages in SLP schemes [60]. They have done this work with three objectives. First, a new relay ring routing (ReRR) protocol is proposed, whereas in second, measuring the safety period of SLP with different parameters is done, and last, reliability of the scheme is evaluated.

George and Babu [61] proposed a semantic clustering-based approach to gain the efficacy of the source location privacy of the nodes. They encrypt each message sent by the sender to the intermediate nodes to minimize the chance of eavesdropping. The message transferred by each of the senders follows energy efficiency mechanisms to enhance the lifetime of the networks. The authors have assumed that the position of the base station is known to the attacker. So this tree-based clustering approach gives a better result as compared to the previous ones. The semantics co-relation-based clustering mechanism has shown better performance metrics such as energy consumption and message overhead in opposition to a universal adversary. The sink node verifies the identity of each source node by using a pseudo-random number. The authors tried to improve the data transmission process by combining the AES with ECC to minimize the chance of detecting the source location of the sender node [62]. A new localization method is proposed by the authors, which reduces the chance of localization error. The network communication overhead is also minimized by employing the authentication process for each sent information.

The summary of the research work published by the researcher using the fake sources and phantom routing techniques are presented in Table 3. To get the network information,

Table 3. A summary of key researches with network view and protocol used to preserve the SLP in WSNs

Proposed by	**Network View**	**Technique/Protocol**	**Issues**
Kamat el al. [6]	Local	PFSR,SLFSR	Yes
Majeed et al. [63]	Local	TARP	Yes
Roy el al. [5]	Local	FSAPR	NA
Kumar el al. [19]	Local	FSAPR	NA
Gupta el al. [36]	Local	2PARS	NA
Mahmoud et al. [4]	Local	CSPSLP	NA
Zhou et al. [39]	Local	Multiple proxy source nodes	NA
Hao et al. [49]	Local	Fake source nodes	Yes
Almalkawi et al. [45]	Local	WMSN and Multipath routing	NA
Han et al. [46]	Local	Cloud and Multisink	NA
Mutalemwa and Shin [22]	Local	Fake source routing	Yes
Bai et al. [47]	Local	Phantom node	Yes
Adilbekov et al. [21]	Local	Fake source node	NA
Wang et al. [20]	Local	PNCS	Yes
Zhou et al. [44]	Local	Proxy source node	NA
Mutalemwa et al. [48]	Local	Multiple path routing	Yes
Shao et al. [24]	Global	ProbRat and FitProbRate	Yes
Doomun et al. [26]	Global	SECLOUD	Yes
Yang el al. [64]	Global	PFS and TFS	Yes
Mehta et al. [38]	Global	PBA, SoSi	NA
Bicakci el al. [65]	Global	PBA	NA
Yang el al. [66]	Global	TCH-WSN	NA
Ortolani el al. [67]	Global	UHT	NA
Lu el al. [68]	Global	$TESP^2$	NA
Ouyang et al. [69]	Global	GOA	Yes
Kokalj el al. [33]	Global	GAFG	NA
Shao et al. [29]	Global	Used fake packets	NA
Yang et al. [70]	Global	ASLP	NA
Abbasi et al. [72]	Global	DRAA	Yes
Tangil et al. [73]	Global	DWUS	Yes
Jhumka et al. [18]	Global	FS1 & FS2	Yes
Han et al. [40]	Global	Multiple sinks and Fake packets	NA
Miao et al. [43]	Global	Multiple sinks	Yes
Chen et al. [71]	Both Local and Global	DBT & ZBT	NA

an adversary may perform a passive or active attacks. The form of attacks is explained as follows:

- **Denial of service:** This is an active attack in which an adversary is able to restrict all further communication between the nodes using the denial of service attacks.
- **Node Compromise:** In WSN, there is a high possibility that the nodes are getting compromised during the communication. There are two different types of node compromise, a) active node compromise and b)Passive node compromise.
- **Packet alteration:** It may be possible that an adversary altered the content of the packet before forwarding to the next hop.
- **Packet drops:** It may be possible that an adversary drops the incoming packet in between.
- **Packet injection:** The adversary is able to inject its own packet on the network.
- **Rate monitoring:** This is a passive attack which comes under traffic analysis attack. Through this attack an adversary looking for those sensor nodes which have a higher transmission rate. Such a node might be closer to either source or sink.
- **Angle of Arrival:** This is a passive attack that allows an adversary to see the incoming packet direction. An adversary needs a sectional antenna (special hardware) to perform this operation.
- **Hop-by-Hop trace:** An adversary able to follow the path of incoming message direction, using this they can easily reach the source of the message.
- **Eavesdropping:** An adversary is capable to overhear or intercept the message but can not decode them. They are only able to see the content of the message with this attack.
- **Timing analysis:** With the help of this attack, an adversary is able to understand the structure of the wireless sensor network.
- **Time correlation:** This is a passive attack in which timing information is used by an adversary to find out the path between source node to the sink node.
- **Traffic analysis:** The adversary has performed a traffic analysis of the WSN to analyze the path between the source and sink node. There is no specific method of traffic analysis is explained. It may be performed with the help of "rate monitoring", "timing analysis" attack.

