A Wireless Sensor Network System for Border Security and Crossing Detection

Fayez AlFayez

PhD 2015

A Wireless Sensor Network System for Border Security and Crossing Detection

Fayez AlFayez

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

Faculty of Science and Engineering

Manchester Metropolitan University

2015

Abstract

The protection of long stretches of countries' borders has posed a number of challenges. Effective and continuous monitoring of a border requires the implementation of multi-surveillance technologies, such as Wireless Sensor Networks (WSN), that work as an integrated unit to meet the desired goals. The research presented in this thesis investigates the application of topologically Linear WSN (LWSNs) to international border monitoring and surveillance. The main research questions studied here are: What is the best form of node deployment and hierarchy? What is the minimum number of sensor nodes to achieve $k-$barrier coverage in a given belt region? Given an appropriate network density, how do we determine if a region is indeed $k-$barrier covered? What are the factors that affect barrier coverage? How to organise nodes into logical segments to perform in-network processing of data? How to transfer information from the networks to the end users while maintaining critical QoS measures such as timeliness and accuracy. To address these questions, we propose an architecture that specifies a mechanism to assign nodes to various network levels depending on their location. These levels are used by a cross-layer communication protocol to achieve data delivery at the lowest possible cost and minimal delivery delay. Building on this levelled architecture, we study the formation of weak and strong barriers and how they determine border crossing detection probability. We propose new method to calculate the required node density to provide higher intruder detection rate. Then, we study the effect of people movement models on the border crossing detection probability. At the data link layer, new energy balancing along with shifted MAC protocol are introduced to further increase the network lifetime and delivery speed. In addition, at network layer, a routing protocol called Level Division Graph (LDG) is developed. LDG utilises a complex link cost measurement to insure best QoS data delivery to the sink node at the lowest possible cost. The proposed system has the ability to work independently or cooperatively with other monitoring technologies, such as drowns and mobile monitoring stations. The performance of the proposed work is extensively evaluated analytically and in simulation using real-life conditions and parameters. The simulation results show significant performance gains when comparing LDG to its best rivals in the literature Dynamic Source Routing. Compared to DSR, LDG achieves higher performance in terms of average end-to-end delays by up to 95%, packet delivery ratio by up to 20%, and throughput by up to 60%, while maintaining similar performance in terms of normalised routing load and energy consumption.

Acknowledgments

Completion of this thesis marks the eventful journey of my doctoral research, which would not have been possible without the support of several people. I thank Allah for being with me and giving me the strength, perseverance and guidance required in every aspect of my life.

First, I would like to express my sincere gratitude and appreciation to my director of studies, Dr. Mohammad Hammoudeh, for his sustained support throughout the course of conducting this research. His enthusiasm, insight and guidance were invaluable assets, which encouraged me to proceed well beyond my initial ideas. I also want to thank the other members in my doctoral supervision team. I would especially like to thank Professor Martyn Amos and Mr. Ian Niell there supervision has been invaluable and my life has been enriched personally and professionally by working with them. I would like to thank Keith Miller, Rita Kenny, Anne-Maria Walsh, Megan Scofield, and Jonathon Roby. I should also like to thank the Ministry of Higher Education, my sponsor, for its generous financial support.

It is an honour for me to thank my wonderful parents for their unlimited love and support, their encouragement and support is a key factor in any achievement I have ever made. I would like to thank my wife, brothers, sisters, friends, and all the people who have supported me along the way.

Dedication

To my parents, for making it possible to embark on this journey

To my wife, for making it possible to conclude it

May God bless you all

Table of Contents

List of Figures

List of Tables

List of Publications

F. Alfayez, Dr.Mohammad Hammoudeh, & Dr.Omar Aldabbas (2015). Understanding Geospatial Challenges & Technologies: Towards a Hybrid System for Border Monitoring. *Journal Paper submitted to the Defence Science Journal (DSJ). (Under review)*

F. Alfayez, Mohammad Hammoudeh, Abdelrahman Abuarqoub, A Survey on MAC Protocols for Duty-cycled Wireless Sensor Networks, Procedia Computer Science, Volume 73, 2015, Pages 482-489, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2015.12.034.

