UNIVERSITY OF RWANDA
COLLEGE OF SCIENCE AND TECHNOLOGY,
AFRICAN CENTER OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)

IoT-BASED SOURCE LOCATION PRIVACY PRESERVATION: THE CASE OF HABITAT MONITORING

PhD thesis submitted in the fulfilment of award of PhD Degree in the Internet of Things
University of Rwanda: Wireless Intelligent Sensor Networking

Submitted by

Florence MUKAMANZI
(Reg No. 218014369)

under the guidance of

Prof. Raja Datta
Ass. Prof. Damien Hanyurwimfura
Dr. Didacienne Mukanyiligira

December 2023, Florence Mukamanzi

UNIVERSITY OF RWANDA
COLLEGE OF SCIENCE AND TECHNOLOGY,
AFRICAN CENTER OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)

IoT-BASED SOURCE LOCATION PRIVACY PRESERVATION: THE CASE OF HABITAT MONITORING

PhD thesis submitted in the fulfilment of award of PhD Degree in the Internet of Things
University of Rwanda: Wireless Intelligent Sensor Networking

Submitted by

Florence MUKAMANZI
(Reg No. 218014369)

under the guidance of

Prof. Raja Datta
Ass. Prof. Damien Hanyurwimfura
Dr. Didacienne Mukanyiligira

- Dedicated to my beloved family

My husband: Dr. Philippe Ndikubwimana

My Kids: Asher Brian Manzi Kubwimana, Atete Billah Linah and Aganze Aryan Bright

Father: Felicien Kamanzi

Mother: Late Dancilla Mukakalisa, may her soul rest in eternal peace

My siblings and my in-laws

Declaration

I declare that this thesis work is entirely unique and was created solely by me with the guidance and support of my supervisors. No other institution or university has received this work for the purpose of conferring any degree or diploma. I have diligently adhered to the university's guidelines throughout the preparation of this thesis, maintaining strict compliance with ethical norms and guidelines. Furthermore, I have consistently given proper credit where due, citing external sources within the thesis text and providing comprehensive references for all resources, including data, analysis, theory, figures, and text, that I have incorporated from such sources.

Florence Mukamanzi

Florence Mukamanzi, a Ph.D. student of UR-ACEIoT student ID 218014369, successfully defended the thesis entitled "IoT-BASED SOURCE LOCATION PRIVACY PRESERVATION: THE CASE OF HABITAT MONITORING", which she prepared after fulfilling the requirements specified in the associated legislations, before the thesis examination members whose signatures are below.

THESIS SUPERVISORS:

- **Prof. Raja Datta, main supervisor:**
- **Ass. Prof. Damien Hanyurwimfura, resident supervisor:**
- **Dr. Didacienne Mukanyiligira, Co-supervisor:**

VIVA VOCE MEMBERS:

- **———————————:**
- **———————————-:**
- **———————————:**

Date of submission:———————————

Date of Defense: $18^{th}/December/2023$

Acknowledgment

This thesis was produced with lots of assistance from many people, even though only my name is on the cover. I extend my appreciation to everyone who contributed in making this dissertation achievable.

My most profound appreciation is extended to Prof. Raja Datta, who was my primary mentor and advisor, for his patience, dedication, and understanding in supporting me with my studies. Throughout my studies, I have been motivated by his great knowledge and depth of experience.

I would like to express my sincere gratitude to my other advisors, Prof. Damien Hanyurwimfura and Dr. Didacienne Mukanyiligira, for all the advice, assistance, and encouragement they provided throughout my PhD studies. Without the constant support and encouragement of my supervisory team throughout my studies, I would not have been able to finish.

My special appreciation goes to Dr. Raja Manjula for her invaluable support, guidance, encouragement, and generosity. Her expertise, friendship and encouragement contributed a lot to this journey. Additionally, I would like to thank Tejodbhav korudu for his willingness and time spent in helping me to produce my works; he went above and beyond to assist me.

I would like to express my sincere gratitude towards the management of African Center of Excellence in Internet of Things for their support. I also thank all the center staff for their contributions to my studies. I would like to convey my deep gratitude to the University of Rwanda for providing me with the opportunity to continue my studies by waiving the tuition cost and reducing the workload.

Furthermore, I'd like to thank IIT Kharagpur's administration for allowing me the chance to take part in the exchange program offered at the E-ECE department. I'd want to use this chance to express my gratitude to all the students with whom I shared the network lab of E-ECE for their kindness and support throughout my visit. The initial clear research ideas were developed from there.

I want to acknowledge the assistance I received from both my friends and ACEIoT classmates during my time at the center and during the writing of my thesis.

Finally, I can never give enough thanks to my husband, kids, my parents, my in-laws, my siblings, and other family relatives.

November 2023 *Florence Mukamanzi*

Abstract

The Internet of Things (IoT) comprises the most essential elements including sensors/devices, connectivity, processing of information, and interfaces for users. The sensor nodes are responsible for detecting a variety of things including temperature, humidity, smoke, etc. A network made up of wirelessly connected deployed sensor nodes is known as a wireless sensor network (WSN). Sensor nodes (also known as motes) contain a transmitter and a receiver, a central processor for performing mathematical calculations, and a memory for storing data. Wireless Sensor Networks (WSNs) and their derivatives such as the Internet of Things (IoT) and the Internet of Industrial Things (IIoT) are used in different domains such as agriculture, health care, smart cities, vehicular technology, etc. The Use of WSN and IoT has not been restricted to those classic applications but has also spread its applicability to even monitor valuable objects, like reporting real-time military information in the battlefield and endangered species location in habitat monitoring. The nature of wireless communication links makes its privacy the utmost important consideration due to its openness and lack of protected physical boundaries compared to wired networks, which may lead to unauthorized interruption and detection. Security and privacy, particularly the anonymity of the source locations, have proven to be significant obstacles to the successful implementation of WSNs. A further issue is that sensor nodes are battery-powered which makes it difficult to create network protocols that could enhance WSN privacy and security because most of those protocols are energy-intensive and replacing dead nodes is very challenging. Therefore, those energy-intensive privacy protocols are not recommended for sensor networks with limited resources.

This thesis aims at proposing contextual source location privacy preservation protocols which achieve enhanced privacy, network lifetime, and achieving privacy, lifetime without influencing latency. It further deals with analyzing the effect of sensor nodes' radio range on privacy strength and network longevity.

In this thesis, we consider the case of habitat monitoring, where sensor nodes are deployed strategically in natural habitat to provide real-time updates on the locations of endangered species to a central base station. To handle the above mentioned issues, we first propose a biased random walk and greedy walk-based routing protocol which uses a three- or four-phase routing strategy. The objective of the solution is to achieve a uniform amount of privacy irrespective of the position of the asset in the network without compromising the network lifetime. The proposed protocol outperforms the existing random walk-based source location privacy schemes in terms of safety period without affecting lifetime and it achieves a uniform privacy level in all network settings. Secondly, we propose a total randomized approach that employs a reverse random walk followed by a walk on annular rings, to create divergent routing paths in the network, and finally, the walk on dynamic rings together with min-hop walk to deliver the

packets toward the base station. In this solution, uniform privacy is achieved with enhancement in the network lifetime, unlike in the first solution where privacy is enhanced without an increase in the network lifetime. Comparing the second solution to the first one, the privacy level is improved since the packet travel is completely randomized. However, the increase in privacy in all solutions comes at the cost of high latency. To overcome this limitation, we proposed an improved random walk-based solution that enhances both privacy level and lifetime without affecting latency. Finally, we study the impact of the sensor nodes' radio range on privacy strength and the Network lifetime metrics in Source location privacy schemes of WSNs.

We assess the effectiveness of the suggested schemes and contrast them with the commonly employed current privacy preservation techniques. Both analytical and simulation results show that our proposed approaches produced good performance benefits in terms of privacy, uncertainty, path randomness, and network longevity.

Keywords: IoT, WSNs, Source Location Privacy, Habitat monitoring, Contextual Privacy.

List of Acronyms and Abbreviations

A-BRW	Adaptive Backward Random Walk
A-EDR	Adaptive Equal Depth Routing
BS	Base Station
BRW	Backward Random Walk
BT	Bidirectional Tree
CPU	Central Processing Unit
DBT	Dynamic Bidirectional Tree
DoS	Denial of Service
FRW	Forward Random Walk
GPS	Global Positioning System
ID	Identity
IDR	Identical Depth Routing
IN	Intermediate Node
IoT	Internet of Things
IPR	Identical Peer Routing
MHR	Min-hop Routing
NLT	Network Lifetime
NMR	Network Mixing Ring
PFS	Phantom Flooding Scheme
PN	Phantom Node
PRBRW	Phantom Routing-based Backward Random Walk
PRLA	Phantom Routing with Locational Angle
PRLPRW	Phantom Routing-based L-Path Random Walk
PSSLP	Position Independent and Section based SLP
RFID	Radio Frequency Identification
RN	Ring Node
RRIN	Routing through Randomly selected Intermediary Node
SDR-m	Stochastic Diffusive Routing with multiple virtual nodes
SLP	Source Location Privacy
SN	Source Node
SLP-R	Enhanced SLP
SPR	Shortest Path Routing
SRWSLP	Strategic Random Walk SLP

TTL	Time to Leave
WSN	wireless Sensor Network
VS	Virtual Source
ZBT	Zigzag Bidirectional Tree

Table of Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

In this chapter, we introduce the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) which is its key component. We then discuss their potential application domains, their fundamental features, the privacy threats associated with them, adversary privacy attack tactics, and the challenges faced by researchers in handling privacy issues seen in these networks.

1.1 Introduction

Nowadays, people are enjoying the benefits of technology's advancement while ignoring some of its drawbacks. One of the most concerns noticed is that individuals' privacy is being compromised progressively with the increase and rapid adoption of ubiquitous computing technologies [1]. Hence, for developing any technology, privacy issues should be taken into account. The Internet of Things, particularly in its important component of wireless sensor networks (WSNs), is one such technology that presents major privacy challenges [2].

The increase in IoT devices is undoubtedly advantageous with a significant change in how daily tasks are carried out. However, as the variety of devices increases, the advantages come with noticeable concerns. The IoT ecosystem's expanding connected devices might cause privacy concerns since it gives hackers and cybercriminals entry opportunities [3].

1.1.1 Internet of Things

The Internet of Things (IoT) refers to the network of physical objects (things) that are integrated with sensors, software, and other technologies for the reason of communicating and sharing data with other systems and equipment through the Internet [4]. Given that Wireless Sensor Network (WSN) technology is made up of a group of sensor nodes interconnected by wireless links and able to provide digital interfaces to objects in the physical world, it is a key component of the Internet of Things (IoT) [5].

1.1.2 Wireless Sensor Network

Wireless Sensor Networks (WSNs) are systems with sensing, computing, and communication components with the goal of enabling their controllers to track, gather data, and respond to events in the monitored environment. They are made up of several inexpensive, small-volume micro-sensor nodes. The sensor nodes are the fundamental building block of a wireless sensor network and are made up of a data gathering module, a data processing module, a wireless communication module, and a power module [6]. Therefore, WSNs are considered as links between the physical and digital worlds and they are among the information technologies that have developed most quickly over the past several years due to their enormous range of applications [5]. With no extra infrastructure, the deployed sensor nodes establish an ad hoc network that enables them to interact with one another directly over a common wireless connection. Each node has a wireless transceiver and can function as a router to send packets to their intended destinations.

Due to the aforementioned characteristics, WSNs have been employed in a variety of fields, including agriculture, the medical industry, smart cities, the military, the environment, habitat monitoring, etc [7, 8]. In order to realize agricultural modernization and agricultural environment protection, the wireless sensor network is deployed to obtain real-time information on environmental monitoring like temperature and humidity which may help in smart irrigation scheduling, gathering information on soil nutrients to predict crop production, or taking other agricultural decisions [9, 10]. Real-time remote patient monitoring, supervision, and help were made feasible in the healthcare industry by the use of IoT and WSN. Patients' various vital conditions, such as blood pressure, breathing rate, the temperature of the body, movement, and salt levels, can be remotely monitored [11].

Different IoT-based systems are implemented for creating smart cities, such as waste management systems that may facilitate the simple collection of garbage in large cities [12], since traffic is seen as a major problem in large cities, the IoT-based solutions were suggested to control traffic [13]. The use of IoT and WSN-based disaster management, air quality control, and other technologies with the aim of making cities smarter were also implemented [14, 15]. IoT and WSNs can also be used to monitor priceless assets, such as reporting in-the-moment military data from a battleground and tracking the whereabouts of threatened species in their habitats [16, 17, 18, 19], etc.

1.1.3 The features of Internet of Things and Wireless Sensor Network

- An essential component of the IoT architecture is connectivity. IoT systems should be connected to IoT devices.

- The Internet of Things (IoT) depends on embedded sensors and actuators in a variety of different ways. They enable IoT devices to communicate with the environment, gather and send data.

- Every IoT gadget has its own distinct identity. This identity is beneficial for locating the equipment and for checking its status.
- IoT is scalable due to the way it can handle the enormous growth of data.
- IoT devices dynamically adapt to changing conditions.
- The nature of IoT architecture is not homogeneous. It is a hybrid that enables a variety of manufacturers' things to function correctly in an Internet of Things network.
- Since Internet of Things (IoT) systems and devices manage sensitive data and are linked to essential infrastructure, security, and privacy are major concerns. IoT systems are a prime target for hackers due to the increase in linked devices and data being exchanged over the Internet.
- With a minimum of human involvement, IoT devices can update their software to meet requirements. They can also set up the network, enabling the integration of additional devices to an already established network.
- No matter the underlying technology or manufacturer, IoT devices have the capability to share data with other systems and communicate with them. Therefore, IoT has an interoperability feature.
- IoT systems and devices may function autonomously and make choices without human interaction. They also gather enormous volumes of information from sensors and other sources, which may be examined and utilized to make data-driven choices.
- Devices and systems connected to the Internet of Things (IoT) are aware of their operational environment and context and can respond to it. This is accomplished by utilizing sensors and other technologies that can detect and gather information about the environment.
- In WSN, since the sensor nodes are deployed to gather data, due to their battery-powered nature, nodes are subject to stringent limitations on their ability to compute and communicate. As a result, complex calculations or more energy-intensive routing protocols are not appropriate for these kinds of networks.
- The deployment of sensor nodes in a WSN could either be strategic or random and their nature can be either static or mobile, homogeneous or heterogeneous.
- Privacy and security are a prime concern in Wireless Sensor Networks (WSNs) and its derivative such as the Internet of Things (IoT). This is due to the fact that the Sensor nodes are deployed in uncontrolled and hostile areas, which makes them vulnerable to many active and passive attacks due to the wireless nature of communication links, their physical magnitude, and the limited resources they possess.

1.1.4 Privacy issues in WSN and IoT

Due to deployment in hostile environments and the open nature of wireless links in Wireless Sensor Networks (WSNs) and the Internet of Things (IoT), the privacy of certain events' locations monitored using these technologies poses significant vulnerability issues[20]. For implementing a wireless sensor network, multiple tiny sensor nodes are deployed in the environment and use multi-hop communication to exchange information using a broadcast transmission method which leads them to privacy assaults. Furthermore, wireless sensor networks are particularly vulnerable since nodes are frequently positioned in risky and uncontrollable environments without physical protection [21].

The privacy of endangered animals becomes a significant concern in the case of wildlife monitoring applications. In order to find the location where the animal is present and rapidly catch it, an attacker (the hunter) may employ strong tools to intercept the channels of communication and find the origin of the arriving packets, due to the open nature of wireless communication [22, 23, 24]. Hence, although WSNs offer services to people, also present a number of security and privacy risks that must be addressed by solutions that protect privacy.

Privacy preservation solutions can be classified in two categories such as:

- Content Privacy:

  Content privacy is related to the payload data collected by sensor nodes and transmitted across the network to the base station. Data concealment (or encryption) is an essential method for protecting content privacy in sensor networks [25].

- Contextual Privacy:

  Contextual privacy is pertinent to the transactional information gained through message generation rate, message size, and routing of data messages in the network. Traffic analysis attacks can provide confidential information about a network's users, their usage, the location of source and destination, etc. [26].

In this thesis, the term "privacy" is specifically referring to the source-location privacy, which means the precise location of a sensor node that initiated the message transmission after detecting an event. Source Location Privacy (SLP) is usually evaluated in terms of "Safety-period," which is defined as the number of event reports successfully transmitted to the base station before the adversary tracks the source of information origin [27].

1.1.5 Contextual privacy attacks information

In order to conduct privacy-related attacks against WSNs, the adversary uses a variety of transactional information such as:

- Routing pattern: A significant amount of information can be given to the adversary by traffic patterns in the network. If the shortest path routing protocols are used, for example, the adversary might readily determine where the information originated. In order to do this, it either does backtracking from the BS position or can determine the volume of traffic present at various locations across the network [27, 28, 29, 30]. The routing method employed determines the degree to which an adversary might obtain transactional information about a sensor network structure. Thus, when designing routing algorithms, it is essential to be careful about privacy issues that may arise.

- Message rate: In a rate monitoring attack, the adversary keeps track of the nodes close to him and travels toward the ones with the highest packet sending rates. The adversary may be able to determine the location of the subjects or objects in the network as well as the frequency with which events are being observed by using the message rate [20].

- Carrier Frequency: With the aid of a spectrum analyzer, the adversary might quickly learn the frequency at which the motes are using in a WSN, which results in a confidentiality breach [26].

1.1.6 Challenges of Wireless Sensor Networks

The constraints faced by wireless sensor networks (WSNs), which render conventional privacy preservation solutions unsuitable for these networks, are explained in this section.

- Resource limitations: The sensor nodes are often powered by batteries, which have a limited lifespan when used continuously without breaks. It's not always simple to change

these batteries, especially in remote regions. Any proposed solution for WSNs must be energy efficient in terms of both processing and communication power.

- Physical layer security: In WSNs, where sensor nodes are typically resource-constrained in terms of power, processing capabilities, and memory, the design of the physical layer must take into account these limitations. This layer plays a critical role in determining the overall performance and efficiency of the network, as it directly influences the ability of sensor nodes to communicate with each other and with the central monitoring or data processing unit. The physical layer in a Wireless Sensor Network (WSN) can affect source node privacy through eavesdropping, signal leakage, and signal analysis. To enhance source node privacy, WSNs should implement physical layer encryption, artificial noise, secure beamforming, physical layer authentication, and interference mitigation to secure wireless transmissions, confuse eavesdroppers, and authenticate communication partners, thereby protecting sensitive data from unauthorized access.

- Fading Effects: Fading effects in WSNs using multi-hop communication networks involve cumulative signal attenuation, multipath fading, and interference, leading to potential packet loss and variations in the signal-to-noise ratio (SNR) at different hops. These fading-induced challenges can result in error propagation and decreased end-to-end reliability. Mitigation strategies encompass adaptive modulation, error correction, cooperative diversity, routing and relaying optimization, power control, and the use of channel state information to adapt to changing channel conditions. Managing fading effects is essential for ensuring the reliability and efficiency of data transmission in multi-hop wireless networks. Fading effects in Wireless Sensor Networks (WSNs) can compromise the privacy of source nodes by revealing patterns in data transmission, location, and sensitive information to potential eavesdroppers.

- Unattended Environments: Remote locations, including battlegrounds, volcanic monitoring stations, forests, and frontier regions, are where sensor nodes usually deployed. These locations are especially vulnerable to a number of attacks including node tampering, node compromise, adversary deployment of its false nodes, etc, since the network administrator rarely visits them.

- Topological limitation: Due to the wireless sensor nodes' constrained communication range, the network must use multi-hop communication. However, multi-hop communication necessitates that various nodes handle various traffic loads. Particularly, nodes close to the BS must handle more traffic than nodes situated close to the network boundaries. These networks are particularly vulnerable to traffic analysis attacks due to the imbalanced nature of the traffic communication. The adversary uses this information to determine where the BS is located. When the base station is found, it can be destroyed, making the entire sensor network ineffective. The similar strategy can be used to identify the source of the information.

- Broken nodes: Due to difficult climatic conditions like forest fires, moisture buildup, etc., it is possible that a set or a group of nodes in a specific location may be harmed because the nodes are placed in uncontrolled environments. The information from this region will never reach the network's central controller, or the BS, if a number of nodes in a certain limited geographic area fail. The base station is unaware of any criminal activity taking place in these areas. Thus, the privacy of the asset being monitored is at risk.

1.2 Motivation

Wireless sensor networks (WSNs), the skin of IoT have recently become the focus of research [31, 32, 33]. In order to assist individuals to find information in various fields, WSN deployment intends to collect data via a wireless connection [34, 35, 36, 37]. The use of WSN and IoT has not been restricted to classic applications such as smart homes, vehicular networks, and Industry 4.0 but also has spread its fragrance to even wildlife conservation, to monitor most threatened animals [38, 39, 40, 41].

To overcome scalability issues and cover a wide area of natural habitats, WSNs are usually adopted for gathering information about the whereabouts of these endangered animals. The collected data is then sent to the central controller known as a base station (BS), which is either directly connected to the internet or via an IoT system. Just like good and bad exist, these digital technologies, including the internet, not only help to monitor endangered animals but also bring in several threats to wildlife monitoring applications —one such threat is cyber poaching [42]. Even hunters have evolved over the course of time and are using the latest technologies such as cyber- and internet-related gadgets for finding out the location of the assets or events. Here, assets or events mean animals under observation. The attackers or smart hunters can perform various attacks on these networks and try to gain information on the location of the animals in the target field and finally capture them.

Implementing physical layer security by hiding the location (i.e., preserving the privacy) of the source node—the node that detects an asset in its radio range is the one considered as a source node—is very important and complicated. It is important because disclosing the location information of certain events/assets say, for instance, military troops or an endangered animal is highly dangerous as enemies might take advantage of this information. It is complicated because several factors have an influence on the effectiveness of location privacy protection solutions. These factors include the following: i) The type of an attacker—an attacker that compromises nodes, tries to decrypt packets content, discards the packets selectively, etc..., often known as the *active attacker* [43, 44]; an attacker that can try to locate a source node based on received signal strength, decipher important information using packet timings, etc..., often known as the *passive attacker*; ii) Nodes state—the nodes could be either mobile or static [32].

Our investigation shows that early research on source location privacy has limitations in

practical implementation due to the weaker Network Lifetime caused by the path sensor nodes taken during routing the information packets to the BS or by the methods used to obfuscate back tracking attackers. Similarly, the privacy issues of information sources were not fully handled. The unnecessary message transactions lead to extra energy consumption and thus reduce the performance of the network. We, therefore, feel that there is enough scope to improve the efficiency and the performance of the privacy-preserving algorithms developed for WSNs in contextual privacy. This observation has motivated us to investigate further the source location privacy (SLP) and subsequently develop efficient solutions that can achieve improved privacy without degrading the performance of the system—the network.

It is further seen that the current source location privacy (SLP) solutions in the literature are broadly classified into two categories namely, phantom routing-based SLP and fake packets/fake source-based SLP techniques. Random walk techniques are employed to randomize the routing paths while in fake packets/fake sources-based solutions dummy packets or fake sources are employed to introduce anonymity and unobservability features to the original traffic. The aim of these approaches is to obfuscate the attacker who tries to implement contextual privacy attacks [25].

However, it is observed that fake packets/ fake sources approaches are energy expensive, this motivated us to explore the research under the category of random walk-based SLP as they are promising for resource constraint WSNs. And we have noticed that the poor performance of the existing random walk-based routing techniques lies it the fact that the *safety period* metric is dependent on the position of the source node in the network, where the position is measured w.r.t the base station (BS). It is essential to ensure that the safety of the asset(s) i.e, privacy, remains uniform in any network settings and in any given instance of the time period. This makes traffic analysis even more complicated and thus impedes the adversary's effort. Similarly, Considering the case of habitat monitoring, where sensor nodes are deployed in a hostile environment (say forest areas), the replacement of dead nodes is not an easy task. Therefore, improving the lifetime of a network (NLT) helps in better monitoring of the assets for a longer time duration. Additionally, providing solutions with improved SLP and NLT with reasonable delays (i.e., keeping delay as low as possible) is given less attention in the literature. It is even noticed that there is no SLP work in the literature which checked the effect of the sensor nodes' radio range on the safety period and NLT.

These observations motivated us to fill the gap and inspired us to develop improved source location privacy (SLP) protection techniques by considering the above-mentioned issues seen in the existing SLP solutions.

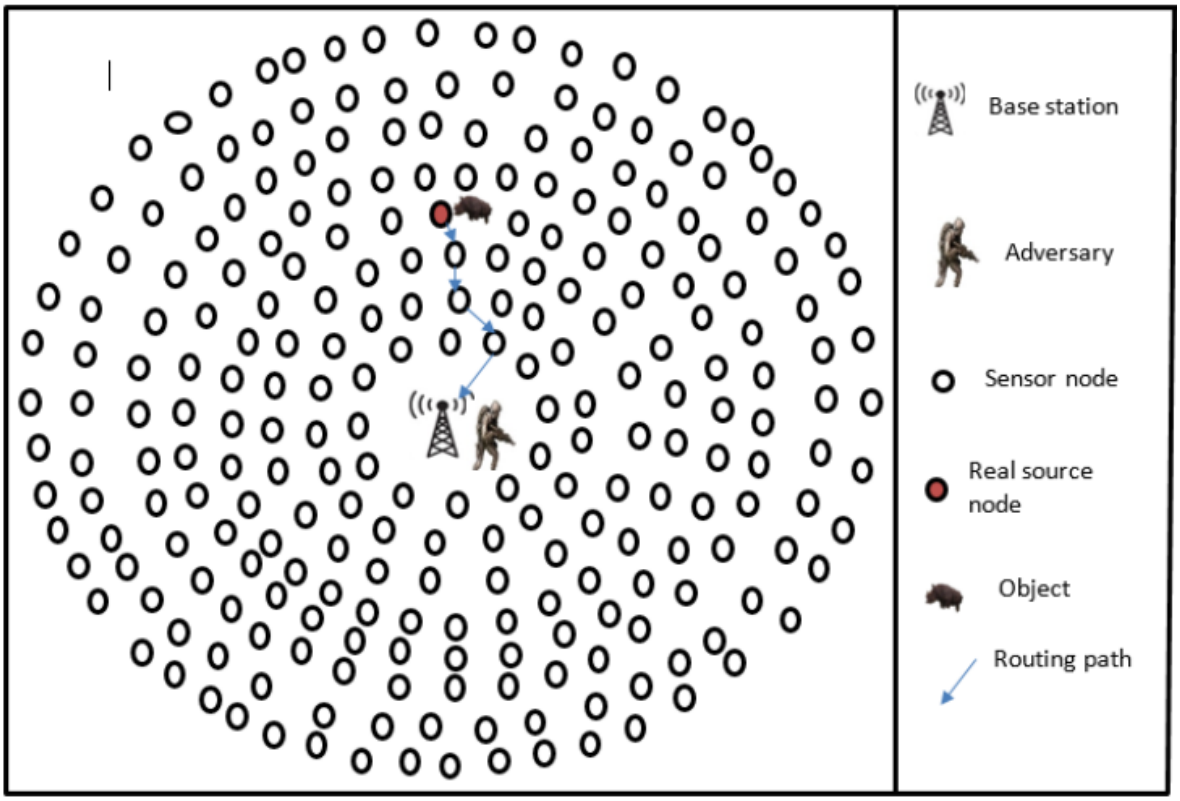

Figure 1.1: Weaker privacy (no SLP) with circular deployment

Figure. 1.1 shows an example of a contextual weaker privacy scenario with circular deployment. In that case, a source node keeps sending packets to the base station (BS) by utilizing the shortest path after detecting an asset(animal). In the shortest path routing, the neighbor nodes whose distance to the BS is less than that of the node of interest —the nodes which are closer to the BS, make up the forwarding list. In that situation, once an attacker begins its backtracking operation from the BS, he may find the source of information easily.

Generally, SLP techniques can be implemented in real-world scenarios for green wireless sensor networks; however, they can present several key challenges. These include the complexity of key management in large dynamic networks [45], the delicate balance required between maintaining location accuracy essential for WSN applications and preserving source privacy [24], the added complexity of dynamic network topologies due to sensor mobility and potential failures [46], etc. Addressing these challenges necessitates advanced solutions that can effectively harmonize data accuracy, security, and adaptability. The other potential challenges which may occur in implementing Privacy in wireless sensor network include physical layer security and fading effect.

The enhancement of security within wireless networks has elevated the importance of addressing physical layer security as a paramount concern. The essence of physical-layer security revolves around the utilization of apt signal processing and coding techniques to harness the inherent properties of the communication channel, thereby enhancing the overall security of communication. Researchers have contributed their knowledge of multi-antenna signal processing, channel-aware adaptive coding and signaling, and networking architecture to create channel

quality asymmetry between adversaries and authorized users. This asymmetry could then be used to ensure physical layer secrecy. Secret-key generation and authentication at the physical layer have been made possible by taking use of the location-specific or device-specific features of the wireless channels. Nevertheless, as far as our current knowledge extends, scant consideration has been directed toward preserving source location privacy within Wireless Sensor Networks (WSN) when addressing the entire issues related to physical layer security concerns [47, 48].