Based on the capability, an adversary may view the entire network communication, or a part of network communication at a time. The different types of network access by the adversary are explained as follows.

- **Local view:** In this network view, an adversary is able to view only local (i.e., within their range) communication of the network.
- **Global view:** In this network view, an adversary is able to view the communication of the entire network [68,65,66].
- **Multi-Local view:** In this network view, there are many adversaries present in the networks and located at different network locations. Also, they are exchanging their information with each other. The other type of multi-local adversary includes a semi-global adversary, which is more powerful than the local adversary.

There may be a chance that the network nodes are compromised, and hence the important information may be shared with the adversary. For example:

- **Distribution of event:** An Adversary knows how the event is distributed in the network.
- **The protocol:** The adversary knows which protocol is used in the networks.
- **Identities of node:** An adversary knows the identity of the mentioned node in the message.
- **Location of the sink:** The adversary knows the location of the sink node.
- **Part of the routing algorithm:** The adversary knows some parts about the routing algorithm used on the network.

In the last column of Table 3 we have a parameter *Issue* which can be treated as follows: a) an adversary knows how the event is distributed in the network, b) adversary knows which protocol was used in the networks. Due to these issues, the source node's privacy may not be preserved for a longer time.

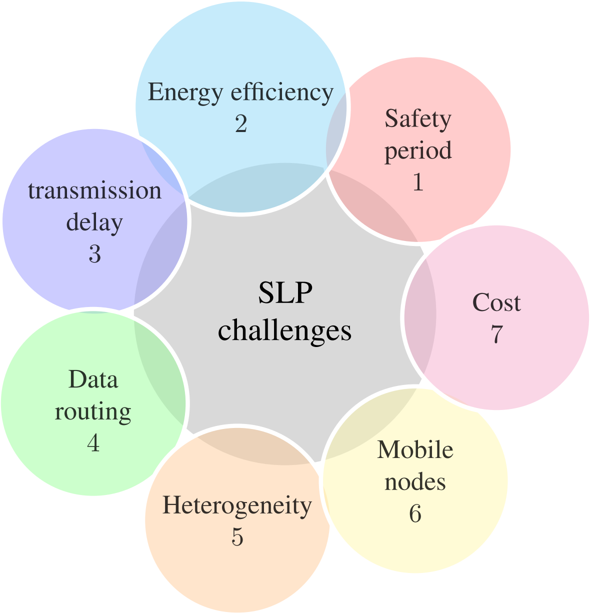

Fig. 13. SLP challenges of WSN with an increasing priority.

4. SLP challenges for WSN

The SLP model is an important area where many researchers have contributed their ideas and published papers. Our survey suggested several major challenges that required proper attention based on the reviewed journals in this area. These challenges are illustrated in Fig. 13 based on their priorities and discussed in detail. The priority is calculated depending on the published literature on these topics.

Safety period: The safety period is the total network duration earlier than the adversary is attacked or seized. It can be measured by calculating the total number of packets successfully transmitted to the destination [74]. The main challenge is how long the source node deviates from the adversary to reveal its location in this context. **Energy efficiency** Energy efficiency is always a vital parameter to increase the lifetime and performance of WSN. In SLP, we can save energy as well as privacy by using compressors or aggregators which aggregates the received data so that any adversary could not find out the original data and its source easily [75]. Privacy-preserving using aggregators to minimize the energy consumption are discussed in these articles [76,77,78].

Transmission delay: Maintaining transmission delay in the SLP context is the most challenging task. To preserve the source's location privacy, we need to deviate the routes of packets from source to destination or vice versa. It leads to extra delays in the network. Protocols proposed by [5] and [6] offer the best trade-off between transmission delay and SLP for WSN.