F. Alfayez, & Ian Niell (2012). Topology-based Optimization of Linear Wireless Sensor Networks. In 2015 European Intelligence & Security Informatics Conference (EISIC 2015). Manchester, The UK, 2013.

F. AlFayez, A. Abuarqoub, M. Hammoudeh, & A. Nisbet (2013). Wireless Sensor Network Simulation: The Current State and Simulation Tools. *Sensors and Transducers Journal (ISSN 1726- 5479) Vol. 18, Special Issue, January 2013, pp. 145-155.*

A. Abuarqoub, **F. Alfayez**, M. Hammoudeh, T. Alsboui, & A. Nisbet (2012). *Simulation Issues in Wireless Sensor Networks: A Survey.* Paper presented at the SENSORCOMM '12: Proceedings of the 2012 Sixth International Conference on Sensor Technologies and Applications, Rome, Italy.

F. Alfayez, (2012). *Linear Structure-based Optimization for Wireless Sensor Networks*. Workshop presented at the OPTNet 2012: International Workshop On Planning And Optimization Of Wireless Networks, Sheffield, The UK.

CHAPTER 1

Introduction and Motivation

This chapter introduces WSNs technologies and their different application as monitoring and control systems. It also gives an overview of the current disadvantages and restrictions of the existing systems implemented for border, pipeline, railway monitoring. The chapter then defines the nature and the specifics of the LWSNs architectures and the challenges present in their implementation in the specific scenario of border surveillance. The motivation for building a new, effective, and scalable network LWSNs architecture explicitly designed for border surveillance is also outlined here.

1.1 Introduction to Border Monitoring

Illegal crossing of international borders has been of serious concern to many countries for the protection of their citizens and to stop any potential threat to homeland security, especially due to the steady increase in organised crime, terrorist threats, smuggling activities, etc. [1-3]. Any gap or monitoring shortfall within the borders might cause severe damage to a country's security. Today, border surveillance is a challenge and requires a high degree of accuracy.

Traditionally, countries, such as those in the European Union (EU), have viewed international border control as mostly an immigration- and customs-based challenge. However, with the increased risks of terrorism, illegal movement of drugs, weapons, contraband, and people, these countries face unprecedented challenges in the area of border security. Border agencies have deployed unprecedented levels of personnel, technology, and resources at international ports, such as airports, to make critical security improvements to secure and manage their borders [4]. However, less attention has been given to safeguarding land and coastal borders from potential threats. There is a growing consensus among EU member states that they need to address the external border challenges and opportunities they face [5].

External border security is now critical to a country's safety and the challenges it poses are changing and likely to intensify. Securing international borders is a complex task that involves international collaboration, deployment of advanced technological solutions, and professional skill-sets. However, there are many factors hindering the development of an effective system for international border security and surveillance. In the current tight financial climate, governments strive to secure their borders while keeping the costs low. This is particularly challenging to achieve given the very long land and maritime border. For instance, the external land borders of the EU from 1 January 2007 are 7,958 km (4,946 miles) and the maritime borders are nearly 80,000 km (50,000 miles) long [6].

With borders of this length, a very large number of trained border guards and resources are essential. However, training and equipping border guards is very expensive. Low paid border guards can lead to problems of corruption, especially in the presence of well-funded gangs. Moreover, it is not always feasible to deploy border guards due to hostile topography, severe weather conditions, and political or military conflicts.

Recent statistics show an increase in the number of threats caused by illegal activity in the eastern border of the EU [4, 5], including illegal border crossing and smuggling of tobacco, vehicles, petroleum products, drugs, etc. One incidence of tobacco smuggling with a value of 15 million euro was discovered in the Belarus-Polish border [4]. Additionally, in one operation, 4 million cigarettes were smuggled between the Russian-Finnish border [4, 5]. In 2012, there were 77.437 illegal crossing between check points in the EU, 1.597 of which were on eastern border [4].

Traditionally, border monitoring is conducted through physical checkpoints conducted by border guards or military units. However, for cost, safety and other resource limitations, the best form of border surveillance involves minimal human intervention. There are many existing systems designed for border surveillance ranging from basic fences and walls to very complex systems. There is an emerging interest in developing intelligent border monitoring systems to increase the efficiency and reduce the cost. Therefore, this research proposes Wireless Sensor Nodes (WSNs) technology as a good candidate to deliver such a system. However, the linear network topology resulting from the linear structure of the monitored area raises new challenges that need to be addressed. The new network structure poses several challenges that have not been addressed in previous literature. We refer to such networks as Chain-typed WSNs (CWSNs) or as Linear WSNs (LWSNs).

