Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks

by

Petros Spachos

A thesis submitted in conformity with the requirements for the degree of Master of Applied Science Graduate Department of Electrical and Computer Engineering University of Toronto

Copyright © 2010 by Petros Spachos
Abstract

Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks

Petros Spachos
Master of Applied Science
Graduate Department of Electrical and Computer Engineering
University of Toronto
2010

Wireless sensor networks (WSN) are an attractive solution for a plethora of communication applications, such as unattended event monitoring and tracking. One of the looming challenges that threaten the successful deployment of these sensor networks is source-location privacy, especially when they are used to monitor sensitive objects. In order to enhance source location privacy in sensor networks, we propose the use of an opportunistic routing scheme and we examine four different approaches. In opportunistic routing, each sensor transmits the packet over a dynamic path to the destination. Every packet from the source can therefore follow a different path toward the destination, making it difficult for an adversary to backtrack hop-by-hop to the origin of the sensor communication. Through theoretical analysis, we attempt to justify the use of opportunistic routing for the source-location problem. Moreover, simulations have been conducted in order to evaluate the performance of all the proposed schemes, in terms of source-location privacy.
Dedication

To my parents,

Kleomenis and Eleftheria

and to my sister,

Dimitra.
Acknowledgements

First and foremost, I would like to sincerely thank my advisor Prof. Dimitrios Hatzinakos. He gave me guidance and direction that was needed to produce this work. Without his generous help, this research would not have been possible. I benefit tremendously from him, and truly appreciate his countless dedications to the intellectual and personal growth of the students.

I also gratefully thank members of my thesis committee, Prof. Konstantinos Plataniotis, Prof. Ashish Khisti and Prof. David Johns for taking time to provide useful insight.

The Communications group has been a highly enriching environment for me, as I have met so many incredible individuals during my study here. I would like to thank all my colleges and specially Francis M. Bui and Liang Song for their inspiring interaction and support in my M.A.Sc. study.

I would also like to thank my cousins, Jim and Dawn, and my friends, Taso and Gianni, for their constant support and encouragement during my studies.

Last but not least, my thanks must be paid to my family. Their loves have been the origin of my energy all through.
Contents

Abstract ii

List of Figures viii

List of Algorithms x

List of Tables xi

Principle Symbols and Abbreviations xiii

1 Introduction 1

1.1 Wireless Sensor Networks: the Challenges 2
1.2 Security and Privacy in WSN 3
1.3 Problem statement 5
1.4 Research Goals 8
1.5 Methodology 8
1.6 Contributions 10
1.7 Organization 11

2 Source-Location privacy in monitoring wireless sensor networks 12

2.1 Wireless Sensor Network Security 12
2.1.1 Constraints of Sensor Security 13
2.2 Privacy Issues in Communication Networks 15
2.3 Source-Location Privacy Problem ........................................ 16
2.4 Related work ................................................................. 17
2.5 Asset Monitoring Sensor Network ......................................... 20
  2.5.1 The Panda-Hunter Game ............................................. 20
  2.5.2 System Model ............................................................ 21
  2.5.3 Eavesdropper Model .................................................. 23
  2.5.4 Design Goal ............................................................. 24
2.6 Summary ............................................................................ 25

3 Opportunistic Routing in Wireless Sensor Networks .................. 27
  3.1 Opportunistic Routing Principles ....................................... 27
  3.2 Related Work .................................................................. 31
  3.3 Security Metrics and Network Topology .............................. 33
  3.4 Module Design and Implementation .................................... 34
    3.4.1 Network address ...................................................... 34
    3.4.2 Radio implementation ................................................. 35
    3.4.3 Collision avoidance .................................................. 36
    3.4.4 Transmission process ............................................... 36
    3.4.5 Node selection process .............................................. 38
    3.4.6 Module state diagram ............................................... 40
    3.4.7 Network Example .................................................... 41
  3.5 Opportunistic Routing in Panda-Hunter Game ....................... 42
  3.6 Security Analysis ........................................................... 45
  3.7 Summary ........................................................................... 47

4 Performance Evaluation in Terms of Privacy ............................ 48
  4.1 Routing Protocols ............................................................ 48
    4.1.1 Shortest-Path Routing ............................................... 48
List of Figures

2.1 Backtracking Technique. .............................................. 22
3.1 Relay-based opportunistic example. .............................. 29
3.2 Path-based opportunistic example. .............................. 30
3.3 Packet error probability curve for BPSK without channel coding. 37
3.4 Packet relaying mechanism. ...................................... 40
3.5 Node State diagram. ................................................. 41
3.6 Example three-node network, with packet error rate shown along the edges of the graph and the distance(d) from the destination node. .......... 42
3.7 Algorithms for the source node and any relay candidate node. ...... 43
3.8 Opportunistic Routing in Panda-Hunter Game. .................. 44
3.9 Different paths toward the destination. .......................... 45
3.10 First security advantage. .......................................... 46
3.11 Second security advantage. ........................................ 47
4.1 Example of Phantom Routing. ...................................... 51
4.2 Probability of the distance between phantom and real source after $h_{walk}$ hops. ......................................................... 52
4.3 Average safety period for different source-destination separation. 56
4.4 Average message latency for different source-destination separation. 57
5.1 Energy Consumption. .................................................. 64
5.2 Node participation under different traffic volume. .......................... 66
5.3 Message delivery ratio for different message frequencies. .............. 68
5.4 Average message latency for different message frequencies and for 1000 messages. ................................................................. 69
5.5 Average safety period for different source-destination separation. ....... 71
5.6 Average message latency for different source-destination separation. .... 72
A.1 Node participation for each scheme under different traffic volume. ...... 78
A.2 Message latency for different message frequencies. .......................... 79
# List of Algorithms

<table>
<thead>
<tr>
<th></th>
<th>Algorithm</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Eavesdropper Strategy.</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>Source Node.</td>
<td>43</td>
</tr>
<tr>
<td>3</td>
<td>Candidate Node.</td>
<td>43</td>
</tr>
<tr>
<td>4</td>
<td>Candidate Node- Approach 2.</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>Candidate Node- Approach 3.</td>
<td>61</td>
</tr>
<tr>
<td>6</td>
<td>Source Node - Approach 4.</td>
<td>62</td>
</tr>
</tbody>
</table>
List of Tables

4.1 Variable Notations and Parameters ........................................ 54
4.2 Communication Parameters Setup ........................................... 54
Principle Symbols and Abbreviations

c_{n,d} \quad \text{cost of delivery between the node } n \text{ and the node } d

P_t \quad \text{transmission power}

PER \quad \text{packet error rate}

Q_x \quad \text{cumulative distribution function of } x

\sigma_n^2 \quad \text{noise power}

\hat{D}_{s(i)} \quad \text{distance between the node } s \text{ and the node } i

E_s \quad \text{set of all candidate nodes for the node } s

V_s \quad \text{relay candidate set of nodes for the node } s

T_i \quad \text{backoff period}

T_A \quad \text{timeout period for receiving an ACK}

T_w \quad \text{timeout period for receiving the data}

T_c \quad \text{timeout period for receiving a CTS}

T_R \quad \text{timeout period for receiving a RTS}

T_{R_{all}} \quad \text{timeout period for receiving all RTS}

d_{ph} \quad \text{distance, in hops, between the real and the phantom source}

h_{walk} \quad \text{number of random walk hops}

R \quad \text{radio transmission range}

S \quad \text{square range area}

P_{r/i} \quad \text{power consumption in receiving/idle mode}

SIFS \quad \text{smallest time interval composed of the module processing time and transceiver switch time}

ACK \quad \text{Acknowledgement}

ARQ \quad \text{Automatic Repeat Request}
CEM  Cyclic Entrapment Method
CORE  Coding-Aware Opportunistic Routing Mechanism
CRC  Cyclic Redundancy Check
CTS  Confirm To Send
DROW  Direct Random Walk
EAX  Expected Any-path Count
ETX  Expected Transmission Count
ExOR  Extremely Opportunistic Routing
GeRaF  Geographic Random Forwarding
GROW  Greedy Random Walk
HARBINGER  Hybrid ARQ-Based Intercluster Geographic Relaying
LRU  Least Recently Used
MAC  Media Access Control
MANET  Mobile Ad Hoc Network
MEMS  Microelectromechanical Systems
MORE  MAC-Independent Opportunistic Routing and Encoding
OAPF  Opportunistic Any-Path Forwarding
OPRAH  Opportunistic Routing in Dynamic Ad Hoc Networks
PET  Privacy Enhancing Technology
QoS  Quality of Service
ROMER  Resilient and Opportunistic Routing Solution For Mesh Networks
RTS  Request To Send
WLAN  Wireless Local Area Network
WSN  Wireless Sensor Network
Chapter 1

Introduction

Wireless technologies promise to change the manner by which everyone communicates and has access to a plethora of information. Over the past two decades, communication networking has shifted from the static model of the wired communication toward the new and exciting “anytime-anywhere” service model of mobile communication, where information is exchanged between wireless devices and made available to mobile users. This has increased the need for advancements in wireless technologies which will provide the ubiquitous communication coverage that is so necessary for all these services.

A quick survey of existing and emerging technologies will reveal a vast heterogeneity of platforms. Wireless local area networks, as best represented by “WiFi” (802.11) hotspots, are increasingly being deployed in many public locations to allow users to have access to the WEB from anywhere. Another class of wireless technologies are ad hoc networks (MANETs) and mesh style networks which promise to offer high-bandwidth at low cost and, unlike WLAN technologies, provide pervasive connectivity. Moreover, sensor networks are being deployed to monitor environmental conditions as well as to support deference-related applications involving battlefield monitoring. A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or close to it [1].
Wireless communication is necessitated when it is difficult or expensive to lay guided media between the communicating nodes, or when the nodes are arbitrarily mobile. Wireless sensor networks (WSN) have been envisioned as a technique with great potential in a variety of applications. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants.

Wireless sensor networks have quickly gained popularity. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size. However, the unique characteristics of sensor nodes and their wireless communication can pose significant challenges.

1.1 Wireless Sensor Networks: the Challenges

During the last two decades, the rapid convergence of advantages in digital circuitry, wireless transceiver, and microelectro-mechanical systems (MEMS), has made it possible to integrate sensing, data processing, wireless communication and power supply into a low-cost inch scale device. Consequently, the potential of an easily deployed and inexpensive wireless sensor network (WSN) consisting of thousands of these nodes has been attracting a great deal of attention. However, the broadcast nature of wireless communications and the unique nature of sensor networks, which are application-specific and energy resource limited pose great challenges.

First, wireless communication poses significant challenges on data security and protection. Sensor networks rely on wireless communication, which is by nature a broadcast medium without any physical boundaries, making it more vulnerable to security and privacy attacks than its wired counterpart. Any potential eavesdropper with the proper equipment, such as an appropriate wireless receiver, can monitor and intercept the communication between nodes. The eavesdropper can interact with the network even from
a distance and overhear crucial information exchanged between nodes.

Second, inch scale sensor devices have been designed to work unattended with limited power requirements, for long periods of time. Compared to portable devices, such as cellular phones and laptops, where batteries can be recharged frequently, sensor node battery recharging or replacement is sometimes not feasible or impossible. The lifetime of any individual node, and as a consequence, of the whole network, is solely decided by how the limited amount of energy is utilized.

Third, the variety of applications where WSNs can be used have made those networks application-driven. Prior to sensor networks, research was predominantly focused on other network constraints such as bandwidth availability, power consumption and message latency. Brought by sensor networks, research in wireless communication is also correlated with the details of application-specific implementations.

Generally, the research in wireless sensor networks is directed toward satisfying application-specific Quality of Service (QoS) requirements under limited energy consumption, so as to maximize network lifetime. This is a fundamental tradeoff in wireless sensor networks.

