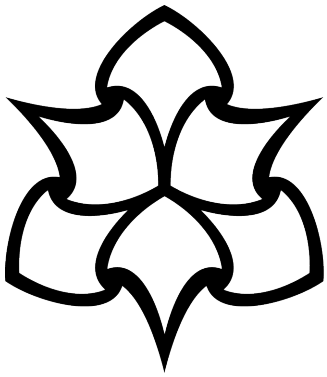

A NOVEL ROUTING APPROACH FOR SOURCE LOCATION PRIVACY IN WIRELESS SENSOR NETWORKS

A thesis submitted in partial fulfilment of the requirement of The Manchester Metropolitan University for the degree of Master of Philosophy

Ehtesham Hassan

School of Computing, Mathematics and Digital Technology
The Manchester Metropolitan University

November 2018

Abstract

Wireless sensor networks (WSNs) allows the world to use a technology for event supervision for several applications like military and civilian applications. Network privacy remained a prime concern in WSNs. Privacy of Source location is assumed to be one of the main un-tackled issues in privacy of WSNs. Privacy of the source location is vital and highly jeopardized with the use of wireless communications. For WSNs, privacy of source location is become more complex by the fact that sensor nodes are low cost and energy efficient radio devices. So, use of computation intensive encryption methods and large scale broadcasting based algorithms are found to be unsuitable for WSNs. Several schemes have been proposed to ensure privacy of source location in WSNs. But, most of existing schemes depends on public-key cryptosystems, while others are either energy inefficient or have certain security flaws like leakage of information using directional attacks or traffic analysis attacks.

In this thesis, we propose a novel dynamic routing based approach for preserving privacy of source location in WSNs, which injects fake packets in network and switches the real packet information among different routing patterns. It addresses the privacy of source location by considering the limited features of WSNs. Major contributions of this work includes two aspects. Firstly, different from the existing approaches, the proposed approach considers enhancing the security of nodes with minimal transmission delay and consumes power with minimum effect on the lifetime of the network. Secondly, the proposed approach is designed to defend many attacks like hop by hop, directional attacks by choosing a suitable path to send information from node to BS dynamically without affecting network life significantly. Thus, it becomes difficult for the attacker to find the exact path, and hence the original location of node. The proposed approach is implemented and validated by comparing its results with that of the existing approaches in the field of source location privacy in terms of Power consumption, Transmission delay, Safety period, and network lifetime. The analysis of comparative results indicates that the proposed approach is superior to the existing approaches in preserving the source location privacy.

Dedicated to

My Family

Acknowledgements

It is not imaginable for me to complete this thesis of the M. Phil. journey without the significant support of many great people. There are many people who have had an impact in one or another way. There are so many people that deserve a 'thank you' here, but it will not be possible to express my gratitude by name to all these people. I would like to give many, many thanks to all.

First and foremost, I am greatly indebted to great mentor Prof. Liangxiu Han, Professor, School of Computing, Mathematics and Digital Technology for her guidance, encouragement, and motivation throughout my journey of this research. She has allowed me to pursue my research interests with sufficient freedom, while always being there to guide me.

I am very thankful to Dr. Mohammed Hammoudeh, and Prof. Martyn Amos for their guidance and continued support in this research work. Working with them has been one of the most rewarding experiences of my professional life. They provided me with sound advice and lots of ideas for not only in this research, but also in other aspects of my life. I wish to be associated with them throughout my life and pray to God to bless them and their family with good health and true happiness throughout their life.

I also thank to express my deepest and sincere gratitude to my wife and parents, for the essence of affection, kindness and commitment. They have been a guiding force in my life. With their teaching and blessings only, it has been possible for me to achieve, what I have and what I am today.

Finally, all thanks and praise are due to God for giving me the strength and knowledge to complete this work.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

BS	Base Station
CR	Cyclic Routing
DR	Directional Routing
ER	Estimated Routing
GROW	Greedy Random Walk
HA	Hotspot Area
LN	Leader Node
LR	Leader Ring
MAC	Media Access Control
RFID	Radio-Frequency Identification
SN	Sensor Node
SSN	Source Sensor Node
TTL	Time To Live
WRS	Weighted Random Stride
WSN	Wireless sensor network

CHAPTER 1

Introduction

Wireless sensor networks (WSNs) is visualized as a technology having huge potential for its usage in diverse applications like civilian applications, military applications. Network privacy is the most analyzed issue in WSNs. It is considered as one of the main and the un-tackled issues in the privacy of WSNs using adequate source location privacy on the basis of routing [25]. Sensor networks depend on wireless communications using broadcast communication mechanism. But, wireless communication susceptible to network based attacks on its security than its counter part in wired network because of no physical limits.

The receivers available in the wireless network equipped with compatible devices may intercept network traffic being transmitted through wireless media [4]. An attacker can carry powerful transceivers with him to capture network information. He can intercept network traffic from more than one positions on the wireless network. An attacker can find out location of source of event by using Radio Frequency localization approaches in absence of appropriate protection on routing paths. Using this information, he can traceback the source of event using a hop-by-hop method. So, a advance encryption approach fails to protect the identity of source of information.

This chapter discusses the importance and use of WSN in different application domains. The need for preserving the source location in WSNs and motivation of this research work is highlighted in Section 1.1. The chapter presents the problem statement for preserving source location privacy in Section 1.2 and main objectives of the thesis in Section 1.3. Finally, it presents the structure of thesis to meet its objectives in Section 1.4.

1.1 Background & Motivations

A wireless sensor network (WSN) is a collection of heterogeneous network elements like small low cost equipments, called as sensor nodes (or motes) and a general purpose set of computing equipments called as as sinks or base stations [23]. Generally, WSN is developed to supervise certain physical quantities like pressure, temperature, light present in the region of its deployment. Sensor nodes are capable of acting as a communication point having processing capability, power source and sensing capability. They are limited in their capability of processing capacity and power backup. In contrast, base stations or sink consists of laptop abilities with non-limited power resources. The base stations are responsible for communication between different types of network including WSN.

Recently, WSNs has been deployed in diverse field [1] for monitoring the events, including military events [2], habitat event monitoring [28], shopping habits monitoring, patient health monitoring, and bridge structural health monitoring [40].

WSNs can be categorized into different classes on the basis of its affect on security protocol design [23]. One way of dividing the WSNs is concerned with movement of sensor nodes as well as the sink. The sensor nodes can be a moveable node or static node. Similarly, sink can also be moveable or static in nature. Another way of dividing WSNs is on the basis of placement of sensor nodes. The sensor nodes can be distrusted either manually at particular location using certain identified network structure or in a random way in WSNs. The number of sensor nodes is also a vital parameter whose value can range from ten to ten thousands.

One significant aspect of network security is concerned with privacy [15]. Privacy is crucial in some critical applications requiring privacy of sensitive information transmitted over the network. However, attackers may intercept sensitive information from network by exploiting broadcast nature of WSNs and try to subvert underlying network system.

There are many different WSN applications, which pose privacy preservation requirements. Prominent areas include:

- Healthcare and well-being applications (including remote monitoring of patients or elderly), which typically collect and process private data about the subjects [41]. The latter data include healthcare record information, as well as lifestyle and behavioral data.
- Traffic management and urban mobility applications, such as traffic control, smart parking systems and connected car applications. These applications are likely to derive and process information about the location and context of the citizens (e.g., through their license plates).
- Personalized retailing applications, such as the use of AutoID technologies (e.g., RFID, barcodes, QR codes) in shopping applications and loyalty management. These applications collect and manage data about the citizens' shopping behavior.
- Energy generation and management applications, which are typically developed and operated by energy operators and utility companies. Such applications store and leverage energy consumption data about citizens and businesses.
- Urban security and civil protection applications, which are in most cases based on the collection and processing of large amount of sensor data (e.g., cameras, energy consumption sensors) in order to identify and track suspicious behaviors. Therefore, these applications are potentially threatening citizens' freedom and privacy.

The above list is non-exhaustive, yet indicative of WSN applications that raise privacy issues and are therefore in need of privacy preserving applications.

The network threats for disrupting the privacy over WSNs can be divided into two main classes as described below and depicted in Fig. 1.1 [15].

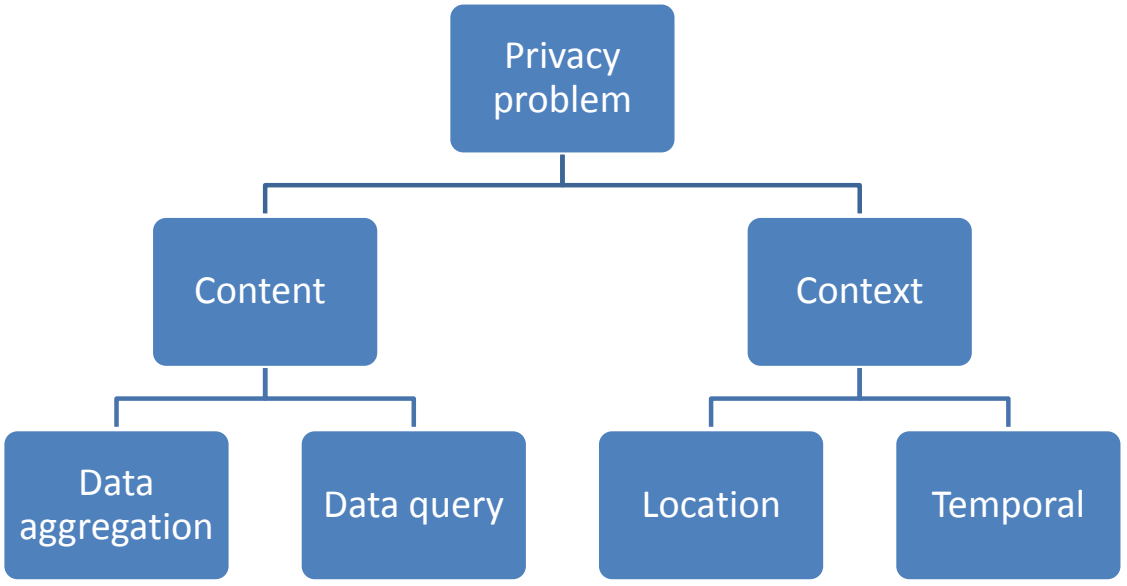

FIGURE 1.1: Privacy problem in WSNs.

1. **Content privacy threats:** These threats are concerned with the content of information sent over the WSN. For example, information headers added by various network layers like application layer or network layer [37].

2. **Context privacy threats:** These threats are concerned with context of measurement and transmission of sensitive information. Context is considered as a multiple attribute aspect that involves many environment factors related with sniffed data, like its timing and location. It is found that content privacy threats are clearly understandable [15], whereas context privacy threats are the major concern and importance of the research community. For content privacy threats, sensor nodes who mount the network attacks are generally modeled as Byzantine nodes. In this case, cryptographic approaches are applied to tackle these issues [3]. But, cryptographic approaches do not suits to context privacy threats.

Location aspect of context privacy is the most significant for several mission critical applications[15]. The most common example is the applications related to military. Here, in this case, location may refer to the location of a soldier. Another example is the location of any costly painting lying in a musem for an asset

monitoring application. During transmission of information, location of object can be combined with the message in an encrypted form. Thus, it is difficult for an attacker to retrieve the location information from the original message. But, an attacker can attempt to locate the object using several other approaches like network traffic analysis [8].

Therefore, in most of mission critical applications deploying WSNs, preserving the location of source of event or object is most critical. The node who detect the locations of object or source of event is called source node. The source nodes are programmed to transmit source location information on regular basis to the base station or sink node. If during transmission, an attacker successfully retrieve the source information, then he can easily capture the object or asset being monitored. The current study targets the preservation of source location privacy, considering the object being supervised as a panda that is considered as endangered animal [18].

An attacker can attempt in different ways to find out the location of object being monitored based upon his power of the attacker. Some of researchers assume that attackers are equipped with their own wireless networks, enabling them to capture information about the monitored object using intercepted messages[29]. Whereas, some of researchers suggested to use triangulation approach to locate the location of objects[19].

In this work, we focus on the dynamic routing approach for preserving the source location privacy. The proposed approach involves injecting the fake packets into the network and switches the real information packets between different routing patterns based on certain conditions. This results in confusing the attackers from accessing the source location in WSN, and hence enhances the source location privacy without compromising network lifetime.

1.2 Research Problem

The privacy of WSNs is considered as one of the major and the un-tackled an issue using adequate source location privacy on the basis of routing. Sensor networks

depend on wireless communications using broadcast communication mechanism. But, wireless communication susceptible to network based attacks on its security than its counter part in wired network because of no physical limits. The receivers available in the wireless network equipped with compatible devices may intercept network traffic being transmitted through wireless media. An attacker can carry powerful transceivers with him to capture network information. He can intercept network traffic from more than one positions on the wireless network. An attacker can find out location of source of event by using Radio Frequency localization approaches in absence of appropriate protection on routing paths. Using this information, he can traceback the source of event using a hop-by-hop method. So, a advance encryption approach fails to protect the identity of source of information.

Sensor nodes or devices used for sensing the data also pose severe limitations for ensuring source location privacy. These nodes are usually designed for low cost and power optimized devices. Organizations can spread these devices in WSN and supervise the events in the network from a central point called base station or sink node. Once,these nodes are spread in a network with an human attention afterwards for a long time. Or even these nodes are spread where human attention is not feasible. Thus, it is not practically possible to replace their power source. Therefore, computation intensive encryption approaches and power eating transmitters are not appropriate for WSNs. So, power consumption and preserving the privacy of source location are considered as important parts for designing WSNs.