Data routing: To deliver data successfully from source to destination and vice versa, several routing schemes have been proposed like phantom routing, ring routing, random walk, etc. But still, more improvement is required. It is a major challenge to design an optimal routing scheme with a higher safety period to enhance the SLP [79].

Heterogeneity: Most of the research is done in homogeneous sensor networks for SLP, but real-world WSNs is heterogeneous. So we required some robust protocols for SLP, which can perform well in all scenarios. Design such types of schemes are a challenging task [80].

Mobile nodes: Nowadays, many WSNs are hybrid in terms of static and mobile nodes [81]. In mobile WSN, protecting the source is more challenging as compared to static [82]. Many researchers have proposed some SLP techniques using mobile nodes. **Cost:** Cost is always a major factor in any type of network. In WSN, to preserve the SLP, so many extra special nodes and devices are deployed, increasing the total cost of WSN. This can not be considered in most of the scenarios because one of the main advantages of WSN is the least cost [83].

4.1. Lesson Learned

Source location privacy in WSN is an important concern in the current era where everything is moving towards automation. The researchers propose many protocols to handle these issues using different approaches. The target of each approach is to preserve the location privacy of the source from the adversary. The popular technique used for this task is Phantom routing, where the source node delivers the message to the phantom node, and further, it is delivered to the base station using either the shortest path or flooding approach. Another popular approach to preserving the SLP is fake sources, which are created in the network. All created sources generate a similar message to the real one and flood the network. This message flood cerates challenge for the adversary to find the real one and trace the source node. Apart from this, the flooding technique is also used. In the flooding technique, the message is flooded in all directions of the network to deliver it to the base station. The researchers identified major issues with network lifetime. The sensors used in the network have limited power and can not be alive more time. Based on the network activities like sending the messages, receiving, or processing them, the power of sensor nodes decreases. Hence, to develop a robust privacy-preserving protocol, energy consumption is an important parameter. Another parameter is latency. The aim of the network is to deliver sensitive information. Hence the latency must be minimum. The future researcher may considered these parameter for developing a new efficient privacy preserving protocol.

5. Future research directions

To secure the privacy of sources and data in WSN, new techniques with different domains increasing day by day. Researchers have tried many areas and techniques to improve SLP protocols' efficiency, but several areas are untouched or not explored properly. Fig. 14 illustrates some future research topics for SLP in WSN.

Content-oriented privacy: In the privacy model, several SLP schemes are designed as compared to content, or data-based privacy [84]. SLP is a part of content privacy only, but it requires special attention to keep its integrity, freshness, and confidentiality.

Energy harvesting: Energy harvesting in WSN is an emerging area of research. A few researchers have applied this energy harvesting to secure the source node [85]. However, this area has many possibilities to explore and develop some robust schemes for SLP.

Cloud-based: Cloud-based source location privacy is a new area where many scopes are there for new research. Few papers are published in this area where authors are used cloud with some fake sensor nodes to mislead the adversary [46] and [27].

Mobility: The impact of the mobility model on SLP is not being fully exploited in WSN. A mule mobility pattern [86] has been proposed to make a trade-off between SLP and delay. WE can also use mobile sinks or nodes to develop effective SLP techniques with minimum energy consumption.

Internet of Things (IoT): Now WSN is evolved with a new wing and applications known as IoT, which emerges new challenges and future works. The SLP is also important in IoT due to a large number of sensor nodes and real-time applications. IoT for SLP introduced [87], but a lot of things are required to do in this area.

Light-weight encryption algorithms: Several schemes have been proposed to protect the source from the adversary, but each has its problems. Most of the adversaries backtrack the source and destination messages and finds the actual source. A light-weight encryption algorithm is the most effective technique to protect the source but problem is designing a light-weight encryption algorithms [88][89]. In the future, designing a lightweight encryption protocol for WSN which suits the sensor nodes.

Network Coverage: Network coverage is an essential topic for all scenarios of the WSN. Many SLP related techniques are compromised with network coverage in the WSN [90]. To make a trade-off between SLP and network coverage is an important area where researchers need to give some more attention.