1.2 Security and Privacy in WSN

In the field of networking, network security relies on

1. the provisions made in an underlying computer network infrastructure,

2. policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and

3. consistent and continuous monitoring and measurement of its effectiveness (or lack of).

Basic network security considers authenticating the user, commonly with a username and a password. However, the requirements for security have increased as the complexity and
the effectiveness of the attacks have been continuously improved.

Securing wireless networks is different from securing traditional wired networks, mainly because wireless networks are open networks. They are open because the radio medium is a broadcast medium, in which any potential eavesdropper can easily gain access to the data which are transmitted, and they are open because the wireless devices are commodity items, allowing any adversary to purchase low-cost wireless devices and launch a variety of attacks [2].

The first response from the security community was to translate traditional network security services to the wireless domain. Although the application of conventional cryptographic protocols to wireless networks is essential, such an approach is incomplete, leaving out unique characteristics of wireless communications. In general, traditional approaches to network security are important to secure wireless systems but they cannot protect against the full range of threats facing wireless networks.

Privacy means that one can control when, where, and how information about oneself is used and by whom. It may be defined as the guarantee that information is observable or decipherable by only those who are intentionally meant to observe or decipher it. Privacy is not about hiding one’s personal information from everybody else in the world. In fact, revealing personal information to authorized parties under well-defined circumstances can be very useful and should be made possible. It is clear, however, that we do not want everyone to have access to private information and therefore, hiding personal information from unauthorized parties is indeed very important.

Communication networks require privacy in order to control information related to communication [3]. One major issue is keeping the context of messages unavailable to unauthorized parties. This problem can be solved by adapting encryption mechanisms. Conventional encryption, also referred to as symmetric encryption or single-key encryption, was the only type of encryption in use prior to the development of public key encryption. It remains by far the most widely used of the two types of encryption [4].
However, even if any potential eavesdropper is unable to have access to the content of the messages, it can still overhear important private information. It can correlate this information with the identities of the communication partners, by inspecting the header of the message and the frequency and the duration of the communication session, which is usually called traffic analysis. Header information is used by the network to route the messages to their destination and thus is not encrypted by default. The identity of the communication parties and the frequency and the duration of their communication session can reveal important personal information. For instance, the kind of Web sites that someone visits can indicate his/her area of interest. Hence, communication privacy is about controlling access to the content of the communication, as well as to the meta-information related to the communication (e.g., who is communicating with whom, how often, how long, etc.).

The operating principles of upcoming wireless networks are very different from those of existing networks. One important difference is that some of the upcoming networks are based on multi-hop wireless communications. This represents some risk with respect to privacy. In particular, there is a privacy problem in the way routes are discovered by on-demand routing protocols proposed for wireless ad hoc networks. These protocols flood the entire network with route request messages, in order to discover new routes, where the route request contains the identifiers of the source and the destination of the intended communication. Thus, any potential eavesdropper can easily observe who wants to communicate and with whom.

1.3 Problem statement

Wireless sensor networks have been increasingly considered an attractive solution for a plethora of applications, such as unattended event monitoring and tracking. One of the looming challenges that threaten the successful deployment of these sensor networks
is source-location privacy, especially when they are used to monitor sensitive objects. With source-location, we are referring to the actual location of a node which starts the transmission of a message toward a destination.

Many of the privacy techniques employed in general network scenarios are not appropriate for protecting the source location in a sensor network [5–7]. The main reason is that security mechanisms for general networks are not able to fully address the unique challenges of source-location problem. For example, any encryption mechanism of a message will prevent a potential eavesdropper to access the exact content of the message. However, it will not protect the context of the sensing data and the measurements. The eavesdropper may overhear communication patterns and routing paths, without triggering any security mechanism, and ultimately reveal the location of the communication partners.

Another important reason for the lack of general networks privacy techniques in source-location privacy problem, is the fact that many of these techniques introduce overhead. This is too burdensome for sensor networks with limited power, limited memory and storage space and limited computational capabilities [8].

There are a number of network examples where source-location privacy is an important security issue. In monitoring applications, visual sensor cameras can be deployed to monitor civilian activities. The cameras have been placed in locations where they cannot be noticed and their locations are intended to be kept private from unauthorized persons. An eavesdropper may try to reveal the location of each camera by following the network information that the cameras exchange periodically. In a battlefield, sensor nodes can be used to detect enemy intrusion instead of using landmines. The nodes will communicate periodically with the base station, exchanging useful information. The exact location of each sensor node should be available only to authorized persons. In an environmental monitoring network, sensors can be deployed to monitor the presence or the activities of endangered species. For instance, a hunter may want to reveal the location of that species
Chapter 1. Introduction

and starting from the base station and can do so by using back tracking techniques. Also, wireless traffic emitted from a company can expose important information concerning the whereabouts of employees, provided the location of the source can be deciphered. As it can be inferred, source-location privacy is an important security issue.

Different techniques have been proposed to cope with this problem in sensor networks. They can be categorized in three main classes with different approaches. The first class consists of techniques which use fake messages. Apart from the actual messages that the source sends toward the destination, a number of fake messages can also be transmitted in order to confuse potential eavesdroppers. In related literature, there are techniques that transmit fake-dummy messages during the whole transmission of a real message [9, 10] and also there are techniques that use limited fake messages in order to hide the real event traffic patterns [11].

The second class is based on secure multiparty computation techniques. A number of mixed servers are used in order to mix the received messages. Statistical properties of the background traffic are also exploited to achieve better anonymity [12, 13].

The third class consists of routing based protocols for enhanced source-location. Different network protocols have been proposed in order to make it difficult or impractical for any potential eavesdropper to reveal the location of the source [14–23]. These protocols have different energy consumption and can deliver different security levels, in terms of the time they can keep the location of the source unavailable to the eavesdropper.

The first two classes have main drawbacks for wireless communications. For example, mixed servers should be wire connected with the nodes while the use of the fake messages consumes too much energy from the limited power resources of the sensor nodes. The third, more promising approach for wireless sensor networks is further examined in this thesis; opportunistic routing protocols are considered to enhance the privacy of source location in sensor networks.
1.4 Research Goals

Opportunistic wireless mesh networks can provide an attractive solution to the source-location problem, based upon the cognitive networking concept [24], in which every node in the network observes network conditions and—in accordance with prior knowledge gained from previous interactions in the network—plans, decides and acts on this information. The routing path between the source and the destination dynamically changes according to node availability, which makes it difficult for any adversary to locate the source. In the proposed approach, the overall objective is to verify these assumptions and demonstrate how opportunistic routing can improve the source-location privacy in wireless ad-hoc and sensor networks. In particular the research goals are:

- Demonstrate that an opportunistic network utilizing opportunistic message routing is an inherent Privacy Enhancing Technology (PET).

- Identify and quantify the levels of privacy achieved by different designs of opportunistic networks. Examine how size and scalability of the network is related to privacy.

- Investigate the interactions among privacy, security and message latency in message delivery by opportunistic networks.

- Propose and evaluate opportunistic design principles that exhibit high level of privacy with minimal increase in resource consumption.

1.5 Methodology

This dissertation defines, implements and analyzes an opportunistic routing protocol. It promotes different opportunistic approaches to achieving end-to-end network objectives in the context of source-location privacy.
In particular, this work formally defines the problem of source location privacy in wireless sensor networks, differentiating it from other security issues in wireless sensor networks. In order to illustrate that this problem needs special treatment, a security analysis of commonly used routing protocols was conducted. Current and commonly used network protocols such as single path routing, shortest path routing and flooding routing are examined in order to evaluate the security they can provide for the source-location problem. All these protocols have been examined theoretically while a number of simulations have been performed under different security metrics.

For better understanding of the problem, previously proposed approaches toward the source-location privacy problem are also discussed. The first routing protocol that was introduced in order to provide sufficient source-location privacy is examined [15]. Theoretical analysis points out some main drawbacks of that protocol while a number of simulations have been conducted to explore the performance of the protocol under different network conditions.

The following section describes an opportunistic routing protocol. In order to explain the use of the final opportunistic protocol, all the available opportunistic protocols are described and classified. The final protocol is presented in detail through each module design and implementation. A comparison between the proposed protocol and the first source location privacy protocol follows in order to examine whether the opportunistic protocol can enhance privacy.

The comparison between the two protocols enables the understanding of the problem in greater detail and leads to the introduction of three more approaches of the opportunistic routing protocol. These additional approaches have been examined through simulations, both in terms of privacy and in terms of network performance, such as throughput, delivery ratio and energy consumption.
1.6 Contributions

In this thesis, we attempt to manage the source-location privacy problem in wireless sensor networks, with the use of an opportunistic routing protocol. The primary objective of the current research work is to address the following issues:

1. Simulation analysis and contribution of an opportunistic routing protocol. An opportunistic routing scheme, based on existing opportunistic routing protocols, is introduced. In order to evaluate the performance of the proposed scheme in terms of privacy, the protocol was implemented and simulated with the use of a discrete event simulator system. The security metrics that were used are

   (a) the number of messages that the source will send before the eavesdropper reveals the location of the source and
   (b) the average duration of the message transmission.

A previously proposed routing protocol which provides source location privacy is also examined and compared to the proposed solution.

2. Investigation and implementation of different opportunistic routing approaches. Based on the conclusion of the proposed scheme’s performance evaluation, three extensions of the opportunistic routing are introduced. Each approach is investigated and implemented. All four approaches are examined through simulations concerning privacy. Furthermore, the approaches are also examined in terms of general network performance such as throughput, delivery ratio and energy consumption.

These materials have partly appeared in the following publication:

1.7 Organization

This thesis is organized as follows:

- **Chapter 2**: Presents privacy issues in communication networks, introduces the problem of source-location privacy and discusses the related work. It also introduces and describes in detail an illustrative example of the problem and sets the design goals.

- **Chapter 3**: Describes the opportunistic routing protocol which is adopted and presents and classifies the different opportunistic protocols that exist in the literature. The protocol is presented in detail and a security analysis is provided to explain how that protocol can facilitate the desired privacy to the network.

- **Chapter 4**: Presents performance evaluation in terms of privacy. Shortest path routing, flooding and “phantom” routing are discussed. The lack of privacy in these protocols is pointed out. Finally, a comparison between these protocols and the proposed scheme is presented.

- **Chapter 5**: Three extensions of the opportunistic protocol are introduced. They are described in detail with illustrative algorithms. Moreover, a number of simulation results are presented in order to explore the performance of the different approaches both in terms of network protocols (energy consumption, delivery ratio etc.) and in terms of security.

- **Chapter 6**: Conclusion and future work is presented.
Chapter 2

Source-Location privacy in monitoring wireless sensor networks

In this chapter wireless sensor network security and constrains are discussed. Next, privacy in wireless sensor network is presented and we focus on the source-location privacy problem. The previous work in the area is discussed. Finally, the system model and the eavesdropper model for an asset monitoring network is described, in order to capture the relevant features of wireless sensor networks and any potential eavesdropper in source-location applications.

2.1 Wireless Sensor Network Security

As wireless sensor networks become more popular, so does the need for effective security mechanisms. Sensor networks may interact with sensitive data and/or operate in unattended environments. In contrast with traditional network security, security in sensor networks poses different challenges, due to inherent resource and computing constraints.

The low cost of sensor nodes provides a mean to deploy large sensor arrays in a variety of application such as civilian and environmental monitoring. However, sensor networks also introduce severe resource constraints due to their lack of data storage and
power restrictions. Moreover, wireless sensor networks are even more vulnerable to a number of attacks, compared to their wired counterparts. The radio medium in WSNs is a broadcast medium without any protected physical boundaries while the unreliable communication channel and unattended operation make the security defenses even harder [25]. Furthermore, as pointed out in [5] wireless sensors tend to have the processing characteristics of old machines and the industrial trend is to reduce the cost of wireless sensors while maintaining similar computing power.