A majority of the approaches have not considered the impact of the source location privacy protection approach on the performance of the network's lifetime. Some of the researchers proposed public key based encryption approaches for source location privacy protection approaches [5, 25]. These approaches are highly computationally and communication expensive. So, these approaches are not suitable for source location privacy protection approaches. It is also noticed that approaches that depends upon broadcasting of messages for preserving privacy in WSNs are power inefficient [6, 22, 27, 31]. The approaches using routing approach for ensuing privacy can lead to leakage of the information related to source location [13, 18, 42, 45, 48].

So, there is an acute requirement to propose a routing approach that ensures preserving the source location in WSNs without affecting the network lifetime. In

this thesis, we focus to investigate the problem of source location privacy in WSNs and propose an appropriate approach for enhancing source location privacy without affecting lifetime of the network.

1.3 Research Objectives

The aim of the this research work is to present an approach for preserving the source location privacy in WSN. More precisely, it focuses on the study and proposal of routing approach that injects fake packets in network and switches the real packet information among different routing patterns for preserving the source location privacy.

The followings are the main objectives of this thesis:

1. To critically analyze state of the art in the field to assess the current status of privacy preserving approaches in WSNs. Particularly, approaches addressing the issue of source location privacy in WSNs and their limitations.
2. To access the effective performance metrics to measure & compare the performance of source location privacy preservation approaches in WSNs.
3. To design and develop a novel dynamic approach for preserving privacy of source location without affecting the network lifetime of WSN by switching the real information among different routing patterns and injecting fake packets in the network.
4. To Implement and validate the proposed dynamic routing approach for source location privacy by comparing its performance regarding safety period, transmission delay, network lifetime and power consumption with that of representational approaches in the field using a benchmark experimental setup.

In order to meet the objectives of thesis cited above, we structure the thesis as described in Section 1.4.

1.4 Thesis Layout

The rest of the thesis is organized as follows.

Chapter 2 presents an updated review of the state of the art in the field of WSN, particulary, the approaches addressing the problem of preserving source location privacy. Finally, it presents the use of routing approaches for preserving the source location in WSNs and highlights the gaps in research work in the field.

Chapter 3 presents the proposed approach for effective preservation of source location in WSN by injecting fake packets into the network and switching real packets among different routing patterns based upon conditions without affecting network lifetime of WSN.

Chapter 4 provides the details of the experimental setup, results and their discussion. A comparative analysis of the reported results is presented with existing researches in the field at the end of this chapter.

Chapter 5 finally concludes the thesis by presenting a summary of the thesis, key contributions & conclusions followed by recommendations for future extensions to this research.

A comprehensive bibliography in the field of privacy of source location and WSN is appended at the end of the thesis.

CHAPTER 2

Literature Review

This chapter presents an updated review of the main contributions and the principal trends in preserving network privacy of WSNs. It presents an overview of taxonomy of network privacy in Section 2.1 and further presents state of the art with respect to the privacy taxonomy including content privacy and context privacy in Section 2.2 and 2.3 respectively. Different studies in the field are summarized as per taxonomy in tabular form for better understanding the current status of source location privacy approaches in WSNs in Section 2.4. Related issues and major limitations of existing researches in the field are summarized at end of this chapter in Section 2.5.

2.1 Introduction

Privacy is concerned with autonomy right and consists of right to remain alone. It covers the right to assure information about myself and to grant of limited access to others[10].

For WSNs, privacy comprises the privacy of the object being monitored in addition to privacy of sensor nodes and base stations [23]. It has been observed

that privacy of these objects is linked with each other to some extent. Breaching the privacy of one object results in intrusion into privacy of the object being monitored. Privacy in WSNs can be divided into two classes, described as below [18].

1. Content privacy
2. Context privacy

Content privacy is menaced by an attacker whose goal is to control or access message details transmitted over a network. In case of context privacy, it is concerned with securing contextual information about the content. Particulary, context related information contains location of the data or its measurement time.

Li et al [24] proposed a general taxonomy for different privacy protection approaches in WSNs. The authors classified privacy into two classes as content (data) privacy and context privacy. Content protection approaches are further classified into two categories dealing with data aggregation and private data queries. Context protection approaches are classified into two classes, namely location privacy preserving approaches, containg source and sink location protection approaches, and temporal privacy preserving approaches. The taxonomy is graphically depicted in Fig. 2.1.

In this chapter, we present an critical analysis of related work as per taxonomy depicted in Fig. 2.1. Several researchers have reviewed various researches, taxonomy and attacks on network privacy in the field of privacy in WSNs [20, 24, 36, 44]. An updated review of significant researches in the field are presented with respect to taxonomy depicted in Fig. 2.1 in following sections.

2.2 Content Privacy Approaches

Content (data) privacy problems usually can be tackled through message encryption or authentication [13]. Content privacy protection approaches focus on ensuring network privacy of aggregated data and data queries passed.

There exists two kinds of attackers that threaten the data privacy.

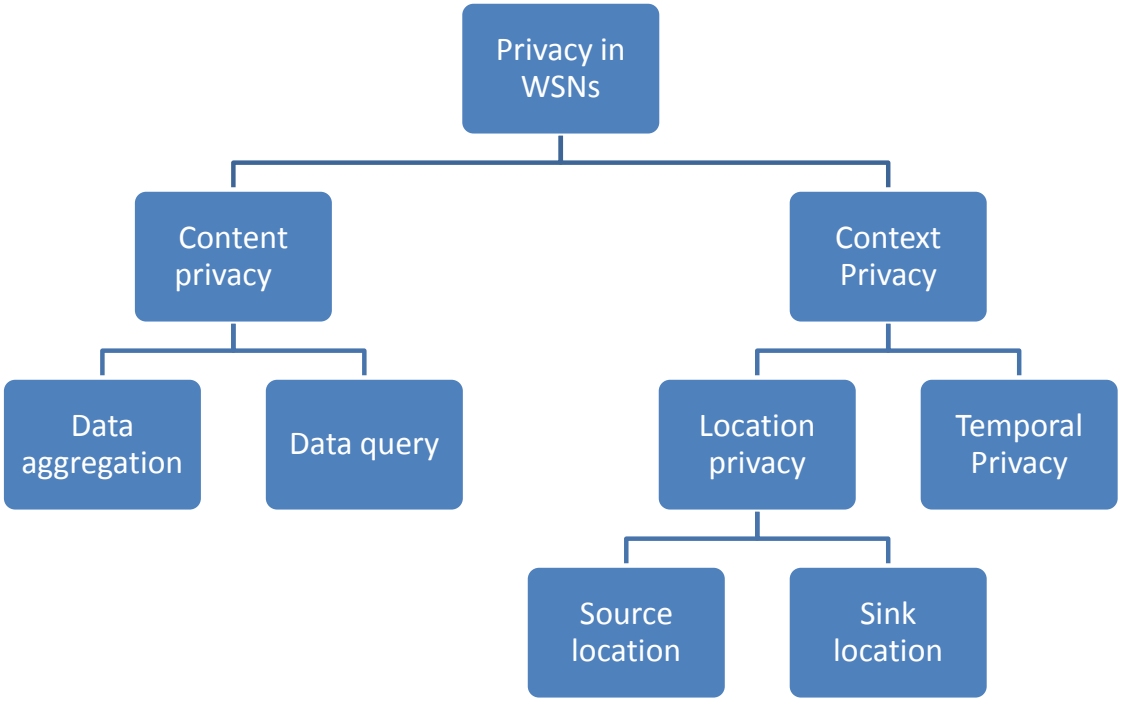

FIGURE 2.1: A taxonomy of privacy in WSNs.

1. External attacker

2. Internal attacker

The external attacker only intercepts data during transmission over a network. Strong cryptographic approaches such as SPINS [32] or pDCS [39] can help tackle such attackers. The internal attackers manipulate multiple sensor nodes by exploiting the known keys used for encrypting the messages. A straight forward method to deal with this problem is to use end to end encryption keys from sensor nodes to sink node and vice versa [23]. However, the use of cryptographic approaches leads to difficulty of data aggregation in a network. Therefore, it is considered as an issue for providing privacy during data aggregation in the presence of such attackers. Several researches have been proposed to tackle the issue. In this thesis, we are mainly concerned with context based privacy. so interested readers may refer to [11, 14, 43, 50].

2.3 Context Privacy Approaches

It is noticed that context realted issues are difficult to trace due to vulnerability of network signals [13]. A sensor node can lead to leakage of contextual information in spite of use of various encryption approaches[23]. Specific context related information can divided into following classes.

1. Location privacy: It contains the information on data source location or sink location.
2. Temporal privacy: It contains the information about event timing.

External attackers generally gain such information using network traffic analysis approaches [33]. We provide updated review of studies related to context protection approaches in the succeeding subsections.

2.3.1 Location Privacy Approaches

Location privacy approaches are very significant in WSNs. It deals with the information concerned with source location or sink location, that can be of a main focus of the attackers. For example, Panda-Hunter Game involves deployment of WSN for supervising pandas in their habitat [18]. It is enough for the attacker to search out sensor node's location, observing pandas to complectly locate and trap the panda. In similar way, the attacker only requires to search sink location for mounting a physical or other attacks to disrupt its availability like DoS attack. Thus, such attacks lead to make the whole network inactive for its users.

The attacker in this model can be divided in two categories as described below.

1. Local attackers
2. Global attackers

The local attacker has limited radio range, thus he can only observe network traffic in a small portion at a time in WSN. However, global attacker has the ability to observe the entire network, thus can locate all transmitting nodes instantly.

Location privacy approaches can be further categorized into privacy of data source and data sink (base station) as described in Section 2.3.1.1 and 2.3.1.2.

2.3.1.1 Source Location Privacy Approaches

The problem of privacy of source location was coined by Chaum et al. [5]. The authors suggested a mixnet to conceal detail on a source of information. Further, Reed et al. [34] provided source location privacy in public computer networks on the basis of onion routing. After that several researchers proposed various approaches for providing source location privacy on the basis of spatial and temporal cloaking [12], demand routing with untraceable routes [21], phantom flooding [18, 31, 47] and many more. It is noticed that several approaches developed for source location privacy are inadequate for resource limited WSNs due to their high requirements of power and memory [23].

Source location privacy approaches in WSNs can be divided as described below.

1. **Flooding based source privacy approaches:** Several researchers used flood of network traffic to handle the problem of privacy of source location.

   Ozturk et al. [31] suggested a metric for assessing the privacy of source location called the safety period. The authors formulated safety period as message count that source node transmits before getting localized by the attacker. They validated the affect of baseline and approaches based on probabilistic flooding for privacy of source location in terms of safety period metric. The authors presented the conclusions that these existing approaches offer the minimum protection. It may leads to traceback location of source having least values of safety period. This happens due to following the shortest path by the message in beginning and it reaches the attacker.

This approach was further extended by using probabilistic flooding [31]. The extended approach is proved to be energy efficient and offers more privacy of source location in WSNs. Here, sensor node passes a message packet with some probability value and hence involves a small set of sensor nodes while forwarding the message packets. So, no constant stream of packets is generated, thus make difficult for the attackers to trace back the location of source nodes.

In another study, Ozturk et al. [31] also suggested a novel approach for privacy of source location using routing approach called phantom flooding approach. The proposed approach involves two phases. Firstly, it involves sending of a message packet to a random node following a random or directed walk. This randomly selected node is called phantom node. Finally, the phantom node floods the message packets into the network to arrive at the sink node. It is noticed that this approach enhances safety time for exchanging the messages over the existing approaches based on flooding approach.

Luo et al. [27] suggested a approach based on a phantom single path routing. In their approach, a path is started from the phantom node for imitating the actual event routing.

Kumar et al. [22] suggested a approach using multiple phantom scheme. The suggested approach ensures the confusion for an attacker that each source node consists of double phantom nodes.

Chen et al. [6] proposed a routing approach, ignoring source location preservation in WSNs. The authors proposed that nodes having information for BS will transmit the information packets using the shortest possible route. This approach involves a minimum number of packets transmitted over the network. Thus, it exhibited high performance in terms of the long lifetime of network, minimum power consumption, but at the cost of security of source nodes. The attackers can easily detect the location of SSN and attack it.

Jhumka et al. [15] proposed cyclic defense during transmission of information packets from SSN to BS. This approach used dummy message packets with phantom routing to confuse the attackers in finding the real path followed by the real information packets to reach BS.

The authors proposed two different solutions on the basis of fake information sources. The first solution, called fake source solution 1 (FS1) works as follows. A source node reports to the sink by broadcasting a message to its neighboring nodes. The neighboring nodes analyze the packets for its duplicate receipt. If it has not already received message, the hop count of the received message is incremented and broadcasted again. Otherwise, the message is discarded. This process is repeated till the message packet meets the BS.

Next, the BS floods away-message with the hop count of the message that informed the BS of the event. Nodes that receive the away-message checks if they have a message from the source with a hop count of one. If a node received such a message, then it takes the hop count from the away-message minus one and uses it as the value of a TTL counter for its choose-message. The node then broadcasts the choose-message. If a node receives a choose-message, it uses a probability p to decide whether to forward the choose-message. If $p \geq P$ (where P is a set threshold), then the node decrements the TTL -counter of the choose-message and forwards it to its neighbors. If the TTL-counter of the message equals to zero, then the node that had received the message uses probability p to decide whether it should become a fake source. If $p \geq P$, then the node becomes a fake source.