The new monitoring systems have much more demanding requirements, which need to be taken into account. The proposed system should address the following challenges [7]:

1. Large, busy, and complex landscape
2. Real-time monitoring of a landscape taking into account variable topography: coastal plains, high mountains, sand dunes, and large deserts
3. The real-time acquisition and interpretation of the evolving landscape
4. Instantaneous flagging of possibly critical circumstances in any weather and illumination conditions
5. The use of heterogeneous technologies to detect a variety of parameters
6. Ability to integrate with other systems
7. The use of passive monitoring

1.2 Introduction to WSN Technology

In the last few years, the world has witnessed the fast-paced development of communication and technology. In terms of communication, ad-hoc networks have advanced the use of mobile devices to establish their own communication links without any intermediary form of connectivity. It has made the nodes more independent, and, therefore, more useful and practical. Technologically, devices have been made smaller, faster, and smarter than ever before. For instance, artificially intelligent devices are no longer dependant on the human to operate correctly. All together, these advancements have led to the invention of technology such as WSNs. A WSN is a combination of small smart devices using an effective way of communication to sense, process, and transmit. They organise themselves and operate to target a specific mission that is addressed by an application.

WSNs are a low cost technology that can provide an effective solution to the range of problems faced in securing borders effectively. This technology offers an intelligence-led, cost effective solution to strengthen vulnerable points on the international borders. A WSN is a set of resource-constrained devices with a communication infrastructure that uses a radio to monitor and record physical or environmental conditions. A network of

unattended self-organising sensors can significantly cut the number of personnel in a border agency. Additionally, the continuous monitoring reduces the chances of missing any potential criminal activity. The ability of a WSN to operate without human involvement and in situations where other surveillance technologies are impractical has made it a favourite for deployment in hostile and/or hazardous environments. For instance, in rough terrains, such as forests, or in severe weather conditions, satellites or air surveillance methods are rendered ineffective. However, WSNs can be easily integrated with existing systems to provide a common data set at every point of intervention. Data integration from multiple systems is a key feature of modern day border control and surveillance systems.

WSN technology is a now a stable technology supported by a vast amount of research, applications, and hardware platforms. Most of the current research and deployments target applications where nodes are deployed with a certain level of redundancy. It is assumed in such deployments that nodes are deployed in a square, circular, or hexagonal area such that each node has multiple neighbours. Node redundancy can be exploited in many ways, including multiplexing traffic over multiple paths to balance energy consumption among nodes and reduce end-to-end delays, prolong network life using duty cycles, provide fault tolerance, and so on.

There is a class of WSN applications that imposes a linear network topology, e.g., international border security, gas/petrol pipeline monitoring, and rail track monitoring. The linear topology has nodes daisy chained using radio communication. Linear WSN topologies are characterised by sparse node deployment, long transmission distances, and alignment of nodes along a virtual line. This range of characteristics introduces new challenges, which makes solutions proposed for traditional WSNs inapplicable to linear WSNs, LWSNs for short.

A WSN can be defined as a group of cooperative nodes forming a network to assess a

common task, that could be monitoring or controlling/allowing interaction between the human/computer and the surrounding area/environment [8]. The advance of WSNs was motivated by military applications, such as battlefield surveillance. Today such networks are used in various applications, such as building security, industrial machine process monitoring, patient remote monitoring, rail track checking, international border monitoring, etc.

Figure 1.1 demonstrates simple WSN architecture.