As it can be inferred, wireless sensor network security is complicated and in order to cope with a specific aspect of the problem, such as source-location privacy, the challenges should be well addressed.

2.1.1 Constraints of Sensor Security

A wireless sensor network is a special network which has many constraints compared to traditional computer network. Due to these constrains, it is difficult to apply existing security approaches to the area of wireless sensor networks. Therefore, in order to develop a useful security mechanism, it is necessary to understand all these constrains [26].

Sensor Node Constrains: The capabilities and constraints of sensor node hardware is always an important factor for the type of the security mechanism that will be applied. In recent years, sensor nodes with great capabilities have been developed. However, the majority of the sensor nodes that are used are inexpensive and with limited capabilities.

- Energy Limitation: Energy consumption is the major challenge in every sensor network. Usually, sensor networks are designed to operate unattended for long periods of time because battery replacement or rechargeability is sometimes infeasible or impossible. Therefore, the battery charge must be conserved to extend the life of each sensor and the entire sensor network. When applying a security mechanism to a sensor node, the impact that this mechanism has on the lifespan of the sensor should always be considered. The energy required to transmit related security
data should always be considered when implementing a cryptographic function or a security protocol within a sensor node.

In order to conserve energy, the security scheme that will be applied should force the nodes to spend most of their operational time in low-power *sleep* modes and to process (e.g. target detection, data transmission) only when it is required. As a result, a node’s availability within the network change dynamically and may be limited. An energy inefficient scheme may result in potential unavailability of a node to receive data. The routing protocol that is applied then should try to make use of all the other available nodes.

The communication range of sensor nodes is also limited in order to conserve energy. A great reduction in the transmission power can save sensor node energy. However, it reduces each sensor node detection probability and communication range. As a consequence, more nodes are needed to cover an area, while the nodes should be placed close enough to be able to communicate.

It can be inferred that sensor nodes energy limitations are different based on their application and the desired level of security.

- **Resource Limitation:** Sensor nodes usually are tiny devices with only a small amount of memory and storage space for code. Any proposed security mechanism should limit the code size of the security algorithm.

  Moreover, because of the limited storage space, the necessary information associated with the security algorithm (e.g. security information messages, message overhead etc.) should also be limited. Sensor nodes usually are unable to store all the necessary information for a security scheme and schemes with more sophisticated security algorithms should be applied.

  **Networking Constrains:** Distributed wireless sensor networks have unique limitations which are never encountered in more typical wired networks. These are:
• **Channel Error Rate:** Wireless medium may lead to the packets damage or loss due to channel errors. Wireless communications are facing many unpredicted challenges such as air interference, channel fading, environmental changes etc. A reliable security protocol should handle appropriately any lost or missing packets.

• **Conflicts:** Even if the channel is reliable enough, the broadcast nature of wireless communication causes one more problem. If multiple packets meet in the middle of transfer, conflicts will occur and the transfer will fail. In a large scale network with high traffic volume this can be a major problem.

• **Latency:** Multi-hop routing protocols can lead to greater latency in the network, making it difficult to achieve synchronization between the nodes. Synchronization issues can be critical in network security where security mechanisms rely on critical event reports.

### 2.2 Privacy Issues in Communication Networks

Privacy is becoming one of the major issues that jeopardizes the successful deployment of wireless sensor networks. The issue of privacy is concerned with keeping all the crucial information of a communication unknown from unauthorized entities. In the context of network communication, where two entities communicate by exchanging messages over a network, a threat to privacy involves the ability of an eavesdropper who, intentionally or not, gain access to information concerning the identities of the participant, the meaning of the communication, and the time and the place the communication takes place.

Privacy in sensor networks can be categorized into two classes: content-oriented privacy and contextual privacy [14]. **Content-oriented privacy** refers to the ability of an eavesdropper to have access in the exact content of the message that is transmitted. This message corresponds to actual sensed-data or lower-layer control information about the network. The appropriately design of a network security protocol can cope with this
problem. A number of such protocols have been proposed in [5–7].

Contextual privacy refers to the ability of an eavesdropper to have access to the context of the sensing data and the measurements. The eavesdropper can infer information from observations of sensors communication without interfering with the proper functioning of the network, and without triggering security mechanisms overseeing the content of the message. Communication patterns and routing paths information can be crucial especially for monitoring sensor networks as we will see in the following section.

In this work, we are trying to alleviate the problem of contextual privacy with the use of a routing protocol.

### 2.3 Source-Location Privacy Problem

Despite strong encryption techniques of the data, wireless communications still expose significant information about the traffic carried in the network, routing paths and communication patterns, due to its inherent broadcast nature, including susceptibility to unauthorized wireless data interception. As a result, an eavesdropper with the necessary equipment, like a radio transceiver and a workstation might be able to illegally access the network. It could also eavesdrop the communication between sensor nodes, and either identify the source message or even reveal the source-location, without interfering with the proper functioning of the network.

Location privacy is an important security issue for such networks. Lack of location privacy can lead to subsequent exposure of significant traffic information on the network and the physical world entities. For example, wireless sensor networks can be used to monitor the activities or the presence of endangered species. This information should be kept unavailable to any illegal hunter who may try to reveal the location of the source and finally reveal the location of the animals. In a health-care network, cardiologic data packets coming out of a hospital enable an eavesdropper to analyze and find out
Chapter 2. Source-Location privacy in monitoring wireless sensor networks

at-risk heart patients, if the source location of those packets can be determined. Web surfing packets coming out of a company in a Mesh network enable an eavesdropper to analyze the surfing habits of the employees, if the source location of these packets can be determined. In order to provide sufficient network privacy in a military intelligence network, the source of a message and the corresponding path toward the destination should be protected from any eavesdropper.

Privacy enhancement in such networks is challenging because these networks consist of low-cost radio and low-power devices. Usually these devices are designed to operate unattended for long periods of time with limited energy since battery recharging or replacement is sometimes infeasible or impossible. Therefore, it is important that any proposed privacy enhancement technique does not come at the cost of a significant increase in resource consumption. Bandwidth availability and energy consumption should also be considered in a sensor network. A solution that will enhance the privacy of the network should utilize the network resources including both spectrum bandwidth and station availability. Consequently, any proposed solution for the enhancement of the source privacy in a sensor network should satisfy, apart from the source privacy, spectrum availability and energy efficiency.

2.4 Related work

In the past two decades, a number of source-location communication protocols have been proposed. In mixnet protocol [12], the author proposes the use of a number of “mix” servers in order to mix the packets being received. In order to achieve the desired anonymity, statistical properties of the background traffic are exploited. In the DC-net protocol [13], the approach is based on secure multiparty computation techniques. The main drawback in both approaches is that they require a public-key cryptosystem, making them ineffective for wireless sensor networks.
A different approach for source-location privacy was proposed in [9] and [10]. The main idea is a mixture of valid and fake messages. Each node transmits either a valid or a fake message, consistently. The main disadvantage of this approach is that the broadcasting of fake messages consumes significant amounts of the limited energy in each sensor node. Moreover, because in every time slot each node has to transmit a packet, this increases the number of collisions and decreases the packet delivery ratio. Therefore, these approaches are not suitable especially for large scale wireless sensor networks.

Routing based protocols can also provide source-location privacy [14–17]. In [14] the authors introduced the Panda-Hunter model to formalize the source location problem in sensor networks and they proposed a phantom flooding approach. Phantom flooding routing involves two phases: a random walk phase, and a subsequent flooding path routing. During the first phase, the message follows a random walk through the network for a number of hops. After that, the sensor node that has the message, becomes the new “phantom” source which will deliver the message to the destination with flooding routing. In [15] the authors extended the work of [14] and they proposed a phantom routing technique based on both flooding and single path routing. As we will see in a subsequent chapter random walk is inefficient at placing the “phantom” source far enough from the real source while flooding provides the least possible privacy protection.

In [16] a two-way greedy random walk (GROW) is proposed. The destination first initiates a random walk for N-hops. Then, the source initiates a random walk for M-hops. Once there is an intersection between the two paths, the message is forwarded toward the path created by the destination. In order to detect when two paths intersect, local broadcasting is used. Moreover, in order to minimize the chance of backtracking along the random walk, the nodes are stored in a bloom filter and each intermediate node is checked against the bloom filter to ensure that a node has not been used before in order to minimize backtracking. Although this technique consumes less energy than the “phantom flooding-based” technique, it tries to use almost all the nodes in the network
by increasing message latency and node power consumption without placing the phantom source far enough from the real source. To address this problem, in [17] a direct random walk (DROW) is proposed. Initially the source chooses a direction for the random walk of the message. This can be achieved by storing direction information in the header of the message. The exposure of the direction information decreases the complexity for the adversaries to trace back to the true message source.

In [18] a non-geographical, overlay routing method (iHide) for packet delivery was adopted to provide source-location privacy. They proposed a routing protocol that conforms rings which communicate through a Bus. Ring is a virtual circle structure that consists of a static number of sensor nodes. Between the sensors, there is one that is the main node, BUN node, of the ring. BUNs are networked with each other to form the Bus. Bus is a virtual “rope” that connects each ring with the destination. In order to make the location of the source infeasible to any potential eavesdropper, the message is exchanged for a number of times between the nodes that conforms a ring, before it forwarded to the destination. The main drawback of that approach is that the network should have a configuration phase in order to conform the buses and the rings. Moreover, this scheme is more secure than previous approaches but it adds extra delay in each message delivery while it increases every message overload for the necessary routing inside the rings and the buses. In [19] a similar approach with cyclic entrapment method (CEM) is proposed. This scheme additionally uses fake messages in the rings and performs better in terms of security while the fake messages consume more energy.

In [20, 21], the authors introduced a randomly selected intermediate node scheme for local source location privacy protection. In [22, 23], they have extended the idea in a two-phase routing process. In the first phase, the message selects randomly an intermediate node before it is routed to a ring node. In the second phase, the data packet is mixed with other packets through a network mixing ring before being transmitted to the destination. The main drawback of this approach is that the nodes which form the network mixing
ring consume more energy than the other nodes in the network. To address this problem, a periodic change of the nodes that conform this ring has been suggested. This increases the number of the nodes that should operate during a message transmission. Moreover, the total energy consumption increases since almost all the nodes in the network will have to operate periodically.

2.5 Asset Monitoring Sensor Network

An important class of sensor-driven applications are those that monitor a valuable asset. For example, a sensor network can be deployed in natural habitats to monitor endangered animals. In an international airport, visual sensor cameras can be used for surveillance monitoring services. In a battlefield, the position of a soldier could be located from a sensor network. In all these application, source-location privacy is of high importance.

In order to facilitate the discussion and the analysis of source-location privacy in wireless sensor networks, we will use an exemplary scenario that captures most of the relevant features of both sensor networks and any potential eavesdropper. This scenario was first introduced in [15] and is used from then on as a representative scenario for the source-location problem. Next, the system model and adversaries model will be presented and the design goal of the model will follow.

2.5.1 The Panda-Hunter Game

The Panda-Hunter Game was first introduced in [15]. A large array of panda-detection sensor nodes have been deployed in a monitoring predefined geographical area, by the Save-The-Panda Organization. The purpose of the network is to observe a vast habitat for pandas. When a panda appears in the coverage area of a sensor node, this node becomes the source of the network. It will observe all the necessary information (place, date, time etc), it will create a message with all these information and it will send it to the destina-
tion, which is a monitoring room, through multi-hop routing techniques. The potential eavesdropper is a hunter who tries to capture the panda. The hunter will try to reveal the location of source of the message and as a result the location of the panda.

The easiest way for the hunter to reveal the location of the panda is by using backtracking techniques. Figure 2.1 illustrates that technique. The source node is with the red color, the destination node is with the green color and the hunter is the rectangular. In the Panda-Hunter Game, we assume that the hunter is located beside the destination node, shown in Figure 2.1(a), and its hearing radius is equal to node transmission radius. When the hunter overhears a message, it physically moves to the sender node of the message, as depicted in Figure 2.1(b). Following that strategy, in the next slot the position of the adversary is illustrated in Figure 2.1(c), if the distance between the source and the destination is 8 hops, the hunter will finally reveal the source node after 8 messages and will capture the panda, depicted in Figure 2.1(d).