The second solution proposed by the authors is called fake source solution 2 (FS2). The main difference between these two solutions is in the method choose-message is moved forward. In FS2, each node that receives choose-message decrements the TTL counter and forwards the message until the TTL counter reaches 0, without deciding on the basis of P.

This approach uses cyclic defense to confuse the attacker for preserving the source location privacy. It suffers from the limitation in trading off network energy consumption against source location privacy; there are times when there are no fake sources that are selected, thereby reducing the level of privacy. It involves the transmission of a large number of fake message packets in all areas including hotspot area, so it affects the power consumption of nodes in hot spot areas. Thus, it impacts the lifetime of the network.

In this approach, cyclic routing and inter cluster communication, both lead to a large transmission delay. This approach is proposed on the basis of panda-hunter model. Here, it is possible that a panda may remain in one specific area for a relatively longer time. In that scenario, an attacker can determine the event ring quickly. Because, the backbone route in this approach is the shortest path from the trigger node to the sink. This leads to leakage of location information of the source node in the network.

These approaches mainly contribute by confusing an attacker to classify real network traffic from the fake network traffic.

2. **Random-walk based source privacy approaches:** Xi et al. [48] proposed a approach for privacy based on a greedy random walk method. They proposed to initiate a random walk by the sink node. Further, the source node is allowed to create and passes packets for different events using a random walk approach in a same way for an intersection node linking two paths. Afterwards, message packets are communicated towards the sinks route in the reverse order. They used a bloom filter for avoiding the repeating cycles.

   Tan et al. [42] proposed an approach for source location privacy using a directed random walk method, known as EDROW. Here, they allowed the message packets to be passed by sensor nodes denoted as parent nodes. These nodes are found near the sink. Different packets leads to generation of multiple routes. A large number of parent nodes leads to the better source location privacy in WSNs.

   The research on flooding approaches proposed by [31] was further explored for covering single routing based approaches by Kamat et al [18]. Kamat et al [18] concluded that existing single route based approaches are not able to source location privacy same as that of flooding based approaches. However, they extended the phantom based flooding approach and suggested a phantom routing. Here, a flooding phase is introduced that is replaced by a single path routing. They concluded an improvement of safety period for every message that is following different route to reach the sink. In this way, an attacker could not listen a steady stream of packets for traceback of source location.

Xi et al. [47] extended the concept phantom routing based approach in preserving source location privacy. They suggested for employing a two way random walk method and called it as Greedy Random Walk (GROW). The proposed approach starts the source node as well as sink node. It involves starting a random walk of the message from source node and in reverse direction from the sink node. When, the walks intersect, the message is sent in a direction opposite to arrive at the sink node. In order to enhance the intersection probability, the message packets are passes by local broadcast method. It ensures that all adjacent nodes should know the message forwarding.

Wang et al. [45] also extended the approach of random walk routing. They suggested a approach based on weighted random stride (WRS) approach and random parallel routing approach. Each sensor node is preassigned more than one different routes to the sink in Random Parallel routing approach. The route selection is made based on preset probabilities. However, in the WRS, each message follows a directed random walk to reach the sink. The walk consists of multiple strides.

Li et al. [24] attempted to enhance method proposed on basis of phantom routing. They noticed that pure random walk as well as directed random walk applied in case of phantom routing suffer from limitations. Pure random walk method attempts to remain close to source node. However, directed random walk method may cause leakage of sensitive information for location of the source. So, the authors suggested to forwards a message using single or multiple randomly selected intermediate nodes.

Ouyang et al. [30] suggested to trap an adversary in a false cyclical route for increasing the safety period. here, they proposed that many cyclical route are pre-created in WSNs. Fake messages begin circulating the route after crossing the real message by one of the cyclical route. In this way, backtracking of real messages leads to multiple cyclical paths to an attacker.

It can be concluded that most of the approaches based on random walks, flooding, path confusion, or multiple paths focused trapping the local attacker only. But, these approaches are vulnerable to global attackers having broader view of the WSN and its network flows.

3. **Fake source traffic based source privacy approaches:** The approaches proposed on fake source and dummy traffic for providing source location privacy works on the basis of hiding the real information packets and their source by fake information packets.

   Ozturk et al. [31] suggested an approach based on a short lived and persistent dummy source. The major limitation of this method is that it is not capable to source location privacy from a global attacker due to activation of the fake sources by real messages. So, the global attacker can find out initial source of information as the real source.

   Mehta et al. [29] suggested two types of protections as source simulation and periodic collection. The periodic collection provides privacy for source location at the cost of more latency and high communication over head. In this apporach, each sensor node is allowed to transmit regularly a fake or real message after a fixed time slot. It helps to conceal real messages with fake messages. The source simulation uses the dummy event of source nodes in WSNs. These dummy sources are formulated as per the conduct of the real sources for confusing the adversary. The major problem of the source simulation is that it does not simulate the source conduct accurately.

   Shao et al. [39] suggested an improvement of periodic collection as FitProbRate method to reduce its latency. Sensor nodes pass the message packets at pseudo random time slots than passing message packets at a fixed rate in a fixed time slot. Upon receiving real packet by sensor node, it pass message packet before fixed time slot. But, these pseudo random time slots follow the same distribution at all nodes for concealing information from an adversary.

4. **Cross-layer based source privacy approaches:** approaches in this category are important by considering the resource-constraint nature of WSNs. These approaches helps to ensure better services at nominal cost.

   Shao et al. [38] utilized IEEE 802.15.4 MAC layer beacons to ensure privacy of source location. Here, The beacons are broadcasted regularly by sensor nodes to declare some parameters. The authors proposed to use the beacons as a carrier of real packets. They followed principle for providing protection same as that of periodic collection [29]. But, it does not involve generation of fake

network traffic. The real message packets are concealed within the beacons. It is achieved at the cost of more latency due to sending of beacons in long time slots. Thus, the authors suggested two and four phase approaches. Two phase approach involves propagation of message packet in many hops by the beacons on MAC layer for ensuring privacy of source location. It is followed by delivery of message packet to the sink node by a single path routing through network layer.

2.3.1.2 Sink Location Privacy Approaches

Sink location privacy is significant for correct functioning of WSNs. The sink node accumulates information from the entire WSN and generally behaves as a gateway to other networks. Thus, it acts as a single point of failure. The adversary can launch several attacks upon discovering the sink location, thus rendering the whole network useless [7, 23]. Therefore, protection the sink location is very significant.

Deng et al. [7] proposed three approaches for analyzing network traffic to discover the sink location:

1. **Rate supervising attacks:** Here, an attacker observes sensor node packet sending rate and comes near to a sensor node with maximum rate.

2. **Content analysis attacks:** In this kind of attack, an attacker tries to access valuable data regarding sink location from message packet headers and packet payloads.

3. **Time correlation attacks:** In this case, an attacker supervises association between sending times of sensor node and its adjacent nodes. The attacker attempts to find our the node that passes the current message packet and traces the route directly to the sink.

They also proposed protection approaches to defend such attacks. For defending these rate supervising attack, each sensor node transmit message packets at a fixed rate. Thus, a child sensor node regularly sends a message packet till it is received by a parent sensor node. If the child sensor node has nothing to transmit, then it

adds a fake packet. This approach allows a regular transmission rate throughout the whole WSN. However, it reduces the lifetime of WSN. Cryptographic methods can be employed to preserve the sink against content analysis. But, end to end cryptographic methods are not up to the satisfaction [7, 23].

This work was extended by the authors using some advance methods to encounter the network traffic analysis based attacks [8]. The rate supervising attack can be avoided using multiple parent routing method as network traffic distributes in more than one routes. In this method, every sensor node consists of more than one parent sensor nodes for sending message packets to the sink. For sending a message packet, sensot node randomly find one of its parent sensor nodes. A controlled random walk method can be used to extend this method. A sensor node passes a message packet to one of its parent sensor nodes with probability p. The node passes the message packet randomly to one of its adjacent sensor node with probability $1 - p$. The proposed method presents delivery time delays proportional to additional hops consumed by the message packets. However, it has flaws for time correlation attacks.

To address this issue, Deng et al. [9] proposed an approach known as multi parent routing method with fractal propagation. Whenever a sensor node comes to know that an adjacent node passes a message packet to the sink, then it creates a dummy message packet with probability p and moves it to one of its adjacent node. The major issue here is that it creates huge amount of network traffic near the sink. Because, sensor nodes close to the sink generally pass more message packets.

It is observed that that these approaches offered to provide sink location privacy against the local attacker. Few approaches target the global attacker.

It is noticed from the analysis of literature that some approaches originally proposed for source location privacy protection are also applicable for providing sink location privacy [31, 38, 39, 49].

2.3.2 Temporal Privacy

Temporal privacy is concerned with significant contextual information being derived by an external attacker. It contains the timing information of supervised events or a message rate. An attacker may use temporal information for localizing the object under supervision. Based on the time and place of the packet generation, the attacker can approximate movement of the object.

Kamat et al. [16] formalized the problem of temporal privacy. They suggested an approach based on rate controlled adaptive delaying (RCAD) to preserve temporal privacy. Here, each node stores received message packet and randomly holds its transmission again as per the exponential distribution. Stored preemption approach is involved to handle the issue of overloaded storage. Whenever the storage of sensor node becomes full, sensor node sends the message packet instantly [17].

It can be concluded that such methods for preserving location privacy in WSNs have the great potential to ensure temporal privacy. Specifically, the methods suggested using random walks and time delays. It can also be found that periodic collection method that transmitting at a constant rate in the entire network, provides optimal temporal privacy. Because, in this case network traffic is not dependent of the happening of events.

2.4 Key Findings

Recently, several approaches have been proposed for preserving network privacy in WSNs. An updated review of network privacy and various approaches proposed to address the problem of network privacy are presented in Section 2.2 and 2.3. The review of above cited text can be summarized as per identified taxonomy (refer Fig. 2.1) in Table 2.1.

By critically analyzing state of the art in the field of privacy of source location in WSNs, Followings are the key findings.

TABLE 2.1: Overview of literature review.

	Protection type			**Approach**	**Research work**
Privacy in WSN	Content	-	-	-	[24] [33] [40]
	Context	Location	Source Location	Flood based	[5] [14] [16] [23] [28] [32]
				Random walk based	[19] [25] [31] [43] [46] [48] [49]
				Fake source traffic based	[30] [32] [40] [50]
				Cross layer	[30] [40]
			Sink Location	-	[8] [9] [10] [32] [40] [50]
		Temporal	-	-	[17] [18]

1. A majority of the approaches have not considered the impact of the source location privacy protection approach on the performance of the network's lifetime.

2. Some of the researchers proposed public key based encryption approaches for source location privacy protection approaches. These approaches are highly computationally and communication expensive. So, these approaches are not suitable for source location privacy protection approaches.

3. Broadcasting based source-location protection approaches are found to be energy inefficient.

4. Routing based approaches for preserving source location may cause leakage of information of source location to an attacker.

To address these limitations, this research work aim to propose a routing based approaches that enhances source location privacy in WSNs without affecting the network lifetime.

2.5 Summary

This chapter presented an updated review of the main contributions of network privacy protection approaches and the principal trends in this research field. It presented an overview of types of network privacy approaches that were used to successfully provide privacy, particulary source location privacy. Various privacy protection approaches utilized in WSNs are summarized. Finally, the chapter highlights the key findings of literature review and major research gaps in the current source location approaches, that motivate us to propose a routing based approach for enhancing privacy of source location in WSNs without affecting network lifetime.

CHAPTER 3

The Proposed Source Location Privacy Preserving Approach

Recently, several approaches have been proposed to preserve source location privacy in WSNs on the basis of routing [6, 27] and fake traffic [29, 31]. These approaches enables the concealment of source location in WSNs if properly used. However, most of existing approaches are energy inefficient or computational intensive [26, 31].

To address the limitations of existing approaches, this chapter introduces the proposed an approach for preserving source location privacy in WSNs on the basis of dynamic routing and injecting fake message packets in the network in Section 3.1. The proposed approach is an enhancement to that of proposed in [15]. It highlights the basic assumption about network, power consumption and underlying network in Section 3.2. It presents the proposal of dynamic routing based approach for enhancing source location privacy in WSNs in Section 3.3 after explaining various types of routing patterns. It highlights the working of the proposed approach in Section 3.4. Finally, it summarizes the content of this chapter in Section 3.5.

3.1 Introduction

Recently, several applications in the field of monitoring and tracing have evolved with the advancement of Wireless Sensor Networks (WSN). These applications involve distributed sensor nodes (SNs) for monitoring of the limited area around it and communicate the events to a fixed location called Base Station (BS). Many real time applications like surveillance, health, military have successfully deployed SNs for monitoring for specific events. However, some mission oriented applications like military require security of information for transmitting information from SN to BS [15]. Privacy is considered as significant aspect of security, and plays a vital role in protecting sensitive information. However, the open nature of WSN enables the attackers to intercept the information during transmission. An attacker can use powerful radio transceivers to intercept the information and attack the network. Due to this flaw, WSNs, suffer from different privacy threats like data fabricating, route disrupting, information eavesdropping, and node compromising. Concealing the location of SSN is a critical problem in WSN that requires immediate addressing. Many source location privacy approaches have been proposed in WSNs on the basis of routing [6, 27] and fake traffic [29, 31]. These approaches enables the concealment of source location in WSNs to some extent. However, most of existing approaches are energy inefficient or computational intensive [26, 31].