Hot Spot: Energy hot spot is a common phenomenon in WSN where a node consumes higher energy than other nodes, and that node dies early. Generally, the source and its nearby nodes transmit more packets than other nodes, resulting in an energy hot spot. Due to this problem, an adversary can easily detect the source, which is not acceptable in SLP methods [4]. So a lot of different things we can explore in SLP with an energy hot spot. In this area, a small number of researchers have shown their interest. Apart from the discussed future areas and challenges, many other sensor network-related issues come

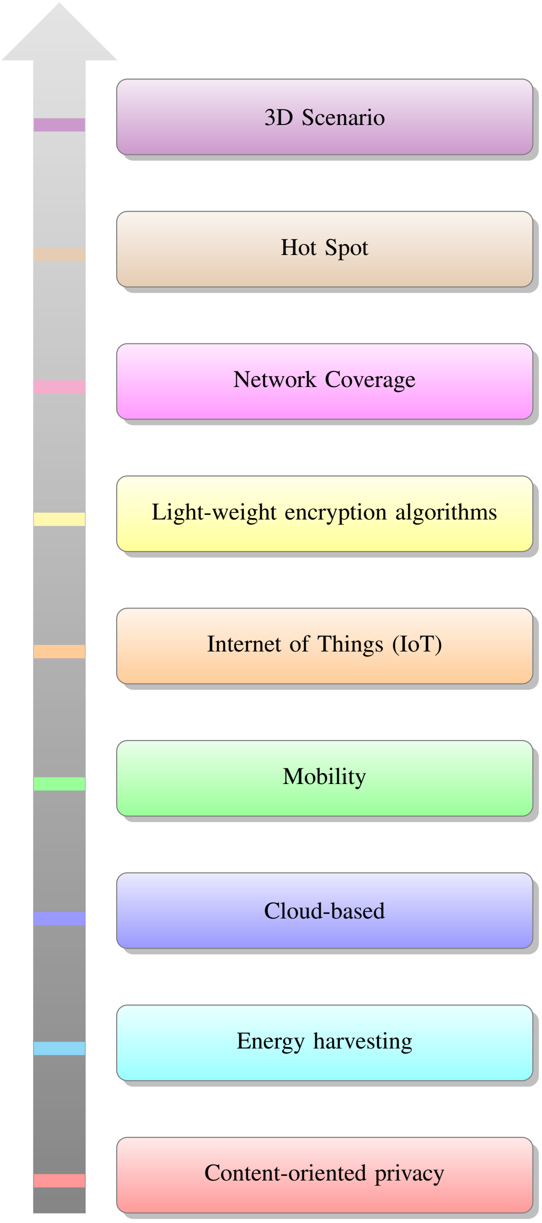

Fig. 14. Priority-wise research area for SLP in WSN

in the future, affecting SLP like new attacks or new technology. Researchers need to be ready for new solutions for new challenges and future works in WSN for SLP.

3D Scenario: Generally, authors consider a 2D scenario for their experiment in wireless sensor network but in the real-world 3D scenario is the best suited in this area [91]. Therefore, location privacy is also an important topic in 3D scenarios, but it has not received proper attention. In this area, a lot of potential work's scope is there, which the researchers need to deal with.

6. Conclusion

The source location privacy issue is continuously getting the attention of worldwide researchers, which shows the importance of this topic. Research has been done in this area, and many important milestones have been achieved, but certain issues still need to be explored. We have done an extensive survey on recently published papers on detecting SLP in Wireless Sensor Networks in this work. The Panda hunter game first explains the SLP problem. The WSN privacy issues are mainly categorized into two parts, a) Data privacy and b) context privacy. This article focused on the context of privacy, whose objective is to provide privacy to context, such as the location of the sensor nodes. The context of privacy is again divided into two categories: source location privacy and sink location privacy. In this paper, we intensely focused on source location privacy mechanisms.

The existing SLP schemes focused on local adversaries to be less capable of global and multi-local adversaries. Sending more fake packets attracts more energy consumption and maximum chance of congestion in the network. The SLP is not only possible to achieve by hiding the identity of a node. Additionally, dummy traffic, fake source nodes, and multi-path routing are used to counter the traffic analysis problem. In the future, this work can be extended by discussing the other location privacy issues such as sink location, temporal location privacy, and others. We discussed more than 90 papers on SLP, which were published in recent times. All the research works have been grouped based on their adversary model and network model. The readers of this paper will get insights into the different categories of SLP schemes used in WSNs. Lastly, the challenges of SLP towards the WSN is briefly discussed in this paper.

References

1. T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency internet of things," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 72–84, 2017.
2. P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.
3. B. Chakraborty, S. Verma, and K. P. Singh, "Differentially private location privacy preservation in wireless sensor networks," *Wireless Personal Communications*, vol. 104, no. 1, pp. 387–406, 2019.
4. M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.