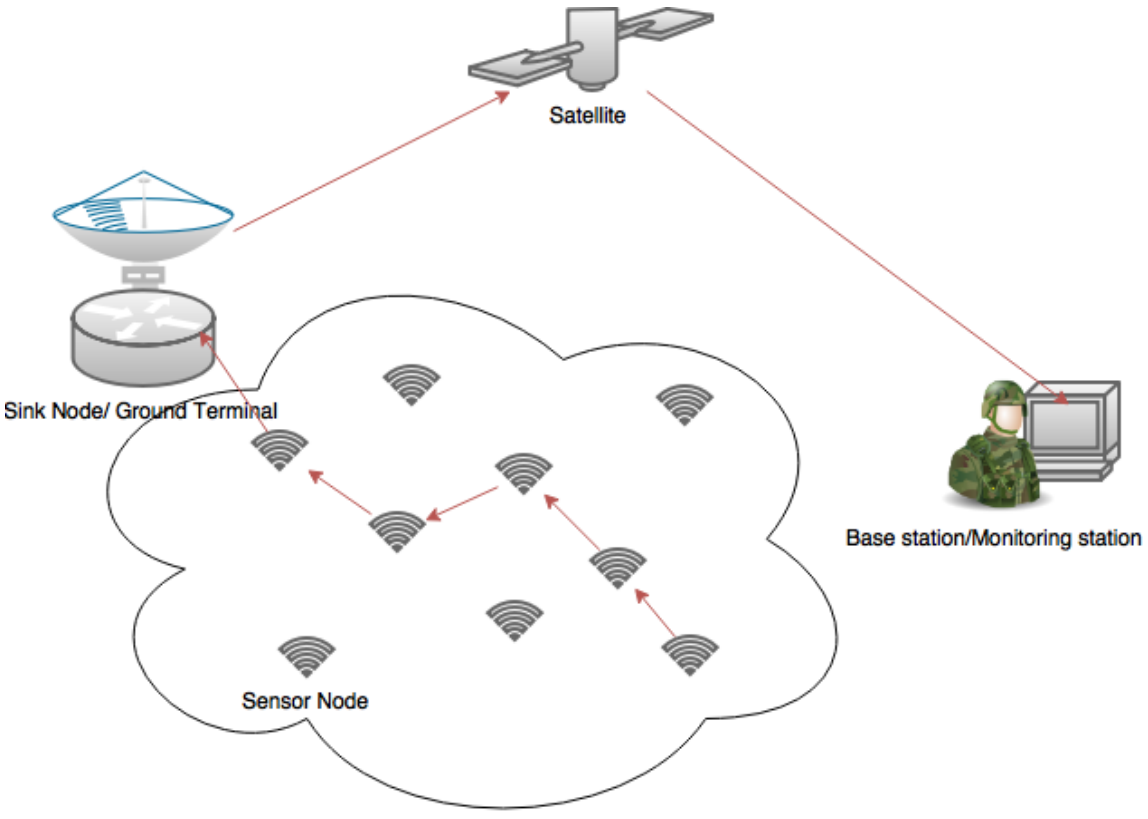


Figure 1.1 Illustrates Simple WSN Deployment

Clearly, specific application requirements and problem domain concerns have a strong influence on WSN system design and implementation. They consist of spatially

distributed autonomous sensors that include monitoring physical or environmental conditions. They started as military technology, mainly for the purpose of battlefield surveillance, but in modern times they are used in many industrial and consumer applications. Their limitations include energy constraints and data collection ability.

1.3 LWSN Definition

WSNs are a well-established and advanced technology that is expected to extend human-centred applications in large-scale remote sensing. Such networks are used in diverse applications to provide accurate assessment where the human presence is difficult, dangerous, and/or expensive. This technology can be deployed to monitor large-scale environments, such as international border surveillance, railway track monitoring, gas/oil/water pipelines leak detection, search and rescue disaster management, river flood alarm, etc. All these applications have a common topological structure that is inherently linear. This is a result of carefully controlled and planned deployment of sensor nodes to closely track the monitored environment, which is linear in nature. We refer to this class of networks as Linear WSNs or LWSNs. The linear architectural network raises a number of issues and new requirements that need to be addressed. An LWSN is defined as any form of WSN that can be limited between two long parallel lines. Jawhar et al. defines LWSNs as “a new category of WSNs where the nodes are placed in a strictly linear or semi-linear form. A WSN is considered linear if one of the following conditions are true: (1) if all the nodes are aligned on a straight line, strictly forming a line, or thin LSN; (2) if all of the nodes exist between two parallel lines that extend for a relatively long distance as compared to their transmitting range and the distance separating them constitute a semi-linear or thick LSN”[9].