In this work, we propose a dynamic routing based approach for preserving the source location privacy in WSNs to address the limitations of existing approaches. The proposed approach address the source location privacy by considering the limited features of WSNs like power backup, lifetime, transmission delay etc. The proposed approach contributes in two aspects. Firstly, it considers enhancing the security of SSNs with minimal transmission delay and consumes power with minimum effect on the lifetime of the network. However, existing researches in the field focused on one aspect without considering the other. Secondly, the proposed approach is designed to defend most commonly used attacks like hop-by-hop, directional attacks by choosing a suitable path to send information from SSN to BS dynamically without affecting network life significantly. Thus, it becomes difficult for the attacker to find the exact path, and hence the original location of SSN.

3.2 Basic Assumptions

The proposed approach aims to address the issue of preserving source sensor node privacy in Wireless Sensor Network (WSN) by transmitting the information from source sensor node (SSN) to a base station (BS) through a dynamically selected path. It increases the number of paths for transmitting the information from SSN to BS, thus enhancing the security of location of SSN without compromising network life, and delay in the transmission of information. It is robust against the most commonly used attack approaches by the attackers to access the location information of SSN, namely hop-by-hop tracing, eavesdropping, and direction based tracing. For implementation of the proposed approach in this work, we consider following assumptions in regard to power consumption, WSN, and attacker.

3.2.1 Power Consumption Related Assumptions

Power consumption is assumed to be a significant measure for accessing the performance of any routing approach as sensor node exhaust power during the reception and transmission of network packets in WSN. It has been observed that the sensor nodes in the surrounding area of BS called hotspot area (HA) exhaust more power in comparison as they have more interaction for communication with BS. Thus, their power consumption directly affects the lifetime of WSN. So, an efficient routing approach must cause a minimum power consumption of hotspot sensor nodes to enhance the lifetime of the WSN.

In this work, we consider the power consumption by the sensor nodes while receiving data in WSN as described in Eq. 3.1 as proposed in [26, 45].

$$P_{receive} = L * P_{loss} \tag{3.1}$$

where, L represents the length of the received data in number of bits and P_{loss} gives a loss of power during transmission. Power consumption for transmitting the data can be represented as per Eq. 3.2.

$$P_{transmit} = L * (P_{loss} + P_{amp} * AmpPLoss) \tag{3.2}$$

where, AmpPLoss is a factor that represents the amplifier power loss. It depends upon the distance between transmission sensor node and receiving sensor node. It follows the free space model (d^2 amplifier power loss) for distance between transmission sensor nodes and receiving sensor nodes below the threshold value of $d_{threshold}$, otherwise it follows the multi-path fading model (d^4 amplifier power loss). P_{amp} represents power required for amplifying the signals. The values for these parameters are adapted from [46] as $d_{threshold}$, P_{loss}, P_{amp} for free space model, and Pamp for multi fading model 87m, 50nJ per bit, 10pJ per bit per m^2 and 0.0013pJ per bit per m^4 respectively.

3.2.2 WSN Related Assumptions

In this work, we assumed the deployment of WSN on the basis of classic and well known panda-hunter game model [24] that involves monitoring of the sensor area and detects the presence of pandas. Detection of the panda's activity in sensor area triggers the sensor node to act as SSN and transmit encrypted information to BS. However, the open nature of WSN can lead attackers to intercept the information during transmission and access the location information of pandas. Thus, the objective of routing approach should be to transmit the information of pandas in such a way so that the location of pandas may be preserved from the attackers.

So, for simplicity and successful implementation of the proposed approach, we assume that WSN contains uniformly distributed and interconnected sensor nodes having limited power backup. Further, the whole WSN is configured as grids and rings of sensor nodes as shown in Fig. 3.1. The each sensor node is assigned a grid number, and ring number. The sensor node having highest power backup act as a leader node (LN) and is responsible for communicating with adjacent LNs in an encrypted mode to reach the BS. The power consumption of sensor nodes in a grid is regularly updated.

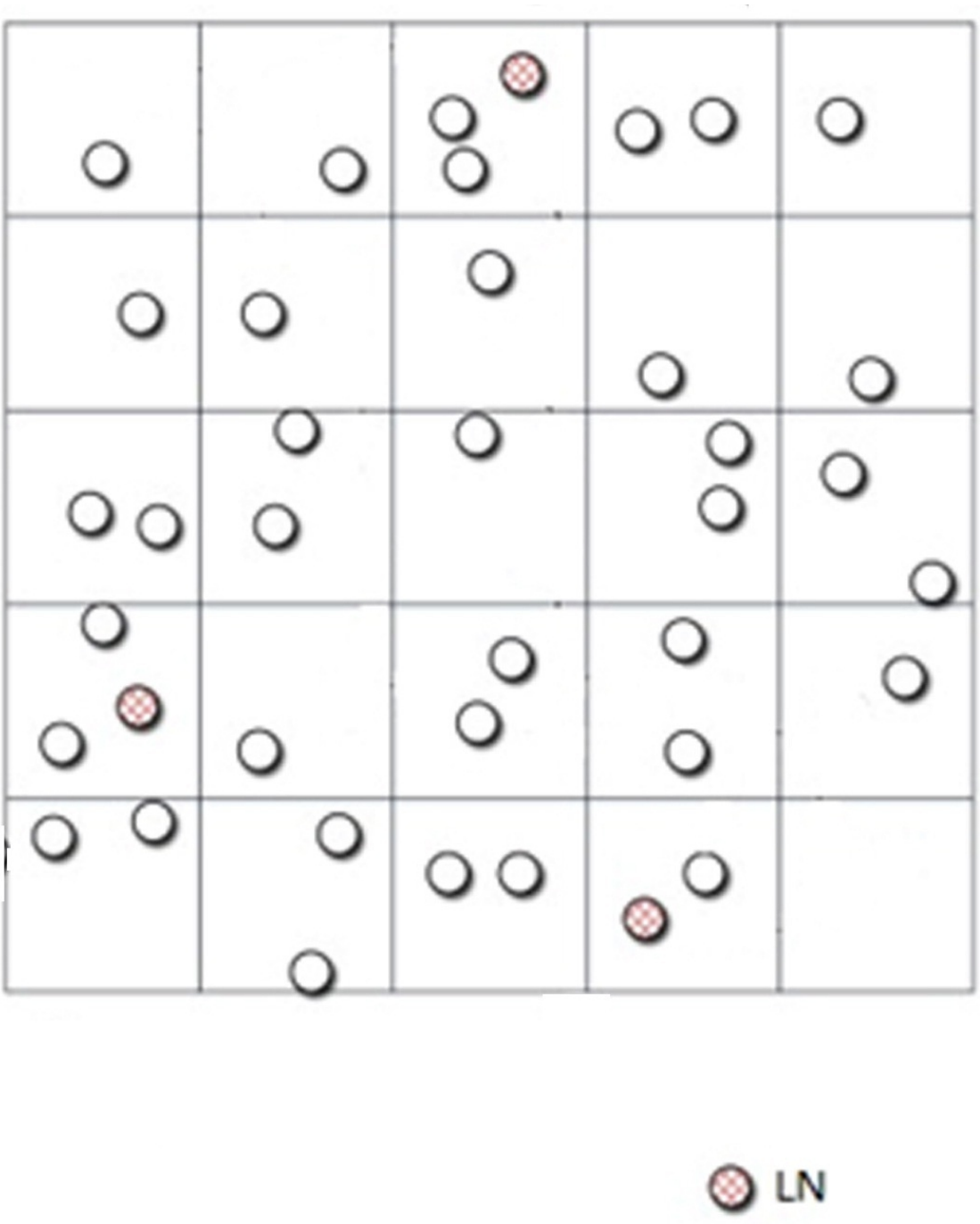

FIGURE 3.1: The topology of WSN

3.2.3 Attacker Related Assumptions

The attackers generally sniff and analyze the network traffic with some advance approaches and attempt to find the source location. They are well equipped with advance hardware / software, huge amount of power backup and computing as well as storage capacity. They can easily eavesdrop the WSN for accessing the source location information without affecting the normal functioning of the WSN. They can also compromise or damage the network communication. Even, the attackers are capable of tracing the source location using hop-by-hop strategy. In addition, they can reuse the historical information related to specific sensor nodes, traffic flow to estimate the direction of location of SSN using a backtracking strategy called direction oriented attacks.

3.3 The Proposed Approach

The proposed approach involves the dynamic routing of network information transmitted from SSN to BS with an aim of preserving the source location privacy without compromising the lifetime of WSN and delay during transmission of information. We propose a dynamic 2-phase routing approach. The phases are

1. Initialization phase
2. Switching phase

The first phase involves selection of start node to initialize the routing process. In the second phase, it undergoes switching in three different types of routing patterns as below.

1. Estimated Routing (ER)
2. Cyclical Routing (CR)
3. Directional Routing (DR)

The information from SSN to BS is transmitted by switching it in different paths using proposed routing algorithms dynamically with an aim to confuse the attacker about the exact path of real information flow. In this way, the proposed approach attempts to hide the location of the real source node from the attacker. Thus, the proposed approach involves the transmission of some dummy information packets into the network to enhance the privacy of the source node location.

The results of the proposed approach prove an enhancement in security level in preserving the location of SSN, reduction in transmission delay, without affecting network lifetime in comparison to the existing researches in the field. The details of routing algorithms are as described below.

3.3.1 Estimated Routing (ER)

This type of routing involves transmitting the information to the pre-determined paths in WSNs [13]. ER is mostly useful for the applications with limited power backup like WSNs. It comprises flooding of information to measure the distance between sensor nodes and BS in terms of number of hops initially. BS starts the process of flooding in the beginning of network configuration and floods the information packets with the hop counter set to zero. Each packet is made to pass through each node and accordingly its counter is incremented. Each sensor node records the hop count value for different packets following different paths. At the end of the initial process, each sensor node selects the path having less value for hop counter. Thus, ER transmits the information to a path having less value of hop counter to reach the BS.

3.3.2 Cyclical Routing (CR)

In this work, we increased the amount of time required by the attacker for tracing the real source location through analysis of the network traffic by proposing a cyclical routing [13, 15]. As discussed in the preceding section, the WSN is assumed to be divided into grids having LNs responsible for communication with adjacent LNs to reach the BS as shown in Fig. 3.1. Each LN will receive the information packet

and analyze it for representing the real event of the network. It then forwards adjacent LNs in both clockwise as well as counterclockwise directions. Adjacent LN stores the real information and releases fake information packets. Following this way, the information packets will make a round journey in the cyclical path as depicted in Fig. 3.2.

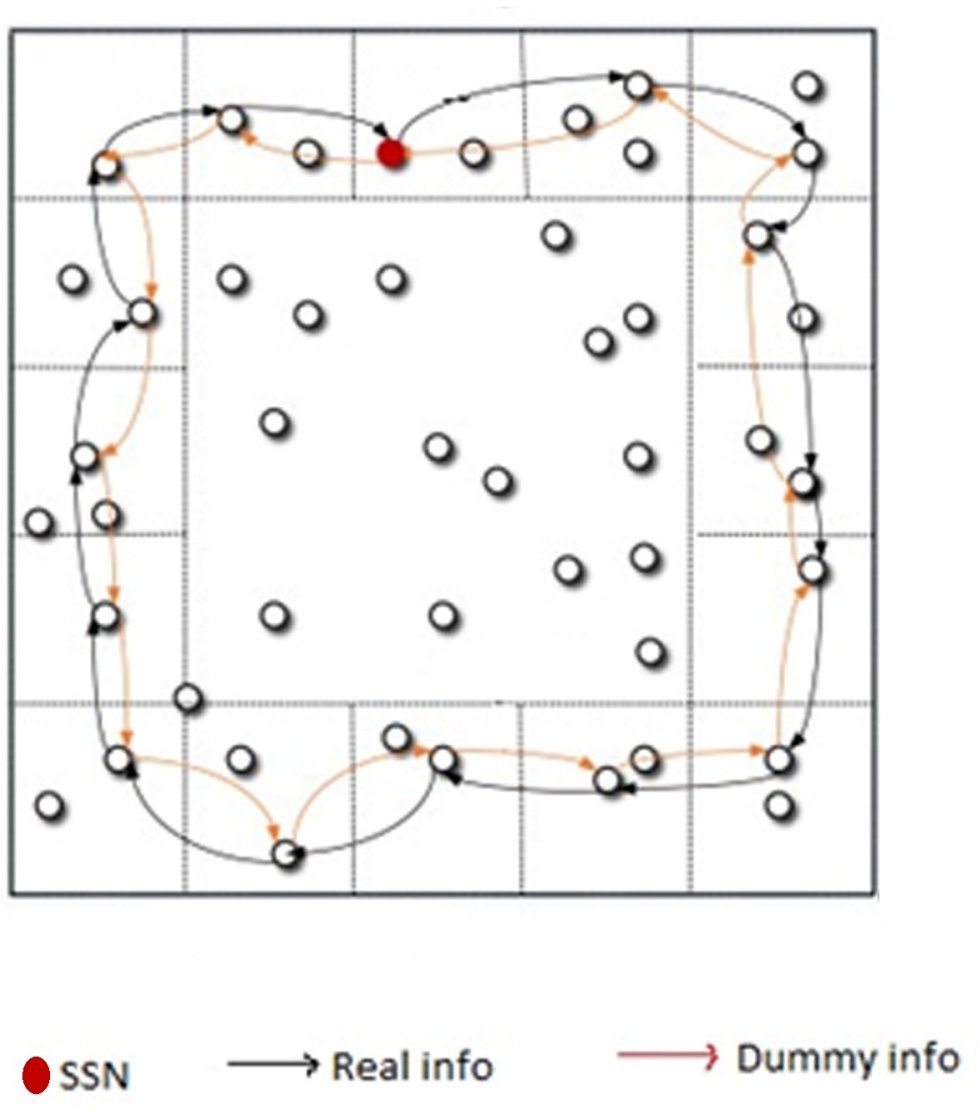

FIGURE 3.2: Cyclical routing

3.3.3 Directional Routing (DR)

This routing involves the routing the information packets inter grids in a direction of BS through adjacent LNs [13]. Further, the adjacent LN after receiving the packet

follows the same process and forward the packet to its adjacent LN in direction to BS as depicted in Fig. 3.3. Thus, DR generates multiple routes for reaching BS and leads to attract the attacker to some specific route that is not actually used for transmitting real information from SSN to BS. It makes the back tracking attack more difficult for finding the location of SSN.