In the contributions of this thesis, there are different assumptions made and potential scopes considered. The works in this thesis assumed that the channels are error free and no losses such as loss due to fading, multipath scattering, noise etc., exist as there are taken care by the MAC layer protocols in practical. Since the work primarily focuses on source location privacy using contextual routing to protect the asset information, we make assumption that the underlying physical and MAC layer protocols are taking care of these issues. Similarly, we assume that cryptographic primitives-based content privacy is taken care by the upper layers (application layer). However, in real-life wireless systems such the WSNs are prone to fading, channel errors, and noise effects,etc. For instance, in wireless networks, fading is considered as the variation of the signal attenuation which varies with respect to time, geographic location of the sensor nodes and the frequency of operation. Due to multipath propagation, the net signal received at the receiver gets hampered and thus degrades the quality of the received signal. These attributes could be exploited by the attacker to determine the location of the nodes in the network [49, 50]. Therefore, one future research direction that could potentially be explored is the mitigation of the fading effects, or exploiting them and incorporating physical layer security in WSN while developing novel SLP schemes to provide better privacy solutions that were not addressed in the current literature as far as our knowledge is concerned.

1.3 Research Objectives

Our research's major goal is to provide improved IoT-based source location privacy preservation techniques for habitat monitoring.

1.3.1 Specific objectives

- Review the existing source location privacy preservation techniques designed for WSNs for finding their weaknesses and limitations.
- Design, develop and evaluate an improved SLP preservation technique that provides enhanced privacy for any position of the source/asset in the network or any network configurations without compromising the network lifetime.
- Design, develop and evaluate a total randomized SLP technique that simultaneously improves the safety period and network longevity, achieves uniform privacy and network

lifetime (NLT) irrespective of the position of the source in the network.

- Study the impact of the sensor nodes' radio range on privacy strength and the network lifetime metrics.
- Design, develop and evaluate a novel SLP technique which achieves an improved privacy and network lifetime without affecting delay.

1.4 Contributions

In this section, we present in brief the work done on the objectives as given in Section. 1.3.

- In chapter 2, we provided an overview of the most recent state-of-the-art study in area of privacy protection in IoT intended Wireless Sensor Networks (WSNs. We firstly discuss the attackers' characteristics and then the suggested privacy-preserving methods for WSNs in the literature.
- In chapter 3, We aimed to provide a SLP solution which achieves a uniform amount of privacy irrespective of the position of the asset in the network without compromising the network lifetime. A biased random walk and greedy walk using a three- or four-phase routing strategy was employed, where the number of phases depends on the network segment in which the source is situated. The biased random walk is intended to send packets away from the source of information and make routing paths appear dynamic to the eavesdropper, whereas the greedy routing ensures that the packets converge at the base station. The network was divided into three sections, where each section is of size one-third the network radius. Depending on the position of the source node w.r.t the BS, i.e., based on the segment in which the source is situated, the proposed framework adapts accordingly and applies the right choice of the routing mechanism.

  In each case, the proposed routing framework comprises multiple phases while routing packets to the BS. Neighbor nodes for relaying the information packets are identified as near, equivalent, or far away based on the number of hops at which these are placed. Neighbor nodes are chosen based on: (i) the residual energy and (ii) the direction in which it is situated in the network. This approach of neighbor selection for forwarding a packet leads to the uniform selection of the nodes. Every time a node makes this decision to relay a packet, it chooses a neighbor that has not participated in the previous round(s). This in turn helps in choosing all the neighbors' nodes to relay every new packet with equal probability and leads to graceful (i.e., uniform) degradation of energy levels at each node and helps improve the lifetime of the network. In summary, the proposed technique aims at maximizing the safety period (uniform privacy) while maintaining the network lifetime.

Mathematical models for the analytic estimation of the proposed protocol's average hop count or average delay were provided. The Performance evaluation done using developed analytical models and simulation results reveals that PSSLP achieves significant improvement in terms of safety period and NLT respectively compared to the existing privacy (SLP) protection techniques.

- In chapter 4, we aimed to simultaneously improve the safety period and network longevity, achieve uniform privacy and network lifetime (NLT) irrespective of the position of the source in the network. In this technique, the packets are transmitted to the base station in a controlled random walk manner to ensure a better safety period and network longevity. To balance the distance they cover before reaching the BS, the packets take several routes. To establish fairness between the network lifespan (also known as network lifetime) and safety period, the hop threshold notion is presented. A random neighbor is chosen from the far-off neighbor list to relay a packet. This choice is based on the quantity of residual energy present in the nodes that are on the list of far neighbors. Like the walk in a game of a maze, the packets initially travel backward from the source for specific hops before taking clockwise or anti-clockwise paths across the annular rings of the network. In this stage of the routing process, the routing paths are lengthened to decrease the likelihood that packets will travel across the source node's radio range (known as the visible area). The packets are then routed through walk on dynamic ring together with minimum hop routing to the base station (i.e, shortest path routing). The suggested method achieves consistent privacy, independent of the location of the source sensor in the network while maximizing both the safety period and the network's longevity.

  The performance measurements, done using the proposed analytical models and simulations, indicated an improvement in the safety period and network lifespan compared to existing SLP techniques and it showed improvement when compared with other similar techniques. Regardless of the source node's position inside the network, the proposed solution achieved uniform and enhanced privacy and Network lifetime simultaneously.

- In chapter 5, we aimed to develop a new SLP protocol which increases the safety period and network lifetime (NLT) without increasing packet transmission delay. The proposed technique routes the packets from the source node to the base station (BS) using three-phase routing namely: i) adaptive backward random walk (A-BRW), ii) adaptive equal depth routing (A-EDR), and forward random walk (FRW). To give an impression, to a backtracking attacker, that the routing pathways are dynamic, the A-BRW and A-EDR phases were designed to carefully route the packets away from the source node. The packets were converged to the base station by the forward random walk.

  For reaching the goal of improving the safety period and NLT without experiencing heavy latency costs, the length (i.e., the number of hops) of the random walk in the A-BRW and A-EDR phases is dynamically controlled to optimize the delay metric. For every new

packet that the source sends to the BS, the random walk length is varied. To accomplish this task, the region between the source and the network edge is divided into circular rings. These rings are in turn grouped into three sets namely, closer rings-set, middle rings-set, and farther rings-set. A random number is generated that acts as a time to leave (TTL) value that will be specified in the packet for relaying purposes. If this random number lies in the closer rings-set, then the packet is initialized with that value as the TTL value and sent in a backward direction in a random walk fashion. Now, the intermediate node will generate another random number that is used in phase two (i.e., in the A-EDR phase) as the new TTL value. The length of the new random number is chosen based on the one that was used in the A-BRW phase. That is if the TTL value in A-BRW is large, then the new TTL value in the A-EDR phase will be small. This criteria of choosing the TTL values in both these phases helps in achieving a balance in the total number of hops that the packet has to travel in the A-BRW and A-EDR phases. Simulation results have demonstrated that the proposed technique performs better than the existing random walk class of SLP techniques.

- In chapter 6, we studied the impact of the sensors' radio range on privacy strength and the Network lifetime metrics as the most important performance metrics in SLP of WSNs. We further checked if the sensor's radio can affect other metrics like capture percentage, entropy, energy consumption and delay. For checking the impact of sensor's radio range on different performance metrics, we use the developed SLP protocol and change the sensing range to different values in evaluating the proposed protocol with aim of checking the behavior of each performance metric on different radio range values. The simulation results demonstrated that the sensors' radio range has an impact on the safety period, capture ratio, and NLT.

1.5 The organization of the thesis

Chapter 2 provides a state-of-the-art survey of the WSN-specific privacy preservation methods already in existence. We only discuss methods that are relevant to the category of solutions that the suggested algorithms fall under.

Chapter 3 presents the first proposed solution to enhance existing SLP solutions. The solution aims at achieving a uniform amount of privacy irrespective of the position of the asset in the network without compromising the network lifetime. outcomes from analysis and simulation show that the proposed technique, when compared to the existing systems, provides favorable results.

Chapter 4 provides total randomized SLP algorithm that simultaneously improves the safety period and network longevity and achieves uniform privacy and network lifetime (NLT) irrespective of the position of the source in the network was proposed and evaluated. The analytical and simulation results demonstrate that the proposed technique outperforms the existing SLP preservation techniques.

Chapter 5 presents a novel SLP technique that achieves improved privacy and network lifetime without affecting delay. developed and evaluated. Simulation results have demonstrated that the proposed technique performs better than the existing random walk class of SLP techniques.

Chapter 6 studies the impact of the sensors' radio range on privacy strength and the network lifetime metrics. The simulation results demonstrated that the sensors' radio range has an impact on the safety period, capture ratio, and NLT.

Chapter 7 concludes the thesis with a brief discussion on the possible extension to the future work.

CHAPTER 2

Literature Review

An overview of the most recent state-of-the-art study in the area of privacy protection in Wireless Sensor Networks (WSNs) is given in this chapter. Firstly, we discuss the attackers' characteristics and then the suggested privacy-preserving methods for WSNs in the literature.

2.1 Attacker Characteristics

An attacker may possess one or more of these characteristics: The internal or external attacker, active or passive attacker, and an attacker can have a local view of the network or a global view of the network [51, 32].

2.1.1 Internal or External attacker

Two categories of adversaries (attackers) that may compromise content-oriented privacy are described by Li et al. in [51]. These include external and internal adversaries. External adversary listens on the communication channels between the network's sensor nodes with the aim of reading the exchanged packets' content. Traditional cryptographic basics like authentication, decryption, and encryption can be used to protect against this type of attacker. An internal attacker is one who can deploy additional nodes in the target network to compromise private information.

2.1.2 Active or Passive attacker

The passive attacker does not actively influence the nodes or the traffic between the nodes, for instance, packet dropping attacks, denial of service attacks (DoS), etc. Under this model, the attacker is assumed to eavesdrop the network traffic and tries to inspect the content that is exchanged between the nodes, performs hop-by-hop trace-back attacks in which the adversary

follows the traffic between the nodes to get to the source of information origin. In the advanced case, the passive attacker may even monitor the rate and time correlation between the message packets sent in the network to locate the source of origin. Passive attacker may look at the node with the higher transmission rate, as these nodes are probably closer to the source of an event or maybe the sink node. On the other hand, an active attacker may alter the traffic or behavior of the nodes, pollute the data transmitted across the network, drop few packets, etc. [43, 44].

2.1.3 Local or Global View of the Network

The global attacker has a full view of the network. One simple way to get such global view of the network's traffic is just by deploying snooping (or monitoring) nodes onto the target field. The number of these snooping nodes can be typically the same as that of the number of sensor nodes in the network. The attacker is assumed to be passive, well-informed and resource rich. With all these capabilities, it should be feasible to monitor the entire network communication patterns and locations of the events in the sensor network via global eavesdropping [52, 53].

On the other hand, a local attacker has only a local view of the network, based on eavesdropping capabilities [27, 30, 54, 20, 55]. In the existing literature [30, 20, 56, 57, 57, 58, 23, 59, 60] and in this thesis, a local adversely is assumed to possess the following characteristics and strengths:

- The adversary is assumed to be mobile, capable of having sufficient energy resource, adequate computation capability and memory for information storage.
- The adversary is assumed to be passive attacker that just eavesdrops the local traffic among the neighborhoods nodes.
- Since the BS is the only destination where the entire network traffic is routed to; it is presumed that adversary starts his journey from the BS location to collect the data traffic.
- The adversary is ceaselessly in a listening/receiving mode. Whenever an event is detected, nearby sensor nodes will generate this event detected information and transmit it to the BS on a hop-by-hop basis. Once the adversary hears the first message, it knows which node among its neighborhood sent that message, and accordingly move in that direction to reach that node.
- The adversary is non-malicious in nature, which means that it does not interfere with the normal operation of the network. If the adversary is malicious in nature, then its presence can be somehow detected.

2.2 Privacy in Wireless Sensor Networks

Privacy is defined as "the state of not being seen among the throng"[61]. In the context of WSNs, privacy refers to the confidentiality of the monitored assets, the confidentiality of the

sensor nodes and BS(s), and the confidentiality of the information content transferred via the WSN.

2.2.1 The categories of privacy-preserving techniques for WSNs

The existing research on privacy-preserving methods for WSNs can be categorized into two primary categories: *Context-oriented privacy preservation methods*[26] and *Content-oriented (data) privacy preservation methods* [62].

1. *Content Privacy*

   Two classes such as: "Data aggregation" and "Data Querying" can be used to further categorize the current approaches in the domain of content-oriented privacy. While "data querying" is concerned with securing the queries broadcast or flooded by the BS, "data aggregation" deals with safeguarding the private data of the sensors. Traditional cryptography basics like authentication, decryption, and encryption can be used to address these issues.

2. *Context Privacy*

   Contrarily, context-oriented privacy-preserving techniques put a greater emphasis on protecting the privacy of contextual data, such as the location and the time of network traffic flows.

In this thesis, we review only source-location privacy preservation solutions for WSNs under the category of context privacy since it is our focus; specifically in safeguarding the source location privacy of the events or assets monitored.

Location privacy issues may appear for both sensor nodes acting as data sources and the BS acting as the data's final destination. In many applications, including the monitoring of endangered species, medical applications, military surveillance, etc., location privacy is a significant problem. Considering the case of using WSNs to monitor habitats, for instance; WSNs are being used by a number of nonprofit organizations throughout the world to monitor endangered species including tigers, rhinoceroses, and pandas [27, 63, 64, 65, 66]. A node that detects an event or asset is referred to as the source node in these applications. The source node sends information concerning event detection to a base station, often referred to as a sink. However, the nature of these sensor nodes' wireless links causes serious privacy issues for the asset (animal) being monitored as we consider the case of habitat monitoring. We would like to point out that the suggested solutions are not limited to this application only, though; they may be conveniently expanded to cover more application domains.

One might wonder why privacy is such a big deal in habitat monitoring initiatives. Animals constantly run the risk of being stolen, especially those that are uncommon. Because the rewards for poaching endangered species are high on the black market. Hunting or poaching of

threatened or endangered species disturbs the ecosystem's equilibrium and diminishes a country's fauna. Therefore, it is essential to provide safety and privacy to animals wherever on the globe.

Several studies have been made in the literature to address the issues of privacy preservation in WSNs [67, 20, 58, 68, 55, 69, 23, 70, 59, 71, 72, 73, 74, 75, 76, 54, 51, 77].

Source Location Privacy preservation techniques could be classified based on attacker models and on the type of approaches used to mitigate the eavesdropping attacks. In the former case, the attacker is assumed to have either local knowledge of the network or global view of the network. In the second type of classification, the solutions are either random-walk based, or fake-source/fake-packets based. In fake-packet/fake approach, the sensors generate fake packets in addition to the real traffic with the aim of enhancing privacy [78, 79, 80, 81, 82, 83, 84, 85, 55, 76, 73]. However, it is shown in [86] that for certain scenarios SLP based on fake-source/fake-packets performs poorly compared to random-walk based solutions. The fake-sources/fake-packets based approaches also add additional burden on energy budget for these resource constrained sensor networks. Hence, we realized that for energy-constrained WSNs, such schemes would be energy expensive and we do not focus on them.

Motivated by these observations, The approaches suggested in this thesis fall under the category of "Random walk-based based solutions". Therefore, we only discuss the solutions that is related to random-walk based Source Location Privacy Preservation techniques. Conti et al., in [32], provide an in-depth review of the Source Location Privacy (SLP) preservation methods suggested for WSN; for more details on this topic, we recommend reading this article. The fundamental goal of employing random walk-based approaches is to make a packet's journey appear entirely random to an adversary in order to defend against hop-by-hop and traffic analysis attacks. As relaying or forwarding nodes are picked at random from a sending node's neighbor set, the packet's journey takes on a random patter [27].

For the first time, a random walk based SLP solution was proposed by Ozturk et al. [27]. Based on panda hunter game [27] as baseline, in order to provide SLP in WSN, their work introduced the Phantom Flooding Scheme (PFS), which is based on the conventional random walks. Every message goes through two phases such as a directed walk phase, followed by a flooding phase that sends the packet to the BS. In the directed walk phase, the packet is relayed for up to H hops in a random manner. Baseline flooding is used to flood the data packet once the hop count H reaches zero. The phantom node (PN) is the node at which the hop count H is zero. This solution may provide the significant safety period because every new packet follows a different shortest path from the phantom node to reach the BS and the attacker maybe dragged away from the information source. However, because the packet forwarding probability is less evenly distributed among the neighboring nodes, establishing a pure random walk is not a simple one. A node may therefore send a packet to a neighboring node from which it has received the packet contents.

Different routing techniques were proposed to improve PFS, including [87, 88, 89]. In [89], the authors proposed a new SLP routing technique namely a phantom routing with a locational

angle (PRLA). The key idea was to forward a packet to the neighbor node that has the greatest inclination angle with reference to the base station. Each node in the network determined the angle of inclination between itself and its neighbors with respect to the base station. Each node then calculated the forwarding probability using this inclination angle. The chance was greatest for the node with the highest angle of inclination. When an event is detected, a node chooses its neighbor with the highest inclination angle and sends the packet to that node. The above procedure continues until the hop count H reaches zero, or if a node cannot transfer the packet to a neighbor node with the required inclination angle, it converts into a phantom node and forwards the packet via shortest path routing to reach the BS. The authors assume that the attacker stays near to the sink, where it starts tracking the source. The outcome of the approach is that each packet sent from the source node takes a unique path, making hop-by-hop tracing challenging. It is observed that this scheme has enhanced the safety period compared to PSF. This is due to the fact that in PSF, tracing back the source of information can be easy, since the packet forwarding probability is less evenly distributed among the neighboring nodes of the source of information as shown in [88, 90, 91]. However this proposed scheme routing path is not random enough to provide strong privacy of the source of information.

Li and Ren proposed a scheme which uses three- phase routing process [51]. In first the phase, The data packet is transmitted by the message source to the randomly chosen intermediate node (RRIN) in the sensor domain, which then routes it to a ring node. The objective of this phase was to provide the local source-location privacy. It is projected that the intermediate node will be far from the actual source node, making it difficult for the attackers to learn about the real source from the intermediate node chosen. The data packet was then mixed with other packets using a network mixing ring (NMR) in the second routing phase with the aim of providing source-location privacy at the network (global) level. In the end, selected nodes on the mixing ring forwarded the data packet to the SINK node. This scheme has the same latency and power consumption as PFS, but a higher safety period. The more routing strategies were proposed by Li and Ren[29, 92] to improve the proposed routing protocol in this work by enhancing the safety period, since it is seen that this technique provides weaker privacy due to the lack of enough routing path randomization.

In [30], Chen et al. developed a source location privacy systems with the aim of protecting both source node and the sink. Although the work has four solutions namely, forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively, we discuss only forward random walk (FRW) scheme as other three schemes are based on fake packet-based solutions, which are a separate class of privacy preserving techniques. In FRW approach, every node that has packet to be forwarded towards the BS randomly chooses a neighbor node that is closer to the BS. This ensures convergence of the packets at the BS. The nodes within the BS radio range directly forward the packet to the BS as it is the final destination.

For improving existed random walk based routing protocols, a directed random work was proposed by Gu et al., in [77]. In directed random work, each node splits its neighbors into two

groups that are opposite alongside one another. Instead of employing a pure random walk, next hop node is chosen randomly from two groups to reach an intermediate node. Then, from the intermediate node, the next hop is chosen from the opposite group. It seems that the proposed scheme may provide some improvement in safe period, however the routing path is not diverse enough to confuse adversary and the Network lifetime was not taken into considerations.

The work in [58] proposed a novel source location privacy preservation technique that focuses on privacy as well as the network lifetime metrics. The work dealt with hiding the physical location of the source of the event and make it difficult for the adversary to backtrack the origin of information. The concept of escape-angle and random walks based on potential energy, and multiple virtual sources were proposed. Although the work improved the safety period (i.e., the privacy level) without hampering network lifetime, it makes use of fixed virtual sources for creating randomness in the traffic. This leads to energy hole problems in the network.

An enhanced source location privacy preservation technique was proposed in [20] to protect source node against local eavesdropper near by the base station. In this work, three phases for sending event information from the source node to the base station were considered. The proposed phases are backward-directed random walk (BRW), identical depth routing (IDR) and min hop routing (MHR). In BRW the source node forwards the information to a distant intermediate node in the backward direction. In IDR, intermediate node forwards the packet to a certain defined angle along the neighbors whose depth to base station is the same as that of the virtual source node. In the last phase (MHR), the packets are forwarded to the BS using shortest path routing scheme (SPR). This work improves existing solutions in terms of safety period. However, this scheme does not take into consideration the residual energy at nodes and the location of source node, in terms of its depth to the BS while relaying the packets.

In [93], a source location privacy protection scheme is proposed. In this approach, the source node selects the phantom nodes from the phantom-area designated for these type of nodes. The packets are sent to the sink through those phantom nodes by using three routing strategies (shortest path routing, random routing and ring routing). Although an improvement is seen in privacy level, it is distant dependent. That privacy is low when source is located closer to the BS and it increases as the distance between the source node and the BS increases. This leads to leakage of contextual information.

In [70] a random walk based solution was proposed to hide the real source of information from the local adversary. This scheme divides the network into four sectors with a single BS located in one sector. Upon detecting an asset, a source node sends the packet randomly to the selected sector and then it is forwarded to the BS randomly using the shortest path. This work also suffers from poor NLT.

According to the research in [23], the network is segregated into sectors to set some conditions in order to improve privacy. The selection of the sector is made randomly for each new packet that is sent from the source node. Once the packets reach that intended sector, they travel toward the BS. The sectors that are closer to the source are given less priority than the ones that

are far away from the source. The attacker is perplexed by this strategy because the pathways are varied. However, the equipoise between privacy and network lifespan has not been well investigated.

Two solutions namely, Phantom Routing-based Backward Random Walk (PRBRW) and Phantom Routing-based L-Path Random Walk (PRLPRW) are proposed in [24] to enhance the safety period. The first approach delivers the packets in the reverse direction followed by greedy approach towards the BS. However, this approach has limitation in network lifetime. To mitigate this issue a second approach is proposed. In this technique, the packets are initially sent using pure random-walk phase and then L-walk phase. These two phases are intended to create routing path diversities and increase traffic uncertainty. Finally, the packets are sent to the BS using shortest-path routing. However, network lifetime is still an issue.

In the majority of these techniques, the privacy strength is dependent on the position of the source in the network; the farther the source node's position w.r.t the BS, the better the privacy. This shows that there is a dire need to develop new SLP techniques that can achieve uniform privacy at any position of the source node in the network. Enhancing privacy and NLT jointly while maintaining uniform privacy for any position of the source in the network is also needed since most solutions enhance privacy only or enhance privacy without hampering the NLT. It is further seen that in the most existing random walk based techniques privacy strength was obtained at the high expense of additional delays. All those observations motivated us to develop the improved SLP solutions to mitigate those mentioned issues noticed in the existing solutions.

2.3 Conclusion

In this chapter, we discussed the existing solutions related to our research work. Most of the proposed schemes were initiated to provide better outcomes than the earlier ones. However, these approaches can still be improved in terms of metrics such safety period (privacy), delay, and network lifetime. Therefore, we feel that the random walk-based routing techniques for providing SLP in WSNs could be further investigated and provide solutions with better performance. In the next chapter, we present our first method to mitigate one of existing SLP issues.

CHAPTER 3

Position-independent and Section based Source Location Privacy

In this chapter, we address the issue of position dependence privacy seen in the existing random walk-based solutions. It was observed that the majority of existing random walks have developed solutions that exhibit distance-dependent behavior of the privacy-protection strength. That is, if the source node is closer to a BS, the lower is the privacy level. Whereas, as the distance between the source node and the BS increases, the privacy level also increases. This privacy which is depending on the asset/event position in the network could leak some contextual information to the attacker leading to weaker privacy protection. Similarly, improving the lifetime of a network helps in better monitoring of the assets for a long time duration. This motivated us to study and develop an improved source location privacy (SLP) protection technique.

The proposed scheme employs a biased random walk and greedy walk using a three- or four-phase routing strategy, where the number of phases depends on the network segment in which the source is situated. The biased random walk is intended to send packets away from the source of information and make routing paths appear dynamic to the eavesdropper, whereas, greedy routing ensures that the packets converge at the base station. The objective of the solution is to achieve a uniform amount of privacy irrespective of the position of the asset in the network without compromising the network lifetime. Hence, the proposed protocol is named "Position-independent and Section-based Source Location Privacy (PSSLP)".

PSSLP assumes that the network is divided into three sections as shown in Figure. 3.1, where each section is of size one-third the network radius. Each sensor node divides its neighbors into three groups as nearer, equivalent, and far-away neighbors (details are given in Section 3.3.1). Depending on the position of the source node w.r.t the BS, i.e., based on the segment in which the source is situated, the proposed framework adapts accordingly and applies the right choice of the routing mechanism. In each case the proposed routing framework comprises of multiple phases while routing packets to the BS. Neighbor nodes for relaying the information

packets are identified as near, equivalent or far away based on the number of hops at which these are placed. Neighbor nodes are chosen based on: (i) the residual energy and (ii) the direction in which it is situated in the network. This approach of neighbor selection for forwarding a packet leads to the uniform selection of the nodes over large trials. Every time a node makes this decision to relay a packet, it chooses a neighbor that has not participated in the previous round(s). This in turn helps in choosing all the neighbor nodes to relay every new packet with equal probability and leads to graceful (i.e., uniform) degradation of energy levels at each node and helps improve the lifetime of the network. In summary, the proposed technique aims at maximizing the safety period (uniform privacy) while maintaining the network lifetime.

The performance evaluation done using developed analytical models and simulation results reveals that PSSLP achieves significant improvement in terms of safety period without hampering the network lifetime compared to the existing privacy protection techniques (SLPs).

3.1 Application scenario and Network Model

We took into consideration a WSN-based habitat monitoring system that consists of a single base station and several static sensors scattered around the area. Either a panda, a rhino, or a tiger is the target under observation. The asset can unpredictably come into the network, stay for a while, wander, drink water, and then return back to its home. It was assumed that the asset (for instance an endangered animal) was tagged with Radio Frequency Identifier (RFID) and each sensor node in a network was equipped with an RFID reader. This combination made them capable of detecting the asset(s) with these RFID tags. This scenario was inspired by the panda-hunter game model suggested in [87].

We considered a network with a circular deployment model where sensor nodes are strategically deployed and a single base station (BS) is located in the center of the network. The nodes were assumed to be arranged in the form of annular rings around the BS as shown in Fig. 3.1. This arrangement was made based on the depth value of the nodes w.r.t the base station (BS) position. Here the nodes that lie within the BS's radio range have a depth value of one, the next set of nodes that are two hops away from the BS has a depth value of two, and so on. Further, the network is divided into three sections namely S_1, S_2 and S_3, each segment being one-third of the network radius R. The total number of annular rings was given by R/r_s, where r_s is the sensor node radio range. Therefore, the total number of rings per section is given by $R/3r_s$.

Each sensor node is battery-powered that serves as an energy resource. It was assumed that the nodes are static, homogeneous, and have the same communication radius (r_s). Here homogeneous means that all the sensor nodes in the network have the same initial power along with the same computing and storage capabilities [94]. Each node was assigned a unique ID. A node can only communicate with its one-hop neighbor nodes (that is the nodes that lie within its radio range r_s) as they have a limited communication range. To send a message to a distant BS, the message is relayed in a hop-by-hop fashion. Each sensor can determine its position in

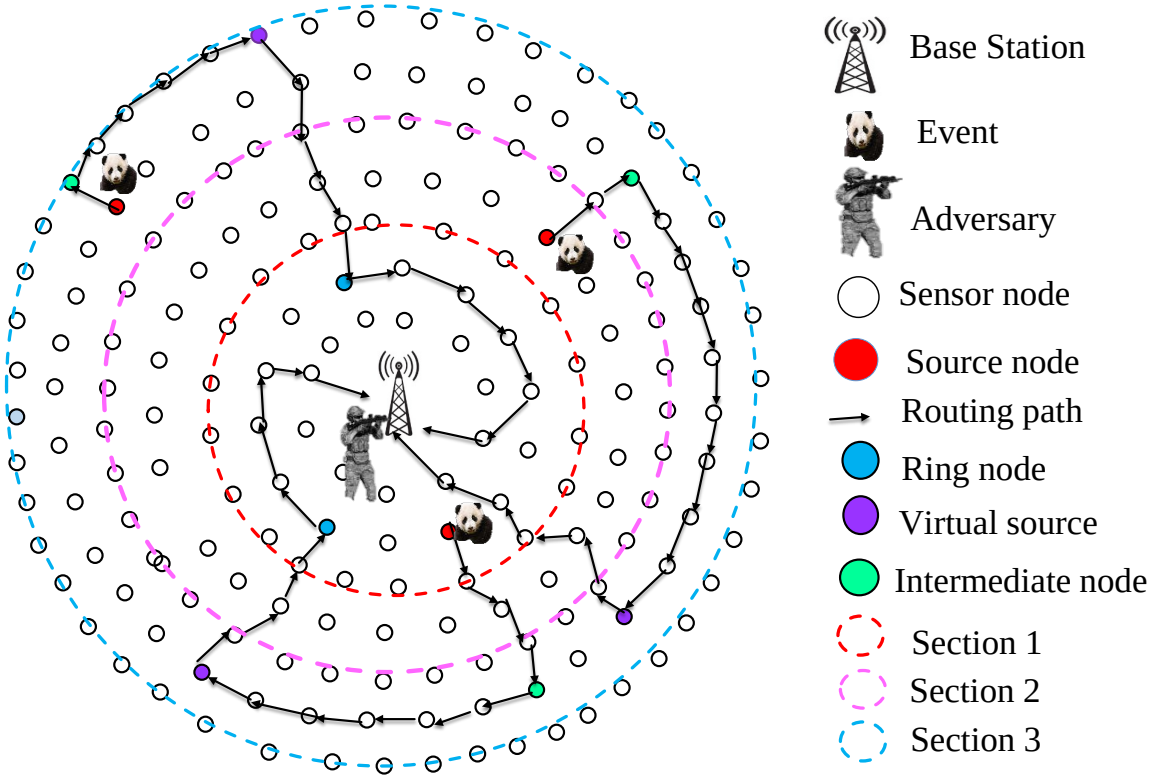

Figure 3.1: Network Model for PSSLP

the network using the existing localization techniques [95]

The BS was assumed to be secure, resource-rich, not compromised, and located in the center of a network. Further, the work assumed that the communication links are secured using secret keys so that the attacker cannot read the content of the packets [96].