5. P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, “3rd international conference on recent trends in computing 2015 (icrtc-2015) source location privacy using fake source and phantom routing (fsapr) technique in wireless sensor networks,” *Procedia Computer Science*, vol. 57, pp. 936 – 941, 2015.
6. U. Kamat, Y. Zhang, and C. Ozturk, “Enhancing source-location privacy in sensor network routing,” in *25th IEEE International Conference on Distributed Computing Systems (ICDCS*, 2005, pp. 599–608.
7. 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, Third 2013.
8. N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, “Privacy preservation in wireless sensor networks: A state-of-the-art survey,” *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.
9. J. Lopez and J. Zhou, “Wireless sensor network security, vol. 1 of cryptology and information security series,” pp. 223–250, 2008.
10. S. Lee, J. Kim, and Y. Kim, “Preserving source-and sink-location privacy in sensor networks.” *Comput. Sci. Inf. Syst.*, vol. 13, no. 1, pp. 115–130, 2016.
11. R. Rios, J. Lopez, and J. Cuellar, “Location privacy in wsns: solutions, challenges, and future trends,” in *Foundations of Security Analysis and Design VII.* Springer, 2013, pp. 244–282.
12. J. Jiang, G. Han, H. Wang, and M. Guizani, “Privacy models in wireless sensor networks: A survey,” *Journal of Sensors*, vol. 2016, pp. 1 – 18, 2016.
13. S. Gupta and B. Prince, “Preserving privacy of source location using random walk: A survey,” in *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, 2016, pp. 2047–2051.
14. J. Jiang, G. Han, H. Wang, and M. Guizani, “A survey on location privacy protection in wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 125, pp. 93–114, 2019.
15. M. Kamarei, A. Patooghy, A. Alsharif, and V. Hakami, “Simple: A unified single and multipath routing algorithm for wireless sensor networks with source location privacy,” *IEEE Access*, vol. 8, pp. 33 818–33 829, 2020.
16. V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, “Malicious node detection using heterogeneous cluster based secure routing protocol (hcbs) in wireless adhoc sensor networks,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–7, 2020.
17. C. Ozturk and Y. Zhang, “Source-location privacy in energy-constrained sensor network routing,” in *In ACM SASN*, 2004, pp. 88–93.
18. A. Jhumka, M. Leeke, and S. Shrestha, “On the use of fake sources for source location privacy: Trade-offs between energy and privacy,” *The Computer Journal*, vol. 54, no. 6, pp. 860–874, 2011.
19. P. Kumar, J. P. Singh, P. Vishnoi, and M. P. Singh, “Source location privacy using multiple-phantom nodes in wsn,” in *TENCON 2015 - 2015 IEEE Region 10 Conference*, Nov 2015, pp. 1–6.
20. Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, “Sps and dps: Two new grid-based source location privacy protection schemes in wireless sensor networks,” *Sensors*, vol. 19, no. 9, p. 2074, 2019.
21. U. Adilbekov, A. Adilova, and S. Saginbekov, “Providing location privacy using fake sources in wireless sensor networks,” in *2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT).* IEEE, 2018, pp. 1–4.
22. 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, pp. 1–30, 2020.
23. Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, “Entrapping adversaries for source protection in sensor networks,” in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, 2006, pp. 23–34.
24. M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.* IEEE, 2008, pp. 466–474.