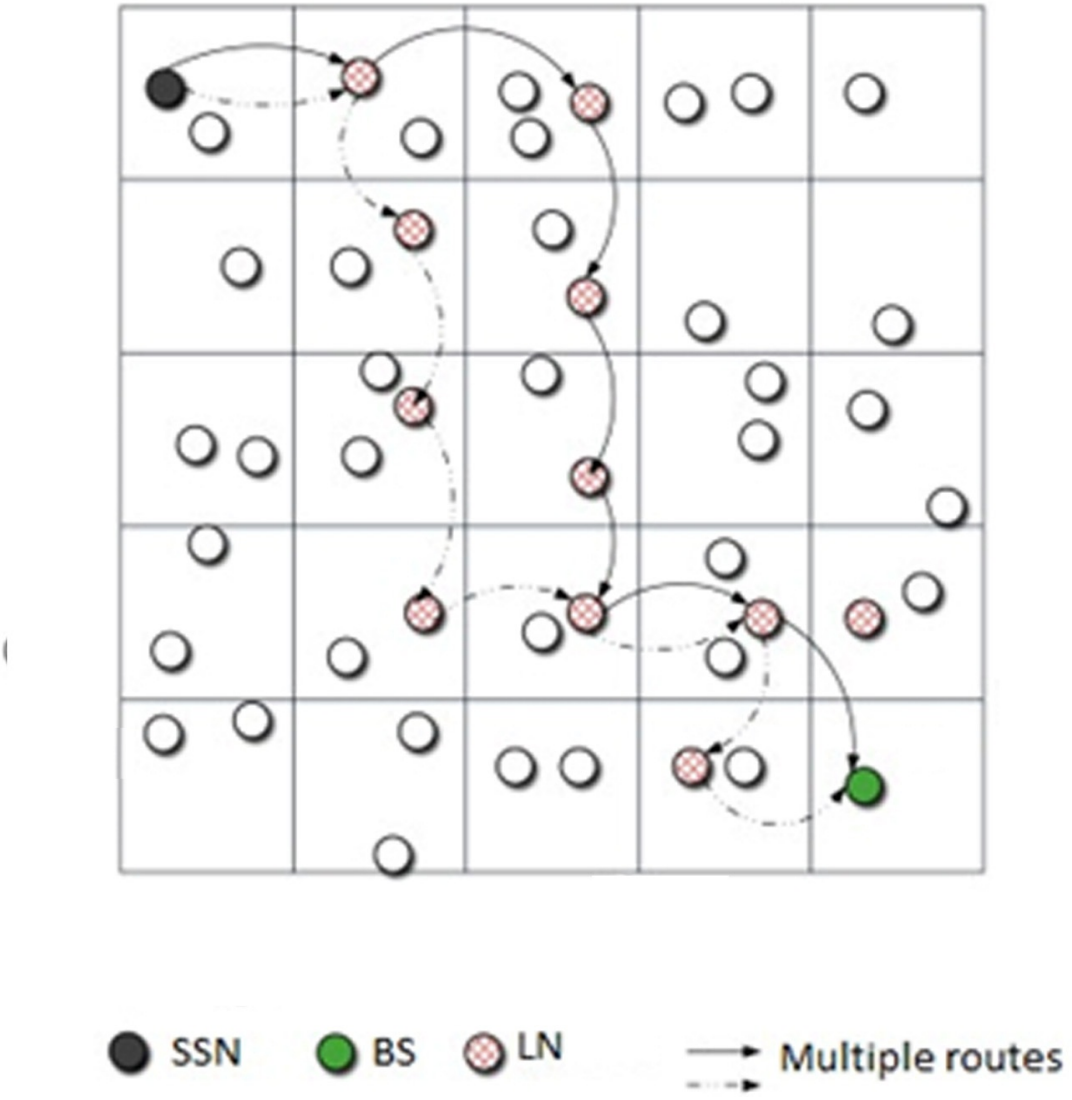

Figure 3.3: Directional routing

3.4 The Working Principle of the Proposed Approach

The proposed approach involves injection of fake message packets in addition to real message packets and packets are transmitted to BS by switching among different routing patterns based upon conditions. The routing patterns are cyclic routing, directional routing and estimated routing. In brief, the proposed approach consists selecting a random starting sensor node for injecting an empty packet using the ER approach initially. Meantime, the message packet from a SSN is circulated into rings using CR approach, followed by DR approach transmission of real packet from the intersection point of empty packet and the ring. This results into a selection of different route for each transmission of the real message packet, hence it becomes difficult for an attacker to guess the exact location of SSN using backtracking attack.

The working principle of the proposed approach is completed in two stages, namely, 1) **Grids and rings segmentation** and 2) **path formation**. The phases of the proposed approach are graphically presented in Fig. 3.4 and are described in Section 3.4.1 and 3.4.2.

3.4.1 Grids and Rings Segmentation Phase

The WSN is assumed to be segmented into grids and rings as depicted in Fig. 3.1. There exists a leader node (LN) in each grid having a maximum power backup in comparison of other nodes in that grid. Power backup values are regularly updated in the grid. If there is any other node having more power backup than LN, then it is selected as LN. All the information packets from the grid nodes are transmitted through LN. Each sensor node of WSN retains its grid position in the network.

Rings are formulated in the area after the hotspot area on the basis of its distance from the BS. Ring is the established path of LNs at a given distance from BS followed by message packets in a logical circular shape as shown in Fig. 3.2.

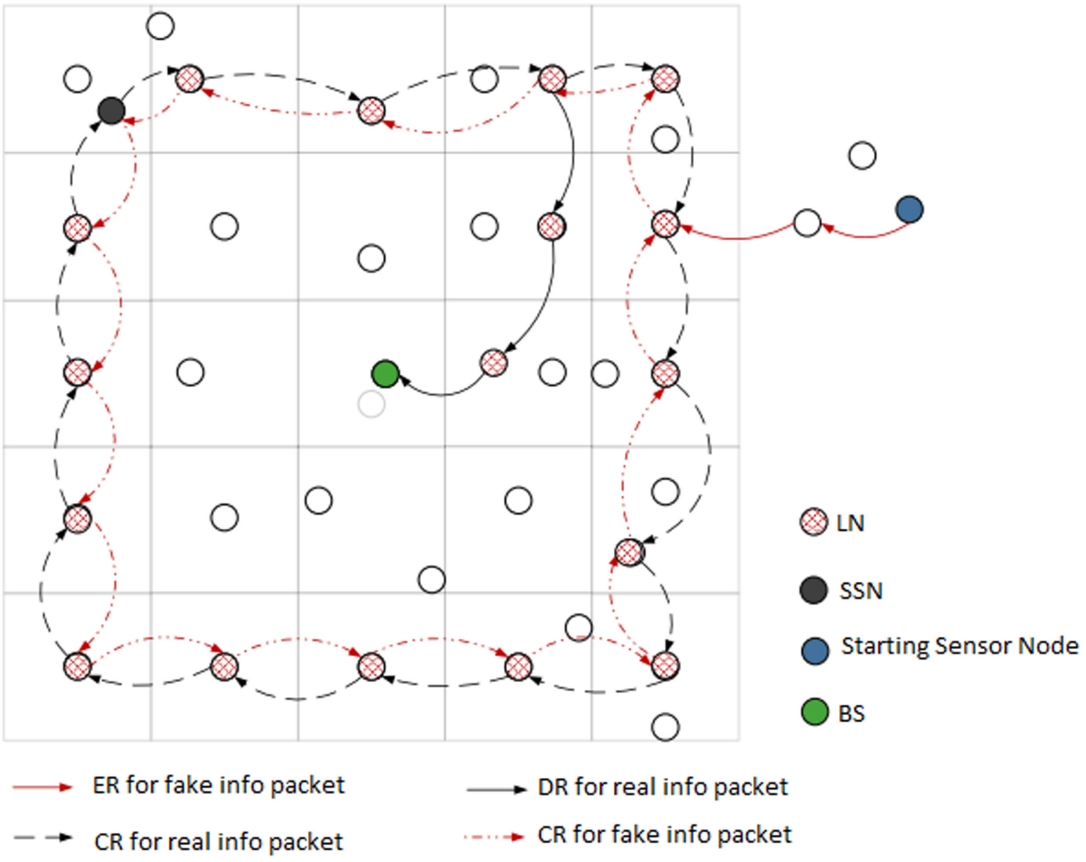

FIGURE 3.4: The proposed dynamic routing approach

Formulation of rings helps to generate cyclically routing in the area after hotspot area. The real message packets are forwarded in a clockwise or anti clockwise direction selected randomly and fake message packets are forwarded in the opposite direction to that of real message packets by the LNs of that ring. After the formulation of rings, each sensor node is assigned a ring number. The values of grid position and ring numbers of the sensor nodes are shared adjacent sensor nodes. In this way, each sensor node maintains a list of adjacent nodes consisting of nodes having 1) lesser number of hops to reach BS, 2) large number of hops to reach BS, 3) adjacent nodes in all directions of the grid.

3.4.2 Path Formation Phase

In the beginning, we propose to choose a sensor node from the outermost ring as start sensor node of the path by adapting token approach mentioned in [35].

The principle for token approach is that if a node has information to transmit, it will claim the token. The node is allowed to transmit only after taking control of token for a fixed time interval. The start sensor node circulates the token after holding it for a specific time interval. The same process is repeated by the next token grasping sensor node. The starting sensor node creates a fake empty packet, and forwards to the other node by following ER approach. During the transmission of the fake information packet, if any sensor node finds some real information to transmit to BS, like information of Pandas, then it becomes SSN. The corresponding ring is assigned as leader ring (LR). The SSN creates information packet over LR in any one direction selected randomly.

Simultaneously, SSN creates a fake information packet and forward in the opposite direction of real information packet over LR. All LNs of LR receive the information packets, fake as well as real. They retain a copy of the real information packet and discard the fake information packets. In this manner, a copy of the real information packet gets stored at each LN in the LR. In this way by following CR approach, each LN on LR has a copy of the real message packet and is able to transmit to BS on behalf of SSN. Whenever the empty information packet already routed using the ER approach by the starting node intersects the LR, and then corresponding LN of that intersecting grid replaces the empty packet with the real information packet. The replaced real information packet is transmitted to BS using DR approach.

Since, we are selecting a starting sensor node randomly, then it will intersect the LR at different points for each transmission of the message packet to BS. Thus, it will make difficult for the attacker to guess the real location of SSN. The whole dynamic routing approach is depicted in Fig. 3.4.

3.5 Summary

Recently, several applications in the field of monitoring and tracing has evolved with the advancement of WSN. These applications involve distributed sensor nodes

(SNs) for monitoring of the limited area around it and communicate the events to a fixed location called Base Station (BS).

However, some mission oriented applications like military require security of information for transmitting information from SN to BS. Privacy is considered as significant aspect of security, and plays a vital role in protecting sensitive information. But, the open nature of WSN enables the attackers to intercept the information during transmission. An attacker can use powerful radio transceivers to intercept the information and attack the network. Due to this flaw, WSNs, suffer from different privacy threats like data fabricating, route disrupting, information eavesdropping, and node compromising. Concealing the location of SSN is a critical problem in WSN that requires immediate addressing.

Recently, several approaches have been proposed to preserve source location privacy in WSNs on basis of routing and fake traffic. These approaches enables the concealment of source location in WSNs if properly used.

This chapter introduced the proposal of a dynamic routing approach for preserving source location privacy in WSNs without affecting network lifetime. It highlighted the basic assumption about network, power consumption and underlying network. It also presented various types of routing patterns used in the proposed approaches. Finally, it highlights the working of the proposed approach.

CHAPTER 4

Implementation and Experimental Evaluation

This chapter presents the implementation details and experiment results of the proposed approach in comparison to the existing approaches in the field.

Here, Section 4.1 introduces performance metrics briefly for measuring performance of the proposed approach used in this set of experiments. The working of the existing approaches and their imitations are described in Section 4.2. Section 4.3 highlights the metrics used for measuring the performance of the proposed approach. Section 4.4 provides the description of the evaluation of the proposed approach in terms of identified metrics including experimental setup and initialization values in Subsection 4.4.1 followed by experiment results in Subsection 4.4.2. The discussion of the results is provided in Section 4.5 at the end of this chapter.

4.1 Introduction

New approaches are generally validated by measuring their performance in terms of defined performance metrics by comparing them with the existing approaches.