In the Panda-Hunter Game, we assume that there is only one panda in the monitoring area, so we will have only one source and we also assume that this source is stationary. When a node becomes the source of the network, it starts sending packets to neighboring sensors that are within its limited radio range. The source node will continuously send packets until the hunter discovers the source, or the panda disappears from the monitoring area. We also assume that the source includes its ID in encrypted messages and only the destination node can understand the location of a node from its ID. As a result, even if the hunter decrypt a message, it will not be able to reveal the location of the source.

2.5.2 System Model

We assume a large predefined geographical area that needs to be monitored, and deploy a wireless sensor network consisting of many randomly distributed sensor nodes. The network continuously monitors activities and locations of the target in the area. Based on the initial description of the system model, as introduced in [15], we make the following
assumptions about our system:

- There is only one destination node at any time, while there can be more than one source. This is usually the case for the most monitoring applications. The destination node is predefined during an initialization phase. If the destination node changes, there should be another initialization procedure for the network.

- In monitoring sensor networks, usually any node in the network can become the source node. When a node becomes the source node, it generates a packet with all
the necessary information concerning the target. All the nodes in the network can participate in message transmission, hence, apart from detection capabilities they all have transmit and receive functionality, based on the applied protocol.

- Every node in the network knows the address of the destination node. The information of the destination node location is made public. When a node detects an event, it generates a packet which is transmitted toward the destination though a multi-hop routing.

- Every node in the network knows its relative location. We also assume that each node has knowledge of its adjacent neighboring nodes. The information about the relative location of each node can also be broadcasted through the network for routing information update [27–29].

2.5.3 Eavesdropper Model

The eavesdropper will try to reveal the location of the source by being well equipped and having some technical advantages over the sensor nodes. The eavesdropper is assumed to have the following characteristics [2]:

- The eavesdropper knows the location of the destination and can determine the location of the sender sensor from the instance of the message that it overhears. Initially, the eavesdropper is located beside the destination node.

- The hearing radius of the eavesdropper is equal to the transmission radius of the nodes. As a result, the eavesdropper can monitor only the traffic area around the node which it observes and not the whole network.

- The eavesdropper is device-rich and well equipped. It has a radio transceiver, a workstation and any equipment it might need to have illegal access to the network.
• The eavesdropper is resource-rich. It can physically move from one sensor to another and has an unlimited amount of power.

• The eavesdropper will not interfere with the proper functioning of the network, such as destroying sensor nodes or modifying packets in order to not trigger other security mechanisms.

• The eavesdropper has storage capabilities. It can remember all the messages it has overhear and decide if a message is new or it is the same with another it has already overhear. This is because, same messages can follow different paths toward the destination and use the same nodes in different time slots. The eavesdropper should be able to verify the new messages.

Algorithm 1 illustrates the eavesdropper model. Initially, the eavesdropper is located next to the destination node and waits for message to arrive. When a message arrives, it checks if it has already overheard that message. If the message is not new, the eavesdropper will not follow the message. Otherwise, it physically moves to the sender node of the message and continues overhearing messages from that node.

**Algorithm 1**: Eavesdropper Strategy.

```java
1 eavesdropperLocation=destination;
2 while (eavesdropperLocation != sourceLocation) do
3     overhear(node[eavesdropperLocation]);
4     message= node[eavesdropperLocation].ReceivedMessage();
5     if (message == isNewMessage()) then
6         MoveTo(message.GetSenderNode());
7         eavesdropperLocation= message.GetSenderNode();
8     end
9 end
```

### 2.5.4 Design Goal

The design goal can be summarized as follows:
• The eavesdropper should not be able to reveal the location of the source, based on
the messages it managed to overhear and the information these messages contained.

• The destination node is able to identify the location of the source node, based on
the source ID which is included in the message. The recovery of the ID to the
location of the source should be very efficient.

• Each message should arrive at the destination time in a time limit. If the message
travels around the network for long time, it might provide privacy for the source
but the destination will not get it in time and in a monitoring network the messages
should always received on time.

• The number of the sensor nodes that participate in the transmission of each mes-
   sage should be as short as possible to reduce sensor nodes energy consumption.
   Moreover, sensor nodes should operate only during messages transmission and all
   the other time they should only sensing the the area around them.

• The length of each message should be as short as possible to save sensor nodes
   power. This is because, on average, the transmission of one bit consumes about as
   much power as executing 800-1000 instructions [30].

2.6 Summary

In this chapter, we have discussed the problem of source-location privacy in wireless sen-
sor networks. We have presented the unique characteristics of sensor nodes and wireless
communications and the challenges they pose in network security and privacy. We have
focussed on the problem of source-location privacy. We have described a representative
scenario for the problem and the general assumptions of the models that we will use. We
have also discussed the design goal of the models. Different approaches have been pro-
posed to alleviate the problem. They are based on different techniques such as dummy
messages and mixed servers. The main drawback of these approaches is that they consume significant amount of the limited energy in the sensor nodes. A promising approach comes from routing based protocols. There are protocols that are able to provide privacy but may have other drawbacks such as message latency. In this chapter we discussed most of those approaches, while some of them we will discuss again in the chapter with the performance analysis.
Chapter 3

Opportunistic Routing in Wireless Sensor Networks

In this chapter we are introducing an opportunistic routing protocol. We are describing the main opportunistic routing principles and the related work. Next, we describe our implementation and the different states for the nodes. We are using this scheme in the Panda-Hunter game and we conclude this chapter with the security analysis of the proposed scheme.

3.1 Opportunistic Routing Principles

Many works are devoted on improving the performance in wireless ad hoc and sensor networks, in terms of power consumption, message latency and throughput. One promising approach is to allow the relay nodes to cooperate, thus using the spatial diversity to increase the capacity of the system. However, the main drawback of that approach is that it needs information exchange between the nodes, which introduces an overhead and increases the complexity of the receivers. A simpler way of exploiting the spatial diversity is referred to as opportunistic routing, also called opportunistic forwarding.

In opportunistic routing, the intermediate nodes collaborate on packet forwarding
in order to achieve high throughput in the face of lossy links. Opportunistic routing tries to overcome the drawback of an unreliable wireless link by taking advantage of the broadcast nature of the wireless medium such that one transmission can be overheard by multiple nodes. A cluster of nodes serves as a relay candidate but only one node finally will forward the packet. This selection process is crucial and based on opportunistic rules, which we discuss later in this chapter. Opportunistic routing in wireless sensor networks can provide better performance in terms of network transmission reliability and network throughput.

Routing is crucial in wireless sensor networks. The task of routing includes the next node selection process and the route selection process toward the destination. Traditional routing protocols in wireless sensor networks usually perform best path routing which has been fixed before the transmission starts. The highly dynamic and lossy nature of wireless medium causes frequent transmission failure which lead to retransmission and waste of network resources, or even to system breakdown. Opportunistic routing takes advantage of the broadcast nature of the medium and change both the relay node selection and the number of the possible paths toward the destination in order to improve the performance of the traditional best path routing. Compared to traditional end-to-end multi-hop routing, the core idea in opportunistic routing is that, at each hop, a set of next hop relay candidates receiving the packet successfully compete to act as a relay. Instead of choosing a single route ahead of time, the path is determined as the packet moves through the network, based on which sensor receives each transmission.

We will try to illustrate these two important aspects of opportunistic routing with the following examples [31]:

**Relay node selection.** An illustrative example of the relay node selection in opportunistic routing is depicted in Figure 3.1 where a directed graph represents a wireless network. There is one link between the source node $s$ and each intermediate node, $A, B, C$, and $D$, with delivery probability of 25%, and a link between each intermediate
node and the destination node, \( G \), with delivery probability of 100%. Traditional routing will achieve 25% end-to-end delivery probability through any possible intermediate node. An opportunistic routing scheme can use all the intermediate nodes as relay nodes and achieves a delivery probability of:

\[
(1 - (1 - P_{sA}) \times (1 - P_{sB}) \times (1 - P_{sC}) \times (1 - P_{sD})) =
\]

\[
= (1 - (1 - 0.25)^4)) \approx 68\%
\]

\[\text{Route Selection.}\] An illustrative example of the route selection and the different paths toward the destination that an opportunistic routing can provide is in Figure 3.2. The links with the dots represent opportunistic links while there has been assigned a delivery probability \( P \) for each link. Traditional best path routing will always choose the most reliable links, which result in the path \( s \rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow G \), which has end-to-end delivery probability \((0.9)^5 \approx 59\%\), after 5 hops. An opportunistic routing scheme, with the restriction of 3 hops has the following paths: \( s \rightarrow A \rightarrow C \rightarrow G \), \( s \rightarrow B \rightarrow D \rightarrow G \) and \( s \rightarrow B \rightarrow C \rightarrow G \). The first path has successful delivery
probability of:

\[ P_{sA} \times (1 - P_{AC} \times P_{CG}) = 0.9 \times (1 - 0.6 \times 0.6) = 57.6\%. \]

The other two paths have successful delivery probability of:

\[ P_{sB} \times (1 - (1 - P_{BD} \times P_{DG}) \times (1 - P_{BC} \times P_{CG})) = 0.6 (1 - (1 - 0.6 \times 0.9) \times (1 - 0.6 \times 0.6)) \approx 42.3\%. \]

The overall successful delivery ratio of the above 3 paths is:

\[ 1 - (1 - 0.576) \times (1 - 0.423) \approx 75.5\%. \]

From the previous two examples, it can be inferred that an efficient node selection and route selection, through an opportunistic routing scheme, can improve the performance of a network in end-to-end packet delivery.

The key issue in the design of an opportunistic routing scheme are [31]:

- forwarder set selection,
- prioritization of forward set and
- duplicate transmission avoidance.

Forwarder set selection for source \( s \) for the first example was \( A,B,C,D \) and for the second \( A,B \). We can define different forwarder sets based on different assumptions. In the first example, all the nodes have the same priority while in the second if we are interested
in higher end-to-end delivery ratio then node B should be in higher priority from node A for the source node s. Finally, the greater challenge is the avoidance of duplicate transmissions. When the relay node is selected, any other node which is a relay candidate and might have overheard the transmission of that packet, should avoid transmitting the same packet. Based on these three major issues, a number of opportunistic routing protocols have been proposed.

3.2 Related Work

During the last decade, a number of opportunistic protocols have been developed. The first opportunistic routing has been introduced in [32]. Extremely Opportunistic Routing (ExOR) selects the next relay node by a slotted ACK (acknowledge) mechanism. Having successfully received a data packet, the node calculates a priority level, which is inversely proportionate to the expected transmission count metric (ETX), [33], which is based on the distance between the node and the destination. The shortest the distance, the highest the priority. The node with the highest priority will then be selected as the next relay node. The main drawback of ExOR is that it prevents spatial reuse because it needs global coordination among the candidate nodes. Candidate nodes transmit in order, only one node is allowed to transmit at any given time while all the other candidate nodes trying to overhear the transmission in order to learn which node will be the next relay node. Moreover, the simple priority criteria that it uses, (ETX distance), may lead packets toward the destination through low-quality routes. To overcome this problem, Opportunistic Any-Path Forwarding (OAPF) [34] introduces an expected any-path count (EAX) metric. This can calculate the near-optimal candidate set at each potential relay node to reach the destination. However, it needs more state information about the network and it has high computational complexity.

ExOR ties the MAC with routing, imposing a strict schedule on routers access to
the medium. The scheduler goes in rounds. *MAC-Independent Opportunistic Routing and Encoding Protocol* (MORE) [35] tries to enhance ExOR. MORE uses the concept of innovative packets in order to avoid duplicate packets which might occur in ExOR.