LWSNs share the following characteristics that make their deployment and operation a challenging task:

1. Linear topological structure: Sensor nodes are distributed in a linear fashion that includes nodes on curved or approximately straight lines [10, 11].
2. Sparse deployment: In comparison to classical WSN deployments, the number of neighbouring nodes is dramatically limited. Ideally, the network density should be high enough to ensure appropriate sensing coverage and communication reliability in the presence of node failures.
3. Shared communication routes: A node will have two directions of communication: right/forward and left/back. This means that one route through multiple levels can be the efficient route for whole segments, while general WSNs must maintain a route for each node, as the topology is random.
4. Known node location: Typically, node locations are known and the trajectories of any mobile nodes are known.
5. Structure-based duty cycles: As a consequence of 2 and 3, inter-node communication patterns are more constrained than those of standard WSN deployments. Consequently, this structural information may be used in the creation and synchronisation of simple, but effective, duty cycles.
6. The density of deployed nodes must be sufficient to ensure appropriate sensing coverage and communication reliability in the presence of node failures. Often nodes have long radio coverage due to the line of sight deployments; this leads to sparsely interconnected network segments [12] between subsets of nodes over which multi-hop messages can be sent directly from one node subset to another. That means one route through multiple levels can be the efficient route for whole segments, while general WSNs must maintain a route for each node, as the topology is random.

In this work, we focus on the class of applications where node locations closely track

monitored phenomena along a geometrically or topologically linear area, such as a train track or gas pipeline. More precisely, any form of WSN that can be limited between two long parallel lines we consider it to be a LWSN. We refer to this class of WSN as a Linear WSN (LWSN), a form of structured wireless network, and in this proposal we seek to optimise WSNs [12] via exploitation of linear structure within key aspects of a WSN's functionality that will include QoS [13] and efficient routing protocols [14]. The review of existing literature indicates that techniques for exploitation of WSN structure are under investigation and still limited. Many of the research investigations cited in this proposal do not assume nor do they seek to exploit that a network does not have a predetermined WSN structure, which could potentially exploit node redundancy in various sensing and communication tasks [15].

This research seeks to explore the notion that a linear structure can be exploited to further advance reliability, performance, and quality in comparison to a general WSN. For example, positioning sufficient nodes close to data sources and exploiting node location information can ensure that power consumption associated with transmitting sensed information can be shared between a set of nodes when enhancing the performance of a WSN system. LWSNs can enhance spatial and Temporal Resolution TR (indicate the precision of a measurement with respect to time) of the operational environment [16]. Application specific logic can be deployed in sensing networks to increase efficiency by operating only the required portions of a linear network; for instance, in lighting applications we can operate only the needed lights, and calculate the projected requirements concerning the presence and movement of people or cars on and along a road or street. To the best of the author's current knowledge, to date only limited application specific attempts have been made to specialise a WSN to exploit LWSNs' structural and organisational aspects and no generic structure and routing scheme exists for LWSNs. A review of the state-of-the-art research in the LWSN field shows that researchers have dealt with LWSNs from a narrow applications perspective;

for instance, by applying specific routing protocols for monitoring rolling bearings in freight trains [17].

LWSNs have been developed to monitor topologically linear regions, such as oil, gas, and water pipelines [16]; rivers; railways; roads; tunnels; international borders; and electrical power transmission lines [9]. Jawhar et al. [12] proposes potential advantages of LWSNs over general WSNs: fast/cost efficient deployment, reduced requirements for maintenance/human expertise, increased reliability/security, and the ability to efficiently adapt multi-hop message routing protocols.

To date, to the best of the author knowledge, there is no such system that provides a generic and coherent framework for the deployment of LWSNs that exploits knowledge of the underlying network topology in conjunction with application and problem domain specific requirements. According to Jawhar [9], there are many reasons to develop a framework that considers LWSNs' characteristics. For instance, existing routing protocols use generic route discovery, which is far more complex than what is needed for LWSNs and fails to exploit potential optimisations tailored for LWSNs [9, 18]. Avoiding these drawbacks will increase routing efficiency and reduce power consumption. The reliability of LWSNs can be improved as alternative routing links are known in advance [19] and/or more easily determined using structural knowledge rather than relying on generic routing for unstructured networks. Furthermore, generic WSNs have not considered the potential for the exploitation of linearity during the initialisation, configuration, and installation phases. Furthermore, in order to achieve efficient and rapid recovery from node faults, location management and adaptive routing algorithms are needed to reorganise nodes into different subsets for multi-hop routing. It is believed LWSNs can be made more robust by developing customisable protocols to deal with all their specialised requirements.