As per updated literature review presented in Chapter 2, it is observed that most of researchers have measured performance of their approaches for preserving source location privacy in WSNs in terms of metrics, namely, Power consumption, Transmission delay, Safety period (Security level) and Network lifetime. So, keeping this into consideration, we measure the performance of our proposed approach as well as existing approaches in terms of these identified metrics under similar experimental setup environment. The results are further compared to validate our proposed approach in the field of source location privacy of WSNs.

4.2 The Existing Approaches for Comparative Analysis

The proposed dynamic routing approach is implemented in MATLAB for proving its validity in the field of source location privacy in WSNs along with the approaches proposed by Chen et al. [6] and Jhumka et al. [15]. The reporting results are compared in terms of identified performance metrics. The details of these approaches can be refereed in Chapter 2 Section 2.3.1.1.

In this thesis, we proposed a dynamic routing approach that randomly initializes a starting node and switches different routing patterns on the basis of certain conditions as described in Chapter 3. The proposed approach addresses the limitations of Chen et al. [6] and Jhumka et al. [15] by enhancing security level for preserving location of SSN without compromising network lifetime, transmission delay and power consumption.

We performed a set of experiments to validate the proposed approach. The results are compared and analyzed against the results proposed by Jhumka et al. [15] and Chen et al. [6] in terms of the most important performance metrics for WSNs, namely, Power consumption, Transmission delay, Security level, and WSN lifetime. The comparative analysis of the results indicates that the proposed approach has provided comparable results to that of Chen et al. [6] with an enhanced security level, comparable transmission delay & network lifetime at the cost of total power consumption. It can also be concluded from the results that the proposed

approach has provided improved results than Jhumka et al. [15] by enhancing security level in preserving location of SSN, decreasing the network transmission delay and still maintaining lifetime of the WSN at the cost of more power consumption from non hot spot area. Thus, the reporting results validate the proposed approach for preserving the location of SSN in WSN.

4.3 Evaluation Metrics

The design of WSN is a challenging task as due to consideration of many influencing factors like scalability, operating enlightenment, network topology, power consumption, safety period, transmission latency and many more. The network performance is measured in many qualifiable performance metrics known as performance metrics. The selection of performance metrics for measuring the performance of WSN depends upon need and nature of application of WSNs.

In this work, we measure the performance of network in terms of most commonly used metrics as described below [13, 15].

4.3.1 Power Consumption

Power consumption is an important metric to evaluate the performance of an approach [13]. The amount of power consumed in hot areas has a direct impact on the lifetime of the whole network, since nodes near the sink must act as intersections to relay all the data packets. Sensor nodes consume energy when receiving or transmitting packets.

4.3.2 Security Level

The Security level (also known as safety period) is defined as the safety period from the time that an adversary starts to eavesdrops on the first packet in the network to the moment when the adversary successfully captures the real source.

4.3.3 Transmission Delay

It measures time to send and receive a unicast packet from one node to another. In WSN, it is delay in data collection from nodes to BS and its interpretation.

4.3.4 WSN Lifetime

Lifetime of network exhibits the number of rounds in simulation experiments that determines the longevity of the nodes. It is considered as crucial aspect for utilization of power in WSN. We define network lifetime as the period from the start of the WSN to the moment when the first node is out of power [13].

4.4 Experimental Evaluation

4.4.1 Experimental Setup

In this work, we implemented the proposed approach in MATLAB for analyzing its performance in comparison to the existing approaches, namely, [6, 15]. Chen et al. [6] proposed a routing based approach without considering protection of the source nodes. Whereas, Jhumka et al. [15] proposed an approach that uses a cyclic entrapment to confuse the attackers. We simulated the proposed approach by deploying sensor nodes in the square shaped region with initial parameters, namely, Sensor nodes, Network radius, Transmission range, and Data bits in a message are taken as 2000, 500m, 45m, and 100 bits respectively. Nodes are assumed to be uniformly distributed over the entire network. Location of BS is assumed to be fixed at the center of the region.

4.4.2 Experimental Results

In this section, we computed the results of the proposed approach and compared them with identified approaches in terms of Power consumption, Transmission delay, Security level, and WSN lifetime as described below.

4.4.2.1 Power Consumption

We computed power consumption of sensor nodes (in $10^{-6}J$) for different amount of distances (in m) from SSN to BS in our experiments. The reporting results are depicted in Fig. 4.1. It can be observed that Chen et al. [6] approach consumes minimum power in comparison to the other approaches. This is due to that their approach follows a shortest path to transmit information packets without injecting any fake packet into the WSN. Whereas, Jhumka et al. [15] reported more power consumption in comparison to Chen et al. [6]. Because, the authors inject a large number of fake information packets into the WSN for protecting source location and follows the cyclic defense. The power consumption of our proposed approach is highest among them as we also propose to generate and inject more fake information packets to confuse the attacker in the outer rings after the hotspot area. The proposal of circulating fake message packets in the outer rings leads to the consumption of power from outer ring nodes only, and has no affect the power consumption of hotspot area nodes. Hence, the lifetime of the network of our proposed approach is comparable to that of Chen et al. [6] and Jhumka et al. [15], with enhanced security level of preserving the location of SSN.

It can also be noticed from Fig. 4.1 that power consumption increases with increasing the distance between SSN and BS as more number of sensor nodes are involved in forwarding information packets of LR. As the number of rings changes, the power consumption also varies. We computed the total power consumption by varying the number of rings. The reporting results are depicted in Fig. 4.2.

It can be observed from Fig. 4.2 that Chen et al. [6] approach resulted in less power consumption in comparison to the other approaches. The power consumption to the 4 number of rings is least.

4.4.2.2 Transmission Delay

Fig. 4.3 provides a comparison of transmission delay of network packets using different approaches employed in this work. It can be noticed from the Fig. 4.3 that the delay is more in case of the approach proposed by Jhumka et al. [15] than

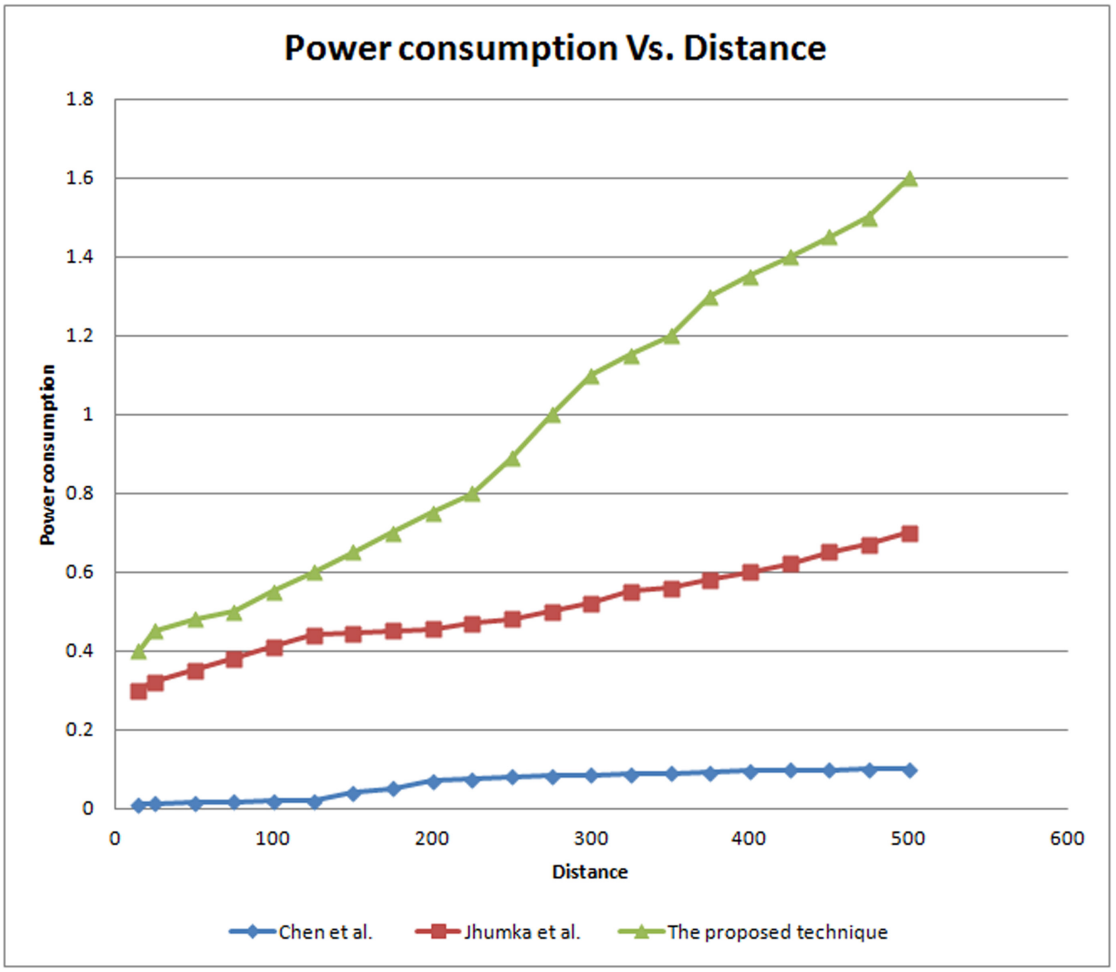

FIGURE 4.1: Power consumption Vs. Distance

our proposed approach and Chen et al. [6]. This happened due to that inter cluster communication and cyclic routes increase the delay in transmission. But, such trend is not reported by our proposed approach as packets do not move through cyclic paths. The message packets switch between different routing patterns and this leads to reduce the transmission delay in comparison to Jhumka et al. [15]. The reporting results of our proposed approach are comparable to that of Chen et al [6] with more security level in preserving the location of SSN. Thus, it proves the applicability of our proposed approaches for applications requiring low transmission delay.

4.4.2.3 Security Level

In this part of our work, we measured the network security level, also called safety period for the identified approaches and our proposed approach. In this work, we

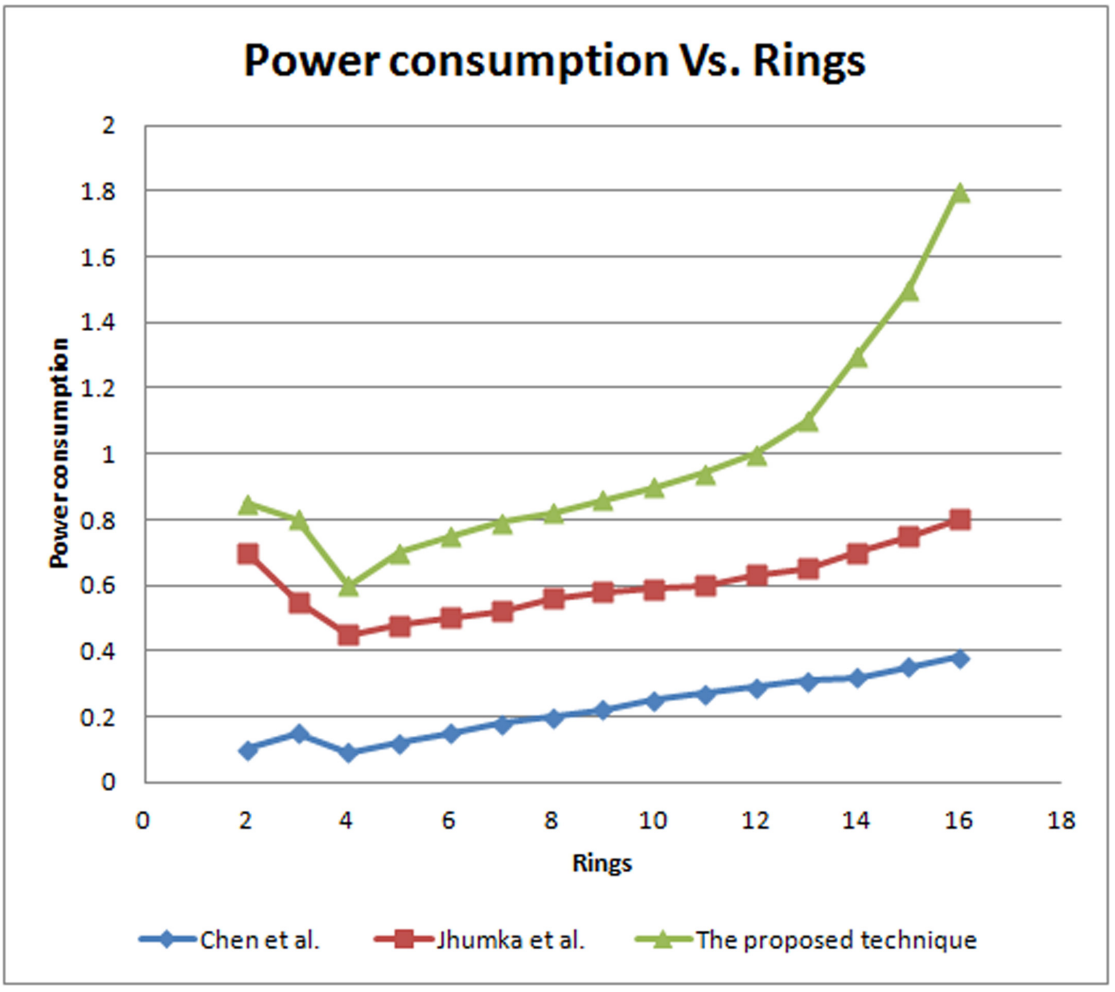

FIGURE 4.2: Power consumption Vs. Rings

propose to measure security level in terms of number of hops that an attacker has to traverse in accessing the source location. The comparative results are depicted in Fig. 4.4. It can be observed from Fig. 4.4 that security level is directly proportional to network scale. Comparative results indicate the better security offered by our proposed approach with respects to the identified approaches protecting source location privacy in WSNs.