3.2 Attacker Model

This work considered only the local and passive attacker model. Here it was assumed that:

- The attacker just eavesdrops on the wireless communication links and does not perform any active attacks such as node compromise, packet content modification, etc.
- The attacker starts its backtracking task right from the BS as it is the destination of all packets [27] . That is, for every new packet sent by the source node towards the sink, the adversary estimates the direction of the signal arrival of the packet.
- The attacker determines the direction of arrival of the packet using a powerful device that has a spectrum sensing and analyzing module equipped with unlimited storage and computing power [88]. Based on this estimation, the adversary moves one hop in the direction of the packet arrival. This movement is towards the source of information and away from the sink.

- Further, the assumption was that the attacker's devices have the same radius as that of the sensor nodes.

  It should be noted that the attacker never retreats to the previously visited location because doing so will only keep him wandering in the network fetching no benefit to it.

3.3 Overview of the proposed technique

This section proposes and gives a description of the proposed protocol that comprises two stages: (i) the Initialization stage and (ii) the operation stage. The details of these stages are explained as follows:

3.3.1 Initialization Stage

Here, each node in the network learns its distance, often measured in hops, to the base station (BS). This is achieved with the BS flooding *depth discovery message*. This message has a depth value initialized to zero by the BS and then it broadcasts this message. Every node that is lying within the BS's radio range receives this message, learns its depth value to the BS as zero, increments the depth count value by one, and rebroadcasts the message. A neighbor node that receives this message updates its depth information to BS as one in its table, increments the depth value by one, and rebroadcasts the packet. This process repeats till the message reaches the edge of the network. During this process, nodes learn one-hop neighbor information from the flooding messages. At the end of this task, each node in the network knows its distance to the BS and also its one-hop neighbor information.

In addition, nodes divide their neighbors into three groups as follows: i) closer-set: nodes whose depth is smaller than the node of interest, ii) equal-set: nodes whose depth values are the same as that of the node of interest, and iii) farther-set: neighbors whose depth values are larger than the node of interest. Following this *depth discovery message*, the BS floods another packet indicating the information about the network segments. Each segment is of size $R/3$, where R is the network radius. This completes the initialization stage.

3.3.2 Operation Stage

This stage presents in detail how the packets from the source node reach the BS through different paths to enhance privacy. The work considers a three- and four-phase routing approach depending on which section the source node is situated in. These phases are explained as follows:

- *Source Node (SN) is located in section one (S_1):* In this case, the packet is sent to an intermediate node (IN) using backward random walk (BRW). The neighbor nodes from the farther neighbor set are randomly chosen, based on residual energy, as relay nodes

and the packet is sent to that neighbor node. The random walk in this phase happens between $R/2r_s$ with reference to the BS and the network boundary. The node at which the BRW ends is termed aa an intermediate node (IN). From the IN the packet is sent either in a clockwise or anti-clockwise direction to reach a virtual source (VS) which is randomly chosen between $45°/\theta$ as lower limit and $180°/\theta$ hops as upper limit; where θ is a sensing range of a sensor node in the circular walk. θ is estimated in Fig. 3.3 and it is delivered in Eq. 3.12. The nodes at the same depth as that of the IN are chosen as the relay nodes in this phase. This second phase terminates on the virtual source (VS). From the VS, the packet is sent to a node on ring two using shortest path routing (SPR) in phase three. A node on ring two that holds this packet is termed a ring node (RN). The RN relays the packet only to a neighbor whose depth value is two. This walk-in phase four continues till the packet reaches a node whose position is in opposite direction to the position of the source node (SN). This is done to enhance privacy. Finally, the packet is sent to BS as shown in Fig. 3.2.

- *Source Node (SN) is located in section two (S_2):* In this case the packet is sent to an IN in the backward direction that constitutes phase one. The nodes in the backward direction set include nodes that are in a higher and equal neighbor set. A neighbor is randomly chosen from this set based on the amount of residual energy. In phase two, the packets are sent in either clockwise or anti-clock direction until it reaches a VS on the same ring. In the third phase, the packet is sent from the VS to the BS using SPR. The random walk in phase one happens between $R/2r_s$ and the network edge and the walk in phase two happens between $45°/\theta$ and $180°/\theta$ hops.

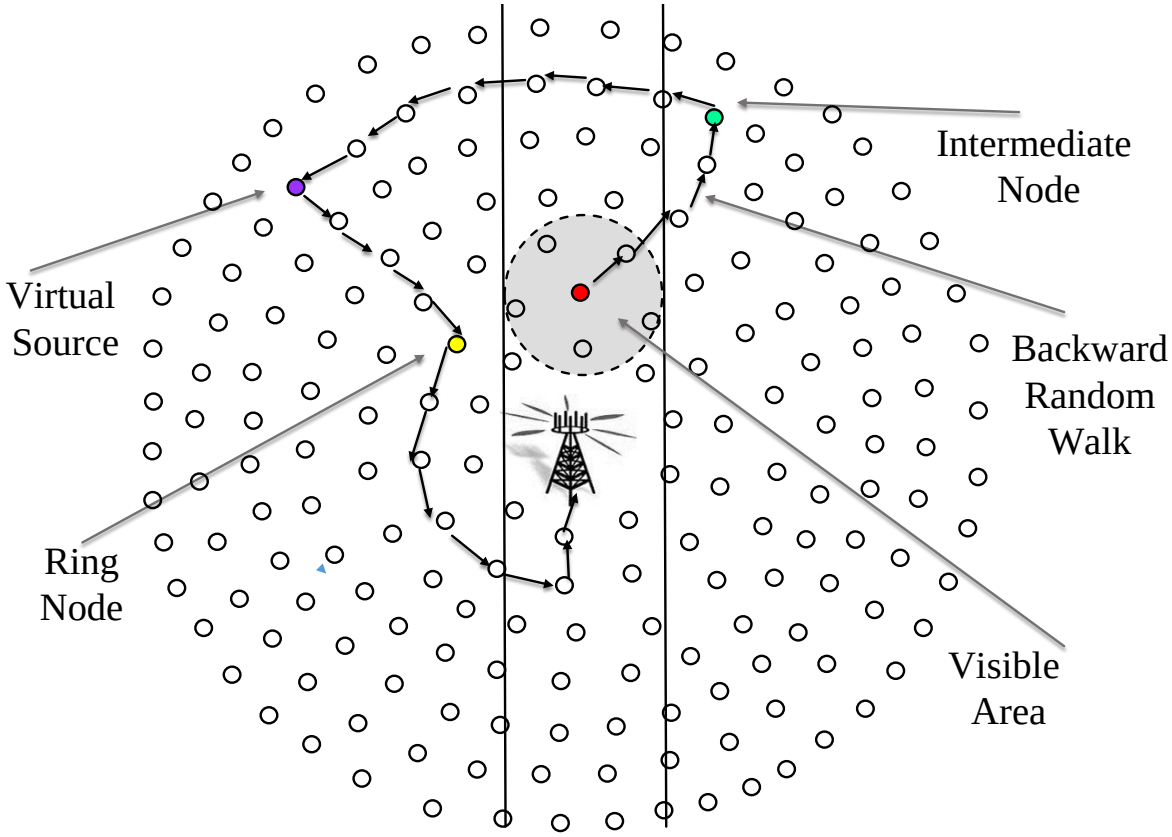

Figure 3.2: Selection of Intermediate Node, Virtual Source and Ring Node in PSSLP

- *Source Node (SN) is located in section three (S_3):* In this scenario, the SN sends the packets in either clockwise or anticlockwise direction towards a distant VS in phase one. The number of hops in this phase is randomly chosen between $45°/\theta$ and $180°/\theta$ hops. In the second phase, the packets are sent to a node on the second ring using the shortest path routing technique (SPR). Once the packet reaches a ring node (RN) on the second ring in phase three, it is relayed to other nodes on the same ring till the packet reaches the position that is opposite direction w.r.t the source node position. Finally, in phase four, the packet is sent to the BS.

The algorithm for PSSLP operation stage is given in Algorithm 1.

Algorithm 1: PSSLP

```
if (AssetDetected) then
    rings ← getTotalRings();
    R ← getSnRing();
    section ← getSnSection(R);
    // Backward Random Walk, get the number of rings from source to the edge ring
    I ← rings − R;
    h1 ← rand(2, I);
    //If source node is in 2nd Section, then consider equal set also
    if section == 2 then
        isEqualSet ← True;
    else
        isEqualSet ← False;
    for i =1:1:h1 do
        // Choose the relay node
        RelayNode ← chooseBackwardListNode(isEqualSet);
        SendPacket(RelayNode);
        CurrentNode ← RelayNode;
    //Clockwise and Anti-Clockwise Walk
    h2 ← getHops(45, 180, CurrentNode);
    isClockwise ← rand(0, 1);
    for i =1:1:h2 do
        RelayNode ← chooseNeighborNode(isClockwise);
        SendPacket(RelayNode);
        CurrentNode ← RelayNode;
    if section == 1||section == 3 then
        //Shortest Walk
        stopRing ← 2;
        r ← getRing(CurrentNode);
        while r ≠ stopRing do
            RelayNode ← BestNextNode();
            SendPacket(RelayNode);
            CurrentNode ← RelayNode;
            r ← getRing(CurrentNode);
        //Clockwise and Anti-Clockwise Walk
        h3 ← getHops(45, 180, CurrentNode);
        isClockwise ← chooseDistantDirection();
        for i =1:1:h3 do
            // Choose the relay node
            RelayNode ← chooseNeighborNode(isClockwise);
            SendPacket(RelayNode);
            CurrentNode ← RelayNode;
    while CurrentNode ≠BaseStation do
        //Choose a neighbour whose distance to BS is the least
        RelayNode ← BestNextNode();
        SendPacket(RelayNode);
        CurrentNode ← RelayNode;
```

3.4 Performance Metrics

We enlisted and defined the metrics that were used to measure the performance of the proposed technique as follows.

1. *Safety period*: *The Safety period* is defined as the period that starts once a source of information sends the first packet to the base station and is terminated when an adversary locates the source node. This metric was measured by considering the number of packets sent to the base station by the source node before the adversary reaches the real source of information [87].

2. *Entropy*: This metric was used to measure the degree of randomness of the routing paths the packets follow. It is given by

$$H(Y) = -\sum P(Y) log_2(P(Y)) \tag{3.1}$$

where Y is defined as the random variable with a probability function of $P(Y)$ [97].

Assume that $M^{'}(n_i)$ is the number of packets forwarded by a sensor node n_i and M is the total number of packets sent by the source for the entire simulation. Then entropy is given by

$$H(N) = -\sum_{i=1}^{i=N} \left(\frac{M^{'}(n_i)}{M}\right) \times log_2\left(\frac{M^{'}(n_i)}{M}\right) \tag{3.2}$$

where N is the total number of nodes in the network.

3. *Capture ratio*: The capture ratio is defined as the number of trials in which the adversary is successful in capturing the asset to the total number of trials carried out in the experiments [86, 98, 99].

4. *Energy Consumption*: The energy expended due to the transfer and reception of the messages alone was considered while measuring the energy consumption metric. To analyze this metric, the power consumption model given in [100] was used. The notations used in analyzing the energy consumption are given in Table. 3.1. Based on distance between sender and receiver (d), the energy for sending a l-bit message is denoted as $E_{Tx}(l, d)$, for free space f_s and multi-path m_p as shown in Eq. 3.3 and Eq. 3.4.

$$E_{T_X}(l, d) = E_{elec} * l + e_{fs} * l * d^2 \qquad d <= d_0 \tag{3.3}$$

$$E_{T_X}(l, d) = E_{elec} * l + e_{amp} * l * d^4 \qquad d > d_0 \tag{3.4}$$

The energy consumption for receiving l-bits message is given by

$$E_{Rx}(l) = l * E_{elec} \tag{3.5}$$

Table 3.1: Notations Related to Energy Consumption

Notation	Description
d_0 = $\sqrt{(e_{f_s})/(e_{mp})}$	Threshold distance
$E_{elec} = 50n$ J/bit	Loss in transmission circuit
$e_{f_s} = 10PJ/bit/m^2$	Free space model's power amplification
l =6392 bits	Packet's length
$e_{amp} = 0.00013PJ/bit/m^4$	Fading model's power amplification
d	Distance between the sender and the receiver

where E_{elec} is the energy loss that depends on the factors such as digital coding, spreading of the signal and filtering in the transmit circuit. The energy of amplifier, $f_s * l * d^2$ or $e_{amp} * l * d^4$, depends on the distance d to the receiver and the acceptable bit-error rate. The threshold distance d_0 is given by d_0 = $\sqrt{(e_{f_s})/(e_{mp})}$ as referenced in [100]. In this thesis, the value used as d_0 is 87 with reference to the work in [20].

5. *Delay*: The delay metric was measured based on the number of hops taken by the packets to reach the BS from the real source of information. This metric is derived in the subsequent section.

6. *Network Lifetime*: This is the time (measured in rounds) that begins when a network starts to operate and ends when the first node in the network dies. In particular, this metric was measured based on the number of packets sent in the network before the first node's battery energy ran out. Each new packet sent to the BS is termed as *round* in this work.

3.4.1 Analytical Models for Average Hop Estimation

The analytical models to estimate the *average hop count* or *average delay* of the proposed technique are presented as follows:

1. ***Source Node is in Section-1:*** When the source node is in section-1, then protocol has the following phases in routing path:

   - *BRW phase (phase-1)*: The maximum number of hops can be traversed by the packets, up to the network edge, in backward random walk (phase-1) when the source is on ring 1 in segment-1. Under such scenario, distance d_{11} between the source node and the network boundary is given by

   $$d_{11} = R - d^{'} \tag{3.6}$$

   where $d^{'}$ is the distance between the base station and the source node.

Table 3.2: Notations Related to Mathematical Equations

NOTATIONS	DESCRIPTIONS
d_{11}	Distance between the source node (SN) and the network boundary in backward direction (BRW) i.e., Phase-1 when SN is in section one (S_1)
$d^{'}$	Distance between BS and SN
R	Network radius
r_s	Sensor node and BS radio range
H_{11}	Number of hops in phase1 (BRW) when SN is in S_1
d_{12}	Distance from Intermediate Node (IN) to the Virtual Source (VS)
H_{12}	The maximum hops between IN and Vs
d_{13}	Distance from the VS to the ring node
H_{13}	The number of hops between Vs and ring node
d_{14}	The distance between ring node and the node which sends the packet to the BS in S_1
H_{14}	The number of hops that packet takes from ring node to the node which sends the packet to the BS in S_1
H_{S_1}	Total hops when SN is in S_1
d_{21}	The maximum distance from SN to the IN in phase one (BRW) when SN is in section 2 (S_2)
H_{21}	Number of hops in phase 1 when SN is in S_1
H_{22}	Number of hops from IN to VS in S_2
H_{23}	Number of hops from VS to BS
H_{S_2}	Total number of hops when SN is in S_2
d_{31}	The maximum distance between SN and IN, when source is in section 3 (S_3)
H_{31}	Number of hops between SN and IN in S_3
H_{S_3}	Total hops when SN is in S_3
$\|\psi(n_i)\|$	Total number of neighbors of node n_i
$\|\psi(n_i)_H\|$	Total number of neighbors of node n_i in higher depth
$\|\psi(SN)_{HE}\|$	Total number of neighbors of node n_i in higher depth and equal depth
$d^{''}$	Tangent drawn from BS to SN's radio range (see Fig. 3.3)

Distance in terms of hops is given by

$$d_{11} = \frac{R - d^{'}}{r_s} \quad in\ hops \tag{3.7}$$

Now, the number of hops in BRW (i.e., phase-1) is given by

$$H_{11} = \frac{R - d^{'}}{r_s \times p_{r_1}} \tag{3.8}$$

where p_{r_1} is defined as the ratio of *number of neighbours in higher depth to total number of neighbours of a node* n_i, i.e.,

$$p_{r_1} = \frac{|\psi(n_i)_H|}{|\psi(n_i)|} \tag{3.9}$$

- *Clock/anti-clockwise direction walk (phase-2)*: In this phase, after the BRW, the packet is sent in either in clockwise or anticlockwise direction. The maximum distance (d_{12}) travelled by the packets in this phase is given by

$$d_{12} = \pi \times R \tag{3.10}$$

Therefore, the maximum number of hops in this phase is given by

$$H_{12} = \frac{\pi \times R}{\theta} \tag{3.11}$$

where θ is calculated as follows:
From Fig.3.3 and using Cosine angle rule, it is shown that

$$\begin{aligned} (2r_s)^2 &= d^{''2} + d^{''2} + 2d^{''}d^{''}\cos(2\theta) \\ (2r_s)^2 &= 2d^{''2} + 2d^{''2}\cos(2\theta) \\ 2d^{''2}\cos(2\theta) &= 2d^{''2} - 4{r_s}^2 \\ \cos(2\theta) &= \frac{2d^{''2} - 4{r_s}^2}{2d^{''2}} \\ \theta &= \cos^{-1}\left(\frac{2d^{''2} - 4{r_s}^2}{4d^{''2}}\right) \end{aligned} \tag{3.12}$$

- *SPR phase (phase-3)*: The maximum distance a packet can traverse in this phase is equal to the distance between the BS and network boundary. i.e., distance R with the assumption that walk the in phase-2 terminated on the boundary (upper bound).

$$d_{13} = R \tag{3.13}$$

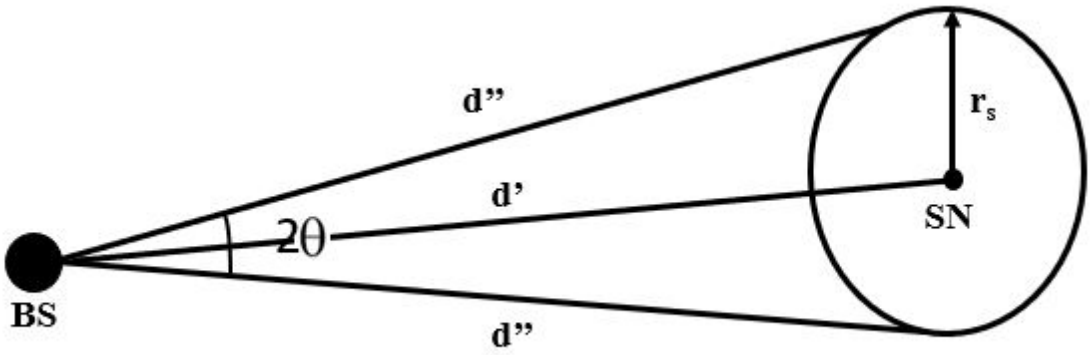

Figure 3.3: Theta estimation-PSSLP

Therefore, number of hops in SPR is given by

$$H_{13} = \frac{R - 2r_s}{r_s} \tag{3.14}$$

The factor $-2r_s$ is because the SPR terminates at a node on 2^{nd} ring in the network.

- *Walk on Second Ring phase (phase-4)*: Since the ring node walk can be maximum half the circumference of second circle, the total distance for packet travel is given by

$$d_{14} = \frac{2\pi(2r_s)}{2} \tag{3.15}$$

in terms of hops, it is written as

$$H_{14} = \frac{2\pi(2r_s)}{2r_s \times \theta} = \frac{2\pi}{\theta} + 2 \tag{3.16}$$

Hence, total hops in section 1 is

$$H_{S_1} = \frac{R - d^{'}}{r_s \times p_{r_1}} + \frac{\pi \times R}{\theta} + \frac{R - 2r_s}{r_s} + \frac{2\pi}{\theta} + 2 \tag{3.17}$$

2. ***Source Node in Section-2:*** When the source node is in section-2, then the protocols has the following phases in routing path:

- *BRW (phase-1)*:
  The maximum distance d_{21} available for BRW (in phase-1) is given by

$$d_{21} = R - d^{'} \tag{3.18}$$

in terms of hops this distance is given by

$$d_{21} = \frac{R - d^{'}}{r_s} \tag{3.19}$$

Therefore, number of hops H_{21} in phase-1 is

$$H_{21} = \frac{(R - d^{'})}{r_s \times p_{r_2}} \tag{3.20}$$

Where p_{r_2} is defined as the ratio of *number of neighbours in higher depth and equal depth to total number of neighbours of a node* n_i, i.e.,

$$p_{r_2} = \frac{|\psi(n_i)_{HE}|}{|\psi(n_i)|} \tag{3.21}$$

- *Clock/anticlockwise direction walk (phase-2)*: Similarly, the number of hops H_{22} in phase-2 is given by

$$\begin{aligned} H_{22} &= \frac{2\pi R}{2\theta} \\ &= \frac{\pi R}{\theta} \end{aligned} \tag{3.22}$$

- *SPR (phase-3)*:
  Number of hops H_{23} in SPR phase (phase-3) is given by

$$H_{23} = \frac{R}{r_s} \tag{3.23}$$

Therefore, total number of hops when source is situated in segment 2 is given by

$$H_{S_2} = \frac{(R - d^{'})}{r_s \times p_{r_2}} + \frac{\pi R}{\theta} + \frac{R}{r_s} \tag{3.24}$$

3. ***Source Node in Section-3:*** When source node is in section 3, then the distance d_{31} in phase-1 i.e BRW is given by

$$d_{31} = \frac{R - (2R/3)}{r_s} \tag{3.25}$$

Therefore, number of hops in BRW phase is,

$$H_{31} = \frac{R}{3r_s \times p_{r_1}} \tag{3.26}$$

Hence total hops when SN is in segment-3

$$H_{S_3} = \frac{R}{3r_s \times p_{r_1}} + \frac{\pi R}{\theta} + \frac{R - 2r_s}{r_s} + \frac{2\pi}{\theta} + 2 \tag{3.27}$$

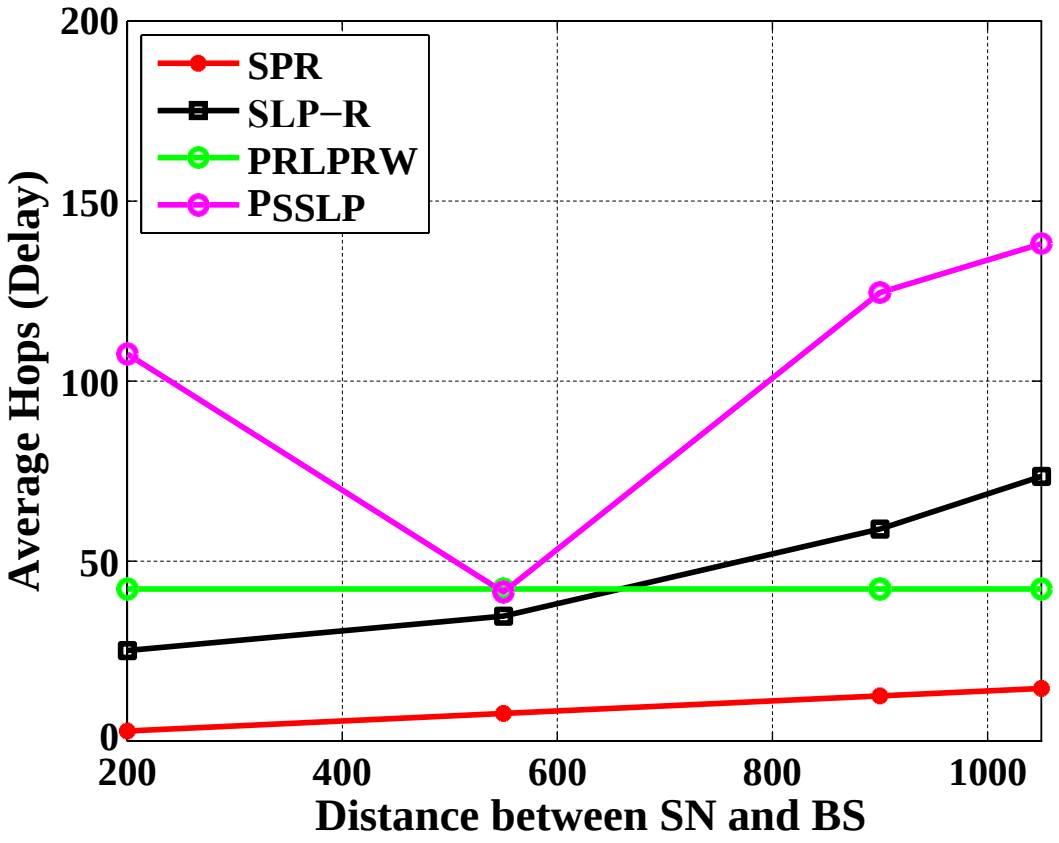

Figure 3.4: delay analytically PSSLP

Fig. 3.4 shows average delay plots calculated analytically. Using equations eq. 3.17, eq. 3.24 and eq. 3.27 for PSSLP protocol, the average delay is computed by varying the position of the source node w.r.t sink position as 200, 550, 900 and 1050 units respectively. The obtained values of the average delay metric are plotted. The delay metric indicated in Fig. 3.4 is expressed in terms of the number of hops the packets take to reach the base station. Similarly, the values of average delay for SPR, SLP-R [101], and PRLPRW [24] are computed and plotted. As the name suggests, SPR has the least delay as the packets follow the shortest path from source to destination (the sink). In the case of SLP-R, for distances (between the source node and the sink) of 200 and 550 units, the average delay is smaller than PRLPRW. However, as the distance between the source and the sink increases i.e., for distances of 900 and 1050 units, the trend is reversed. That is the average delay is higher than the PRLPRW technique. This behavior of SLP-R is due to the nature of the protocol design. Coming to the proposed technique, PSSLP, there is a decreasing trend in the average delay between the source node positions of 200 and 550 units, at position 550 the average delay reaches that of the PRLPRW scheme. It again increases when the source is positioned at 900 and 1050 positions. The large delay in PSSLP is attributed to the fact that it has more randomness i.e, more uncertainty of the routing paths which in turn led to a higher safety period.

3.5 Results and Discussion

The simulation scenario considered in this contribution is described here. The proposed technique was compared with the baseline technique Shortest Path Routing (SPR) (i.e., no privacy protection) and existing SLP protection techniques namely, SLP-R [101] and PRLPRW [102]. To evaluate the effectiveness of the proposed technique, the metrics defined in Section 3.4 were used. The simulation setup was developed using Python coding language and we used Pycharm as an Integrated Development Environment (IDE).

3.5.1 Simulation setup

A circular deployment model was considered with the BS in the center of network as shown in Fig. 3.1. The network radius R was set to 1050 units. The sensor nodes were uniformly deployed on annular rings. we considered 21 annular rings and 1464 sensor nodes including the BS. The area was divided into three sections namely S_1, S_2, and S_3. Each section is for size $R/3$, where R is the network radius. The radio range of each sensor node was set to 71 units; this radio range was considered for the BS, the sensor nodes and the adversary's device. Each sensor node was initially loaded with 0.5 joules of energy.

Let there be a single BS that is located in the center of the network at $(0, 0)$. It was assumed that the adversary starts its backtracking task from the BS as it is the focal point for all network traffic. Further, it was also assumed that there was a single source node in the network. The position of the source node was varied w.r.t to the BS and for each position, the source sent 1000 packets to the BS in one trial. The simulation in each trial ended when the adversary reached the source node or when all the packets from the source node were sent to the BS. Simulation results presented here were averaged over 100 trials. The following coordinates were considered for the source node position in the simulation: $(200, 0)$, $(550, 0)$, $(900, 0)$, $(1050, 0)$. The performance of the proposed technique was gauged using the metrics given in Section 3.4.