25. W.-P. Wang, L. Chen, and J.-X. Wang, "A source-location privacy protocol in wsn based on locational angle," in *2008 IEEE International Conference on Communications*. IEEE, 2008, pp. 1630–1634.
26. R. Doomun, T. Hayajneh, P. Krishnamurthy, and D. Tipper, "Secloud: Source and destination seclusion using clouds for wireless ad hoc networks," in *Computers and Communications, 2009. ISCC 2009. IEEE Symposium*. IEEE, 2009, pp. 361–367.
27. N. Wang, J. Fu, J. Li, and B. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 100–114, 2020.
28. H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.
29. M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang, "pdcs: Security and privacy support for data-centric sensor networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 8, pp. 1023–1038, 2009.
30. P. Winter and M. Zachariasen, "Euclidean steiner minimum trees: An improved exact algorithm," *Networks*, vol. 30, no. 3, pp. 149–166, 1997.
31. B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.
32. B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical framework for source anonymity in sensor networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.
33. S. Kokalj-Filipović, F. Le Fessant, and P. Spasojević, "The quality of source location protection in globally attacked sensor networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*. IEEE, 2011, pp. 44–49.
34. R. Rios and J. Lopez, "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks," *The Computer Journal*, pp. 1–11, 2011.
35. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*. IEEE, 2005, pp. 599–608.
36. S. Gupta, P. Kumar, J. P. Singh, and M. P. Singh, "Privacy preservation of source location using phantom nodes," in *Information Technology: New Generations*, S. Latifi, Ed. Cham: Springer International Publishing, 2016, pp. 247–256.
37. J. Chen, Z. Lin, Y. Liu, Y. Hu, and X. Du, "Sink location protection protocols based on packet sending rate adjustment," *International Journal of Distributed Sensor Networks*, vol. 12, no. 1, pp. 1–10, 2016.
38. K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.
39. L. Zhou and Y. Shan, "Multi-branch source location privacy protection scheme based on random walk in wsns," in *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*. IEEE, 2019, pp. 543–547.
40. 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, 2019.
41. W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in wsns based on path extension," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 461–471, 2014.
42. P. Spachos, D. Toumpakaris, and D. Hatzinakos, "Angle-based dynamic routing scheme for source location privacy in wireless sensor networks," in *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*. IEEE, 2014, pp. 1–5.

43. X. Miao, G. Han, Y. He, H. Wang, and J. Jiang, "A protecting source-location privacy scheme for wireless sensor networks," in *2018 IEEE International Conference on Networking, Architecture and Storage (NAS)*. IEEE, 2018, pp. 1–5.
44. L. Zhou, Y. Shan, and X. Chen, "An anonymous routing scheme for preserving location privacy in wireless sensor networks," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. IEEE, 2019, pp. 262–265.
45. I. T. Almalkawi, J. Raed, N. Alghaeb, and M. G. Zapata, "An efficient location privacy scheme for wireless multimedia sensor networks," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 1615–1618.
46. 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 Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2739–2750, 2019.
47. L. Bai, H. Zhu, and G. Li, "Privacy protection algorithm based on random annular region in wsn," in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*. IEEE, 2018, pp. 64–67.
48. 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.
49. H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, "A probabilistic source location privacy protection scheme in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5917–5927, 2019.
50. M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 115, pp. 67–81, 2018.
51. N. Wang, J. Fu, J. Zeng, and B. K. Bhargava, "Source-location privacy full protection in wireless sensor networks," *Information Sciences*, vol. 444, pp. 105–121, 2018.
52. H. Wang, L. Wu, Q. Zhao, Y. Wei, and H. Jiang, "Energy balanced source location privacy scheme using multibranch path in wsns for iot," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.
53. M. F. Al-Mistarihi, I. M. Tanash, F. S. Yaseen, and K. A. Darabkh, "Protecting source location privacy in a clustered wireless sensor networks against local eavesdroppers," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 42–54, 2020.
54. Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "Psspr: A source location privacy protection scheme based on sector phantom routing in wsns," *International Journal of Intelligent Systems*, 2021.
55. D. Tang, J. Gu, W. Han, and X. Ma, "Quantitative analysis on source-location privacy for wireless sensor networks," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 805–809.
56. A. Arivarasi and P. Ramesh, "Review of source location security protection using trust authentication schema," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, 2020, pp. 215–222.
57. A. Alzaabi, A. Aldoobi, D. Alnuaimi, L. Alserkal, M. Alsuwaidi, and N. Ababneh, "Grid-based source location privacy protection schemes in iot wireless sensor networks," in *2021 4th International Conference on Data Storage and Data Engineering*, 2021, pp. 31–36.
58. A. Arivarasi and P. Ramesh, "An improved source location privacy protection using adaptive trust sector-based authentication with honey encryption algorithm in wsn," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.
59. Z. Zhou, Y. Wang, P. Li, X. Chang, and J. Luo, "Node location privacy protection in unattended wireless sensor networks," *Mathematical Problems in Engineering*, vol. 2021, 2021.
60. 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. 104 820–104 836, 2021.