Because, we injected a number of fake message packets to confuse the attacker regarding location of the real source to BS. The real message packet is transmitted to the BS by following different routing patterns and it becomes difficult for the attacker to back track the real source location. Thus, the proposed is robust to handle back track attacks effectively. In case of the Jhumka et al. [15] approach, it is easy for an attacker to identify LR as backbone path followed is the shortest path. However, in our proposed approach, starting node get regularly changed, resulting

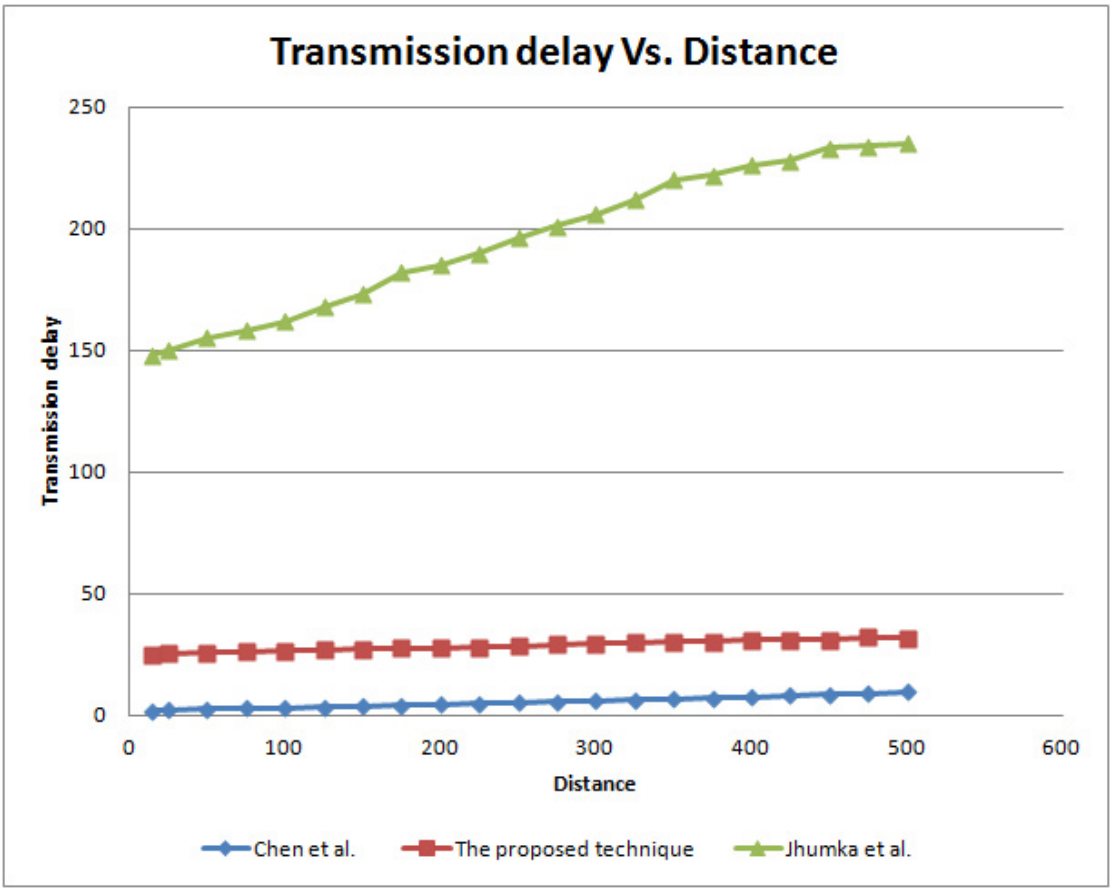

FIGURE 4.3: Transmission delay Vs. Distance

change in new path. Thus, it makes difficult for an attacker to guess the real location of SSN. In a nutshell, the proposed approach leads to enhanced security level in comparison to Chen et al. [6] and Jhumka et al. [15].

4.4.2.4 WSN Lifetime

The comparative results in terms of network lifetime for our proposed approach as well as identified approaches are presented in Fig. 4.5. WSN lifetime is dependent upon the power consumption of sensor nodes in the hotspot area surrounding BS. Since, no approach is generating any fake information packet in hotspot area, so there is no effect on the WSN lifetime.

No doubt, our proposed approach consumes more power in comparison to that of Chen et al. [6] and Jhumka et al. [15]. But, it consumes from the outer sensor nodes after the hotspot area. So, there no significant impact of more power consumption on WSN lifetime as presented in Fig. 4.5. Consequently, the proposed

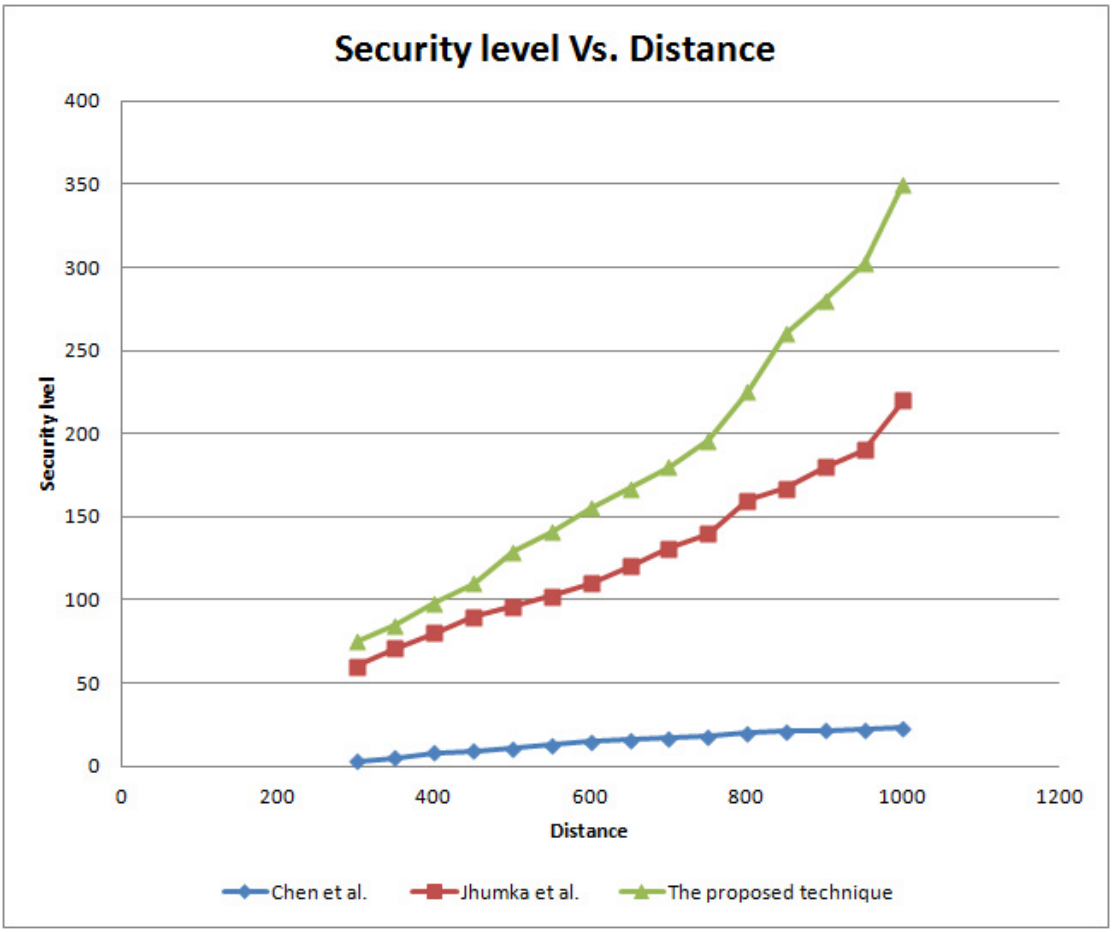

FIGURE 4.4: Security level Vs. Distance

approach leads to comparable network lifetime with the additional security level in preserving the location of SSN.

4.5 Summary

This work an in depth investigation of the source location privacy problem in WSNs and proposes an energy efficient and secure approach for preserving source location privacy against the most commonly used attacks like hop-by-hop tracing, and directional attacks. The proposed approach handles the problem by considering different aspects of WSN like limited power backup, network life, limited memory, limited computing power, and transmission delay into consideration.

It involves choosing a path dynamically for transmitting a message packet from SSN to BS and generation of fake message packets. The transmission process is started from a node located in outer area using ER with an empty packet,

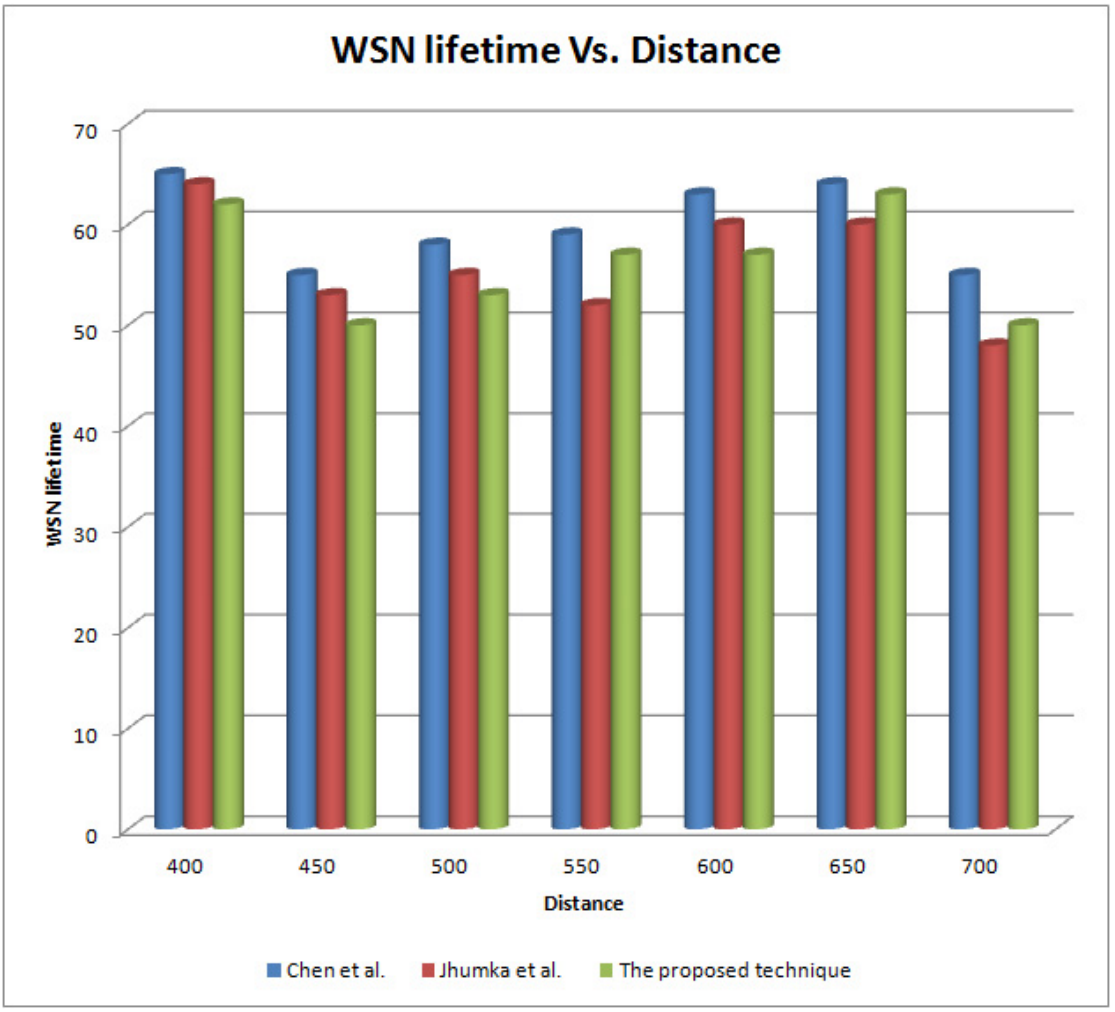

FIGURE 4.5: WSN lifetime Vs. Distance

then later on some fake packets as well as real message packet are injected into the network. The real message packet reaches the BS by following a path dynamically selected using CR and DR. The injection of fake packets and dynamic selection of path confuses the attacker for the exact location of SSN, and hence preserve the source location privacy. In addition, fake packets are injected and routed mostly in the rings lying after the hotspot area. Thus, it consumes the energy of non hotspot area nodes, and hence minimal effect on network lifetime.

The simulation results indicate that there is minimal effect on transmission delay in comparison to the other approaches in the field. The comparative analysis of the results of the proposed approaches and that of other existing approaches proves that the proposed approach is better and more practical in terms of Network lifetime, transmission delay, and security level in preserving source location privacy. The proposed work is based upon some basic assumptions of attacker model.

In our future work, we plan to extend this work by considering a global attacker model equipped with powerful devices and approaches. We also plan to investigate the impact of different network topologies on the efficiency of the proposed approach and considering multiple attackers.

CHAPTER 5

Conclusion and Future Research Scope

5.1 Summary

The aim of the present study is to propose a dynamic routing approach for preserving the source location privacy. The proposed approach involves injecting the fake packets into the network and switches the real information packets between different routing patterns based on certain conditions. This results in confusing the attackers from accessing the source location in WSN, and hence enhances the source location privacy without compromising network lifetime.