3.5.2 Results analysis

To evaluate the performance of the proposed scheme and the existing ones, we simulated various network configurations and then analysed the results obtained as follows:

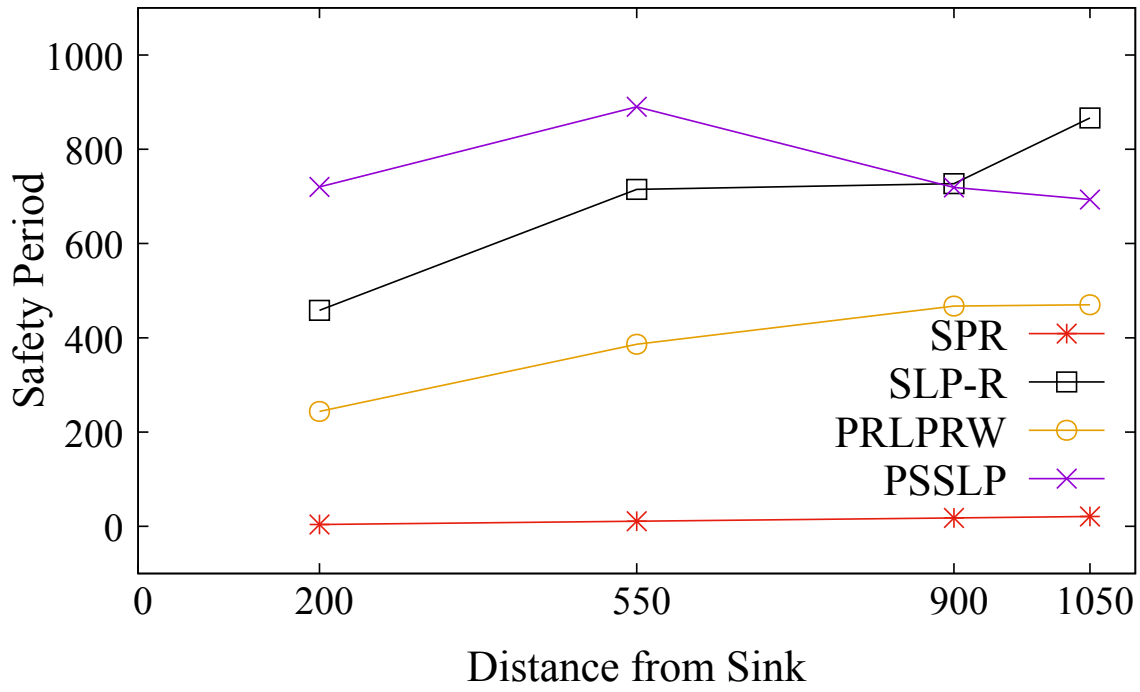

Figure 3.5: Safety Period

- *Safety period:* The *safety period* metric is shown in Fig. 3.5. The privacy level (i.e, safety period) of the proposed solution is compared with the two existing SLP techniques namely SLP-R and PLRPRW; and with no SLP scheme named shortest path routing (SRP). The figure shows that the proposed technique (PSSLP) has better privacy level compared to other techniques; this is due to the fact that PSSLP is able to deliver more number of packets to the base station before the adversary reaches the source of information. The *safety period* of the proposed technique is the best even if the source of information is near by the base station. This is attributed to the fact that PSSLP considers position of the source node while making routing decision, which is not seen in existing techniques. Thus, the main objective of having uniform privacy level irrespective of the position of the source nodes in the network is verified through simulations.

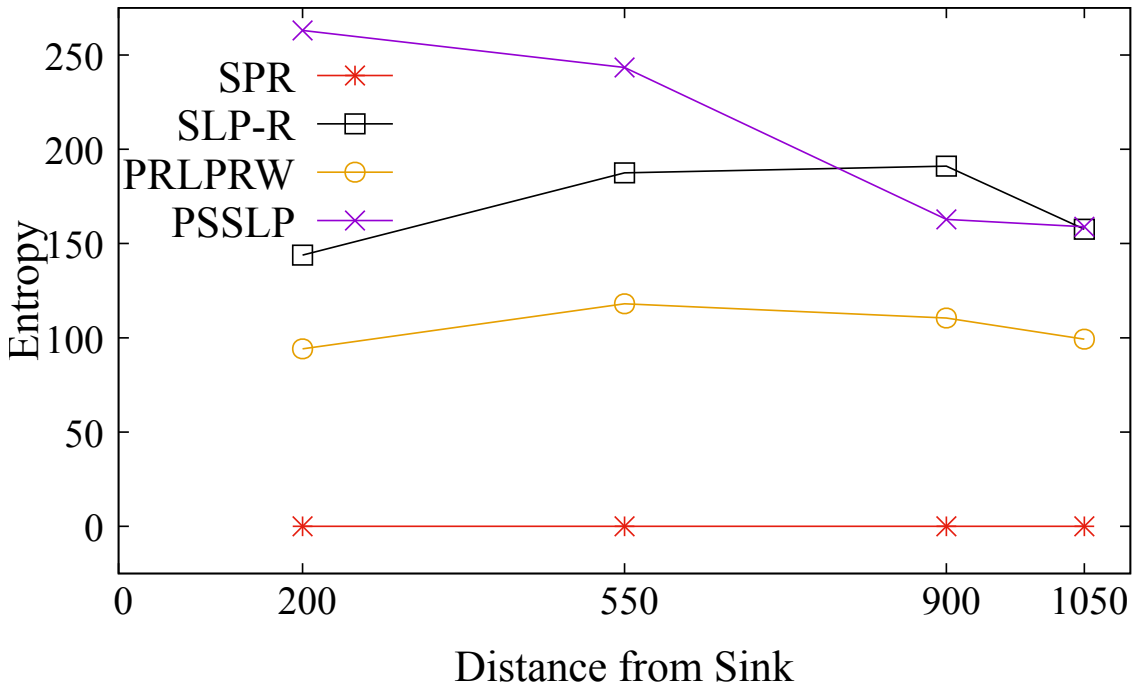

Figure 3.6: Entropy

- *Entropy:* Fig. 3.6 shows the plot for entropy (the degree of randomness) metric as defined in eq. 3.2. *entropy* shows the path diversity of routing protocol, the more the entropy, the more the privacy [97]. It is observed that the entropy of the proposed technique is the best compared to other techniques. Since in the proposed technique (PSSLP), a source of information sends a packet to the BS in a total randomized way, the routing path becomes dispersive which leads PSSLP to increased entropy. It is observed that the entropy increases when the SN is nearby the base station in PSSLP and starts decreasing when SN is far away from the BS. The reason for this decrease in randomness is because the packets from a source node, which is present in S_1, pass through four random phases to reach the BS and has more path diversity. While in other sections i.e., when the source node is either in S_2 or S_3, the path diversity slightly decreases. For example, when SN is situated in section three, there is a possibility of finding SN on the network boundary, in this case, there is no BRW which leads to a decrease in path diversity. However, it is stress that the value of entropy near the boundary region is comparable to that of the existing schemes. The entropy for SPR is zero as the path from source to destination (i.e, the sink) is fixed and its uncertainty is zero. The entropy of PRLPRW is higher than SPR but lower than SLP-R and PSSLP schemes. For the SLP-R scheme, entropy is lower compared to the proposed scheme. However, for distances around 700 units away from the sink node, the trend is reversed. That is SLP-R shows an improved entropy metric compared to the PSSLP technique. Nevertheless, it is mentioned that the overall entropy metric, averaged over all trials and for all positions of the source node in the network, is highest in the proposed scheme compared to the other three techniques. This value

is shown in Table 3.3. Hence in terms of entropy also the proposed scheme performs well compared to the other schemes. Even if SLP-R showed an improved entropy metric compared to the PSSLP technique nearby the network edge, the average entropy in all trials for the proposed scheme is the highest as shown in Table 3.3.

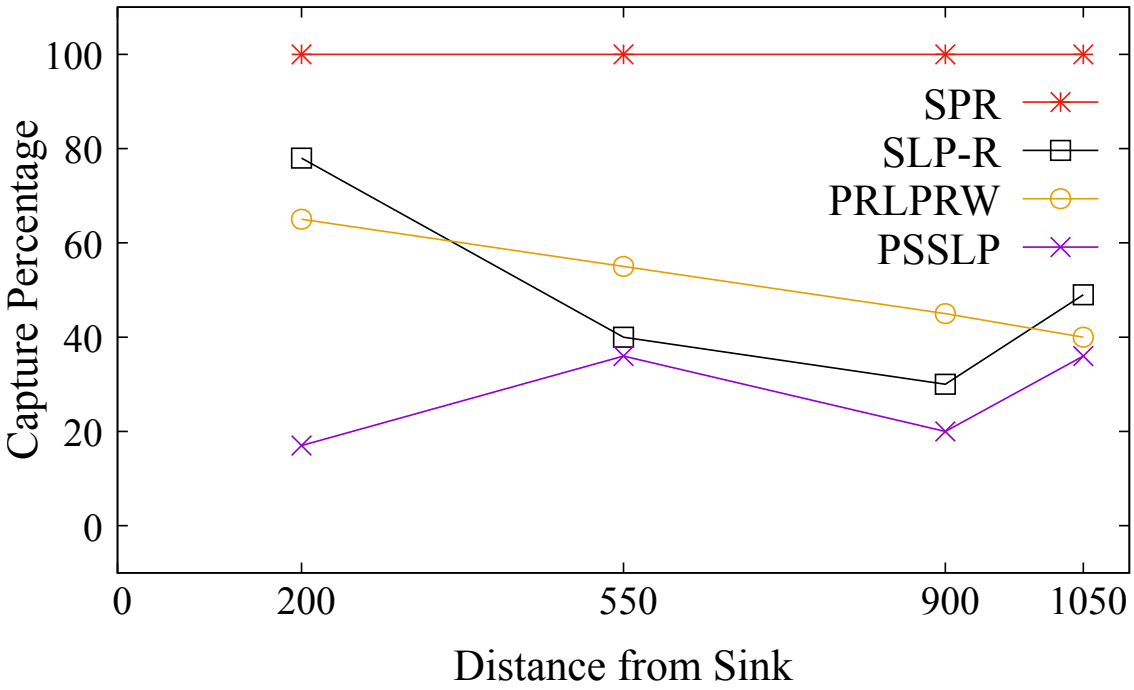

Figure 3.7: Capture Percentage

- *Capture Percentage:* Fig. 3.7 depicts the *capture percentage* that is defined in section 3.4. This metric indicates the attacker's success rate. Therefore, the smaller the values of this metric, the better the performance of the proposed protocol. Fig. 3.7 shows that SPR has the highest *capture ratio* i.e., 100% *success rate* of the attacker. Since the packets follow the same path in the SPR technique, the attacker is always successful if the number of packets sent by the source node is at least the number of hops between the source and the sink. *Capture ratio* metric for PRLPRW is smaller than the SPR technique and its magnitude keeps on decreasing as the distance between the source and the sink keeps on increasing. The *capture ratio* for the SLP-R technique is high compared to PSSLP and PRLPRW for the cases when the source node is closer to the BS and when the source is near the network edge. But in the other cases, the *capture ratio* magnitudes are smaller compared to the PRLPRW scheme. The *capture ratio* metric for the proposed scheme is the least compared to all other schemes. This is because the protocol is designed to take care of the source node position in the network. Also, as claimed in the objective statement, it is seen that PSSLP has an almost uniform *capture ratio* metric level irrespective of the distance of the source node measured w.r.t to the BS's position. In summary, the lower the *capture ratio* values, the higher the protocol's privacy level is. It has been observed that PSSLP has less capture percentage compared

to other protocols, thus better privacy.

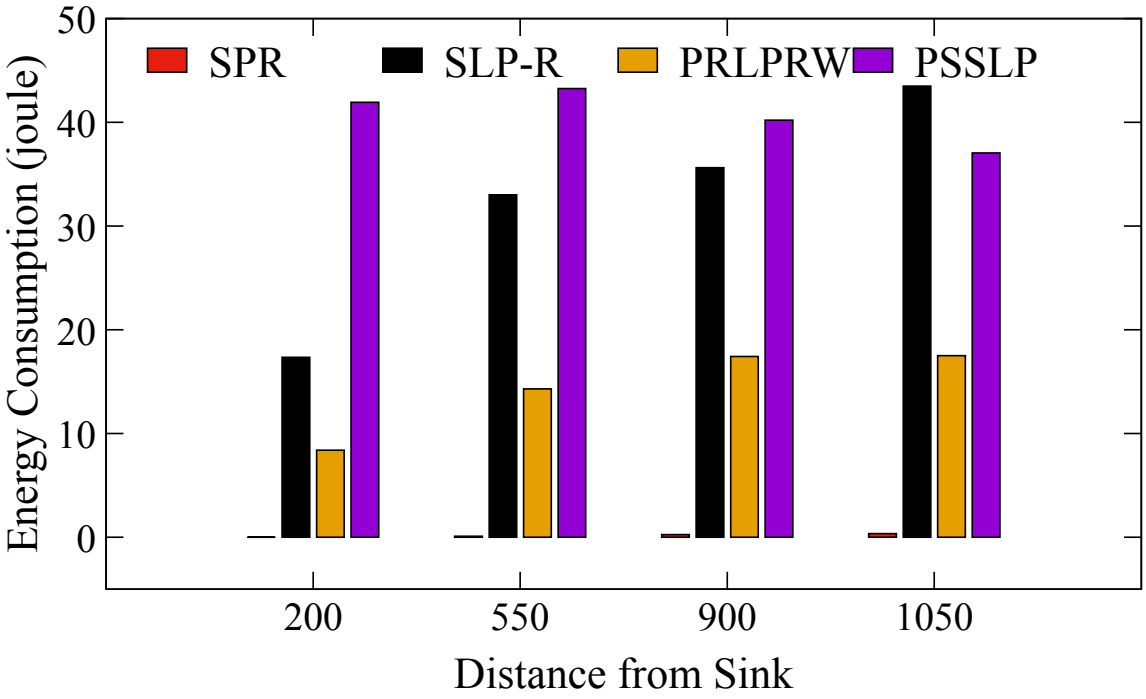

Figure 3.8: Energy Consumption

- *Energy Consumption*: The energy consumption metric of PSSLP is compared with SLP-R, PLRPRW, and SPR schemes. To simulate the energy consumption, energy consumption model given in eq. 3.3 and eq. 3.4 are used. This metric is plotted in Fig. 3.8. It is observed that in all three SLP techniques energy consumption increases with an increase in the distance between the source node and the sink. This is due to the random nature of the routing protocols. It is also found that the energy consumption in SLP-R is very high for all positions of the source node in the network when compared with the PRLPRW technique. Considering the path diversity and randomness of the proposed PSSLP routing technique, it is natural to expend more energy. Hence, the energy consumption in the proposed technique is the highest compared to that of SLP-R and PLRPRW SLP techniques. Also, the amount of energy consumption in the PSSLP technique is uniform for various positions of the source node in the network. This is the limitation of the proposed scheme.

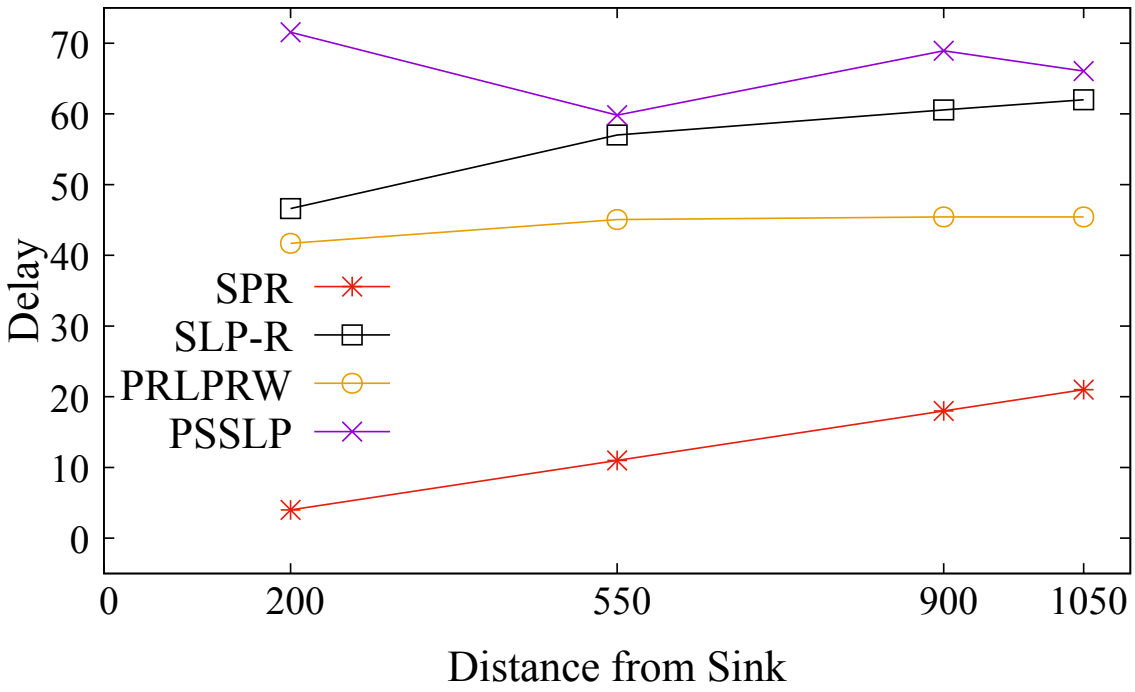

Figure 3.9: Delay

- *Delay:* The packet latency (delay) metric is shown in Fig. 3.9. Latency is measured in terms of the average number of hops the packets take to reach the BS from the source node. The more nodes that are crossed in random walk phases the higher is the delay. No SLP protocol i.e, SPR has the least delay as the packets follow the shortest path from the source to reach the base station. PRLPRW technique has higher delay compared to SPR technique while SLP-R has the highest delay compared to SPR and PRLPRW techniques but lesser than the proposed PSSLP scheme. The delay in PSSLP is attributed to the fact that the packets take more hops to reach the BS than in other techniques. This is another limitation of the work. The simulation results given here are well aligned with the estimated theoretical analyses given in Fig. 3.4.

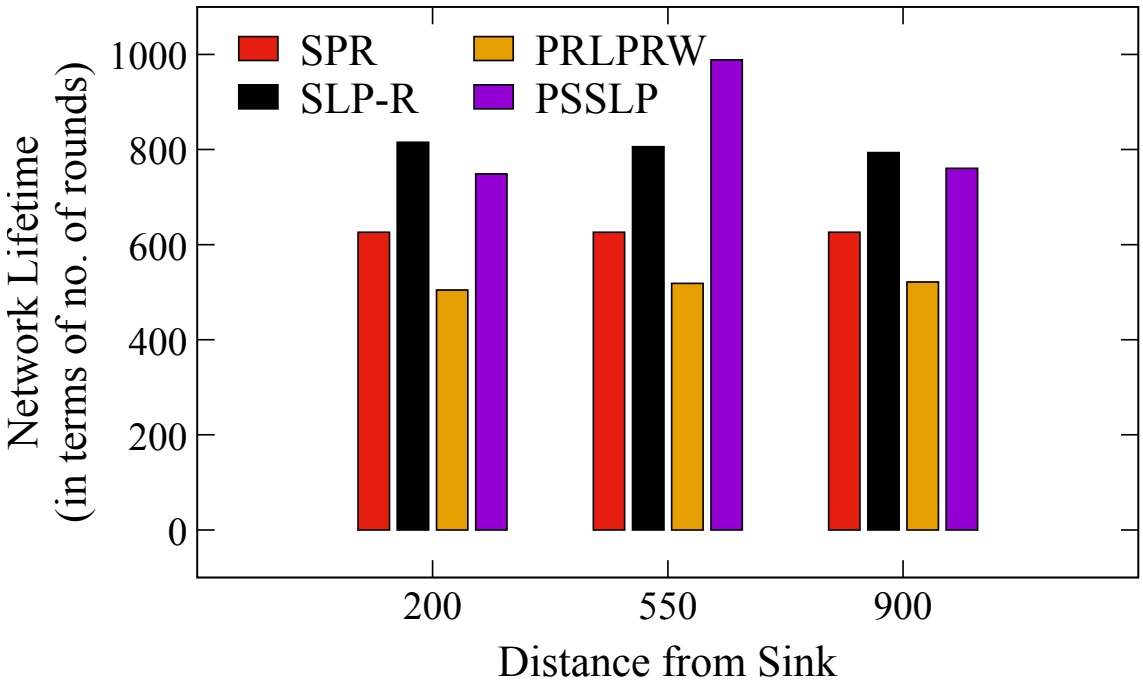

Figure 3.10: Network Lifetime

- *Network Life Time:* Network Life Time (NLT) for four techniques is presented in Fig. 3.10. It is observed that the NLT for PSSLP is quite comparable with that of SLP-R. Although the proposed technique expends the highest energy for the case when the source is situated in segment S_2, the overall energy expenditure is better than the SLP-R technique (see Table 3.3). SPR and PRLPRW have very poor NLT when compared to PSSLP and SLP-R. This is because in these protocols, the packets are sent to the BS without considering the residual energy at nodes and most of the time same set of paths are used by the packets to reach the BS. This leads to the situation where the packets may visit the same node(s) several times during their journey to BS. This in turn leads to energy hole problems in certain areas of the network. Hence the nodes that lie in such paths exhaust their energy at a faster rate compared to other nodes in the network. The proposed technique has achieved improved NLT when compared with all three schemes. Thus, the purpose of enhancing privacy while conserving the NLT is achieved as stated earlier.

Table 3.3: Summary of Performance Characterization

Metrics vs. Protocol	Safety Period	Capture Ratio	Entropy	Energy Consumption	Delay	Network Lifetime
SLP-R	6431.46	-50.75	17001	48308.16	478.79	28.59
PRLPRW	3511.55	-48.75	10551.1	22641.75	380.26	-1804.0
PSSLP	8247.06	-72.75	20701.225	98197.59	657.57	33.0

3.5.3 Results Summarization

Table. 3.3 represents the summary of the overall results, the averaged entity These values are obtained by considering no SLP techniques namely SPR as a base reference. Specifically, each metric value of a given SLP scheme is taken and then its deviation (either increment or decrement in value) w.r.t the SPR technique is computed. Then the percentage deviation is estimated. Finally, all these values for a given protocol are averaged and presented in the table. It is observed that the proposed PSSLP technique has 8247.06 folds improvement when compared to SPR, while SLP-R and PRLPRW have only 6431.46 and 3511.55 folds improvements respectively. The improvements in PSSLP are ascribed to the fact that random walk is position-independent and has multiple routing approaches when the source node is in different sections of the network.

The capture ratio indicates the adversary's success rate and hence its values are negative. It is clear that the proposed technique PSSLP has shown 72.75 folds improvements over SPR while SLP-R and PRLPRW have 50.75 and 48.75 folds of improvements only. Similarly, in terms of entropy, PSSLP outperforms by 20701.25 folds improvements over SPR. Whereas SLP-R and PRLPRW have just 17001 and 10551 folds on improvements.

The improvements in terms of safety period, entropy, and capture ratio of the proposed scheme is achieved at the expense of increased energy consumption and latency (delay). This is the limitation of the proposed solution. However, the network lifetime of the proposed scheme has 33.0 folds improvement while SLP-R has only 28.5 folds improvement. PRLPRW performs poorly in terms of network lifetime. Therefore, the claim of "improved safety period without degrading the performance of the network lifetime" stays valid.

3.6 Conclusion

This chapter presents a newly developed SLP preservation technique (PSSLP) that mitigates the problem of position-dependent based privacy behavior of the solutions that are seen in existing works. The proposed scheme could be seamlessly used in applications such as habitat monitoring, monitoring the physiological status of soldiers in battlefield etc. In particular, the strength of privacy remains uniform irrespective of the position of the source node in the network w.r.t the BS position. The proposed technique achieves 8247.06 folds improvement in terms of safety period and 33.0 folds improvement in terms of NLT compared to no SLP technique. However, it has been noticed that a longer safety period was achieved at the expense of longer delays, and the network lifetime was not increased, but it was also not hampered. This is the scheme's limitation.

CHAPTER 4

A Total Randomized Enhanced Source Location Privacy

In the PSSLP technique, the ring node was chosen on the second ring w.r.t the BS with the idea of making routing path more diverse. This indicates that, each packet delivered to the BS once a source node is in section one or three must travel a specific distance on the second ring before arriving at the BS. As result, continuing to use the same set of nodes for packet transmission (i.e., the second ring nodes) can affect the network lifetime. It is even evidenced in the obtained results; the safety period was enhanced without any enhancement in network lifetime.

In this chapter we proposed a new scheme which is totally randomized namely "SLP-E", to handle the issue of using fixed ring seen in the previous chapter. SLP-E aims at enhancing both privacy and network lifetime together in single solution. It employs a reverse random walk followed by a walk on annular rings, to create divergent routing paths in the network, and finally, a walk on the controlled dynamic rings together with min-hop routing to deliver the packets toward the base station (BS). The objectives of the proposed work are to simultaneously improve the safety period and network longevity, and achieve uniform privacy and network lifetime (NLT) irrespective of the position of the source in the network.

In SLP-E, the packets are transmitted to the base station in a controlled random walk manner to ensure a better safety period and network longevity. In order to balance the distance they cover before reaching the BS, the packets take several routes. To establish fairness between the network lifespan (also known as network lifetime) and safety period, the hop threshold notion is presented. A random neighbor is chosen from the far-off neighbor list to relay a packet. This choice is based on the quantity of residual energy present in the nodes that are on the list of far neighbors. Like the walk in a game of maze, the packets initially travel backward from the source for specific hops before taking clockwise or anti-clockwise paths across the annular rings of the network. In this stage of the routing process, the routing paths are lengthened in

order to decrease the likelihood that packets will travel across the source node's radio range (known as the visible area).

SLP-E then, uses controlled walks on dynamic annular rings that depend on the location of the source node in the network with respect to the BS along with min hop routing to send the packet in the inward direction to reach the BS, in contrast to the existing solutions where packets followed only min hop (shortest path) or forward random walks in the inward direction to reach the BS. Controlled walks on dynamic annular rings in the inward direction help to increase the randomness and diversity of the routing path, which subsequently results in the usage of various set of nodes for packet routing to the BS. Thus, the improvement in network lifespan and the safety period. The suggested method basically achieves consistent privacy, independent of the location of the source sensor in the network, while maximizing both the safety period and the network's longevity. In addition, we also develop analytical models to estimate the average delay the packets take to reach the BS. These models are then used to compare the delay that is obtained through simulations.

The performance measurements, done using the proposed analytical models and simulations, indicated an improvement in the safety period and network lifespan compared to the existing SLP techniques regardless of the source node's position inside the network. The SLP-E achieved uniform and enhanced privacy and network lifetime simultaneously.

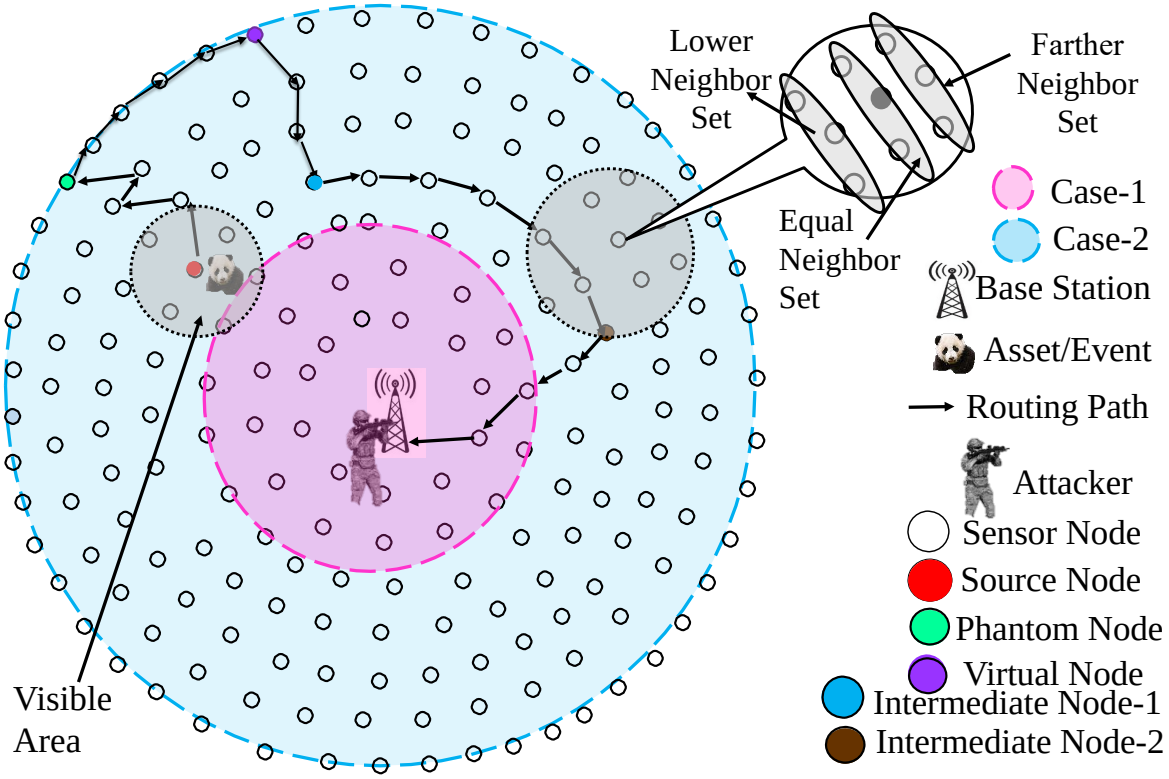

Figure 4.1: SLP-E technique

4.1 Network and Adversary Models

4.1.1 Network Model

The network model is inspired by the panda-hunter game model suggested in [87]. With a single strong BS in the middle, the sensor nodes are distributed uniformly throughout the network. The network under consideration has a circular structure, and it is envisaged that sensors form rings around the base station as illustrated in Fig. 4.1. The sensor nodes are uniform and static in design. In other words, before the network starts up, every node in it has the same beginning energy, computational power, radio range, and storage capacity. The communication range of the sensor nodes is constrained, so two nodes can only connect when they are close i.e., within each other's sensing range.

Therefore, multi-hop routing is used for communication between nodes that are not neighbors. Each sensor can determine its position in the network using the existing localization techniques [95]. Here, we took into account the situation of habitat monitoring, in which a network asset could randomly arrive at any point in the network. A source node continues transmitting the packets to its neighbors after spotting an asset within its radio range to send information packets to the base station. It is expected that the packets have been encrypted using cryptographic methods to prevent unwanted parties from reading their contents [96]. The nodes are arranged in such a way that each node that is not on the network edge has eight neighbors as shown in Fig. 4.1. These neighbors are divided into three groups: i) lower neighbor set, ii) equal neighbor set, and iii) far-away neighbor set based on the depth of each node as measured w.r.t BS.