In [36, 37] a *Geographic Random Forwarding* (GeRaF) technique was proposed. In GeRaF each packet carries the location of the sender and the destination and the prioritization of the candidates nodes is based on location information. This technique is simple to be implemented but it requires location information for all the nodes in the network. *Hybrid ARQ-Based Intercluster Geographic Relaying* (HARBINGER) [38] is a combination of GeRaF with hybrid automatic repeat request (ARQ). In GeRaF, when there is no forwarder within the range of the sender node, everything must start over again while in HARBINGER hybrid ARQ is used for a receiver to combine the information accumulated over multiple transmission from the same sender.

A number of other opportunistic routing protocols have been proposed [39–43]. *Coding-Aware Opportunistic Routing Mechanism* (CORE) [39] is an integration of localized inter-flow network coding and opportunistic routing. By integrating localized network coding and opportunistic forwarding, CORE enables a packet holder to forward a packet to the next hop that leads to the most coding changes among its forwarder set. *Opportunistic Routing in Dynamic Ad Hoc Networks* (OPRAH) [40] builds a braid multipath set between source and destination via on-demand routing to support opportunistic forwarding. For this purpose, OPRAH allows intermediate nodes to record more subpaths back to the source and also those subpaths downstream to the destination via received Route Request and Route Replies. *Resilient and Opportunistic Routing Solution For Mesh Networks* (ROMER) [41] builds a forwarding mesh on the fly and on a per packet basis.
3.3 Security Metrics and Network Topology

In this section, the security metrics and the topology of the network are presented. The metrics that will be used in order to measure and evaluate the privacy performance are crucial for the selection of the opportunistic routing protocol. Apart from that, the topology of the network is important for any opportunistic protocol. For example, GeRaF protocol needs to know the exact location of the sensor and, as a consequence, the topology of the network should be defined in advance.

• Security Metrics

The security metrics that will be used, are the same that have been used in the Panda-Hunter Game [15], when the problem of the source-location privacy was introduced. The purpose of the sensor network is to monitor an asset while the purpose of the routing protocol is two-fold; to enhance the location privacy of the source in the presence of an eavesdropper with a movement strategy, and to deliver the messages to the destination node. The security metrics are the following:

Safety Period: Safety period of a routing protocol, for a given eavesdropper movement strategy, is the number of messages initiated by the source node that is monitoring an asset. The source node will keep transmitting messages until the eavesdropper reveals the location of the source or the target disappears from the monitoring area.

Message latency: Message latency is the number of hops needed for all the messages to arrive at the destination node. In a monitoring application, message latency is crucial, because the message should arrive at the destination node on time. Moreover, if we assume that every sensor consumes energy while transmitting, and the energy consumed in any other state of the sensor is negligible, the average message latency needed to reach the destination can also be used as a metric for the energy consumption of each scheme.
• Network Topology

In source-location privacy problem, we are particularly interested in large-scale sensor networks where there is a reasonably large separation between the source and the destination node. The monitoring area is a rectangular field. The number of the nodes is large enough to cover the monitoring area and the nodes area randomly located in the field. Some of the nodes might be too close to each other, having many neighbors. However, some other nodes might be excluded or a transmission through them leads to deadlocks. Any proposed routing scheme should take into consideration all these issues related to the topology of the network.

3.4 Module Design and Implementation

It is important that any proposed privacy enhancement does not come at the expense of a significant increase in resource consumption. A solution that will enhance the privacy of the network should also utilize the network resources, including station availability. Moreover, if privacy enhancement comes with an increase in the number of nodes in the network, energy consumption represents another challenge. As such, besides source security, any proposed solution for the enhancement of source privacy in a sensor network routing should address energy efficiency.

In this section, some elements of the module design and implementation are presented. The module state diagram is then shown.

3.4.1 Network address

Network address is related to the context and is subjected to a “cost of delivery” criteria. Given a node address \( n \) and the destination address \( d \) of a data packet, this “cost of delivery” \( c_{n,d} \) should be locally obtained. This could indicate the average or the approximate cost of delivering a packet from the node \( n \) toward the destination \( d \), independent
of any dynamic change in the network. Usually, in large-scale wireless sensor network $c_{n,d}$ is correlated with the distance between the two nodes.

In data-collecting networks, the source wants to deliver a number of packets to the destination, in the absence of cross-traffic, which corresponds to our case of monitoring networks. Initially, the destination node broadcasts a number of identity advertisement packets and every node thereon floods the packet to the network. On the reception of a packet, a node can count the smallest number of hops from the destination and use it as “cost of delivery” criteria, $c_{n,d}$. Whenever a new node joins the network, it can estimate its logic address by acquiring the logic address of its neighbor nodes. If the destination node changes, the procedure should start from the beginning.

When the source node changes there is no need to repeat the procedure. This is important for source-location privacy problem, and monitoring application in general. Many nodes can track the monitoring asset and become the source in the network transmission. Opportunistic routing with such network address implementation will avoid the need of an initialization phase, every time the target appears in different part of the area.

If a node leaves the network, it will not take part in the selection process as we will see in a following section. In this way, opportunistic routing adopts quickly to network changes, which is also important in monitoring network scenarios. Some of the sensors might run out of battery or be damaged while some other might be added in an area to cover greater range. Opportunistic routing is able to respond to all these changes without the need of a configuration phase.

3.4.2 Radio implementation

Cognitive radio was first introduced in [44] as an ideal-omnipotent radio for user-centric communications because it takes into consideration all the available parameters. For large-scale wireless network, two propositions were further suggested in [45]:

1. In order to avoid collisions with other simultaneous on-going transmissions, the
radio can sense the spectrum resource, opportunistically, before any transmission.

2. The radio can extract useful information for local cooperation by opportunistically polling one or more proximity radios onto the selected spectrum.

With the above proportions, we can extend the concept of cognitive radio to the area of cognitive network, which implements both dynamic spectrum and radio access.

3.4.3 Collision avoidance

We consider a scheme that prevents collisions by making use of the cognitive radio. Specifically, the radio can have access to a group of data channels. Every channel in that group is associated with two different frequency tones, one for sensing and one for polling which are also distinctive from the data channel frequency. Therefore, the radio hardware should be composed of two transceivers, one for sensing/polling and one for data.

Initially, when a node \( n \) has to transmit a packet, it senses for an available channel and then broadcasts a polling tone. All the nodes which are in the range of node \( n \) can detect this polling tone. A neighbor node can decide to join the transmission based on its own autonomous availability. If a node decides to join the transmission it sends out a polling tone to its surrounding nodes. In this way, sensing and polling tones protect wireless link module from spectrum interference.

3.4.4 Transmission process

In every time slot \( i \), the transmission strategy is decided by \( P_t(i) \) which is the transmission power at the sensor node at time \( i \). We assume that only one packet can be transmitted in one time slot. Every lost packet will be retransmitted in the next assigned slot. If we use BPSK without channel coding, the \( \hat{P}ER(i) \) can be written as [46]:
Figure 3.3: Packet error probability curve for BPSK without channel coding.

\[ \hat{P}ER(i) = 1 - \left( 1 - Q\left( \sqrt{\frac{2P_t(i) \cdot \hat{G}(i)}{\sigma_n^2}} \right) \right)^{F_d}, \]

(3.1)

where \( \sigma_n^2 \) is the noise power, \( Q(x) = \frac{1}{\sqrt{\pi}} \cdot \int_0^\infty e^{-t^2} dt \) and

\[ \hat{G}(i) = A \cdot \hat{D}_s(i)^{-n}, \]

(3.2)

where \( A \) is a constant and \( \hat{D}_s(i) \) is the distance between the sender node \( s \) and the next node \( i \). Figure 3.3 provides the PER in different distances from the source node for different values of transmission power \( P_t \). As the transmission power decreases the PER increases dramatically. As it can be inferred, the transmission range of a node is always correlated with the PER.
3.4.5 Node selection process

We are using four types of packets during the packet relaying process: Request To Send (RTS), Confirm To Send (CTS), DATA and ACK. RTS/CTS are used during the handshake process between neighbor nodes while ACKs are used for verification of DATA delivery.

When a node $s$ has to transmit a packet, first it broadcasts a RTS packet, in which it includes its own address and the destination address, $d$, and then node $s$ keeps listening. All the surrounding nodes which are in the range of $s$ are able to hear this request, conforming a set of candidate nodes $E_s$. There is a subset $V_s \leq E_s$ conformed by any node $i \in E_s$ that satisfying the condition $c_{i,d} < c_{s,d}$ so,

$$V_s = \{ i \in E_s | c_{i,d} < c_{s,d} \}$$ (3.3)

If a node is in $V_s$ subset and is available for receiving a packet, and there aren’t any packets in its buffer waiting to be send, it should send a CTS packet back to the sender node $s$. In order to prioritize the nodes based on their distance from the destination, each node $i \in V_s$ initialize a timer, with timeout period $T_i$, which is inverse proportional to the difference $c_{s,d} - c_{i,d}$ and can be determined as follows:

$$T_i = \frac{C_0}{c_{s,d} - c_{i,d}} + SIFS, i \neq d$$ (3.4)

where $C_0$ is a constant and SIFS is the smallest time interval composed of the module processing time and the transceiver RX/TX switch time. In our simulation, which will be presented in the following chapter, $T_i$ is also slotted according to the minimum carrier-sensing time.

In the next step, node $i$ backs off for the period $T_i$. If the data channel is free after that period, node $i$ sends a CTS to the sender node, otherwise it quits. After that procedure, the sender node $s$ will receive the first CTS from the node which is closer to the destination, and this will be the next hop relay node and it will receive the DATA
packet. When the next node receives the DATA packet it replies with an ACK to the sender and follows the same procedure until the DATA packet reaches the destination.

In the case that the sender node receives more than one CTS packets simultaneously there are certain mechanisms in the sender node, such as cyclic redundancy check (CRC) that can detect this collision and differentiate the nodes.

When a node $i$ sends a CTS it waits for time $T_w$ to receive the DATA packet from the sender node $s$, otherwise it goes back to its previous mode. $T_w$ is the time needed for the sender to transmit the data to that node and can be defined as:

$$T_w = d(s, i) \cdot D_0 + SIFS \quad (3.5)$$

where $d(s, i)$ is the distance between the sender and the relay candidate and $D_0$ is a constant.

In the same way, the sender node has to wait for $T_c$ time to get a CTS packet before it broadcasts a RTS again. $T_c$ is the time needed for a node which is located at the limit of the range $R$ of the sender node, and can be defined as:

$$T_c = R \cdot C_0 + SIFS \quad (3.6)$$

where $R$ is the range of the sensor. The time that a sender node will wait for an ACK before it retransmits the DATA can be also defined as:

$$T_A = d(s, i) \cdot A_0 + SIFS \quad (3.7)$$

where $A_0$ is a constant.

If the set $V_s$ is empty, meaning that there is no available node, within the range of the sender node, which will make process toward the destination, the relay node is not updated. This comes from the fact that in the next time slot there will be other nodes available (because node availability is independently generated) that could provide advancement toward the destination.

The described packet mechanism is illustrated in Figure 3.4.
Figure 3.4: Packet relaying mechanism.

### 3.4.6 Module state diagram

The state diagram of a single module is shown in Figure 3.5. At the beginning, every module is at the sleep stage, (A). If the target appears in the range of a sensor, this node becomes the source node and creates a packet with all the necessary information about the target location, time of appearance etc, (B1). Then, the source node keeps sensing each channel in the data group channel until it finds a vacant data channel, (B2). When an available channel is found, the source node sends a polling tone to its surrounding nodes and waits for the first CTS, (B3). If there is no CTS after $T_c$, the source node sends again a RTS request. When a CTS is received, the node sends the DATA packet to the next node and waits for $T_A$ time, (B4). If there is no ACK it sends the packet again otherwise it goes to sleep mode, (A).