Chapter 1 provides the importance and use of WSN in different application domains. The need for preserving the source location in WSN is highlighted. The chapter also contains problem statement and objectives of the thesis. Finally, it presents the structure of thesis to meet its objectives.

Chapter 2 provides the brief information about present study and literature survey of existing research in the field. It investigates main contributions and the principal trends in preserving network privacy of WSNs. It presents an overview of

taxonomy of network privacy and further presents state of the art with respect to the privacy taxonomy. Different studies in the field are summarized as per taxonomy in tabular form for better understanding the current status of source location privacy approaches in WSNs. Related issues and major limitations of existing researches in the field are highlighted at end of this chapter.

Chapter 3 presents the proposal of a dynamic routing based approach for preserving the source location privacy in WSNs. The proposed approach address the source location privacy by considering the limited features of WSNs like power backup, lifetime, transmission delay etc. The proposed approach contributes in two aspects. Firstly, it considers enhancing the security of SSNs with minimal transmission delay and consumes power with minimum effect on the lifetime of the network. However, existing researches in the field focused on one aspect without considering the other. Secondly, the proposed approach is designed to defend most commonly used attacks like hop-by-hop, directional attacks by choosing a suitable path to send information from SSN to BS dynamically without affecting network life significantly. Thus, it becomes difficult for the attacker to find the exact path, and hence the original location of SSN.

Chapter 4 describes the implementation details and experiment results of the proposed approach in comparison to the existing approaches in the field. It introduces performance metrics, namely, Power consumption, Transmission delay, Safety period (Security level) and Network lifetime, briefly for measuring performance of the proposed approach. After this, the working of the existing approaches and their imitations are described. It describes Experimental setup and initialization values followed by experiment results in terms of identified metrics. The results are discussed for validating the proposed approach in comparison to existing approaches in the field.

Finally, Chapter 5 summarizes the work conducted in this research. It highlights the contributions and provides its conclusions of this research work. Finally, it presents the future scope of this work.

5.2 Contributions

The proposed approach has made contributions in two aspects. Firstly, different from existing approaches, the proposed approach considers enhancing the security of SSNs with minimal transmission delay and consumes power with minimum effect on the lifetime of the network. Secondly, the proposed approach is designed to defend most commonly used attacks like hop-by-hop, directional attacks by choosing a suitable path to send information from SSN to BS dynamically without affecting network life significantly. Thus, it becomes difficult for the attacker to find the exact path, and hence the original location of SSN.

In order to meet the objectives of this research mentioned in Chapter 1 Section 1.3, the proposed work has also made contributions in addition to above cited aspects are described as follows.

1. Investigated state of art in the field of network privacy in WSNs for accessing the current status of existing approaches and their limitations.

   The key finding of the recent literature in the field are highlighted in Chapter 2 Section 2.4.

2. Identified effective performance metrics as Power consumption, Transmission delay, Safety period (Security level) and Network lifetime to measure performance of proposed approach as well existing approaches for comprehensive comparative analysis of the reporting results.

3. Proposed a routing approaches for preserving source location in WSNs that involves injecting fake message packets and real message packets are switched in different routing patterns based upon conditions.

4. Simulated the proposed approach under a controlled environment for evaluating it in comparison to the existing approaches in the field.

5. Validated the proposed approach in comparison to existing approaches in terms of identified metrics. The comparative analysis of the reporting results indicate superiority and applicability of the proposed approach in preserving source location privacy.

6. Achieved a trade-off between power consumption and security level in preserving the privacy of source location in WSNs.

5.3 Future Research Scope

This research work proposed a dynamic routing approach for preserving source location privacy in WSNs by injecting fake message packets in network and switching real message packets among different routing packets without affecting lifetime of network. The proposed approach is simulated and validated in a controlled environment with limited number of sensor nodes. Significant directions for extending this work in future are described below.

- Investigation of the proposed approach in WSNs consisting of a large number of nodes (hundreds or thousands) deployed without a prior topology design.
- Enhancement of this work to explore privacy approaches for WSNs having the dynamic location of the base station and sensor nodes.
- Optimization of number and locations of the fake sources and phantom node.
- Increase in safety periods and lifetime for dynamic networks having mobile sensor nodes.
- Investigation of the proposed approach in the presence of multiple attackers in WSNs.
- Greater exploitation of the utility of surplus energy outside the hotspot area.

REFERENCES

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002), "Wireless sensor networks: a survey", Computer networks, **38**(4), pp. 393–422.

[2] Arora, A., Ramnath, R., Ertin, E., Sinha, P., Bapat, S., Naik, V., Kulathumani, V., Zhang, H., Cao, H., Sridharan, M. et al. (2005), "Exscal: Elements of an extreme scale wireless sensor network", Proceedings of 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2005, IEEE, pp. 102–108.

[3] Avramopoulos, I., Kobayashi, H., Wang, R. and Krishnamurthy, A. (2004), "Highly secure and efficient routing", IEEE INFOCOM, Vol. 1, Institute of Electrical Engineers Inc. (IEEE), pp. 197–208.

[4] Bradbury, M., Leeke, M. and Jhumka, A. (2015), "A dynamic fake source algorithm for source location privacy in wireless sensor networks", Trustcom/BigDataSE/ISPA, 2015 IEEE, Vol. 1, IEEE, pp. 531–538.

[5] Chaum, D. L. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, **24**(2), pp. 84–90.

[6] Chen, J., Du, X. and Fang, B. (2012), "An efficient anonymous communication protocol for wireless sensor networks", Wireless Communications and Mobile Computing, **12**(14), pp. 1302–1312.

[7] Deng, J., Han, R. and Mishra, S. (2004), "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks", International Conference on Dependable Systems and Networks, IEEE, pp. 637–646.

[8] Deng, J., Han, R. and Mishra, S. (2005), "Countermeasures against traffic analysis attacks in wireless sensor networks", Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, IEEE, pp. 113–126.

[9] Deng, J., Han, R. and Mishra, S. (2006), "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks", Pervasive and Mobile Computing, **2**(2), pp. 159–186.

[10] Diffie, W. and Landau, S. (2007), "Privacy on the Line: The Politics of Wiretapping and Encryption (updated and expanded edition edition)". https://mitpress.mit.edu/books/privacy-line-updated-and-expanded-edition.

[11] Groat, M. M., Hey, W. and Forrest, S. (2011), "KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks", INFOCOM, 2011 Proceedings IEEE, IEEE, pp. 2024–2032.

[12] Gruteser, M. and Grunwald, D. (2003), "Anonymous usage of location-based services through spatial and temporal cloaking", Proceedings of the 1st international conference on Mobile systems, applications and services, ACM, pp. 31–42.

[13] Han, G., Zhou, L., Wang, H., Zhang, W. and Chan, S. (2017), "A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things", Future Generation Computer Systems.

[14] He, W., Liu, X., Nguyen, H., Nahrstedt, K. and Abdelzaher, T. (2007), "Pda: Privacy-preserving data aggregation in wireless sensor networks", INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, IEEE, pp. 2045–2053.

[15] Jhumka, A., Leeke, M. and Shrestha, S. (2011), "On the use of fake sources for source location privacy: Trade-offs between energy and privacy", The Computer Journal, **54**(6), pp. 860–874.

[16] Kamat, P., Xu, W., Trappe, W. and Zhang, Y. (2007), "Temporal privacy in wireless sensor networks", Distributed Computing Systems, 2007. ICDCS'07. 27th International Conference on, IEEE, pp. 23–23.

[17] Kamat, P., Xu, W., Trappe, W. and Zhang, Y. (2009), "Temporal privacy in wireless sensor networks: Theory and practice", ACM Transactions on Sensor Networks (TOSN), **5**(4), pp. 28.

[18] Kamat, P., Zhang, Y., Trappe, W. and Ozturk, C. (2005), "Enhancing source-location privacy in sensor network routing", Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, IEEE, pp. 599–608.

[19] Kamath, S., Meisner, E. and Isler, V. (2007), "Triangulation based multi target tracking with mobile sensor networks", Robotics and Automation, 2007 IEEE International Conference on, IEEE, pp. 3283–3288.

[20] Karlof, C. and Wagner, D. (2003), "Secure routing in wireless sensor networks: Attacks and countermeasures", Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, IEEE, pp. 113–127.

[21] Kong, J. and Hong, X. (2003), "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks", Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, ACM, pp. 291–302.

[22] Kumaraguru, P. and Cranor, L. F. (2005), *Privacy indexes: a survey of Westin's studies*, Carnegie Mellon University, School of Computer Science, Institute for Software Research International.

[23] Kur, J. (2010), "Privacy preserving protocols for wireless sensor networks", PhD thesis, Masarykova univerzita, Fakulta informatiky.

[24] Li, N., Zhang, N., Das, S. K. and Thuraisingham, B. (2009), "Privacy preservation in wireless sensor networks: A state-of-the-art survey", Ad Hoc Networks, **7**(8), pp. 1501–1514.

[25] Lightfoot, L., Li, Y. and Ren, J. (2010), "Preserving source-location privacy in wireless sensor network using STaR routing", Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, IEEE, pp. 1–5.

[26] Liu, A., Zhang, D., Zhang, P., Cui, G. and Chen, Z. (2014), "On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability", Peer-to-peer Networking and Applications, **7**(3), pp. 255–273.

[27] Luo, X., Ji, X. and Park, M.-S. (2010), "Location privacy against traffic analysis attacks in wireless sensor networks", Information Science and Applications (ICISA), 2010 International Conference on, IEEE, pp. 1–6.

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

[29] Mehta, K., Liu, D. and Wright, M. (2007), "Location privacy in sensor networks against a global eavesdropper", Network Protocols, 2007. ICNP 2007. IEEE International Conference on, IEEE, pp. 314–323.

[30] Ouyang, Y., Le, Z., Chen, G., Ford, J. and Makedon, F. (2006), "Entrapping adversaries for source protection in sensor networks", Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society, pp. 23–34.

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

[32] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V. and Culler, D. E. (2002), "SPINS: Security protocols for sensor networks", Wireless networks, **8**(5), pp. 521–534.

[33] Raymond, J.-F. (2001), "Traffic analysis: Protocols, attacks, design issues, and open problems", Designing Privacy Enhancing Technologies, Springer, pp. 10–29.

[34] Reed, M. G., Syverson, P. F. and Goldschlag, D. M. (1998), "Anonymous connections and onion routing", IEEE Journal on Selected areas in Communications, **16**(4), pp. 482–494.

[35] Ren, J., Zhang, Y. and Liu, K. (2013), "An energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks", International Journal of Distributed Sensor Networks, **9**(4), pp. 834245.

[36] Roosta, T., Shieh, S. and Sastry, S. (2006), "Taxonomy of security attacks in sensor networks and countermeasures", The first IEEE international conference on system integration and reliability improvements, Vol. 25, p. 94.

[37] Sathishkumar, J. and Patel, D. R. (2016), "Enhanced location privacy algorithm for wireless sensor network in Internet of Things", Internet of Things and Applications (IOTA), International Conference on, IEEE, pp. 208–212.

[38] Shao, M., Hu, W., Zhu, S., Cao, G., Krishnamurth, S. and La Porta, T. (2009*a*), "Cross-layer enhanced source location privacy in sensor networks", Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, IEEE, pp. 1–9.

[39] Shao, M., Zhu, S., Zhang, W., Cao, G. and Yang, Y. (2009*b*), "pDCS: Security and privacy support for data-centric sensor networks", IEEE Transactions on Mobile Computing, **8**(8), pp. 1023–1038.

[40] Stajano, F., Cvrcek, D. and Lewis, M. (2008), "Steel, cast iron and concrete: Security engineering for real world wireless sensor networks", International Conference on Applied Cryptography and Network Security, Springer, pp. 460–478.

[41] Steele, R., Clarke, A. et al. (2013), "The internet of things and next-generation public health information systems", Communications and Network, **5**(03), pp. 4.

[42] Tan, G., Li, W. and Song, J. (2014), "Enhancing source location privacy in energy-constrained wireless sensor networks", Proceedings of international conference on computer science and information technology, Springer, pp. 279–289.

[43] Ukil, A. (2010), "Privacy preserving data aggregation in wireless sensor networks", Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on, IEEE, pp. 435–440.

[44] Walters, J. P., Liang, Z., Shi, W. and Chaudhary, V. (2007), "Wireless sensor network security: A survey", Security in distributed, grid, mobile, and pervasive computing, **1**, pp. 367.

[45] Wang, H., Sheng, B. and Li, Q. (2009), "Privacy-aware routing in sensor networks", Computer Networks, **53**(9), pp. 1512–1529.

[46] Wei, F., Zhang, X., Xiao, H. and Men, A. (2012), "A modified wireless token ring protocol for wireless sensor network", Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, IEEE, pp. 795–799.

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

[48] Xi, Y., Schwiebert, L. and Shi, W. (2014), "Privacy preserving shortest path routing with an application to navigation", Pervasive and Mobile Computing, **13**, pp. 142–149.

[49] Yang, Y., Shao, M., Zhu, S., Urgaonkar, B. and Cao, G. (2008), "Towards event source unobservability with minimum network traffic in sensor networks", Proceedings of the first ACM conference on Wireless network security, ACM, pp. 77–88.

[50] Zhang, W., Wang, C. and Feng, T. (2008), "GP2S: Generic Privacy-Preservation Solutions for Approximate Aggregation of Sensor Data (concise contribution)", Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on, IEEE, pp. 179–184.