4.1.2 Attacker Model

The attacker model used in this chapter is characterised by the following:

- The adversary is of passive type (just eavesdrops the communication) and do not perform any active attacks such as jamming, node compromise, replay attacks etc. Because the adversary's intention is to reach the asset without being detected by the target network.
- We assume that the attacker cannot decipher any kind of information that the packets carry as these information packets are assumed to be concealed using encrypted techniques
- The attacker starts backtracking the traffic flow from the base station. This location serves as an ideal point in the network because the entire network traffic converges at the base station.
- The adversary is assumed to be equipped with sophisticated equipment like spectrum analyzer and directional antennas. The adversary uses these devices to measure the signal

strength and the angle of arrival of the messages. Based on these estimates the adversary can locate the immediate sender of the packet.

- This work considers a patient adversary model in which the adversary waits at a node until it receives the message. Once the message is received it moves ahead in the direction of the packet's arrival.
- The message rate is assumed to be too low, such that the time interval between consecutive packets is more than the time it takes for the adversary to move from one node to the other.

4.2 The proposed technique

Here, we go over the specifics of the suggested SLP-E routing method. The two phases that make up the suggested technique are the network configuration phase and the operational phase. The base station invokes the configuration phase so that each node in the network can determine its own position w.r.t base station and also know its neighbors. The SLP-E protocol is executed during the execution phase.

4.2.1 Network Configuration Phase

The base station floods the network with a depth configuration message during initialization. The base station's neighbors are the first ones to receive the depth configuration message. The *depth* field in this message has an initial value of zero. The nodes that receive this packet increase the depth value by one and change the value in their routing table. The packet is then rebroadcast into the network. The nodes that receive these rebroadcast packets add one to the packet's content, update their respective depth value in their data table and rebroadcast the packet. This process is repeated till the packet reaches the network boundary. In this process, each node also learns its one-hop neighbor details. The neighbor of each sensor node is then divided into three categories: close neighbors, equal neighbors, and distant or far neighbors. A neighbor node is called a close neighbor if its hop count (also known as the depth value) to the base station is smaller than the node of interest; an equal neighbor if its hop count to the base station is the same as its own; and distant neighbor if its hop counts to the base station is higher. Information packets from the source node are routed using this information. *Depth* is defined as the distance between a sensor node and the BS measured in terms of hops.

4.2.2 Protocol Execution Phase

The actual protocol realization is covered in this phase. We consider two scenarios namely scenario-1 and scenario-2. If the source node is at a distance of one-fourth the network radius as measured from the BS's position, it is considered as scenario-1, else scenario-2. Since the

nodes within the base station's range are most susceptible to an adversary who initiates the backtracking process from this location, this threshold value is set to apply particular security precautions to those nodes. This is an arbitrary value (one fourth the network radius) chosen with the intention of granting distinct consideration to sensor nodes positioned in close proximity to the Base Station (BS). In Figure. 4.1, the pink color region represents scenario-1 and the blue color region represents scenario-2 of the network.

Depending on where the source node's position (i.e., its position is in scenario-1 or scenario-2) is in the network, the SLP-E protocol adapts accordingly. This process improves privacy and assists in finding a balance between privacy and the network lifespan by making routing patterns more dynamic. The source node can therefore maintain its anonymity anywhere inside the network.

4.2.2.1 Scenario-1

A sensor node changes into a source node after detecting an asset and begins transmitting packets to the base station using the proposed SLP-E technique. The following five phases of the routing protocol in this instance are described as follows:

- *Phase-1*: To generate a reverse random walk named a backward random walk (BRW), upon detecting an asset within its sensing range, a source node conducts a check of its location in relation to the Base Station (BS). If the distance between the source node and the BS is determined to be less than or equal to one-fourth of the network radius measured from the BS's position, it identifies itself as being in scenario one. Subsequently, the source node examines the details of its neighboring nodes, which are categorized into lower neighbors, equal neighbors, and distant or far-away neighbors. From this analysis, the source node establishes the farther neighbors as its forwarding set, and among these farther neighbors, it selects the node with the highest energy to forward the packet. The packets are sent in the opposite direction using farther neighbor set, away from the base station position. The source determines each packet's hop count to travel in this direction and this value is chosen randomly between one-third and two-thirds of the network radius (both these values are measured in terms of hops. We put these restrictions so that the packet can only travel a certain range (measured in hops). By doing this, when the source node is close to the base station, the packet is prevented from reaching the network boundary. No matter where the source node is in the network, this results in energy conservation, packet delay reduction, and the balance of network lifetime (NLT) and safety period. The hop count number is reduced by one count once this packet is received by a neighbor node and a neighbor node with the highest residual energy is the one chosen from the list of neighbors to relay this packet. This process continues as long as the hop count value in the packet is non-zero. When the hop count value in the packet is zero, phase 2 of the routing process begins. The phantom node (PN) is the node at which the BRW terminates.

- *Phase-2*: In this phase, the packets are routed in either clockwise or anti-clockwise directions. The phantom node decides whether to send the packets in an anti-clockwise or clockwise direction with a coin toss experiment and relays the packets to a neighbor that is in an equal-neighbor set. This procedure of relaying is repeated for H hops, where H is a random number chosen between $45°/\theta$ and $180°/\theta$. Where θ is a sensor node's radio range in a circular walk and its value is determined using Eq. 4.3. Virtual source (VS) refers to the node where the relaying process ends in this phase.

- *Phase-3*: From the virtual source, the packets are sent inward direction towards the BS for certain hops. In this phase, the packets are sent at least two hops in the inward direction from the VS and the maximum distance they travel is up to the boundary of the inner circle (see Figure. 4.1). The inward walk lower limit in this phase is two hops from the VS and the upper limit is the boundary of the inner circle (with pink color). The intermediate node-1 (IN1) is found randomly between those set limits. Unlike in the existing solutions where packets are sent directly to the BS through min hop routing (shortest path routing), in this phase one additional intermediate node (IN1) is chosen randomly between two nodes away from the VS and the boundary of the inner circle which is showing the threshold value. This improves the routing path randomness and diversity. The hop count values used in this phase are taken into account to reduce the likelihood of selecting IN1 that is close to the actual source node. Since in this scenario, a source node is in the inner circle (threshold circle), we make sure that the intermediate (IN1) cannot be found inside that circle.

- *Phase-4*: In this phase, the packets consider the direction they followed in phase two. The packets travel in either a clockwise or anti-clockwise direction to reach the Intermediate node-2 (IN2). The IN1 has to relay the packets in either a clockwise or anti-clockwise direction as was determined in phase-2. That is, if in phase-2, the packets travel in a clockwise direction then in phase-4 the packets will also travel in a clockwise direction. The goal of this phase is to reduce the likelihood that a packet will enter the sensing range of the actual source node in its way to reach the BS. If by any chance the source node is found at the boundary of the inner circle, as the maximum distance a packet can travel in phase two is $180°$, if this distance was travelled in clockwise direction, then in this phase, the packet takes clockwise direction with $90°$ as the maximum distance, with these conditions the packet cannot visit the source node location. we set $90°$ as the maximum distance in order to avoid that a packet may travel a distance which is equal to a complete circle, because doing so, when a source node is found at that inner circle boundary the packet may visit its place, thus the weaker privacy. This is even the reason why the packets must move in the same direction as they did in phase two, to avoid the possibility of discovering the IN2 within the range of the source node's radio or passing through it.

Therefore, in this phase, the packet travels for certain hops whose value is selected between 45° and 90°. The intermediate node-2 (IN2) is the node where this phase ends.

- *Phase-5*: Finally, by utilizing the shortest path walk, the packet is delivered to the BS from intermediate node2.

4.2.2.2 Scenario-2

The routing in this scenario-2 is similar to the one suggested for scenario-1 with the following differences: i) In phase-1, the intermediate node is randomly chosen between $R/2 * r_s$ and the network boundary (measured in hops), and ii) In phase 3, the hop count value is randomly selected between 4 hops from the VS and $2R/3 * r_s$ in the inward direction, where r_s is the sensor node radio range. If the source node is found at the network boundary, then, there is no backward direction, only four phases are to be followed. Due to traffic diversification and energy savings, this aids in enhancing not only the network lifespan metrics but also the safety period, as all nodes in the network participate in routing the packets to the BS in different rounds. This study ensures that all nodes in the network engage in sending the packets to the BS in the different rounds to improve NLT, unlike existing solutions where fixed rings are utilized to make the routing diverse or the shortest path routing to route the packets to the BS.

The SLP-E proposal execution phase is presented in Algorithm. 2.

Algorithm 2: SLP-E

if *(DetectedAsset)* **then**

//Obtain Network's radius in hop count terms: $radius \leftarrow NetworkRadius()$;

//Define Hop Threshold: $h\_t \leftarrow int(round(radius/4, 0))$;

$sn\_hc \leftarrow HopCountSN()$;

if $sn\_hc <= h\_t$ **then**

$scenario = 1$;

else

$scenario = 2$;

//Backward Random Walk (BRW): $onlyFurtherSet \leftarrow True$;

if $scenario == 1$ **then**

$h_1 \leftarrow random(radius/3, (2 * radius)/3)$;

else

$h_1 \leftarrow random(radius/2, radius)$;

for *i =1:1:*h_1 **do**

$NodeToRelay \leftarrow GetBackwardListNode(onlyFurtherSet)$;

$TransferPacket(NodeToRelay)$;

$PresentNode \leftarrow NodeToRelay$;

//Hop count in backward direction: $BW\_hc \leftarrow Int(n)$;

if $n > 0$ **then**

$ContinueTorelaythePacket$;

else

$EnterphaseTwo$;

$walkDirection \leftarrow random(0, 1)$;

$h_2 \leftarrow selectHops(45, 180, PresentNode)$;

for *i =1:1:*h_2 **do**

$NodeToRelay \leftarrow getClockwiseListNode(walkDirection)$;

$TransferPacket(NodeToRelay)$;

$PresentNode \leftarrow NodeToRelay$;

//Determine the hop count necessary based on the scenario

if $scenario == 1$ **then**

$h_3 \leftarrow random(2, radius/4)$;

else

$h_3 \leftarrow random(4, (2 * radius)/3)$;

for *i =1:1:*h_3 **do**

$NodeToRelay \leftarrow getShortestListNode()$;

$TransferPacket(NodeToRelay)$;

$PresentNode \leftarrow NodeToRelay$;

$r \leftarrow nodeRingNum(PresentNode)$;

$h_4 \leftarrow selectHops(45, 90, PresentNode)$;

for *i =1:1:*h_4 **do**

$NodeToRelay \leftarrow getClockwiseListNode(walkDirection)$;

$TransferPacket(NodeToRelay)$;

$PresentNode \leftarrow NodeToRelay$;

while *PresentNode* $\neq$ *BaseStation* **do**

//Select a neighbor node with the least distance to Base Station

$NodeToRelay \leftarrow getShortestListNode()$;

$TransferPacket(NodeToRelay)$;

$PresentNode \leftarrow NodeToRelay$;

4.2.3 Performance characterization

The performance metrics considered to evaluate SLP-E are the same as the ones defined in 3.4 in chapter one.

- Delay Estimation Models

  The analytical models for the suggested solution's maximum delay or hop count are derived in this section. The plots presented in Figure. 4.2 are the delays obtained through the developed analytical model.

- Case-1:

  If the distance (in hops) between the source location and sink is below the established threshold, SLP-E has five phases, with the following maximum delay for each phase:

  - *Max Delay in Phase-1*: There is a backward random walk between $R/3$ and $2R/3$. The BRW packets travel a distance of $\frac{2R}{3}$. Let d represent the separation between the source and sink nodes. The distance that BRW can travel then is $(\frac{2R}{3} - d^{'})$ units. The number of hops in *phase-1* is given by:

$$H_{11} = \frac{\frac{2R}{3} - d^{'}}{r_s \times p_r} \tag{4.1}$$

    where r_s is the radio range of the sensors, and p_r is the proportion of neighbors in equal- and higher-depth to all neighbors.

  - *Max Delay in Phase-2*: The farthest distance that may be covered in *phase-2* is $180°$, therefore we have:

$$H_{12} = \frac{180°}{\theta} \tag{4.2}$$

    where θ is calculated as follows:
    From Fig.3.3 and using Cosine angle rule, we have

$$\begin{aligned} \cos(2\theta) &= \frac{2{d^{''}}^2 - 4{r_s}^2}{2{d^{''}}^2} \\ \theta &= \cos^{-1}\left(\frac{2{d^{''}}^2 - 4{r_s}^2}{4{d^{'}}^2}\right) \end{aligned} \tag{4.3}$$

Table 4.1: Notations and Description

Notations	Description
R	Radius of deployment area
r_s	Radio range of nodes
P_r	Probability of relaying
H_{11}	Hops in phase-1 scenario-1
H_{12}	Hops in phase-2 scenario-1
H_{13}	Hops in phase-3 scenario-1
H_{14}	Hops in phase-4 scenario-1
H_{15}	Hops in phase-5 scenario-1
H_{t1}	Maximum number of hops in scenario-1
θ	sensing range in angular walk
H_{21}	Hops in phase-1 scenario-2
H_{22}	Hops in phase-2 scenario-2
H_{23}	Hops in phase-3 scenario-2
H_{24}	Hops in phase-4 scenario-2
H_{25}	Hops in phase-5 scenario-2
H_{t2}	Maximum number of hops in scenario-2

– *Max Delay in Phase-3*:

In this phase, packets move through a distance to reach a sensor that is at $R/4$ units as measured from the BS. The maximum distance traveled in this phase is $\frac{2R}{3} - \frac{R}{4}$ i.e., $\frac{5R}{12}$ units. Therefore, the number of hops in this phase is given by

$$H_{13} = \frac{5R}{12 * r_s \times p_r} \tag{4.4}$$

– *Max Delay in Phase-4*: The greatest distance covered at this phase is $90°$. Consequently, the number of hops in this phase is provided by

$$H_{14} = \frac{90°}{\theta} \tag{4.5}$$

– *Max Delay in Phase-5*: The distance traversed by the packets in this phase is $R/4$.units, therefore:

$$H_{15} = \frac{R}{4rs} \tag{4.6}$$

Summing up, we have:

$$H_{t_1} = \frac{\frac{2R}{3} - d'}{r_s P_r} + \frac{180°}{\theta} + \frac{2R}{3rs} + \frac{90°}{\theta} + \frac{R}{4rs} \tag{4.7}$$

4.2.3.1 Scenario 2

The maximum delay in all five stages of SLP-E is as follows if the distance between the source site and sink (measured in hops) is greater than the permitted threshold:

- *Max Delay in Phase-1*: Between $R/2$ and R is the backward random walk. Then $R - d^{'}$ units are offered for BRW. Hence, the maximum number of hops in BRW is given by

$$H_{21} = \frac{R - d^{'}}{r_s \times p_r} \tag{4.8}$$

- *Max Delay in Phase-2*:

  Phase-2's maximum distance travelled is $180°$, hence the number of hops in this phase is:

$$H_{22} = \frac{180°}{\theta} \tag{4.9}$$

- *Max Delay in Phase-3*: Here, four hops are the minimum, and $2R/3$ hops are the maximum. The distance traveled by packets in phase-2 is at most up to R, hence the maximum delay or hops in this phase is H_{23} =$2R/3rs$, in the inward direction from the network edge.
- *Max Delay in Phase-4*: The maximum length covered in this phase is $90°$

$$H_{24} = \frac{90°}{\theta} \tag{4.10}$$

- *Max Delay in Phase-5*: The maximum distance we have is R, the remaining path to be traversed by packets in SPR after *phase-4* is $R - \frac{2R}{3}$, therefore we have:

$$H_{25} = \frac{R}{3r_s} \quad (in\ hops) \tag{4.11}$$

  Total number of hops H_{t_2} is

$$H_{t_2} = \left(\frac{R - d^{'}}{r_s * P_r}\right) + \frac{180°}{\theta} + \frac{R}{3r_s} + \frac{90°}{\theta} + \frac{2R}{3r_s} \tag{4.12}$$

The notations used in mathematical models are described in Table. 4.1

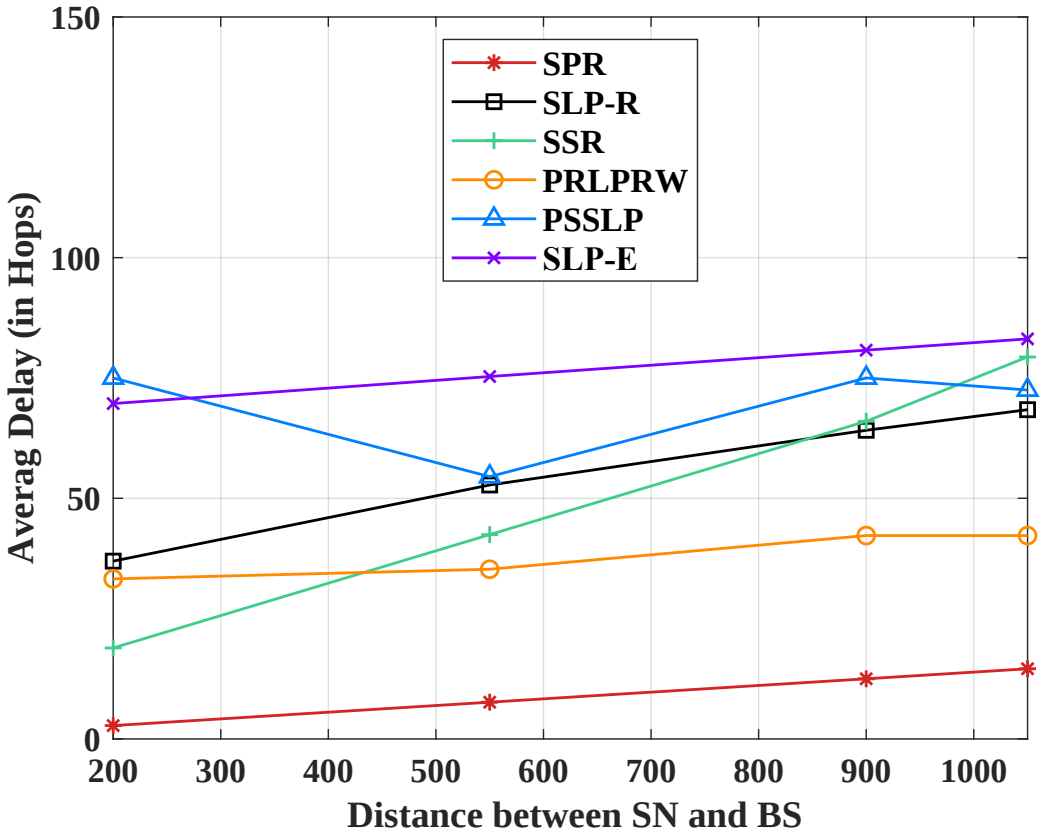

Figure 4.2: Maximum delay analytically (in hops)

4.3 Results and Discussion

To assess our technique's performance, we first contrasted it with Shortest Path Routing (SPR) and then with other approaches that are similar (i.e., SLP techniques based on random walks). Comparisons are made using SPR (no privacy strategy), SLP-R [101], SRR [23], PRLPRW [24], and PSSLP [60] schemes. The performance indicators used to assess the efficiency of the suggested technique were described in Sec. 3.4.

4.3.1 Simulation Scenario

The following simulation settings and parameters were taken into account. We deployed a total of 1460 sensor nodes, including the base station, that are uniformly distributed throughout the network. We took into account a circular deployment architecture with a network radius of 1050 units, as shown in Fig. 4.1. We also took into account the fact that the radio range for the base station, the adversary and the sensor nodes is the same and was set at 72 units. Each node in the network was loaded by 0.5joules as initial energy.

Based on the factor $r_s \times \sqrt{2}/2$, we took into account an offset distance of 50 units between two nodes and the total number of nodes considered in the network is 1460. The total number of annular rings considered are 21 and we divided a network into two groups (scenarios) where

one nodes' group are within a distance of $R/4$ in hops with reference to the BS, otherwise in the other group. Therefore $R/4$ was considered as the threshold value and it has been taken arbitrarily to grant special treatment to the sensor nodes in the close proximity to the Base Station (BS). Here, we took a single source node into consideration and changed its location within the network using BS as a point of comparison. We ran 100 trials and sent 1000 packets to the base station for each position of the source node.

Each trial's simulation came to an end when an adversary found the source node or when all packets were transmitted to the BS. The base station, which serves as the hub for all incoming network traffic, is where the attacker begins its backtracking procedure. Each sensor node in the network was initially charged with 0.5 joules of energy. In this example, we used the locations of the source nodes (200, 0), (550, 0), (900, 0), and (1050, 0). The performance metrics employed to gauge the effectiveness of our proposed technique are outlined in Chapter 1, Section 3.4. In the process of simulating and coding our work, we used Python programming, utilizing PyCharm as integrated development environment (IDE).

4.3.2 Result Analysis for SLP-E

In this section, we go over the performance measures in detail. The safety period metric charts are depicted in Fig. 4.3. We started with the shortest path routing (SPR) protocol, which lacks the SLP protocol. Comparing this protocol to the other SLP methods, it is obvious that it has the shortest safety time. In comparison to SLP-R, SRR, PSSLP, and SLP-E, PRLPRW performs badly. When compared to SLP-R, PRLPRW, SRR, and PSSLP, the proposed technique performs the best. SRR, PRLPRW, and SLP-R display distance-dependent behavior.

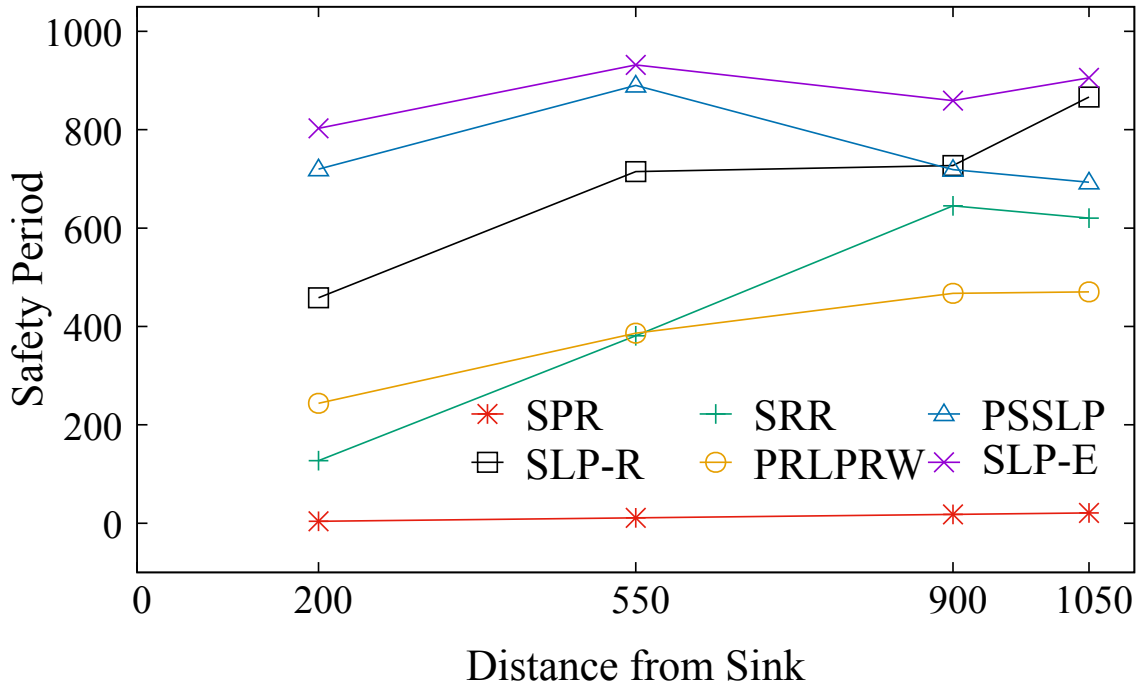

Figure 4.3: Safety Period

That is, the amount of safety period is minimal when the source is close to the sink. As the distance between the source and the sink grows, so does the safety period. When the source node is close to the BS, PSSLP operates pretty well. However, when the source node is close to the network boundary, the safety period shortens. Thus, present methods have non-uniform safety periods. No matter where the source is in the network, SLP-E has nearly the same level of privacy. This behavior of SLP-E is attributed to the fact that the proposed scheme adapts the routing protocol based on the position of the source in the network i.e., whether it is in scenario-1 or in scenario-2. Thus, the goal of attaining uniform location privacy is accomplished.

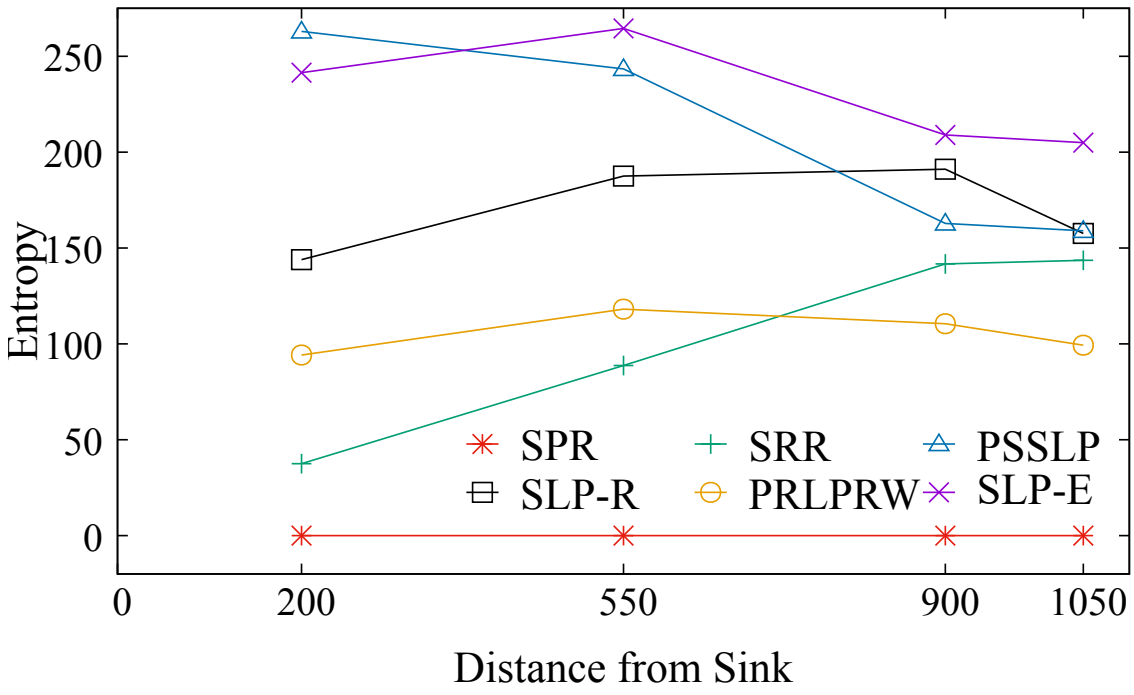

Figure 4.4: Entropy

The degree of randomization in the routing path is indicated by the entropy metric. The entropy increases with the degree of randomness in the routing paths that packets take. In comparison to the other five strategies, the suggested SLP-E has the best entropy, as shown in Fig. 4.4. When compared to other protocols, SRR has less entropy. All source position settings in the network exhibit this tendency. Because routing protocols do not take the location of the source in the network into account, PRLPRW, SLP-R, and SRR have low values of entropy. Compared to other protocols, PSSLP has the highest entropy, although its value is lower than that of the suggested approach (SLP-E). This is because PSSLP's final routing phase is not entirely randomized. As opposed to SLP-E, which completely randomizes all of the routing phases, the source's position in the network relative to the BS's position is taken into account when routing decisions are made. SPR has a defined routing path with no entropy because it doesn't offer any privacy mechanisms. In all five SLP protocols, we see a somewhat declining trend in entropy when the source is close to the network edge. Due to boundary effects and the network's geometry, this behavior is expected.

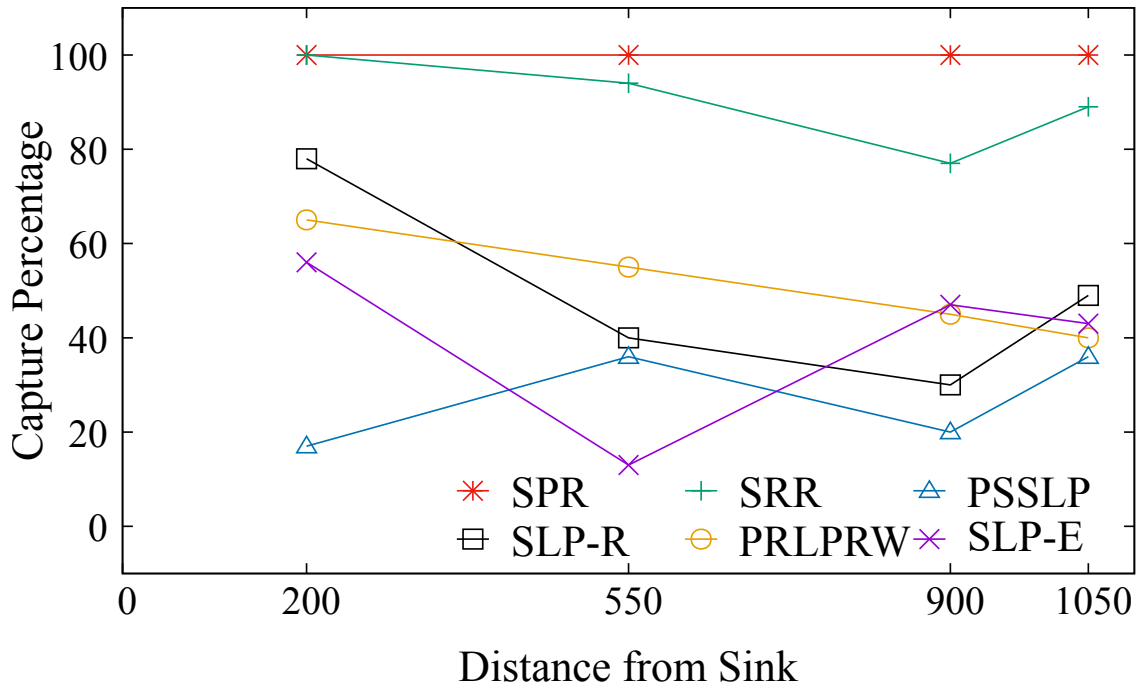

Figure 4.5: Capture Percentage

The adversary's success rate is indicated by the metric capture ratio. As a result, the performance of the protocols improves as the magnitude of this parameter decreases. As seen in Fig. 4.5, the suggested scheme's capture ratio is the lowest when compared to the SLP-R, SRR, and PRLPRW procedures. In contrast to PSSLP, SLP-E has a higher capture ratio. Increased NLT in SLP-E relative to PSSLP makes up for this loss. As the separation between the source and the sink grows, PRLPRW is essentially linear with a small decreasing tendency. As the separation between the source and the sink widens, the capture ratio metrics for SLP-R and SLP-E both show a decreasing trend, followed by an upward trend for the other positions of the source in the network.