When a node receives an activation request, it starts listening to the channel, (C1) for RTS time:

$$T_R = SIFS.$$  \hspace{1cm} (3.8)

If there is RTS, it backoffs for $T_i$ time, (C2), otherwise it goes back in sleep mode. After $T_i$ time it sends a CTS and waits for DATA packet for $T_w$ time, (C3). If it receives any
data, it sends back an ACK, (C4), and tries to transmit the packet, (B2). If there is no data after $T_w$ time, it goes back in sleep mode, (A).

This state diagram tries to reduce the energy consumption of the network. When a node is not participating in any message transmission, it should be in a state of low power consumption. This will expand the lifetime of each individual node and consequently the lifetime of the network.

### 3.4.7 Network Example

Figure 3.6 shows an example of the sensor network. The source node has a link with each neighbor node in its range. Each link has been assigned a delivery probability, while for each node there is also the distance ($d$) between this node and the destination node.

Initially, $E_{src} = \{A, B, C, D\}$ and $V_{src} = \{A, B, C\}$. Node $D$ has been excluded because it is further away from the destination node than the source node. The sender
Figure 3.6: Example three-node network, with packet error rate shown along the edges of the graph and the distance (d) from the destination node.

node will try to transmit to the node closer to the destination, node B. Between each relay candidate in $V_{src}$ and the sender node there is a PER, from formula (3.1). If the transmission is not successful, due to the PER, the sender will try to transmit to the next available node, closer to the destination. In the example this should be node A. If there is another unsuccessful transmission, it will try to transmit to node C. Node C will probably receive the data, because of the low PER. If the transmission fails in all the nodes in $V_{src}$, the sender node will count a hop, and repeat the same procedure. The node which will finally receive the packet, it will become the new sender node and it will follow the same procedure. This procedure is a way to simulate the opportunistic handshake between the different nodes.

### 3.5 Opportunistic Routing in Panda-Hunter Game

In this section we will apply the opportunistic routing described before in the Panda-Hunter Game.

We illustrate the algorithm for the source node $s$ and any relay candidate node in Algorithm 2 and Algorithm 3, respectively.
Figure 3.7: Algorithms for the source node and any relay candidate node.

The whole procedure is depicted in Figure 3.8.

When the Panda appears in the monitoring area of a node, this node becomes the source node and sends an activation request to all the neighbor nodes, depicted in Figure 3.8(a). In this way, the source node finds all the neighbor nodes. Then, it broadcast a RTS message, shown in Figure 3.8(b). The transmission of the RTS message may fail for some nodes which are far away from the transmitting node. This is because the PER increases as we increase the distance between the participating nodes, (Equation 3.1).

The nodes that received an RTS message may reply with a CTS message. The CTS message transmission is subject both in PER and in node availability. A node first decides if it is available to transmit (there are no other messages waiting to be transmitted) and then replies with a CTS. Then, this CTS may fail because of the PER. As a result, some nodes which received a RTS may not reply with CTS and will be excluded from
Figure 3.8: Opportunistic Routing in Panda-Hunter Game.
the relay candidate set, shown in Figure 3.8(c). Nodes that are further away from the destination than the source node, will also be excluded, shown in Figure 3.8(d). Finally, from the remaining nodes, the source node will choose to transmit to the node that is closer to the destination, as shown in Figure 3.8(e). That node is the node which replies quicker with a CTS, according to Equation 3.4. The node which receives the data will become the new source node and will follow the same procedure toward the destination, illustrated in Figure 3.8(f).

3.6 Security Analysis

Opportunistic wireless networks can provide an attractive solution to the source-location privacy problem. The routing path between the source and the destination dynamically changes based on bandwidth and node availability. There are a number of different paths from the source toward the destination node, shown in Figure 3.9. The message can follow any of those paths, based on network conditions, making it difficult for the adversary to locate the source. With the different paths we obtain two main advantages for source location privacy:

Figure 3.9: Different paths toward the destination.
• Any potential eavesdropper does not make progress toward the location of the source with every message. If the eavesdropper moves to a node in a large-scale network, shown in Figure 3.10(a), the possibility that the next packet will be transmitted through that node is minor. Following an opportunistic routing scheme, the packet will be transmitted through other nodes which are available for immediate transmission, as illustrated in Figure 3.10(b). As a consequence, the adversary is not overhearing a message in every time slot.

![Figure 3.10: First security advantage.](image)

• Opportunistic routing scheme, try to achieve high throughput over lossy wireless links. There is always the possibility for a packet to be successfully transmitted over a link with high packet error rate (PER), shown in Figure 3.11(a). However, it is very difficult to follow that link for second or third time, especially in sequence, because of the high value of PER or the link might break. If the eavesdropper has been led to a node which receives packets with high packet error rate, it will have to stay there for too long or it has to go back to the previous node, while the source keeps sending out packets safely, shown in Figure 3.11(b).
Therefore, exploiting the spatial diversity in a more efficient way could provide source-location privacy without increasing the complexity.

### 3.7 Summary

In this chapter we have introduced an opportunistic routing protocol to enhance source-location privacy in wireless sensor networks. We have started with a description of the opportunistic routing which is a relative new approach in the network routing area. A classification and a review of the existing opportunistic routing protocols followed. Opportunistic routing protocols can be classified based on the rules they use for the next relay node selection. Our approach is based on the distance between the nodes. A detailed description of the implementation of the protocol was also presented in this chapter. That protocol was observed in the Panda-Hunter Game where the main advantages on the security was pointed out.
Chapter 4

Performance Evaluation in Terms of Privacy

In this chapter we will present the simulation to evaluate the performance of different protocols in terms of privacy. Shortest-path, flooding, phantom and opportunistic routing have been simulated. First, we point out some main drawback of shortest-path, flooding and phantom routing in source-location problem and then we present results for all the four protocols. We conclude this chapter with a comparison between all the protocols.

4.1 Routing Protocols

In this section, two commonly used protocols, shortest-path and flooding routing are discussed in terms of privacy. “Phantom” routing, which can deliver source-location privacy, also discussed in this section.

4.1.1 Shortest-Path Routing

Shortest-path routing is a commonly used protocol in networks [47]. It is easily implemented and can deliver relative small message latency. When the network has been
deployed, a configuration phase is taking place. After that phase, every node in the network knows the path with the less hops, shortest path, toward the destination. As a consequence, that protocol will provide a small message latency for the source-location problem. As described in the previous chapter, one of the security metrics that are used for that problem is message latency, in number of hops. Hence, when the shortest distance, through reliable links, between the source and the destination is $N$ hops, message latency will also be $N$ hops.

However, shortest-path routing is inefficient in source-location privacy problem. The reason for that is because every message from a node follows the same path toward the destination. The eavesdropper, who is located next to the destination, has just to follow that path and reveal the location of the source. In terms of privacy, when the distance between the source and the destination is $N$ hops, the eavesdropper will need $N$ hops to reveal the source node, hence $N$ messages. As a result, the safety period will be $N$ hops.

### 4.1.2 Flooding

Another commonly used routing protocol is flooding [47]. One may think that flooding can provide strong privacy protection since almost every node in the network will participate in the data forwarding, leading the eavesdropper far away from the real source. Instead, flooding routing provides only a modicum of privacy protection, since it allows the adversary to track and reach the source location within the minimum safety period.

When the source node has a message, it floods it to all the neighbor nodes. Every node that receives the message will follow the same procedure. The eavesdropper is located beside the destination node and as described in previous chapter it has memory in order to remember which messages it has overheard. The first message that the eavesdropper will overhear, is a message that follows the shortest path between the source and the destination. Consequently, the eavesdropper will follow that path and reveal the source. For instance, if the shortest path between the source and the destination is $N$ hops, then
the eavesdropper will reveal the location of the source after $N$ messages, hence, the safety period will be $N$ hops.

Apart from that, flooding routing has another important drawback. It consumes too much energy since there are many message transmissions and almost all the nodes of the network are participating in message transmission. Energy consumption is one of the main challenges in wireless sensor networks, as discussed in previous chapter.

### 4.1.3 Phantom Routing

A well known protocol for the source-location privacy problem is “phantom” routing, introduced from Kamat et al [15]. “Phantom” routing protocol involves two phases: a random walk for a number of hops and a subsequent flooding/single path routing toward the destination.

During the first phase, the message is transmitted toward a random destination for a number of $h_{\text{walk}}$ hops. The node that will receive the message after that phase will become the new phantom source of the network. This procedure is illustrated in Figure 4.1(a). In the second phase, the phantom source will transmit the message toward the destination using a single path routing, shown in Figure 4.1(b).

The asymptotic probability of the phantom source’s location with distance $d_{\text{ph}}$ from the real source, after $h_{\text{walk}}$ random walk steps, is given by:

$$p = 1 - e^{-d_{\text{ph}}^2/h_{\text{walk}}}.$$  \hspace{1cm} (4.1)

According to formula (4.1), the probability for the “phantom” source’s location with distance $d_{\text{ph}} < h_{\text{walk}}$, after $h_{\text{walk}}$, is given by

$$p = e^{-d_{\text{ph}}^2/h_{\text{walk}}} - e^{-(d_{\text{ph}}+1)^2/h_{\text{walk}}}.$$  \hspace{1cm} (4.2)

The main drawback of that approach is that phantom routing is inefficient in making the phantom source far away from the real source of the network, depicted in Figure
4.1(c). The probability for the distance between the “phantom” and the real source, after $h_{walk} \in \{10, 20, 30, 40, 50\}$, is shown in Figure 4.2. It is highly possible that the distance between the “phantom” source and the real source is within $h_{walk}/2$. Although the packet was transmitted a number of times, equal to the number of $h_{walk}$, the distance between the “phantom” source and the real source, in hops, is usually smaller than the number of the $h_{walk}$ hops.

Another important drawback of phantom routing is the energy consumption. Random walk phase is not only inefficient, but also consume too much energy. The message is
transmitted toward any destination and to nodes that are further away than the source node from the destination node. This problem is alleviated with opportunistic routing which only use nodes toward the destination.

During the second phase, a single-path from the “phantom” source toward the destination is followed. A configuration phase should take place before starting to transmit messages, in order for all the nodes to know a single path toward the destination.

### 4.2 Simulation Parameter

#### 4.2.1 Simulation scenario

In order to facilitate the discussion and analysis of source-location privacy in wireless sensor networks, we need to select an exemplary scenario that captures most of the relevant features of both sensor networks and potential eavesdropper in asset monitoring
applications. We will use a generic asset monitoring application, the Panda-Hunter Game, which we described in a previous chapter.

We have one source node, one destination node and an adversary. Initially, the adversary is located next to the destination node. Once it detects a message, it moves to the node which transmits that message. In the same time slot, the adversary may detect more than one message, because in the opportunistic routing each message can choose different paths to the destination node, with different numbers of hops. When the adversary detects multiple messages, it moves randomly to one of the transmitters.

The adversary has also a cache memory. Multiple copies of the same message may traverse different portion of the network, and hence, it is possible for the hunter to overhear multiple copies of a message in different time slots. Therefore, we assume that the hunter can tell whether a message is new or not by comparing it with a list with all the previous observed messages in its cache. Further, because the adversary has a limited memory, we assume that a LRU (Least Recently Used) cache replacement policy is employed, in order to ensure that the most recently overheard messages are always kept in cache.

4.2.2 Experimental Environment

The simulation was performed via the discrete event simulation system OMNET++ [48]. A number of nodes $N$, with radio transmission range $R$, are uniformly randomly distributed over a square target area $S$. All the parameters values conform to the list in Table 4.1 and the communication parameters were chosen based on IEEE 802.15.4, as listed in Table 4.2 while the number of transmission power levels was set to 15.