61. C. M. George and S. L. Babu, "A scalable correlation clustering strategy in location privacy for wireless sensor networks against a universal adversary," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 2019, pp. 1–3.
62. M. A. Tamtalini, A. E. B. El Alaoui, and A. El Fergougui, "Eslc-wsn: A novel energy efficient security aware localization and clustering in wireless sensor networks," in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*. IEEE, 2020, pp. 1–6.
63. A. Majeed, K. Liu, and N. Abu-Ghazaleh, "Tarp: Timing analysis resilient protocol for wireless sensor networks," in *2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE, 2009, pp. 85–90.
64. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in *Proceedings of the first ACM conference on Wireless network security*. ACM, 2008, pp. 77–88.
65. K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, "Maximizing lifetime of event-unobservable wireless sensor networks," *Computer Standards & Interfaces*, vol. 33, no. 4, pp. 401–410, 2011.
66. Y. Yang, J. Zhou, R. H. Deng, and F. Bao, "Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks," *Security and Communication Networks*, vol. 4, no. 1, pp. 11–22, 2011.
67. S. Ortolani, M. Conti, B. Crispo, and R. D. Pietro, "Events privacy in wsns: A new model and its application," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*. IEEE, 2011, pp. 1–9.
68. R. Lu, X. Lin, H. Zhu, and X. Shen, "Tesp2: Timed efficient source privacy preservation scheme for wireless sensor networks," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–6.
69. Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, "Source location privacy against laptop-class attacks in sensor networks," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*. ACM, 2008, pp. 1–10.
70. W. Yang and W. T. Zhu, "Protecting source location privacy in wireless sensor networks with data aggregation," in *International Conference on Ubiquitous Intelligence and Computing*. Springer, 2010, pp. 252–266.
71. H. Chen and W. Lou, "From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks," in *International Performance Computing and Communications Conference*. IEEE, 2010, pp. 1–8.
72. A. Abbasi, A. Khonsari, and M. S. Talebi, "Source location anonymity for sensor networks," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*. IEEE, 2009, pp. 1–5.
73. G. Suarez-Tangil, E. Palomar, B. Ramos, and A. Ribagorda, "An experimental comparison of source location privacy methods for power optimization in wsns," in *Proceedings of the 3rd WSEAS international conference on Advances in sensors, signals and materials*, 2010, pp. 79–84.
74. X. Deng, X. Xin, and T. Gao, "A location privacy protection scheme based on random encryption period for vsns," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1351–1359, 2020.
75. M. Alrashidi, N. Nasri, S. Khediri, and A. Kachouri, "Energy-efficiency clustering and data collection for wireless sensor networks in industry 4.0," *Journal of Ambient Intelligence and Humanized Computing*, 2020.
76. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "Pda: Privacy-preserving data aggregation in wireless sensor networks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, 2007, pp. 2045–2053.
77. Y. Yang, X. Wang, S. Zhu, and G. Cao, "Sdap: A secure hop-by-hop data aggregation protocol for sensor networks," vol. 11, no. 4, pp. 1–43, 2008.

78. Abizar, Farman, Jan, Khan, and Koubaa, “A smart energy-based source location privacy preservation model for internet of things-based vehicular ad hoc networks,” *Transactions on Emerging Telecommunications Technologies*, pp. 1–14, 2020.
79. J. Wu, Z. Chen, and M. Zhao, “An efficient data packet iteration and transmission algorithm in opportunistic social networks,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2019.
80. A. S. H. Abdul-Qawy and T. Srinivasulu, “Sees: a scalable and energy-efficient scheme for green iot-based heterogeneous wireless nodes,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 4, pp. 1571–1596, 2019.
81. S. K. Singh and P. Kumar, “A load balancing virtual level routing (lbvlr) using mobile mule for large sensor networks,” *The Journal of Supercomputing*, vol. 75, no. 11, pp. 7426–7459, 2019.
82. A. Aranganathan and C. Suriyakala, “An efficient secure detection and prevention of malevolent nodes with lightweight surprise check scheme using trusted mobile agents in mobile ad-hoc networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3493–3503, 2019.
83. J.-A. Kim, D. G. Park, and J. Jeong, “Design and performance evaluation of cost-effective function-distributed mobility management scheme for software-defined smart factory networking,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–17, 2019.
84. G. DaSilva, V. Loud, A. Salazar, J. Soto, and A. Elleithy, “Context-oriented privacy protection in wireless sensor networks,” in *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2019, pp. 1–4.
85. C. Huang, M. Ma, Y. Liu, and A. Liu, “Preserving source location privacy for energy harvesting wsns,” *Sensors*, vol. 17, no. 4, p. 724, 2017.
86. M. Raj, N. Li, D. Liu, M. Wright, and S. K. Das, “Using data mules to preserve source location privacy in wireless sensor networks,” *Pervasive and Mobile Computing*, vol. 11, pp. 244 – 260, 2014.
87. G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, “Caslp: A confused arc-based source location privacy protection scheme in wsns for iot,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 42–47, 2018.
88. R.-h. Hu, X.-m. Dong, and D.-l. Wang, “Protecting data source location privacy in wireless sensor networks against a global eavesdropper,” *International Journal of Distributed Sensor Networks*, vol. 10, no. 8, pp. 1–17, 2014.
89. L. Kazatzopoulos, C. Delakouridis, G. F. Marias, and P. Georgiadis, “ihide: hiding sources of information in wsns,” in *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU’06)*, 2006, pp. 1–8.
90. A.-S. Abuzneid, T. Sobh, and M. Faezipour, “An enhanced communication protocol for location privacy in wsn,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 4, pp. 1–15, 2015.
91. J. Kumari, P. Kumar, and S. K. Singh, “Localization in three-dimensional wireless sensor networks: a survey,” *The Journal of Supercomputing*, vol. 75, no. 8, pp. 5040–5083, 2019.