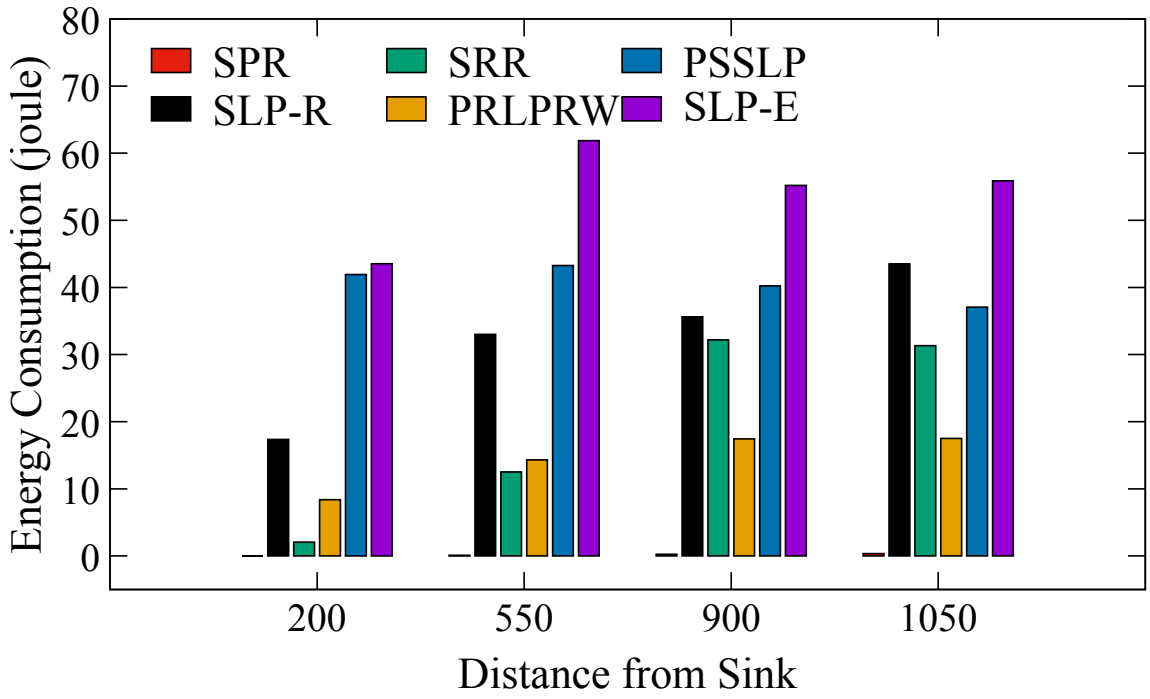

Figure 4.6: Energy Consumption

Fig. 4.6 displays the energy usage metric charts. Energy usage per packet per hop during packet transmitting and receiving was calculated using the energy models given in sec. 3.4. It demonstrates that, when compared to all other existing schemes, including those without SLP, the proposed design SLP-E consumes the most energy. However, it should be noted that SLP-E uses more energy because it can transmit more packets to the BS than any other method. In comparison to the suggested strategy, the simulation is over faster when the attacker reaches the source in the SLP-R, SRR, PRLPRW, and PSSLP schemes. This confirms that fewer packets were sent in SLP-R, SRR, PRLPRW, and PSSLP, which further suggests that less energy was used. We utilize a different statistic, called network lifetime (NLT) to assess the effectiveness of the proposed scheme's overall energy use. In terms of the network's lifespan, the NLT metric shows that SLP-E is more energy-efficient than SLP-R, PRLPRW, SRR, and PSSLP.

It is observed that in SLP-E, trade-offs exist between energy usage metrics and privacy level. By definition, the energy consumption is the amount of energy used by each network node when sending and receiving a packet. Given that SLP-E's primary goal is to provide an increased privacy in conjunction with the NLT; and given that SLP-E employs the random walk routing technique, it is imperative to offer a more randomized path for a packet to travel from the source node to the base station. In order to make routing path more random and diverse enough to enhance the privacy, the source node must send the significant number of the packets to the BS before adversary locate it and each packet should visit the significant number of nodes before reaching the BS. Enhancing the randomness and diversity of the routing path in SLP-E improves privacy but results in higher energy consumption when compared to alternative routing protocols that offer lower levels of privacy and randomization. Although, even with those other protocols, the energy usage is high in comparison to their degree of privacy. The

advantage of SLP-E is that, despite using the most energy, practically every network node participates in routing various packets to the base station (BS), which improves NLT. This is in contrast to the other approaches, which use the same sets of nodes to send packets repeatedly, leading to poor NLT.

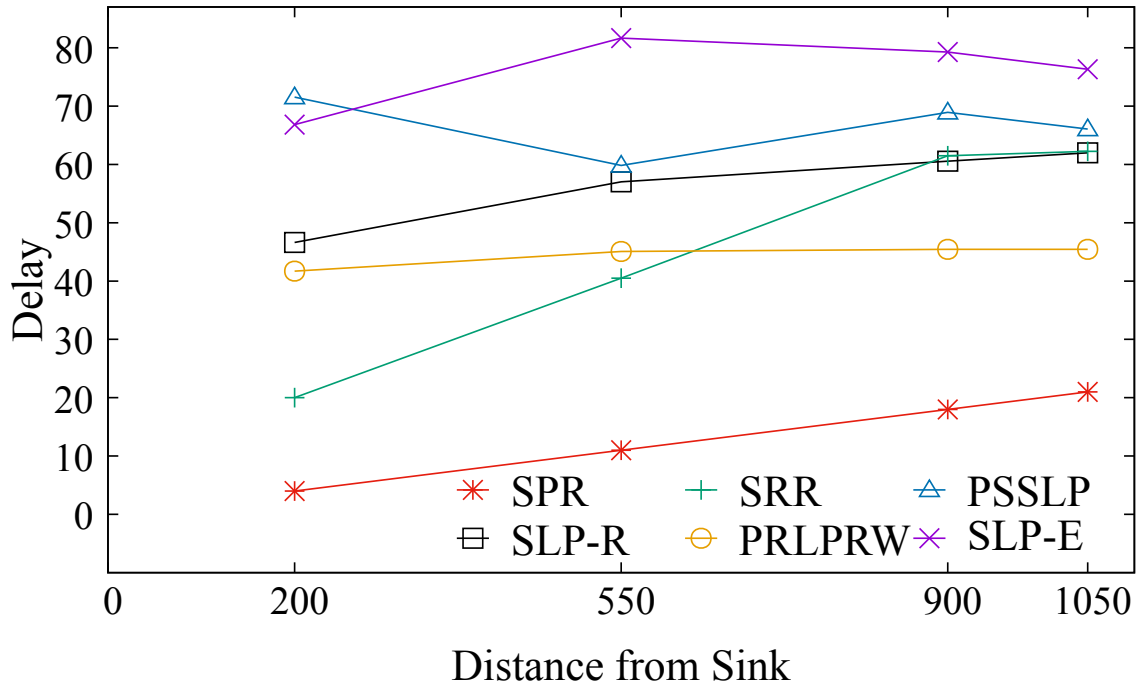

Figure 4.7: Delay

We talk about the average delay measure as it is represented graphically in Fig. 4.7. This indicator shows how long it typically takes for packets to arrive at the base station. This metric counts the number of hops a packet must traverse in order to reach the sink. A hop equals one delay unit. Plots of the delay metrics for five SLP procedures and one non-SLP technique are shown in Fig. 4.7. Compared to all other protocols, SLP-E has the highest delay since it uses longer pathways to improve anonymity. The SPR protocol is the least time-consuming because it offers no privacy protection. The maximum delay estimated using the analytical models and presented in Fig. 4.2 closely matches the trend of the average values of the delay metric present in Fig. 4.7, the simulation values. Hence, both the theoretical and experimental results are consistent with each other. As mentioned earlier, the trade-off observed between packet transmission latency and the level of privacy in SLP-E is because the SLP-E routing protocol sends the packets along a highly random and diverse path to reach their destination (the BS). This trade-off is a common characteristic in most SLP solutions based on random walks.

Table 4.2: Summary of Performance Characterization for SLP-E

Metrics vs. Protocol	Safety Period	Capture Ratio	Entropy	Energy Consumption	Delay	Network Lifetime
SLP-R	5024	-50	17001	17857	318	28
SRR	3185	-10	10287	10726	241	50
PRLPRW	2803	-48	10551	7892	228	-18
PSSLP	5479	-72	20701	22432	393	33
SLP-E	6379	-60	22996	29923	463	50

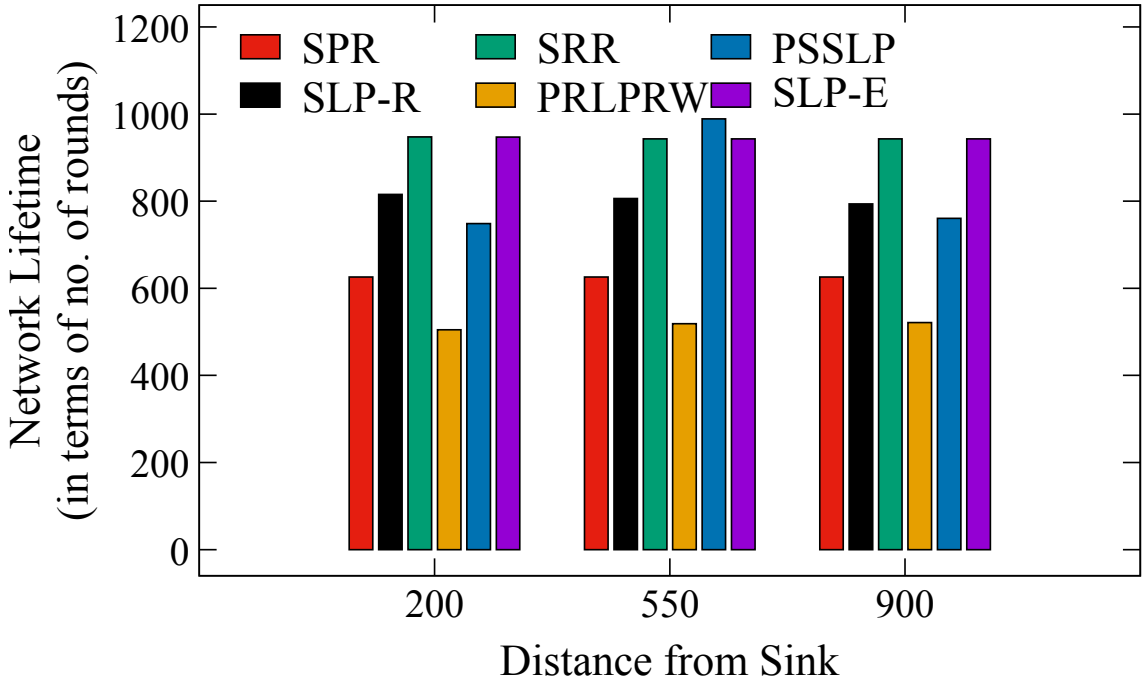

Figure 4.8: Network Lifetime

Next, we talk about how long the network will last if SLP protocols are used to safeguard the asset. In this scenario, a lot of packets are continuously delivered from the source to the BS until the first node in the network runs out of battery power and is deemed to be dead. The simulation comes to an end once a dead node is found. The number of packets transferred to the BS as a whole is then counted to get the network lifespan metric. Fig. 4.8 displays the charts for the network lifespan metric. It can be seen that the proposed scheme performs equally well along with SRR and PSSLP techniques. As discussed earlier, we have demonstrated that the NLT of the SLP-E performs better on an average. Accordingly, the suggested strategy continues to be the optimum for obtaining a consistent and improved safe period and NLT. This achievement in SLP-E, is a result of a well-designed routing protocol, which avoids repeatedly using the same set of nodes to deliver packets to the BS. In addition, each node takes into account the remaining energy of its neighboring nodes when selecting the next relay node in the forwarding process.

4.3.3 Discussions

A list of all metrics that have been averaged over all scenario settings can be found in this section. These average values are shown in Tab. 4.2. We used the SPR as our reference methodology to determine the percentage increase or decrease. The table shows an improvement in SLP performance. The SLP-E's safety period has grown by 6379 times, while SPR, SLP-R, SRR, PRLPRW, and PSSLP have improved by 5024, 3185, 2803, and 5479 folds, respectively. Both the NLT and entropy measurements exhibit comparable increases.

The NLT metric's negative value shows that PRLPRW performs worse than the SP (no SLP) scheme. We want to emphasize that the PRLPRW protocol was suggested and evaluated by the authors for multi-asset scenarios. However, in our research, we have only tested this technique for the situation of a single asset scenario. We stress that the metric capture ratio is negative because it reflects the degree of information loss from the viewpoint of the network administrator. The success rate of the attacker is lowered and the SLP protocol's privacy strength is increased with decreasing values of the capture ratio measure. SLP-E is found to have a lower capture ratio statistic than SLP-R, SRR, and PRLPRW schemes.

Higher energy usage and delay come at the expense of SLP-E's increased privacy strength and NLT. In other words, if privacy must be improved, energy usage per packet and delay must be given up. As a result, we discover that the suggested solution uses somewhat more energy and has a little longer delay than any competing schemes. Future efforts could focus on enhancing these components of the plan.

According to our research, the safety period and network lifespan measures have demonstrated enhanced performances and behavior that is independent of distance. Consequently, the goal of achieving balanced, uniform, and improved privacy and network lifetime measures has been attained. The results of our study suggest that the metrics entropy and capture ratio continue to behave in a distance-dependent manner. In other words, the values of these two measures vary depending on where the source is located within the network.

Based on these findings, we suggest that the future research can focus on developing a multi-objective optimization that takes care of sensors spacing, radio range etc., as optimization parameters to provide an optimal solution. It is strongly believed that q-learning-based approaches can be employed to provide optimal solutions. There are works in literature that have focused on q-learning-based solutions for routing purposes. However, to the best of our knowledge, there is no work that have explored reinforcement learning approach for providing SLP solutions. So, there is scope to explore this dimension too.

Another research direction that can be looked at is the optimal choice for the threshold concept that we used in this work. Although, threshold value of R/4 taken to decide scenario-1 and scenario-2 in the proposed solutions is arbitrary, we were motivated by the fact that nodes near the BS have to expend more energy compared to the nodes that are closer towards the network edge [58]. Investigating the ideal size and quantity of these network segments to use in order to improve privacy and Security may be another study area.

4.4 Conclusion

In this chapter, we suggested a novel privacy-preserved routing scheme that enhances privacy and network lifetime for WSNs. The performance of the suggested method showed an improvement in the safety period and network lifespan by 6379% and 50% respectively when compared with no privacy routing technique (SPR). When compared to the existing SLP solutions, SLP-E has shown improvement in the safety period by 26.5%, 97%, 123%, and 15.7 in SLP-R, SRR, PRLPRW, and PSSLP techniques respectively. Similar to this, NLT of SLP-E has shown improvement by 17%, 0.2%, 83% and 13% in SLP-R, SRR, PRLPRW and PSSLP techniques respectively. When we examined these data, It is evident that the suggested method performs better than the existing ones in both the safety period and network lifetime metrics. In addition, contrary to prior solutions where privacy strength is distance-dependent, the proposed technique demonstrated consistent privacy and network lifetime levels for any position of the source in the network. Therefore, the suggested approach achieves its main objectives of offering an improved safety period and NLT while maintaining uniform privacy levels. However, it is noted that the increased delays are required to obtain a safety period enhancement; this is considered as a limitation of this scheme. Even though these two metrics are trade-offs, future work could focus on improving SLP protection methods that take advantage of the optimization approach to reduce packet transmission latency and energy consumption which is seen in this contribution.

CHAPTER 5

Enhanced Privacy and Lifetime without Affecting Latency

In PSSLP and SLP-E, Privacy was enhanced at the expense of large latency. This can also be a challenge in monitoring the crucial asset. In this chapter, we proposed a new technique which mitigates the issue of high packet latency while improving the safety period and the Network Lifetime (NLT), namely a Strategic Random walk Source Location Privacy (SRWSLP).

The proposed technique routes the packets from the source node to the base station (BS) using three-phase routing namely: i) adaptive backward random walk (A-BRW), ii) adaptive equal depth routing (A-EDR), and forward random walk (FRW). In order to give an impression, to a backtracking attacker, that the routing pathways are dynamic, the A-BRW and A-EDR phases were designed to carefully route the packets away from the source node. The packets were converged to the base station by the forward random walk.

For reaching the goal of improving the safety period and NLT without experiencing heavy latency costs, the length (i.e., the number of hops) of the random walk in the A-BRW and A-EDR phases is dynamically controlled to optimize the delay metric. For every new packet that the source sends to the BS, the random walk length is varied. This attribute of the proposed scheme not only helps in achieving an improved safety period and network lifetime but also maintains the latency to a minimum. Particularly, in A-BRW and A-EDR phases, based on the distance between the source node and the network edge, the length of the random walk (we use the term *time-to-live* TTL for the random walk length in this chapter) is dynamically adjusted to have longer and shorter lengths. Specifically, the longer the distance between the source node and the network edge, the shorter the TTL value (i.e., random walk length), and vice versa. To accomplish this task, the region between the source and the network edge is divided into circular rings. These rings are in turn grouped into three sets namely, closer rings-set, middle rings-set, and farther rings-set. A random number is generated that acts as a TTL value that will be specified in the packet for relaying purposes. If this random number lies in the closer

rings-set, then the packet is initialized with that value as the TTL value and sent in a backward direction in a random walk fashion. Now, the intermediate node will generate another random number that is used in phase two (i.e., in the A-EDR phase) as the new TTL value. The length of the new random number is chosen based on the one that was used in the A-BRW phase. That is if the TTL value in A-BRW is large, then the new TTL value in the A-EDR phase will be small. This criteria of choosing the TTL values in both these phases helps in achieving a balance in the total number of hops that the packet has to travel in the A-BRW and A-EDR phases. Simulation results have demonstrated that the proposed technique performs better than the existing random walk class of SLP techniques.

5.1 Network and Attacker Models

5.1.1 Network Model

The network model of the proposed scheme is based on the Panda-Hunter game as suggested in [27]. This scheme considers a circular network deployment model where sensor nodes are randomly deployed in the network. The network has a single base station (BS) situated in the center of the network. We consider a static network model. As illustrated in Fig. 5.1, it is expected that the sensor nodes are arranged around the BS in the shape of circular rings. The number of circular rings in the network can be calculated using the formula R/r_s, where R is the network radius and r_s is the radio range of each sensor node.

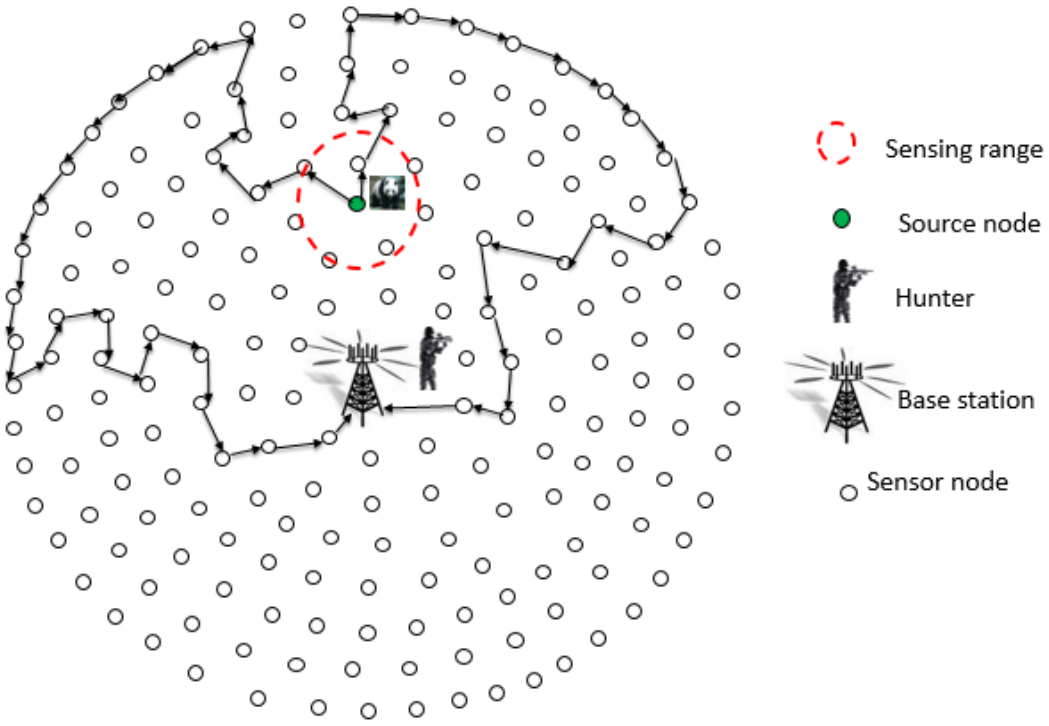

Figure 5.1: The illustration of the proposed scheme (SRWSLP)

Since the nodes form rings around the BS, the nearest ring is the one formed by the sensor nodes which are one hop away from the BS. The second ring is formed by the nodes which are two hops away from the BS, the deployment continues in this way up to the last ring. We further assume that the sensor nodes are homogeneous in nature i.e., all nodes in the network have the same computing, storage capabilities, and initial power. Additionally, each sensor node has a built-in battery that offers energy. Due to their constrained communication range, each sensor node can only communicate with its one-hop neighbor nodes. We further assume that an object (animal) is RFID-tagged and that every sensor node in a network is equipped with an RFID reader, enabling them to detect assets with an RFID transponder within their sensing range.

5.1.2 Attacker Model

The proposed scheme considers the local and passive attacker models. Under this model, the adversary undertakes no active attacks, such as node compromise, changing packet contents, etc. They simply listen to wireless communication channels. We assume that an adversary is a human (a hunter), not a robot and it is equipped with powerful devices capable of detecting and analyzing each received packet. Since the BS is where all packet traffic is sent, an attacker begins its tracking effort from there. For every incoming message in a new direction, the adversary makes a move in that direction with the help of its devices. Additionally, we assume that the sensor nodes' radius and the one of the attacker's devices are identical. It should be emphasized that the attacker never returns to a place he has already visited because doing so would only keep him wandering in the network and bring him no benefit. In this case, the attacker keeps tracing back the packets until it finds the source node.

5.2 The proposed Technique

We present the details of the proposed scheme in this section. The proposed scheme, namely SRWSLP comprises two phases namely, the network configuration phase and the protocol working phase. The network configuration phase is initiated by the BS to find the position of all deployed sensor nodes in the network and record their details, while the implementation of the proposed scheme takes place in the protocol working phase.

5.2.1 Network Configuration phase

The single BS in the network serves as the final destination for all the network packets to reach at. It is considered as the root node in the network with a depth value of zero; where *depth* is defined as the number of hops a sensor node is away from the BS's position. The BS broadcasts a *depth configuration message* into the network with *depth* field in the packet set to zero. The sensor nodes that are close to the BS (i.e, within its radio range) receive this message, update their routing table with the value that is present in the *depth configuration packet*, increment this

value in the packet by one and rebroadcast into the network. The neighbor nodes of each sensor that are in the BS's radio range, receive this rebroadcast packet, update their routing tables with the depth value that is in the packet, increment the value of the *depth* filed (*depth configuration packet*) by one and rebroadcast this updated packet into the network. This process repeats till the message reaches the network boundary. In this phase, any duplicate packets received by the sensor nodes are discarded. Once this process is completed, each sensor node in the network determines its distance (in terms of depth value) from the BS and categorizes its neighbors into three groups as follows: i) closer set neighbors, ii) equal set neighbors, and iii) farther set neighbors. The *closer set neighbors* are the ones whose depth value to the BS is lower than the node of interest, *equal set neighbors* are the ones whose depth value to the BS is equal to its own, and *farther set neighbors* are the ones whose depth value to the BS is higher than its own. These details are used in routing the message from the source node to the BS.

5.2.2 Protocol Working Phase

In this phase, we describe the working of the proposed SRWSLP technique.

- *Adaptive Backward Random Work (A-BRW) Phase:* The sensor node that detected the asset/event becomes the source node and starts sending the packets to BS. In this phase, the source node relays the packets in the backward direction (away from the BS position and towards the network edge) to a randomly chosen neighbor node that is in the forwarding list.

  The forwarding list in this phase consists of neighbors that are in farther neighbors set. Based on its position in the network w.r.t to the network edge, the source node determines its distance (expressed in terms of hops) to the network boundary. This source node's hop count indicates the ring number on which it is located with the network edge as a reference point and aids in determining the total number of rings available from the source node to the network edge. The source then groups those rings into three sets namely set-1, set-2, and set-3.

  Set-1 comprises those nodes that are on the rings which are closer to the source node, set-3 comprises nodes that are on the rings which are closer to the network boundary, including the network edge ring, and the rest of the nodes are grouped as set-2 nodes. To initiate the adaptive back random walk (A-BRW), the source node first randomly chooses one set of these three, and from that set, it then randomly picks one ring number.

  This ring number serves as a time-to-live (TTL) parameter. The source node initializes this value in the packet, specifies the set number that was used for TTL selection in the packet, and randomly relays it to its neighbor in the farther list. The neighbor in the farther list receives the packet, decrements the TTL value by one, and repeats the process of forwarding the packet to the next node. This process repeats until the TTL value in the packet is not zero. Once this value is zero, the packets are sent using the adaptive equal

depth routing (A-EDR) phase. The node at which the TTL value in the packet is zero is termed as *intermediate node* (IN). If the source node is closer to the network edge, say on the edge or one or two hops away from the network edge, then the packets are sent directly using the A-EDR phase.

- *Adaptive Equal Depth Routing (A-EDR) Phase:* In this phase, the intermediate node (IN) forwards the packets in either a clockwise or anticlockwise direction. This time, the forwarding list is formed by those neighbor nodes that have equal depth to the BS. The packet relaying process continues in this way for certain hops to reach a distant virtual source (VS).

  In this phase, the virtual source is chosen randomly between 45° and 180° expressed in hops (the angle value divided by γ to get the hop count value). The γ concept is shown in Fig. 3.1 and it is calculated using the cosine angle rule. The intermediate node now groups these angles into three sets namely, set-1: nodes lying within the angle 45° and 90°, set-2: nodes lying within the angle $> 90^{\circ}$ and 135°, and set-2: nodes lying within the angle $> 135^{\circ}$ and 180°.

  Now, the intermediate node first determines the set that was chosen by the source node in the A-BRW phase. If the source node had chosen a set that led to larger hops in the A-BRW phase, then the intermediate node chooses a set that has the least hops in the A-EDR phase. Once the set is determined, it then randomly chooses an angle (expressed in hops) and from that angle, it forms the TTL value for this phase and relays the packet to its one-hop neighbor that is in its forwarding list (equal neighbor set). The relaying process continues till the node whose angle (measured in hops) is specified in the packet is reached.

  For instance, if set-3 is chosen in the A-BRW phase, then set-1 is chosen in the A-EDR phase. At this point, the A-EDR phase ends. The node at which the A-EDR phase terminates is termed the virtual source. Now the packets are sent to the BS using phase-3. The main goal of the proposed technique is to enhance the safety period and network lifetime by maintaining a delay that is comparable to the delay in the existing techniques. To achieve this goal, an interplay (trade-off) between the number of hops in the A-BRW phase and the A-EDR phase is necessary. Specifically, if the TTL value in the A-BRW phase is more than the TTL value in the A-EDR phase must be less. That is, if set-3 is chosen in the A-BRW phase, then set-1 must be chosen A-EDR phase and vice versa. This balance helps in achieving the delay that is optimal and whose value is expected to be the same as the values of the delay seen in the existing techniques. Hence the word *adaptive* is given to these two phases. This is the novelty of the proposed scheme.