We have chosen randomly 10 different pairs of source-destination nodes, in order to explore different subnetworks of the main network and took the average safety period and average message latency. Moreover we simulated different distances, in hops, between the different pairs. In every pair, opportunistic routing performed better, in safety period and
message latency, than the other three protocols. For the opportunistic routing approach, we only consider links with \( PER < 80\% \). If there is no CTS or there are no more neighbor nodes, a hop count is added to the message which is transmitted back to the previous node.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N )</td>
<td>Number of all the nodes in the network</td>
<td>2000</td>
</tr>
<tr>
<td>( R )</td>
<td>Radio transmission range</td>
<td>12m</td>
</tr>
<tr>
<td>( S )</td>
<td>Square target area</td>
<td>40,000((m^2))</td>
</tr>
</tbody>
</table>

Table 4.1: Variable Notations and Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F_d )</td>
<td>bit</td>
<td>(128 \times 8)</td>
</tr>
<tr>
<td>( n )</td>
<td></td>
<td>2.5</td>
</tr>
<tr>
<td>( A )</td>
<td>dB</td>
<td>−31</td>
</tr>
<tr>
<td>( \sigma_n^2 )</td>
<td>dBm</td>
<td>−92</td>
</tr>
<tr>
<td>( P_t )</td>
<td>dBm</td>
<td>−4</td>
</tr>
</tbody>
</table>

Table 4.2: Communication Parameters Setup

### 4.3 Simulation Results

We have simulated all the four protocols. In this section we show the significant safety period gain achieved by the opportunistic routing protocol, compared to the other three protocols.

**Safety Period**

Simulation results on the average safety period are depicted in Figure 4.3. As it was expected, flooding and shortest-path routing performs the same. Moreover, the safety
period increases linearly and it has the same value with the distance, in hops, between the source and the destination. In opportunistic routing, the safety period is always greater than that in phantom. In phantom, after the random phase, the “phantom” source follows a single path routing toward the destination. After the arrival of the first packet, and since the “phantom” and the real source are close to each other, the probability the adversary overhears a packet in every time slot and making progress toward the area of the two sources, increases. In opportunistic routing, every node can transmit to one of its neighbors in its relay candidate set, based on the PER, decreasing the probability for the adversary to overhear a packet in every time slot. Furthermore, the safety period is greater when we increase the distance between the source and the destination. This is the result of the increased number of dynamic paths that each node has when there are more nodes in the path between source and destination. When there are more nodes between the source and the destination, the relay candidate set of each node increase leading to more paths.

**Message Latency**

Simulation results on average message latency are depicted in Figure 4.4. *In flooding routing, we consider the message latency only for the one message that arrives first to the destination.* As a result, flooding and shortest path routing performs once again the same. The delivery latency for the single-path phantom increases with the distance between the source and the destination. A reason for that is that during the random phase, the message can be transmitted toward any direction. Hence, it might be transmitted to nodes that are further away from the destination than the source node. On the other hand, in opportunistic routing, all the nodes that participate in a message transmission are toward the destination.

Moreover, in opportunistic routing the decision for the next relay node is made locally, before each transmission. In this way, opportunistic routing may succeed in transmitting over a link with high packet error rate and decreasing the number of the hops needed
Figure 4.3: Average safety period for different source-destination separation.

To reach the destination. Shortest path routing follows the shortest path toward the destination, which consists of links with successful delivery 100%. This path, although it can provide 100% delivery ratio, does not make use of the advantage of the broadcast nature of wireless communication. As a result, opportunistic routing can deliver better message latency.

### 4.4 Discussion

Opportunistic routing can enhance source-location privacy. It also performs better than the other three routing protocols. It is not adding extra overhead to the messages (phantom routing include direction information in each message), and it tries to achieve high throughput over lossy links.

However, there is a main drawback for the opportunistic scheme, that was observed
in the simulations. In a stable network, the nodes location are fixed and there is not much changes in the network. Sensor networks should be relatively stable for sufficiently long durations of time during their operation. In this situation, with an opportunistic routing scheme always the same node will win the completion to be the next relay node. As a result, the source-destination path will be fixed (which is usually the case in WSN) and the eavesdropper will simply locate the source location after a while.

In order to cope with that problem we are introducing three different approaches of this opportunistic protocol. We will describe these approaches in the following chapter.

### 4.5 Summary

In this chapter we have evaluated the performance of four routing protocols. We discussed some drawbacks of the commonly used protocols and we also point out a main drawback
of “phantom” routing. Based on simulation results, opportunistic routing protocol was found to deliver better source-location privacy. However, the simulations have pointed out some other drawbacks of the opportunistic routing. In the following chapter, we are trying to cope with these drawbacks.
Chapter 5

Different Opportunistic Routing Approaches

In this chapter, three different approaches based on the previous opportunistic routing protocol will be introduced. In a stable network, opportunistic routing tends to use the same nodes making it easy for the eavesdropper to reveal the location of source. To alleviate this problem, we introduce three extensions, one with memory in order to avoid using the same nodes in sequence transmissions and two with random factors. A performance comparison of all four approaches is also made, in terms of energy consumption and delivery ratio. The chapter will conclude with a performance analysis of all the approaches in terms of privacy.

5.1 Non-repeating Opportunistic

Non-repeating opportunistic routing tries to avoid using the same nodes in sequential transmissions, with the use of memory. In this second opportunistic routing approach, every node in the network is able to remember if it has transmitted a packet in the previous time slot. When a node transmits a packet in a time slot, a true flag in the node is raised. If in the next time slot this node gets a RTS message, it will not respond
Algorithm 4: Candidate Node- Approach 2.

1 if (isRTS(rts)) then
2    if (flag != TRUE) then
3       \( T_i \) = CalculateBackoff();
4       wait(\( T_i \));
5       Channel = ChannelSensing();
6       if (Channel == IDLE) then
7          SendCTS(rts.SenderNode);
8          interval = \( T_w \);
9          reason = Listen(interval);
10         if (reason == DATA) then
11            SendACK(DATA.SenderNode);
12            flag = TRUE;
13          else
14            GoToSleepMode();
15          end
16        else
17            GoToSleepMode();
18        end
19      else
20        flag = FALSE;
21        GoToSleepMode();
22      end
23 end

with a CTS message but it will change the status of the flag to false again. In this way, a node will not transmit two packets in a sequence, and the adversary could not make progress toward the destination in every time slot.

In this approach the algorithm for the source node remains the same while there are differences in the algorithm of the relay candidate node, Algorithm 4. Comparing with the previous Algorithm 3, the differences are in the lines 2,12 and 20. The candidate node in Algorithm 4 before replying with a CTS, checks the value of the flag variable. If this is FALSE, (line 2), and this node becomes the next relay node, after receiving the data, the value of the variable will change to TRUE. Otherwise, if the value of the flag variable is TRUE, it implies that this node has participated in the previous transmission. Therefore, this node will not transmit again in this time slot, but before the node goes
back in the sleep mode, the flag variable becomes again FALSE, (line 20), in order to be able to participate in future transmissions.

### 5.2 Opportunistic routing with random delay

In equation (3.4) we have explained the way a node responds to a RTS message after time $T_i$. The node that is closer to the destination will reply first. In this third opportunistic routing approach we have added a random delay in the backoff time of each node. The node calculates the backoff time from equation (3.4) and then adds a random delay in the range $[0, 1)$. This leads to a more random selection of the relay node. Although it takes into account the distance from the destination, it is also based on a random delay.

Again in this approach the algorithm for the source node remains the same while there are differences in the algorithm of the relay candidate node, Algorithm 5. Comparing with the Algorithm 3, the difference is in line 3, which indicates the backoff time. In the
calculated $T_i$ time, this approach adds a random delay in the range of $[0, 1)$ by employing the \textit{random number generator function} $\text{dlb\texttt{rand}}(0, 1)$ to generate a random double number in the range $[0, 1)$.

### 5.3 Opportunistic routing with random relay node

**Algorithm 6:** Source Node - Approach 4.

```plaintext
1 if (isNewMessage(msg)) then
2   BroadcastRTS();
3   interval=$T_{R_{all}}$;
4   reason=Listen(interval);
5   while (reason!=$T_{R_{all}}$) do
6     if reason==$CTS$ then
7       relaycandidate\_list.push(CTS.SenderNode);
8     else
9       BroadcastRTS();
10      interval=$T_R$;
11      reason=Listen(interval);
12     end
13   end
14   RelayNode= relaycandidate\_list(intr\_rand(relaycandidate\_list.size()-1)) ;
15   SendMessage(msg,RelayNode);
16   interval=$T_A$;
17   reason=Listen(interval) ;
18   while (reason!=$ACK$) do
19     SendMessage(msg,RelayNode);
20     interval=$T_A$;
21     reason=Listen(interval) ;
22   end
23   GoToSleepMode();
24 end
```

In the fourth approach the selection of the relay node is completely random. When a node broadcasts a RTS message, it waits for most of the nodes to respond. The node will wait for a specific time limit, equal to the time needed for a node on the borders of the transmission range to respond. After that time, it selects randomly one relay node between those nodes that have responded with a CTS message.
In this approach, the algorithm for the source node is different, Algorithm 6, while the algorithm for the relay candidate node is the same as Algorithm 3. Comparing with Algorithm 2, the differences are in lines 3, 5, 6, 7 and 14. Line 3, indicates the new backoff time which is $T_{R_{all}}$ and is equal to:

$$T_{R_{all}} = C_0 \cdot RFRange + SIFS, \quad (5.1)$$

where $C_0$ is a constant and $RFRange$ is the transmission range of the sensor, in meters.

This time is sufficient for nodes located in the border of the range of the source node to reply with a CTS. Line 5 indicates that the source node will continue listening for CTSs till the end of the time $T_{R_{all}}$. Whenever the source node receives a CTS message, (line 6), it sorts the ID of the sender in a list off the possible candidates (relaycandidate list), (line 7). At the end of the time $T_{R_{all}}$, the source node chooses randomly, with the use of the $intrand()$ function, the next relay node, (line 14).

### 5.4 Performance Analysis of the Different Approaches

To evaluate the performance of the schemes proposed, we pursued simulations using OMNET++ [48], in terms of energy consumption, delivery ratio and node participation number.

The simulation parameters are the same with those in Chapter 4. The only difference is that this time there is no adversary. The source will send 1000 messages toward the destination.

#### 5.4.1 Energy Consumption

Energy consumption is an important aspect of every sensor network. Measuring the energy consumption of the proposed scheme will also help as to evaluate the performance of the proposed state diagram, in Chapter 3. When a node is not transmitting it should be in a sleeping mode with low energy consumption.
Let the node power consumption in transmitting and receiving/idle modes be denoted by $P_t$ and $P_{r/i}$ respectively. The sleeping mode power consumption is practically 1000 times smaller than $P_t$ and $P_{r/i}$, which is negligible. Let $P_t = 15\, mW$ and $P_{r/i} = 10\, mW$ [49]. Figure 5.1 shows the simulation results.

Non-repeating opportunistic routing approach has similar energy consumption as simple opportunistic routing. These two approaches differ only in the relay node selection process. The non-repeating approach avoids using the same node in sequential packet transmissions, leading to different paths toward the destination. However, the energy consumption is almost the same for both approaches. This can be explained from the fact that the selection process in the non-repeating opportunistic will choose the second best node, closest to the destination. The path through that node toward the destination will have the same or a number of extra nodes, comparing to the path through the node closest to the destination. This will happen in every transmission, leading to the use of a number of nodes close to that of the simple opportunistic routing. As a result, although this approach will lead to a different path toward the destination, the number of the nodes that are used will be almost the same and consequently the energy consumption
as well.

Opportunistic routing with random delay consumes more energy than the previous two approaches. In that approach, each source node has to stay active longer, waiting for a CTS. This is because in every relay candidate nodes an extra delay has been added. In addition, each relay candidate node has to wait, and remain active, for a longer period because of that extra delay. As we have explained, that period is random, leading each individual candidate node to stay active for different period. Some of the nodes may stay active only a modicum of time while some others may stay active for longer period. As a consequence, in this approach we have greater energy consumption, comparing to the previous two approaches.