Pradeep Kumar Roy received the B. Tech degree in Computer Science and Engineering from BPUT University Odisha. He received his M. Tech and Ph.D. degree in Computer Science and Engineering from the National Institute of Technology Patna in 2015 and 2018, respectively. He received a Certificate of Excellence for securing a top rank in the M. Tech course. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT) Surat, Gujarat, India. He also worked in Vellore Institute of Technology, Vellore, Tamil Nadu, India.

His area of specialization straddles across question answering, text mining and information retrieval, social network, and wireless sensor networks. He is part of the technical program committee and chaired many technical sessions of International Conferences. He has published articles in different journals, including IEEE Transaction on Artificial Intelligence, Neural Processing Letters, IJIM, Neural Computing and Applications, Future Generation Computer Systems, and others. He has also published the conference proceedings in various international conferences.

Asis Kumar Tripathy (SMIEEE, MACM, and MIE) is an Associate Professor in the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. He has more than ten years of teaching experience. He completed his Ph.D. from the National Institute of Technology, Rourkela, India, in 2016. His areas of research interests include wireless sensor networks, cloud computing, the Internet of things, and advanced network technologies. He has several publications in refereed journals, reputed conferences, and book chapters to his credit. Dr. Tripathy is serving as the associate editor of International Journal of Computational Science and Engineering (Inderscience). He has served as a program committee member in several conferences of repute. He has also been involved in many professional and editorial activities.

Sunil Kumar Singh is currently working as an Assistant Professor in the School of Computer Science and Engineering at VIT-AP University, Vijayawada, India. He has done his Ph.D. in Computer Science and Engineering form National Institute of Technology Patna, India in 2018. He received the M. Tech and B. Tech degrees in Computer science and Engineering and Information Technology, both from Kalyani Government Engineering College, Kalyani, India in 2010 and 2007, respectively. He has over 30 publications in various National/International Journals & Conferences (viz. IEEE, ACM, Springer and Elsevier). He is also the reviewer of several reputed journals indexed in SCI, SCIE and Scopus. He is also in the Program Committee of various National/International Conferences. He has delivered expert talks and guest lectures at various prestigious institutes. His research area includes Wireless Sensor Networks.

Kuan-Ching Li is currently appointed as Distinguished Professor at Providence University, Taiwan. He is a recipient of awards and funding support from several agencies and high-tech companies, as also received distinguished chair professorships from universities in several countries. He has been actively involved in many major conferences and workshops in program/general/steering conference chairman positions and as a program committee member, and has organized numerous conferences related to high-performance computing and computational science and engineering. Professor Li is the Editor-in-Chief of technical publications Connection Science (Taylor & Francis), International Journal of Computational Science and Engineering (Inderscience) and International Journal of Embedded Systems (Inderscience), and serves as associate editor, editorial board member and guest editor for several leading journals. Besides publication of journal and conference papers, he is the co-author/co-editor of several technical professional books published by CRC Press, Springer, McGraw-Hill, and IGI Global. His topics of interest include parallel and distributed computing, Big Data, and emerging technologies. He is a Member of the AAAS, a Senior Member of the IEEE, and a Fellow of the IET.

Received: October 09, 2021; Accepted: February 01, 2022.