- *Forward Random Work (FRW) Phase*: In this phase, the packets are sent to the BS from the virtual source (VS) using the forward random work (FRW). In this phase, the forwarding list is made up of those nodes that are in the closer neighbors set. The Virtual source

randomly picks a neighbor from this close list and relays the packet to that neighbor node. This process continues till the packet reaches the BS. The details of the operation phase are given in 3

Algorithm 3: SRWSLP

if *(AssetDetected)* **then**
- $rings \leftarrow getTotalRings()$;
- $R \leftarrow getSnRing()$;
- // Backward Random Walk
- //Get the number of rings from the source ring to the edge ring
- $I \leftarrow rings - R$;
- $h_1 \leftarrow rand(2,\ I)$;
- //Consider only further set neighbors
- $isEqualSet \leftarrow False$;
- **for** *i =1:1:*h_1 **do**
  - // Choose the relay node
  - $RelayNode \leftarrow chooseBackwardListNode(isEqualSet)$;
  - $SendPacket(RelayNode)$;
  - $CurrentNode \leftarrow RelayNode$;
- //Clockwise and Anti-Clockwise Walk
- //Choose the number of hops to travel in the current node ring based on the previous backward hops
- $set \leftarrow getSet(h_1)$;
- **if** $set == 1$ **then**
  - $h_2 \leftarrow getHops(135, 180, CurrentNode)$;
- **else if** $set == 2$ **then**
  - $h_2 \leftarrow getHops(90, 135, CurrentNode)$;
- **else**
  - $h_2 \leftarrow getHops(45, 90, CurrentNode)$;
- $isClockwise \leftarrow rand(0, 1)$;
- **for** *i =1:1:*h_2 **do**
  - // Choose the relay node
  - $RelayNode \leftarrow chooseNeighborNode(isClockwise)$;
  - $SendPacket(RelayNode)$;
  - $CurrentNode \leftarrow RelayNode$;
- //Forward Random Walk
- **while** *CurrentNode* $\neq$*BaseStation* **do**
  - $RelayNode \leftarrow chooseForwardListNode(isEqualSet)$;
  - $SendPacket(RelayNode)$;
  - $CurrentNode \leftarrow RelayNode$;

5.3 Results and Discussions

We present the simulation settings in this section. In this article, we compare the proposed technique with Shortest path routing (SPR) i.e., no privacy routing protocol, and other similar random work-based SLP schemes namely SLP-R, SSR, and PRLPRW proposed in [101], [23]

and [24] receptively. These solutions were chosen as they all share the similar goal of extending the safety period while not degrading NLT.

5.3.1 Simulation settings

The simulation setup and parameters are as follows: We uniformly deployed 1462 sensor nodes including the base station (BS). We considered a circular deployment model with the BS in the center of the network as shown in Fig. 5.1. We further considered the network radius of 1050 units and 21 total rings. We assumed that the sensing range of the deployed sensor nodes, base station, and adversary devices is the same and it was set to 71 units. The offset distance between two nodes was set to 50 units and is given by $r_s \times \sqrt{2}/2$. We considered a single source node and we changed its position in the network to check the performance of our scheme at different positions of the source node in the network. We sent 1000 packets to the base station in each trial and the simulation stops when an adversary located the source node or when all 1000 packets were sent to the BS. For each position of the source node in the network, we carried out 100 trials. Since the destination of all packets from the sensor nodes in the network is to the BS, we assumed that an adversary started its backtracking process from the BS. We set the positions of the source node in the network as follows. (200,0), (550,0) and (900,0) and each sensor node was loaded with 0.5 joules of energy before the network started to operate. The assessment criteria used to measure the efficiency of our suggested approach are detailed in Chapter 1, Section 3.4. Throughout the simulation and coding phases of our work, we leveraged Python programming and employed PyCharm as an integrated development environment (IDE).

5.3.2 Results Analysis

In this section, we describe the results obtained through simulations. The performance metrics used to measure the performance of the proposed protocol (SRWSLP) are defined in 3.4.

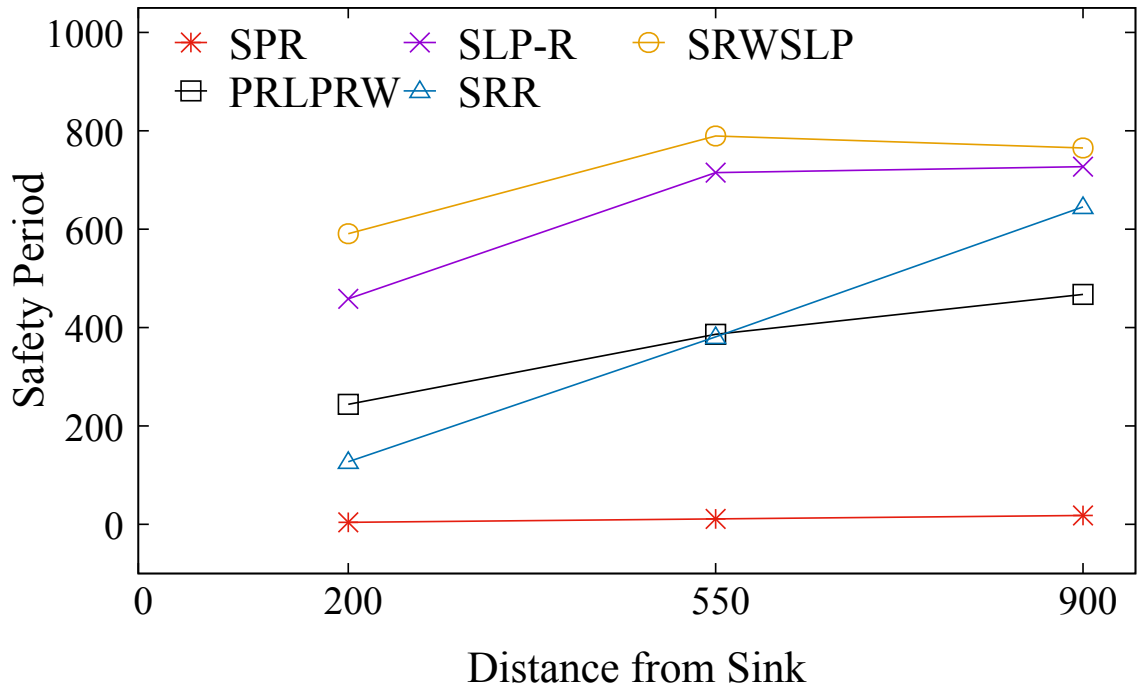

Figure 5.2: Safety Period

The safety period metric is plotted in Fig. 5.2. We compared our scheme with the shortest path routing (SRP) which is no SLP and the other three existing solutions namely SLP-R, PLRPRW, and SRR. It was seen that our scheme performs well in terms of safety period compared to these existing schemes. It is understandable that SPR performs poorly as compared to other schemes since it is no SLP. PRLPRW and SRR perform poorly when compared to SLP-R and SRWSLP. It is further seen that SLP-R performs poorly when compared to the SRWSLP technique, this is due to the fact that in the SRWSLP technique, a packet is sent to the BS strategically which is making the routing path very random, hence the adversary becomes more confused. Table 5.1 shows improvement in each of the SLP schemes when compared with the no SLP scheme.

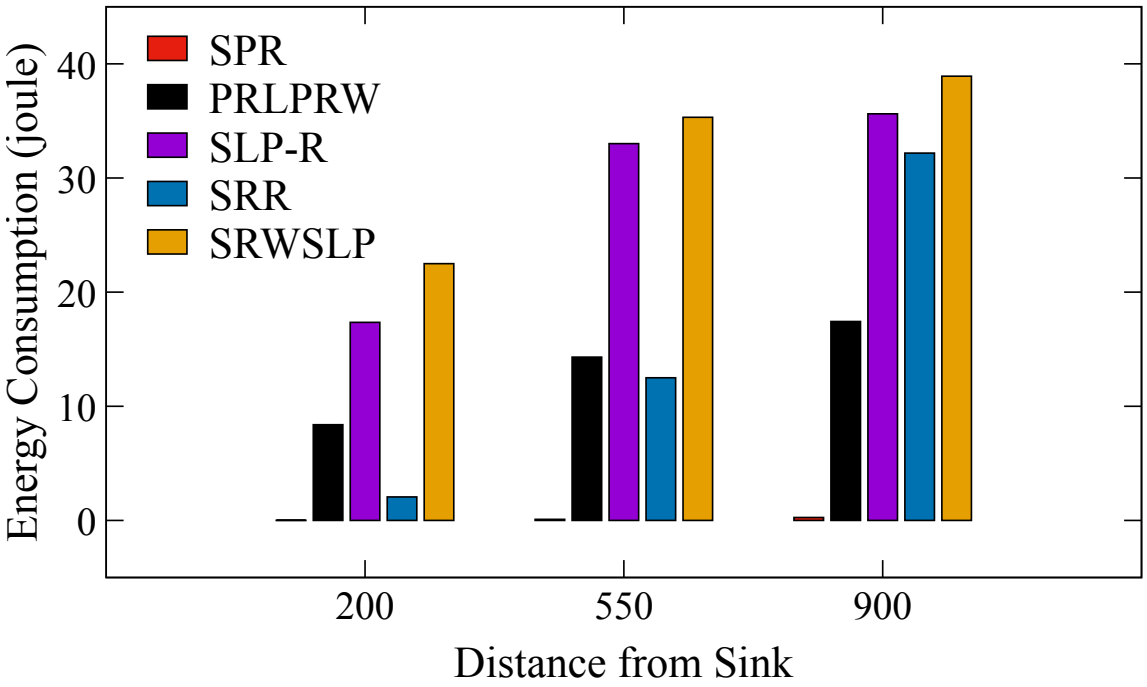

Figure 5.3: Energy Consumption

The energy consumption plot is shown in Fig. 5.3. This metric is defined as the energy consumed during the transmission and reception of packets by each node in the network. It is noticed that the SRWSLP consumes higher energy compared to other protocols. This can be justified since the routing path is very random and diverse than the ones of other protocols.

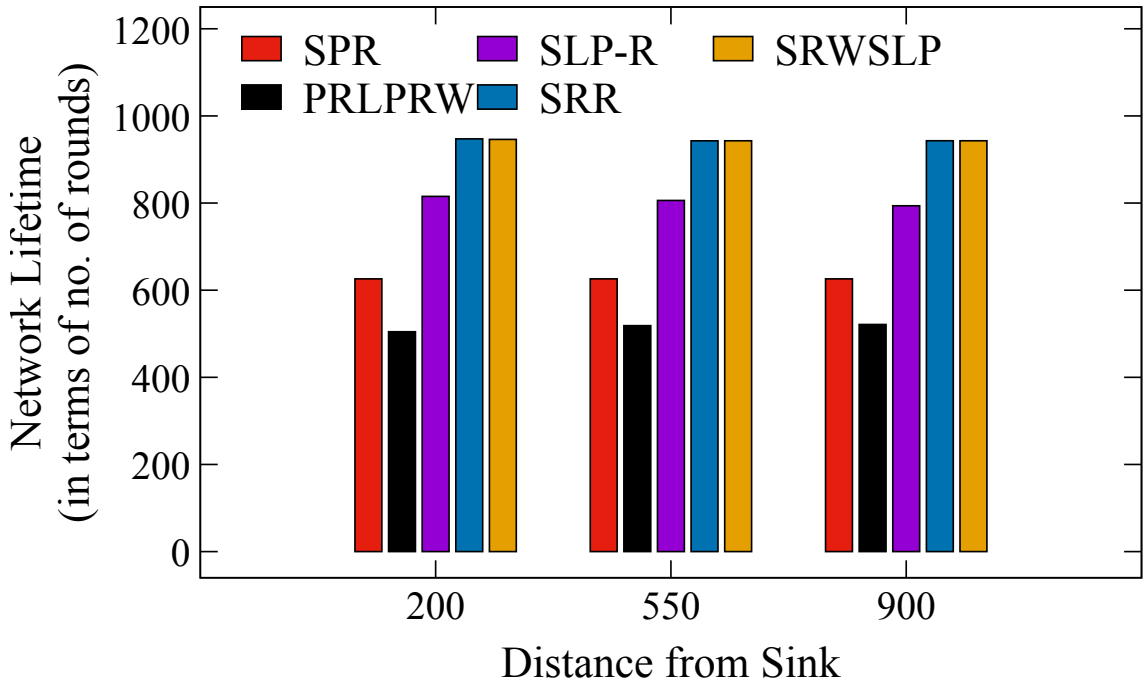

Figure 5.4: Network lifetime

We display the network lifetime (NLT) plot in Fig. 5.4. It was observed that the proposed

Table 5.1: Summary of Performance Characterization for SRWSLP

Metrics vs. Protocol	Safety Period	Energy Consumption	Transmission Delay	Network Lifetime
SLP-R	622.49	28.53	42.72	179
PRLPRW	354.88	13.25	33	-111
SRR	373.5	15.45	32.72	318
SRWSLP	704.11	32.12	42.7	318

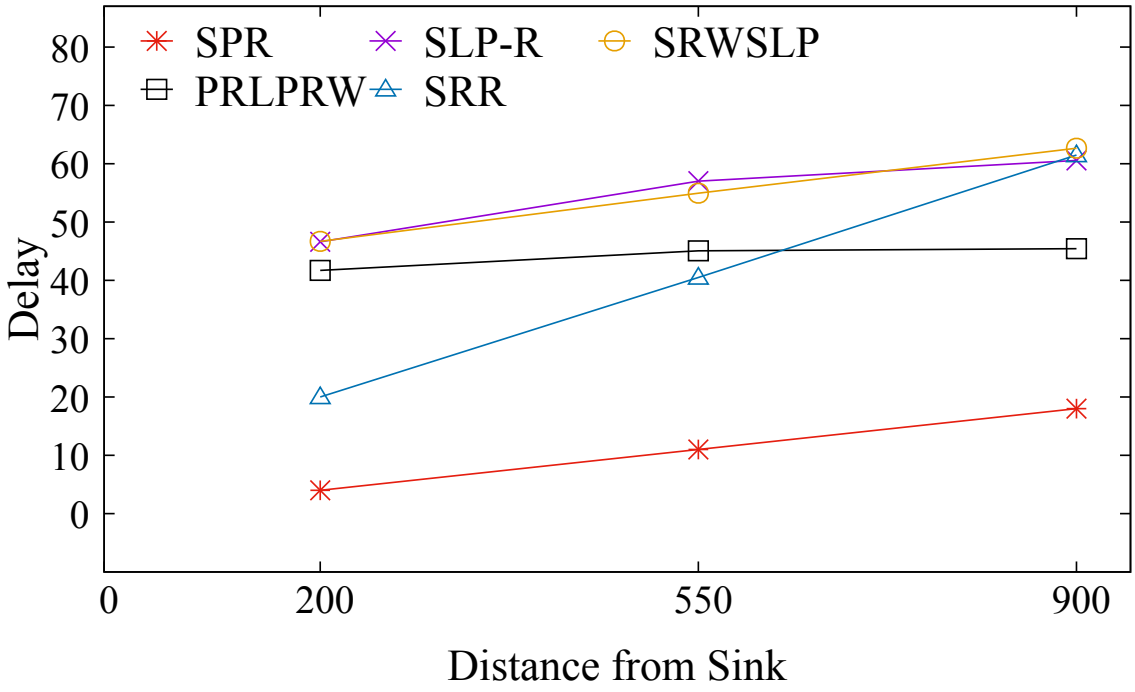

Figure 5.5: Transmission delay

scheme has better NLT along with SRR. The other protocols have lower NLT. This is due to the fact that the packets are delivered to the BS without taking into account the remaining energy at nodes and either the routing path is not more random or fixed which leads to frequent use of the same set of pathways to the BS. As the same node in the path keeps receiving and sending the packets to the BS, those nodes lose their battery in a short period of time. Since the routing path in the proposed scheme is very random, the issue of using the same node is resolved, hence achieving prolonged NLT.

We depict the packet transmission latency metric in Fig. 5.5. This metric shows the average number of hops the packets may visit from the source node to the BS. The delay increases as more nodes are visited during random walk phases. It is seen that the proposed technique (SRWSLP) and SLP-R have similar transmission delays. While SRWSLP and SLP-R techniques have the highest delay compared to SRR and PRLPRW techniques. This is due to the fact that SRR and PRLPRW have weaker privacy (safe time) and they are not totally randomized in packet transmission. Hence, we claim that achieving improved privacy and NLT without affecting latency stays valid.

5.4 Conclusion

In this chapter, we suggested a novel SRWSLP technique that maintains the same delay as the ones in the existing schemes while also achieving improved privacy and NLT. The adaptive phases were used to balance the hops the packets take to reach the BS in each round and contribute to achieving improvement in both the safety period and NLT without affecting latency, in contrast to the earlier systems where privacy strength was obtained at the high expense of additional delays. In comparison to no SLP technique, the proposed method improves the safety period by 707.11 folds and NLT by 31.8 folds.

CHAPTER 6

Impact of Radio Range on Privacy and Network Lifetime

Sensor nodes must be within each other's sensing range in order to communicate, in a Wireless Sensor Network (WSN) that relies on multihop communication. Hence, their deployment needs to be done carefully to make this possible. The sensor node radio range is a critical parameter ti take care of. Selecting the appropriate radio range in a multi-hop communication WSN involves balancing coverage, connectivity, energy efficiency, interference management, security, and other application-specific requirements [103]. Careful design and optimization of the network's physical and data link layer parameters are essential to ensure the WSN operates effectively and efficiently [104].

As it was mentioned in the previous chapters, it is crucial to make sure that the established SLP schemes should put an emphasis on improving asset's level of privacy and lengthening the lifetime of the network. Additionally, we explored many factors that could impact network longevity and privacy in the existing solutions. However, it is pointed out that there has been no investigation conducted to assess the potential influence of the radio range of the deployed sensor nodes on both privacy levels and the longevity of the network lifetime. For achieving prolonged network lifetime of the WSNs, only a study was made in [105] to see the impact of sensors' radio range on the network lifetime. However, this work was not aimed at SLP. Therefore, this motivated us to answer the long awaited question i.e., '*Is there any impact of sensors' radio range on safety period and NLT?'*.

The aim of this chapter is to examine how the radio range of sensors affects two critical performance metrics, namely, privacy strength and network lifetime, which are of utmost significance in safeguarding Source Location Privacy in Wireless Sensor Networks (WSNs). It is noteworthy that there is a notable absence of prior research in the literature addressing this aspect. Additionally, we explored the potential influence of sensor radio range on various other

metrics including capture percentage, entropy, energy consumption, and latency. The simulation results unequivocally reveal that the radio range of sensors has a discernible impact on crucial metrics such as the safety period, capture ratio, and the overall Network Lifetime (NLT).

6.1 Application Scenario

For checking the impact of sensor's radio range on different performance metrics as mentioned above, we used the SLP protocol we developed and discussed in the third chapter (SLP-E).

6.2 Results and discussions

To understand the behavior of the proposed protocol in chapter three (SLP-E), under different radio range settings, we experimented and collected additional results. In particular, the simulation settings for this scenario remained the same as stated in SLP-E but this time the sensors' radio range was varied in step size of five starting from 72 units. That is, we tested the proposed protocol with the following radio ranges: 72, 77, 82, 87, 92, and 97. The objective of this scenario was to answer our long-awaited query "will a radio range have any influence on source privacy strength?" and we tried to answer it here. For this scenario, we have taken the average of all the values for different distances between the source and the BS and summarized these results as shown in Fig.6.1-Fig. 6.6.

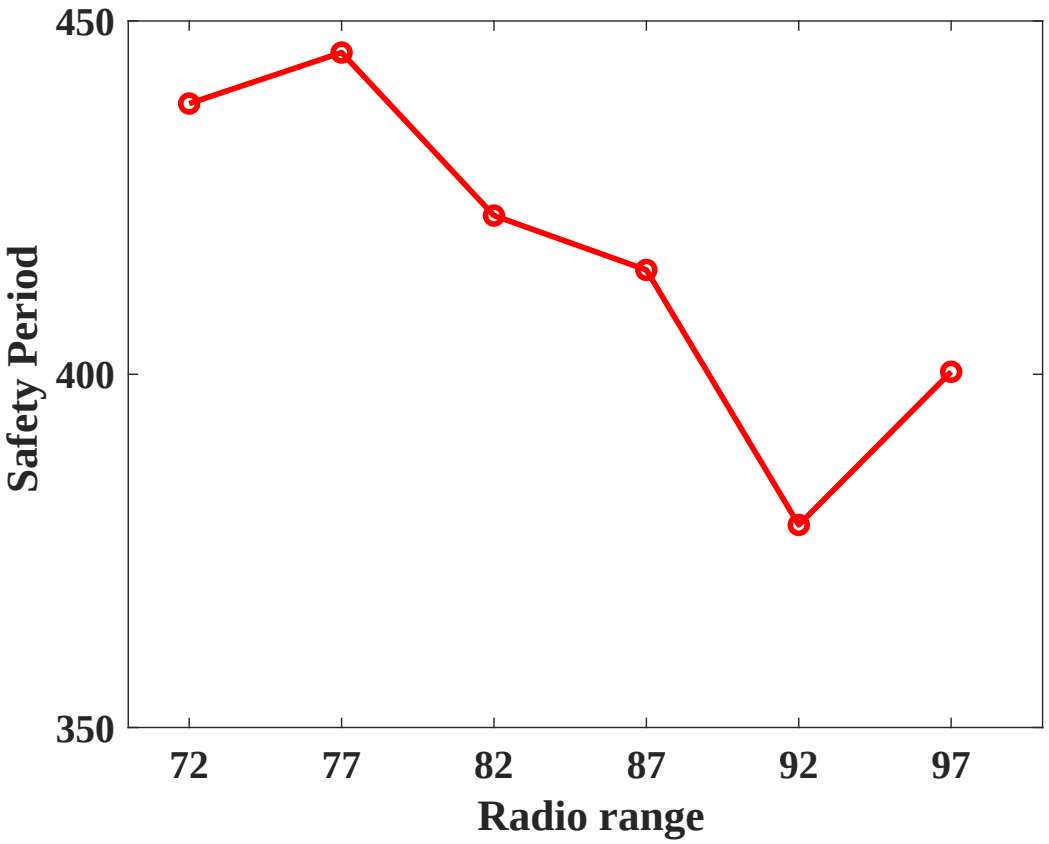

Figure 6.1: Safety Period

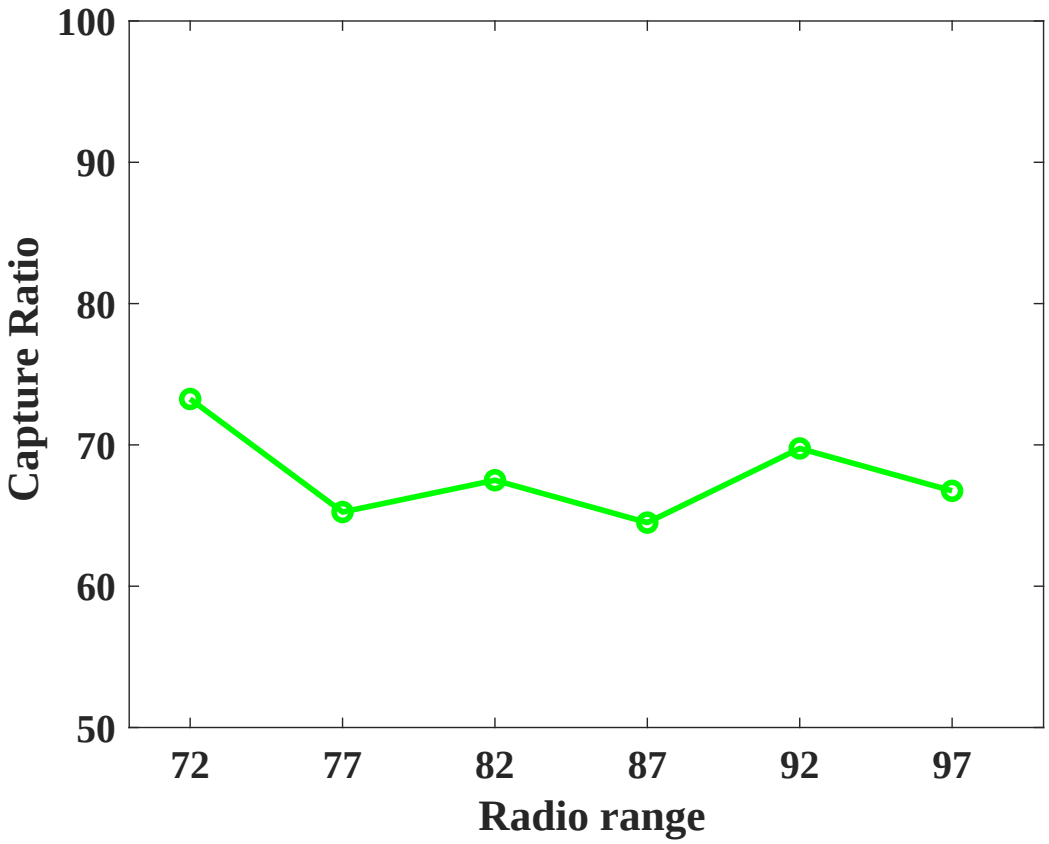

Figure 6.2: Capture Ratio

The plot for safety period vs different values of radio range is shown in Fig. 6.1. It is seen that as the radio range increases, there is a decreasing trend in safety period for radio range values up to 92 units, except for when the radio range is 77 units. After that again the safety period sees an increasing trend. The safety period is highest when the radio range is 77 units.

The capture ratio metric vs radio range plot is seen in Fig. 6.2. This metric has alternating increase and decrease in the values as the radio range increases. The capture ratio is the least when the radio range is 77 and 87. Fig. 6.1 and Fig. 6.2 indicate that radio range value of 77 units gives better results in terms of safety period and capture ratio.