Opportunistic routing with random relay consumes the most energy over all. In this approach, every node that has a packet to transmit stays active the maximum time, waiting for more than one CTS. That maximum time is equal to the time needed for a node which is located on the border of the transmission range of the source node, to reply with an CTS. However, in contrast with opportunistic routing with random relay, every transmitting node and relay candidate node has to stay active for the same period, because all the nodes have the same transmission power. Consequently, based on Equation 5.1 they have to stay active for the same time $T_{R_{all}}$. Moreover, this approach tends to use all the available nodes in the network. This is because the selection criteria are random and any node from the relay candidate set can become the next relay node.

5.4.2 Node Participation

Node participation defines the total number of the nodes participating in message transmission. Node participation can be used as a metric for the number of the paths that have been followed toward the destination. The more nodes that participated the more paths that have been used. We have examined the node participation of the different schemes, under different message frequencies, in order to see the performance of each
approach under different traffic volume. Figure A.1 shows the results.

![Graphs showing node participation under different traffic volume.](image)

Figure 5.2: Node participation under different traffic volume.

In general, in all the four approaches, as we increase the source-to-destination distance, node participation also increases, for all the message frequencies. This can be explained from the fact that there are more nodes between the source and the destination and these nodes should be used to reach the destination. Moreover, every individual node has a larger set of relay candidate nodes hence, it can use more nodes.

For specific distance between source and destination, these two approaches use the more nodes for high traffic volume. As we described before, these two approaches tends to use almost the same nodes for message transmission. When there are too many messages to be transmitted in small time,(high traffic volume), these nodes become unavailable for instant message transmission. Message frequency 1/1 means that in each time slot, the source should send a message. A node has just received a message in the previous time
slot, might not be able to receive another message immediately. As a result, when the traffic volume is high, these schemes are forced to use different nodes. Hence, for specific distance from the destination, as the message frequency decreases, nodes participation also decreases.

Opportunistic routing with random delay uses more nodes comparing to the previous two approaches. This approach has more random criteria for the next relay node selection, hence, it uses more nodes than opportunistic and non-repeating opportunistic routing. However, for specific distance from the destination, this approach also tends to use more nodes for high traffic volume. An explanation for this is that high traffic volume may lead to more collisions and node unavailability. Consequently, more nodes should be used for message transmission.

Opportunistic routing with random delay performs almost the same for any message frequency. Next relay node criterion of that approach is complete random. As a result any change in the traffic volume will not affect it. The probability to use the same node in sequential transmissions is small. Moreover, as we were expecting, this approach tries to use most of the available nodes in the network.

More results on node participation can be found in the Appendix.

5.4.3 Delivery Ratio

Delivery ratio can be used as a metric for the number of the successfully transmitted messages. Delivery ratio is really important in monitoring application where all the messages should arrive to the destination correctly and in time.

In order to explore the delivery ratio of the different approaches under different network traffic, we have simulated all the approaches for four different packet frequencies: 1/1, 1/2, 1/3, 1/10. Figure A.2 shows the results.

In general, for one message in every time slot, it is noticed that the delivery ratio drops when the distance between the source and the destination increases. This is primarily
because of the traffic collisions and the packet losses caused by the high traffic volume.

As the source-to-destination distance increases, simple opportunistic and non-repeating opportunistic routing performs worse than the other approaches. These two approaches tend to use the same node for message transmission leading to more collisions. As the number of the nodes that should participate in each transmission increases more packet losses and collisions take place. Opportunistic routing with random delay performs a little better because of the random criteria for the next relay node. In contrast, the opportunistic with random relay, which is highly probable to use different nodes for every packet transmission, performs better than all the other approaches.

As the traffic volume decreases, the performance of all the approaches is getting much better. Usually, for large scale monitoring networks, it is not necessary for all the nodes to be active at the same time and in practice, the percentage of active nodes might be
very low. The transmission frequency also tends not to be very high, i.e., the traffic volume may be low. If the transmission frequency is one packet in every three or more time slots we can ensure 100% delivery ratio for all the four approaches.

### 5.4.4 Message Latency

Message latency is the number of hops that a message follows toward the destination. Figure 5.4 shows the results for the average message latency of the four opportunistic approaches.

Figure 5.4: Average message latency for different message frequencies and for 1000 messages.

In general, message latency does not change dramatically with the increase of traffic volume. It can be inferred that although different paths are followed under different
traffic volume, as we discussed in node participation section, all these paths have the same message latency on average.

Opportunistic routing with random relay has the greatest message latency. This is mainly because the selection criterion is completely random. The only requirement is the next relay node to be toward the destination. Hence, as we increase the distance, and the number of the nodes, between the source and the destination, more nodes conform to that requirement. As a result, message latency has increased.

5.5 Comparison in Terms of Privacy

In this section, we compare all the four opportunistic routing approaches in terms of privacy. The simulation parameters are the same with those in Chapter 3.

Safety Period We have made the assumption that after 1000 messages the monitoring asset will leave the specific location, hence, the source node will change. In every opportunistic routing approach, the safety period is always greater than that in phantom. Opportunistic routing with a flag performs similarly to the single opportunistic routing when the distance between the source and the destination is small. Only when the distance is greater, and there are more nodes between the source and the destination the use of the flag leads to better performance. For the opportunistic routing with random delay, the performance is much better. Moreover, in greater distance between the source and the destination, the target is provided with enough safety period to disappear from the area. This is because there are more nodes, and as a result more choices for the opportunistic routing with random delay. Opportunistic routing with random relay performs better than all the others because it might use any relay node in every time slot, thus, increasing the different paths toward the destination and making it difficult for the adversary to overhear any packet.

Message latency
The main drawback of the opportunistic routing with random relay approach is the message latency. As can be seen in Figure 5.6, because a node waits for all the neighbor nodes to response to a RTS, this leads to the worst delivery latency compared to all the other approaches and the phantom. The other three opportunistic routing approaches perform much better than the phantom with respect to the delivery latency. The explanation for that is the fact that the decision for the next relay node in every opportunistic scheme is made locally while for the phantom, we have a predefined path toward the destination. In this way, an opportunistic scheme can use paths that will transmit the message to the destination in smaller number of hops than a predefined path, and decrease message latency. We can also use message latency as a metric for the energy consumption. As we can see in Figure 5.6, message latency for the four opportunistic approaches is inversely proportional to energy consumption of those approaches, which was presented in previous chapter.
5.6 Discussion

In terms of security, every opportunistic routing scheme that have been used has advantages and disadvantages while all of them perform better than phantom routing.

Simple opportunistic routing is a good solution for the source location privacy. The main advantage of that approach is that it is simple to be implemented, because only simple processing in the nodes is needed. This approach does not add any overhead while it is easy to program the nodes in order to take advantage of the broadcast nature of wireless communication. Although it can provide enough source-location privacy, with low energy consumption and message latency, the network condition may not be stable. This approach is ideal to be used in a network where nodes are added and removed constantly or the channel has a great interference. For instance, a network with mobile source and/or mobile sink would be a good candidate network for this approach. That will force the nodes to make use of the opportunistic links and adapt to the new network conditions fast. If the network is stable, then the nodes that are used will be the same and the safety period will not be high.
To cope with that problem, we have introduced the non-repeating opportunistic approach. We have added a flag in each node which does not increase the overhead too much. The second approach can perform a little better than the single opportunistic in a non stable network. The main drawback is once again, in a stable network although this approach will perform a little better than the single opportunistic but might not provide the source with sufficient safety period.

For stable network conditions, we have introduced the other two approaches, which are using random criteria in order to include randomness in the choice of the next hop node and eventually to the path.

Opportunistic routing with random delay includes some extra processing in the nodes because of the use of the extra timer needed. In a stable network, that approach performs much better than the other two and can deliver enough safety period to the source. Opportunistic routing with random delay is the best approach, among the four, for a stable network in terms of security and energy consumption. For a non stable network, simple opportunistic would be chosen because of the small message latency.

If we focus on the safety period and we are not interested in message latency, then opportunistic routing with random relay is the best solution. A network that is used to deliver crucial message, like data, between a source and a destination and is not focused on delivery time is ideal for that approach. Moreover, that approach can always provide delivery ratio of 100%. Finally, that approach can provide extremely high safety period for that network.

In general, all the approaches have advantages and disadvantages in terms of network performance and in terms of network security, as pointed out in this chapter. The most important thing is that for almost any network category, an opportunistic routing approach with little or no overhead can be adapted to provide source-location privacy. This indicates that enhanced privacy is an inherent property of opportunistic routing concept.
5.7 Summary

In this chapter we have introduced three different variations of the opportunistic routing and the corresponding algorithms. Moreover, we have compared them in terms of energy consumption, node participation, delivery ratio and message latency. Simple and non-repeating opportunistic routing consume less energy than the other two approaches. At low traffic volumes all the approaches can provide 100% delivery ratio. In the following chapter, we will compare the approaches in terms of privacy and security.

We have also compared our results with an existing technique, phantom routing. Opportunistic approaches perform always better than that technique while they are not adding extra overhead. Moreover, we point out a main drawback of phantom routing and we explain how our approaches can avoid that drawback.
Chapter 6

Conclusions

6.1 Contributions

In this thesis, an opportunistic routing scheme for source-location privacy was introduced. Current network protocols are not designed to provide sufficient security to the location of the source, whereas the first approach, phantom-routing, which manages to provide enough source-location privacy, has some important drawbacks. With opportunistic routing we have tried to eliminate these problems.

The initial approach involved the use of an existing opportunistic routing protocol, with the necessary changes, in order to be applied in a monitoring network. Security analysis of that approach shows that opportunistic routing is able to deliver better security than shortest path routing, flooding and “phantom” routing. Simulation with that approach illustrates the theoretical results while it also points out some drawbacks of opportunistic routing. It tends to use the same nodes under stable network conditions.

In order to manage the source-location privacy problem, three different approaches were introduced. One of them uses memory in order to employ different paths toward the destination while the other two try to introduce some randomness. Performance evaluation of all four approaches was conducted and the advantages and disadvantages
of each approach were presented.

Finally, multiple simulations were performed in order to evaluate and illustrate the effectiveness of the different protocols and approaches in terms of network performance and network security. Once again, every approach, with its advantages and disadvantages, was discussed, while all of them performed better than phantom routing protocol in terms of security.

### 6.2 Future Directions

There are two major topics that could extend the approach described in this thesis.

- **Mobile Source and/or Destination.** The effectiveness of the different schemes toward mobile source and/or destination should be examined. One of the main advantages of opportunistic routing is its quick response in network changes, meaning that the protocol will respond quickly to any change. However, because the source and the destination are moving, other eavesdropper techniques should be adopted.

- **Different Eavesdropper Models.** The eavesdropper model in this thesis follows a commonly used movement strategy for the source-location problem. An eavesdropper with better memory capabilities or an eavesdropper with higher hearing radius should also be examined. Moreover, it would be more challenging if the number of eavesdroppers is increased.

Engineering is an art of exploring different tradeoffs. For telecommunications engineering specifically, the tradeoff between power consumption and security has been extensively investigated. However, when wireless sensor networks are considered, studies focused on the tradeoff between application specific security levels and energy consumption cost are just in their initial stages. The proposed opportunistic routing protocol tries to take advantage of the broadcast nature of wireless communication in order to
enhance source-location privacy. We believe more research over that in this area will help to address this problem in the near future.
Appendix A

Appendix

A.1 Chapter 5 more plots

A.1.1 Node Participation

Figure A.1: Node participation for each scheme under different traffic volume.
A.1.2 Message Latency

Figure A.2: Message latency for different message frequencies.
Bibliography


82