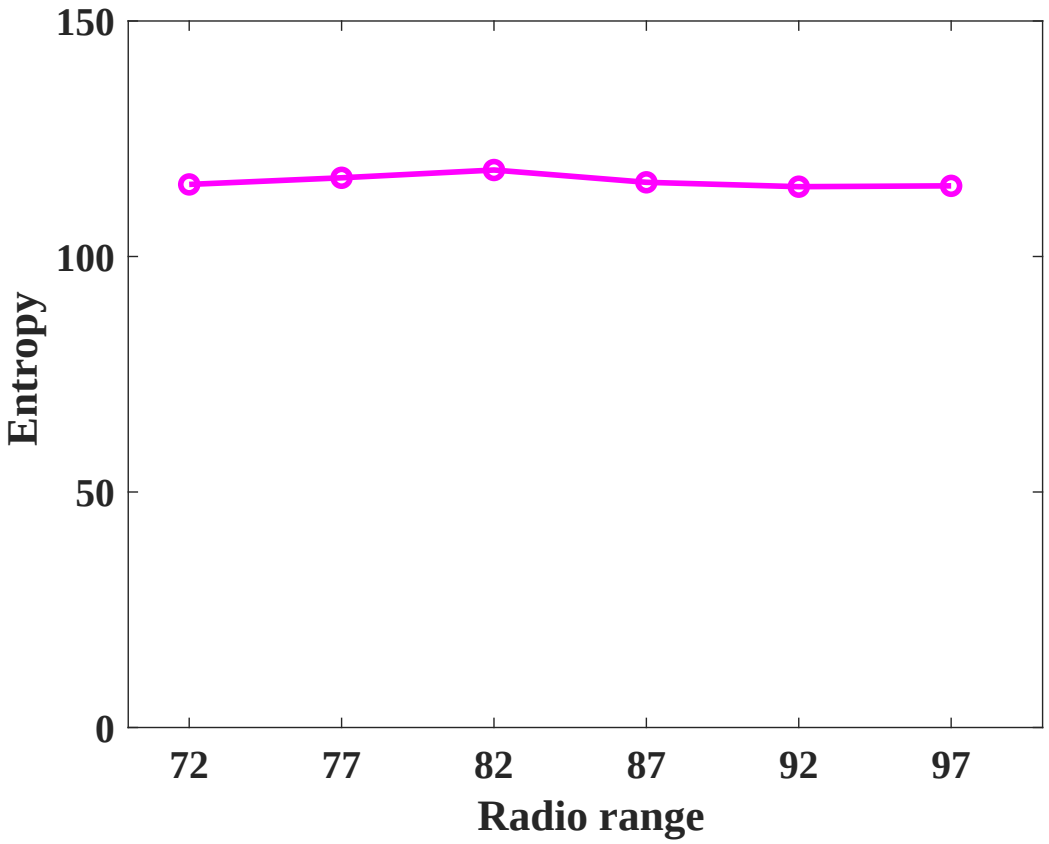

Figure 6.3: Entropy

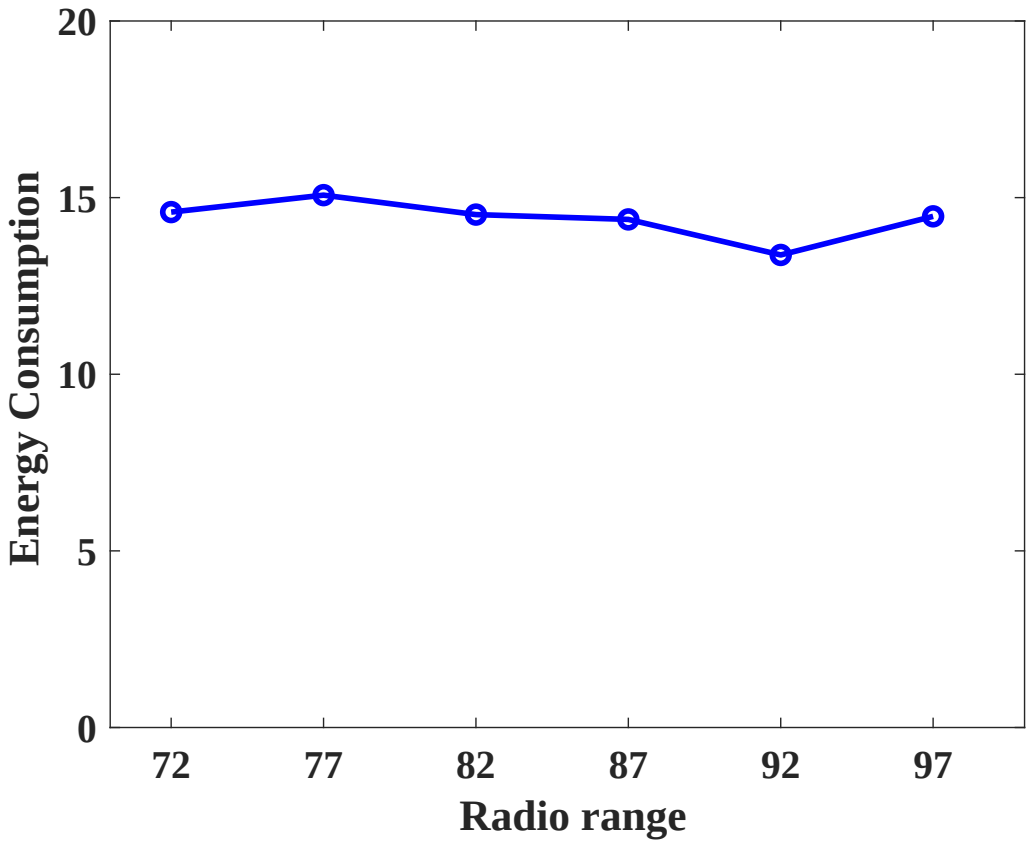

Figure 6.4: Energy Consumption

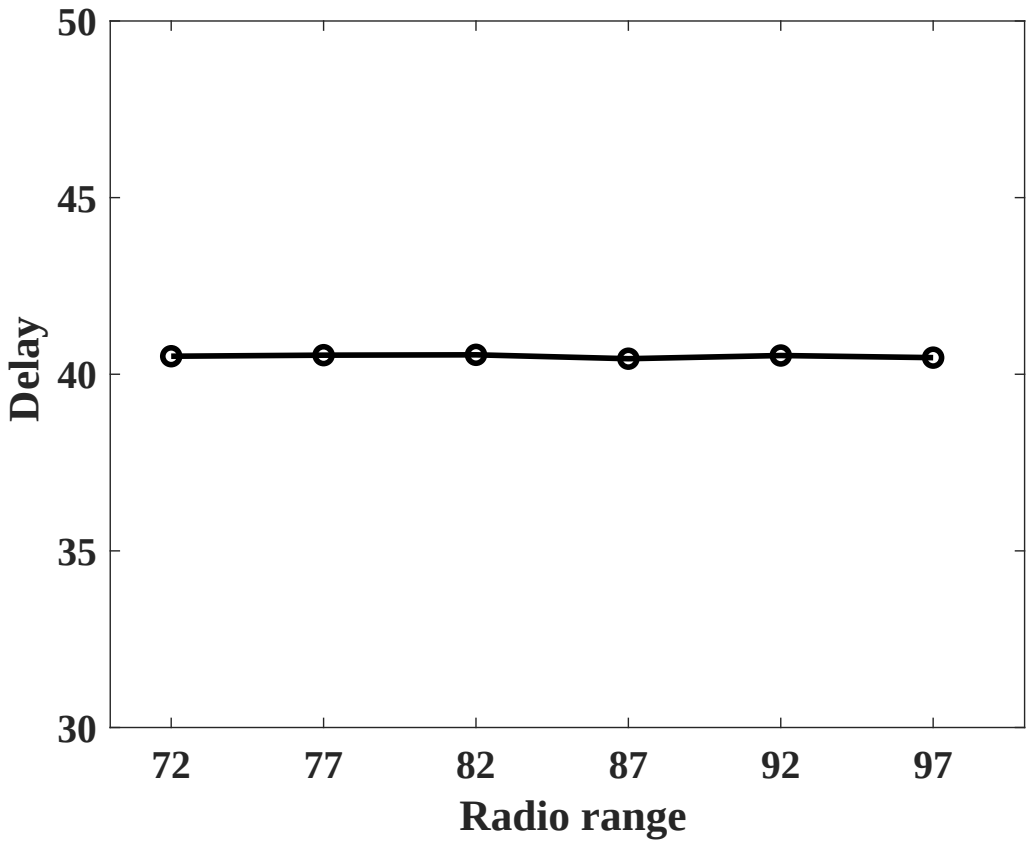

Figure 6.5: Delay

Fig. 6.3, Fig. 6.4 and Fig. 6.5 show the plots for entropy, energy consumption and delay metrics. It is seen that these three metrics almost have same magnitudes for all the settings of the radio range, with minor deviations in energy consumption. It can be concluded that these three metrics are not much influenced by the radio range of the sensor nodes.

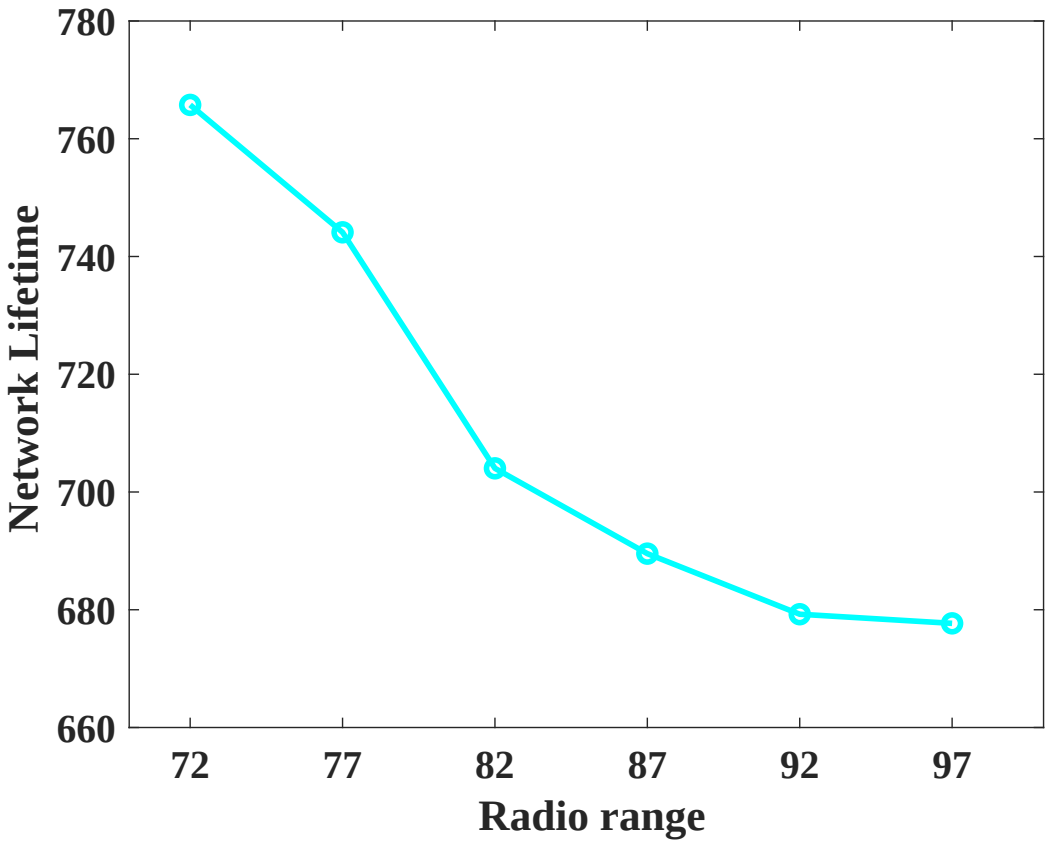

Figure 6.6: Network Lifetime

The plot in Fig. 6.6 is for the network lifetime metric. It is evident that the network lifetime metric is largely influenced by the radio range of the sensor node. The inference is that for the given spacing arrangement of the nodes in the network, smaller radio range has better network lifetime.

Overall, it is concluded that the radio range of 77 units is doing good in terms of safety period and 72 radio range units is good for capture ratio, and network lifetime. It is observed that when the sensor nodes' radio range increases, the safety period and the network life time decrease. Future studies could investigate the cause of this behavior and find the optimal value of better radio range.

6.3 Conclusion

In this chapter, we thoroughly assessed the impact of sensor radio range on vital performance metrics essential for evaluating the efficacy of Source Location Privacy Preservation schemes. These metrics encompass the safety period, capture ratio, entropy, energy consumption, and network lifetime. Our findings unequivocally demonstrate that the sensors' radio range significantly influences the safety period, capture ratio, and network lifetime metrics. As a result, it is imperative to carefully consider the sensing range of deployed sensor nodes, based on specific circumstances and applications in which wireless sensor nodes will be deployed.

CHAPTER 7

Conclusions and Future Directions

7.1 Conclusions

This thesis tackles the prevalent issues observed within current SLP solutions, specifically focusing on the enhancement of contextual information.

WSN technology has enormous advantages for both people and businesses, but it also offers grave security and privacy risks because it exposes contextual data while gathering the data. Secured data collection issues have been addressed by the different researchers. However, addressing the privacy issues that arise due to the nature of these networks is more challenging than securing the data they transmit. Contextual privacy issues are due to the analysis of the data associated with the measurements and transmissions of the data collected by the nodes. Therefore, contextual information privacy becomes a critical service for wireless sensor networks. The location of the event's source in WSNs is one such contextual information that we aim to protect. We consider the case of habitat monitoring and our proposed schemes aimed at protecting the location privacy of animals in their natural habitat. By observing the data flow in the network, the attacker can locate the nodes that are reporting information to the base station.

One of the methods used to confuse the traffic pattern in WSNs is to employ fake traffic. However, we do not recommend such methods for resource-constrained WSNs. Instead, we focused on methods like random-walk-based solutions that do not use false traffic or fake sources. In the literature, a number of random-walk-based SLP approaches were proposed in view of this motivating factor. However, certain limitations related to them were discovered.

The first noticed weakness in the existing solutions is the exhibition of distance-dependent behavior of the privacy-protection strength. This motivated us to develop a new SLP preservation technique (PSSLP) that mitigates the problem of position-dependent based privacy behavior of the solutions that are seen in existing works.

The second noticeable weakness is that the existing phantom walk-based solutions on SLP

have focused only on enhancing privacy i.e., the safety period or enhancing privacy without hampering the network lifetime (NLT). However, enhancing both privacy and network lifetime together in single solutions does not has given less attention in the literature. This motivated us to develop a new SLP solution named SLP-E, which enhances both privacy and NLT at the same time. The proposed SLP-E is also offering a constant level of privacy protection regardless of where the source is located within the network.

Thirdly, we tackle a common concern observed in existing random walk-based methods, where attempts to enhance both privacy and network lifetime often result in significant latency. To address this issue, we introduce a solution called SRWSLP, which offers improved Source Location Privacy (SLP) and Network Lifetime (NLT) without imposing excessive delays.

Lastly, we respond to a long-awaited question that has remained unanswered in the current body of literature: Does the radio range of sensors have any influence on the safety period and Network Lifetime (NLT)? Our investigation unequivocally reveals that the radio range does indeed impact these crucial metrics.

The simulation results revealed that our proposed techniques outperform the existing solutions. The proposed schemes could be seamlessly used in applications such as habitat monitoring, monitoring the physiological status of soldiers on the battlefield, etc.

7.2 Future research directions

In this thesis, we have presented a set of improved SLPs for WSNs, to protect the privacy of contextual and content information respectively. These techniques provide privacy from external, eavesdropping, and passive type of attackers (s) only. we have presented a set of improved SLP for IoT-equipped WSNs, to protect the privacy of contextual information. And these techniques provide privacy from external, eavesdropping, and passive type of attacker(s) only.

We have assumed that the network is free of malicious and compromised nodes and that the attacker will not perform any active attacks such as packet content modification, denial of service (DOS), route modification, and packet drop attacks. However, the attacker may also employ active attacks to disrupt the mission of privacy preservation solutions.

For instance, a compromised node may modify the hop count value in the packet to a smaller value so that the random walk terminates near the source node itself. Due to this effect, the packets will almost follow the shortest path routing instead of larger and wider paths toward the base station. As a result, the attacker's trace-back time reduces and thus reduces the safety period. Similar reasoning could be said of misbehaving nodes. The misbehaving nodes might intentionally choose those neighbors, for relaying the packets, which are closer to the base station. This will result in a random walk that has bias towards the BS and shorten the safety as well as backtracking period. As a result, we also need to address the SLP concerns in context of active attacks.

The research conducted for this thesis also assumed that the channels are error-free and free of losses from things like noise, multipath scattering, fading, etc. In the same way, we presumed that the upper layers (application layer) handle content privacy based on cryptographic primitives. To provide better privacy solutions, one possible future research area is to mitigate the fading effects and incorporate physical layer security in WSN while creating novel SLP solutions.

Another assumption we have made in the thesis is that the nodes are static in nature, but mobile nodes exist too. Therefore, we feel that prospectus researchers need to give attention to the SLP solutions for the case of the mobile nodes' scenario too.

Future studies may concentrate on exploring deeper into and managing the trade-offs among energy consumption, packet delay, and privacy (safety period) metrics, which are common to the majority of current random walk-based SLP solutions.

In the end, this thesis demonstrated that the metrics, capture ratio, network lifetime, and privacy level are impacted by the radio range of sensor nodes. Nevertheless, no studies that focused on SLP have looked into the appropriate radio range size to be used. Future research could therefore look at the reason behind this effect as well as which radio range size is most appropriate for SLP solutions in WSNs.

Bibliography

[1] M. Becker, "Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy," *Ethics and Information Technology*, vol. 21, no. 4, pp. 307–317, 2019.

[2] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2012, pp. 626–633.

[3] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in iot," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, p. 100158, 2023.

[4] M. H. Shirvani and M. Masdari, "A survey study on trust-based security in internet of things: Challenges and issues," *Internet of Things*, p. 100640, 2022.

[5] J. A. Manrique, J. S. Rueda-Rueda, and J. M. Portocarrero, "Contrasting internet of things and wireless sensor network from a conceptual overview," in *2016 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 252–257.

[6] Y. Zhu, J. Song, and F. Dong, "Applications of wireless sensor network in the agriculture environment monitoring," *Procedia Engineering*, vol. 16, pp. 608–614, 2011.

[7] C. Gupta and A. Kumar, "Wireless sensor networks: A review," *International Journal of Sensors Wireless Communications and Control*, vol. 3, 12 2013.

[8] M. F. Othman and K. Shazali, "Wireless sensor network applications: A study in environment monitoring system," *Procedia Engineering*, vol. 41, pp. 1204–1210, 2012.

[9] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Computers and electronics in agriculture*, vol. 118, pp. 66–84, 2015.

[10] M. A. Rahu, S. Karim, R. Shams, A. A. Soomro, and A. F. Chandio, "Wireless sensor networks-based smart agriculture: Sensing technologies, application and future directions," *Sukkur IBA Journal of Emerging Technologies*, vol. 5, no. 2, pp. 13–32, 2022.

[11] T. Malapane, W. Doorsamy, and B. S. Paul, "An intelligent iot-based health monitoring system," in *2020 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*. IEEE, 2020, pp. 95–100.

[12] N. Abdullah, O. A. Alwesabi, and R. Abdullah, "Iot-based smart waste management system in a smart city," in *Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018)*. Springer, 2019, pp. 364–371.

[13] N. Mishra, P. Singhal, and S. Kundu, "Application of iot products in smart cities of india," in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. IEEE, 2020, pp. 155–157.

[14] P. Sakhardande, S. Hanagal, and S. Kulkarni, "Design of disaster management system using iot based interconnected network with smart city monitoring," in *2016 international conference on internet of things and applications (IOTA)*. IEEE, 2016, pp. 185–190.

[15] S. Jha, P. M. Nakade, M. P. Nazare, S. K. Chawla, and S. M. Nadge, "Iot based incident control system using air quality index monitoring system," in *2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*, 2022, pp. 108–112.

[16] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 717–11 731, 2021.

[17] M. Li, Y. Chen, N. Kumar, C. Lal, M. Conti, and M. Alazab, "Quantifying location privacy for navigation services in sustainable vehicular networks," *IEEE Transactions on Green Communications and Networking*, 2022.

[18] N. Sharma and R. Bhatt, "Source location privacy preservation in iot-enabled event-driven wsns," *International Journal of Pervasive Computing and Communications*, no. ahead-of-print, 2022.

[19] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in iot-based healthcare systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*. Springer, 2021, pp. 105–134.

[20] R. Manjula and R. Datta, "Application of the chinese remainder theorem for source location privacy in wireless sensor networks," in *2016 IEEE Students' Technology Symposium (TechSym)*. IEEE, 2016, pp. 202–207.

[21] D. Sora, "Security issues in wireless sensor networks," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 6, no. 4, pp. 26–30, 2010.

[22] 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 Computer Science*, vol. 57, pp. 936–941, 2015.

[23] Y. He, G. Han, H. Wang, J. A. Ansere, and W. Zhang, "A sector-based random routing scheme for protecting the source location privacy in wsns for the internet of things," *Future Generation Computer Systems*, vol. 96, pp. 438–448, 2019.

[24] R. Manjula, T. Koduru, and R. Datta, "Protecting source location privacy in iot enabled wireless sensor networks: the case of multiple assets," *IEEE Internet of Things Journal*, 2021.

[25] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Rate-privacy in wireless sensor networks," in *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2013, pp. 67–68.

[26] S. Pai, M. Meingast, T. Roosta, S. Bermudez, S. B. Wicker, D. K. Mulligan, and S. Sastry, "Transactional confidentiality in sensor networks," *IEEE Security & Privacy*, vol. 6, no. 4, pp. 28–35, 2008.

[27] C. Ozturk, Y. Zhang, W. Trappe, and M. Ott, "Source-location privacy for networks of energy-constrained sensors," in *Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, 2004. Proceedings.* IEEE, 2004, pp. 68–72.

[28] 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.

[29] Y. Li and J. Ren, "Providing source-location privacy in wireless sensor networks," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2009, pp. 338–347.

[30] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.

[31] L. Kaur and R. Kaur, "A survey on energy efficient routing techniques in wsns focusing iot applications and enhancing fog computing paradigm," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 520–529, 2021.

[32] 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.

[33] M. Poornima, H. Vimala, and J. Shreyas, "Holistic survey on energy aware routing techniques for iot applications," *Journal of Network and Computer Applications*, vol. 213, p. 103584, 2023.

[34] G. Han, M. Xu, Y. He, J. Jiang, J. A. Ansere, and W. Zhang, "A dynamic ring-based routing scheme for source location privacy in wireless sensor networks," *Information Sciences*, vol. 504, pp. 308–323, 2019.

[35] M. Bradbury, A. Jhumka, and C. Maple, "A spatial source location privacy-aware duty cycle for internet of things sensor networks," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–32, 2021.

[36] S. Chowdhury, A. Roy, A. Benslimane, and C. Giri, "On semantic clustering and adaptive robust regression based energy-aware communication with true outliers detection in wsn," *Ad Hoc Networks*, vol. 94, p. 101934, 2019.

[37] J. Oh, D. Lee, D. S. Lakew, and S. Cho, "Dacode: Distributed adaptive communication framework for energy efficient industrial iot-based heterogeneous wsn," *ICT Express*, 2023.

[38] T. Naumowicz, R. Freeman, H. Kirk, B. Dean, M. Calsyn, A. Liers, A. Braendle, T. Guilford, and J. Schiller, "Wireless sensor network for habitat monitoring on skomer island," in *IEEE Local Computer Network Conference*. IEEE, 2010, pp. 882–889.

[39] O. a brighter world, "Organizations are turning to technology to save the world's most threatened animals," https://www.nec.com/en/global/insights/article/2020022502/index.html, February 28, 2020 (accessed December 17, 2020).

[40] L. Dinh, "Endangered black rhinos protected by lora," https://www.semtech.com/company/press/semtech-lora-technology-tracks-location-of-endangered-black-rhinos-in-africa, January 17, 2017 (accessed January 17, 2020).

[41] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, 2002, pp. 88–97.

[42] kara Norton, "The 21st century threat to wildlife is cyberpoaching," https://www.pbs.org/wgbh/nova/article/21st-century-threat-wildlife-cyberpoaching/, OCTOBER 31, 2020 (accessed January 22, 2020).

[43] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, 2010.

[44] X. Hong, P. Wang, J. Kong, Q. Zheng *et al.*, "Effective probabilistic approach protecting sensor traffic," in *MILCOM 2005-2005 IEEE Military Communications Conference*. IEEE, 2005, pp. 169–175.

[45] S. A. Khah, A. Barati, and H. Barati, "A dynamic and multi-level key management method in wireless sensor networks (wsns)," *Computer Networks*, vol. 236, p. 109997, 2023.

[46] 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.

[47] W. Shi, X. Jiang, J. Hu, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu, and J. Wang, "Physical layer security techniques for future wireless networks," *arXiv preprint arXiv:2112.14469*, 2021.

[48] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[49] D. W. Matolak and J. Frolik, "Worse-than-rayleigh fading: Experimental results and theoretical models," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 140–146, 2011.

[50] T. Olofsson, A. Ahlen, and M. Gidlund, "Modeling of the fading statistics of wireless sensor network channels in industrial environments," *IEEE Transactions on Signal Processing*, vol. 64, no. 12, pp. 3021–3034, 2016.

[51] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2009, pp. 1–9.

[52] 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, 2011.

[53] S. Song, H. Park, and B.-Y. Choi, "Step: Source traceability elimination for privacy against global attackers in sensor networks," in *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2011, pp. 1–6.

[54] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in wsns for the social internet of things," *Future Generation Computer Systems*, vol. 82, pp. 689–697, 2018.

[55] 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.

[56] N. Wang and J. Zeng, "All-direction random routing for source-location privacy protecting against parasitic sensor networks," *Sensors*, vol. 17, no. 3, p. 614, 2017.

[57] 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.

[58] R. Manjula and R. Datta, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in wsns," *Pervasive and Mobile Computing*, vol. 44, pp. 58–73, 2018.

[59] J. F. Laikin, M. Bradbury, C. Gu, and M. Leeke, "Towards fake sources for source location privacy in wireless sensor networks with multiple sources," in *2016 IEEE International Conference on Communication Systems (ICCS)*. IEEE, 2016, pp. 1–6.

[60] F. Mukamanzi, M. Raja, T. Koduru, and R. Datta, "Position-independent and section-based source location privacy protection in wsn," *IEEE Transactions on Industrial Informatics*, 2022.

[61] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity—a proposal for terminology," in *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings*. Springer, 2001, pp. 1–9.

[62] X. Liu, J. Yu, X. Zhang, Q. Zhang, and C. Fu, "Energy-efficient privacy-preserving data aggregation protocols based on slicing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 1–12, 2020.

[63] F. Lalooses, H. Susanto, and C. H. Chang, "An approach for tracking wildlife using wireless sensor networks," in *The International Workshop on Wireless Sensor Networks (NOTERE 2007), IEEE, Marrakesh, Morocco*, 2007, pp. 76–76.

[64] S. Ehsan, K. Bradford, M. Brugger, B. Hamdaoui, Y. Kovchegov, D. Johnson, and M. Louhaichi, "Design and analysis of delay-tolerant sensor networks for monitoring and tracking free-roaming animals," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 1220–1227, 2012.

[65] J. P. Dominguez-Morales, A. Rios-Navarro, M. Dominguez-Morales, R. Tapiador-Morales, D. Gutierrez-Galan, D. Cascado-Caballero, A. Jimenez-Fernandez, and A. Linares-Barranco, "Wireless sensor network for wildlife tracking and behavior classification of animals in doñana," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2534–2537, 2016.

[66] T. Baig z and C. Shastry, "Design of wsn model with ns2 for animal tracking and monitoring," 2023.

[67] 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.

[68] Y. Li and J. Ren, "Providing source-location privacy in wireless sensor networks," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2009, pp. 338–347.

[69] 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.

[70] L. C. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing," *Sensors*, vol. 19, no. 5, p. 1037, 2019.

[71] 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.

[72] 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.

[73] L. Bai, L. Li, S. Qian, and S. Zhang, "Random selection false source-based algorithm for protecting source-location privacy in wsns," in *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*. IEEE, 2016, pp. 2064–2069.

[74] G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "Kclp: A k-means cluster-based location privacy protection scheme in wsns for iot," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 84–90, 2018.

[75] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 100–114, 2019.

[76] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, "Protecting source–location privacy based on multirings in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 15, pp. 3863–3876, 2015.

[77] C. Gu, M. Bradbury, A. Jhumka, and M. Leeke, "Assessing the performance of phantom routing on source location privacy in wireless sensor networks," in *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2015, pp. 99–108.

[78] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in wsns for the social internet of things," *Future Generation Computer Systems*, vol. 82, pp. 689–697, 2018.

[79] 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.

[80] H. Wang, G. Han, C. Zhu, S. Chan, and W. Zhang, "Tcslp: A trace cost based source location privacy protection scheme in wsns for smart cities," *Future Generation Computer Systems*, vol. 107, pp. 965–974, 2020.

[81] 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.

[82] N. Jan, S. Khan, A. H. Al-Bayatti, M. O. Alassafi, A. S. Alfakeeh, and M. A. Alqarni, "C2s2-loop: Circular chessboard-based secure source location privacy model using ecc-alo in wsn," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[83] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 100–114, 2019.

[84] 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.

[85] 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.

[86] J. F. Laikin, M. Bradbury, C. Gu, and M. Leeke, "Towards fake sources for source location privacy in wireless sensor networks with multiple sources," in *2016 IEEE International Conference on Communication Systems (ICCS)*. IEEE, 2016, pp. 1–6.

[87] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *25th IEEE international conference on distributed computing systems (ICDCS'05)*. IEEE, 2005, pp. 599–608.

[88] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.

[89] 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.

[90] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," in *Proceedings of the 2006 international conference on Wireless communications and mobile computing*, 2006, pp. 33–38.

[91] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*. IEEE, 2006, pp. 8–pp.

[92] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 7, pp. 1302–1311, 2011.

[93] H. Wang, G. Han, C. Zhu, S. Chan, and W. Zhang, "Tcslp: A trace cost based source location privacy protection scheme in wsns for smart cities," *Future Generation Computer Systems*, vol. 107, pp. 965–974, 2020.

[94] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE transactions on mobile computing*, vol. 9, no. 7, pp. 941–954, 2010.

[95] S. S. Mohar, S. Goyal, and R. Kaur, "Localization of sensor nodes in wireless sensor networks using bat optimization algorithm with enhanced exploration and exploitation characteristics," *The Journal of Supercomputing*, vol. 78, no. 9, pp. 11 975–12 023, 2022.

[96] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, p. 102448, 2021.

[97] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 159–186, 2006.

[98] A. Berdibek and S. Saginbekov, "A routing protocol for source location privacy in wireless sensor networks with multiple sources," in *Proceedings of the 15th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*, 2019, pp. 93–99.

[99] J. Kirton, M. Bradbury, and A. Jhumka, "Towards optimal source location privacy-aware tdma schedules in wireless sensor networks," *Computer Networks*, vol. 146, pp. 125–137, 2018.

[100] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on wireless communications*, vol. 1, no. 4, pp. 660–670, 2002.

[101] M. Raja and R. Datta, "An enhanced source location privacy protection technique for wireless sensor networks using randomized routes," *IETE Journal of Research*, vol. 64, no. 6, pp. 764–776, 2018.

[102] R. Manjula, T. Koduru, and R. Datta, "Protecting source location privacy in iot-enabled wireless sensor networks: the case of multiple assets," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 807–10 820, 2021.

[103] S. H. Khasteh and H. Rokhsati, "On transmission range of sensors in sparse wireless sensor networks," *Results in Engineering*, vol. 18, p. 101108, 2023.

[104] A. S. Azhar, S. A. Kudus, A. Jamadin, N. K. Mustaffa, and K. Sugiura, "Recent vibration-based structural health monitoring on steel bridges: Systematic literature review," *Ain Shams Engineering Journal*, p. 102501, 2023.

[105] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, "Secure and energy-efficient disjoint multipath routing for wsns," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 7, pp. 3255–3265, 2012.

List of Publications from the Thesis

Journals

- **F. Mukamanzi**, M. Raja, T. Koduru and R. Datta,"Position-Independent and Section-Based Source Location Privacy Protection in WSN", in IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 6636-6646, May 2023, doi: 10.1109/TII.2022.3183804.
- **F. Mukamanzi**, M. Raja, R. Datta, D. Hanyurwimfura,T. Koduru and D. Mukanyiligira, "A Total Randomized SLP-Preserving Technique with Improved Privacy and Lifetime in WSNs for IoT and the Impact of Radio Range on SLP", Sensors 2023, 23, 9623. https://doi.org/10.3390/s23249623.

International conferences

Mukamanzi, F, M. Raja, R. Datta, T. Koduru and D. Hanyurwimfura,"Increasing Source Privacy and Network Lifetime without Affecting Latency: a Strategic Random Walk for WSNs*", 2023 8th International Conference on Computer and Communication Systems (ICCCS), IEEE, Guangzhou, China, 2023, pp. 677-682, doi: 10.1109/ICCCS57501.2023.10151299.