1.4 Common LWSN Applications

The section briefly reviews some of the most important and common LWSN applications. The purpose of this review is to extract the common features of such applications. The finding from this section will be used to specify the generic LWSN system. Moreover, reviewing the challenges involved in various application areas helps the reader to gain better understanding to the problem of large-scale LWSN system deployment.

1.4.1 Border Monitoring

Illegal crossings of international borders is of great concern to many countries to protect their citizens and to stop any potential threat to homeland security, especially due to the steady increase in organised crime, terrorist threats, smuggling activities, etc. [1]. Any gap or monitoring deficiency might pose a serious security threat. Today, border patrolling has become a challenge and requires a high degree of accuracy. The best form of border surveillance involves minimal human intervention, such as installing WSNs that detect events in the vicinity and report them instantly. There are many existing systems for border monitoring, starting from traditional fences and walls to very complex systems. There is emerging interest in developing intelligent border monitoring systems to increase the efficiency and reduce the cost.

1.4.2 Pipelines Monitoring

Pipelines are an economical way of carrying important resources (i.e. water, oil, gas) over a very long distance that could be several thousand kilometres. One of the longest gas pipelines in the world, the Yamal-Europe Pipeline, distributes gas in Europe from Russia through Belarus, Poland, and Germany crossing a total of $4{,}107km$. This pipeline project started in 1994 and began operating in 2005, with a capacity of carrying 33 billion cubic meters a year [20]. Pipelines have also been built under water, for instance the gas pipeline from Norway Langeled to Easington in England, and even more projects are

being initiated to build underwater pipelines.

Pipelines projects are very important for both economical and residential growth. The cost of any damage to these infrastructures would be highly expensive, not just the cost of repairing but also the cost of being out of service and the harm that may result to the environment.

Such vital resources require constant monitoring to ensure safety and security. It is hard, high cost, and time consuming to detect a pipeline fault or leak. This necessitates having reliable, around the clock monitoring and control of all operations to guarantee a quick response to any problem. This can be approached by LWSNs. Carrillo [21] states that some parameters need to be considered in order to protect the surrounding environment. For instance, the USA Environmental Protection Agency estimated that the maintenance and upgrading of its current water pipes infrastructure would cost $\$ 334.8$ billion, a project that would be undertaken between 2007 and 2027. More than 60% of this will be spent on transmission and distribution [22].

1.4.3 Railway Monitoring

Railway monitoring includes train, underground, over ground, and tram. LWSNs can be deployed in these systems to obtain on time monitoring of the tracks. Transport authorities are very concerned about rail safety and security [23]. Even though transporting by rail is very safe, derailments and train collision still occur [24]. For example, two years ago (2012) a train accident in Buenos Aires killed 49 and left 600 injured. Also, in the same year, 100 passengers were injured in Amsterdam in a train crash. The absence of security monitoring makes railways an easy target for terrorist attacks. Fibre optic sensors have been deployed in railway bridges to monitor dynamic strain and detect any cracks. This system uses phone lines to gather data [25]. In the modern era, WSN technology has also been deployed to monitor tunnels and railways, as it reduces the cost of deployment and increases the scalability of monitoring

railways [26]. In addition, WSNs facilitate the monitoring of the entire railway rather than having a checkpoint at each bridge.

1.4.4 Alternating Current (AC) Link Monitoring

Other applications of LWSNs include an AC link network for both overhead and underground, as LWSNs can help to detect outages that might be caused by any reason, such as overloading. Prompt information can help the utility providers take the right action saving time and expertise. Fault discovery is not needed while the system is providing the location, which reduces the maintenance cost. In addition, this can increase customer trust by delivering a well-monitored service.

New sensors have been developed for electrical parameters, mainly to sense current, power, and voltage. The installation of these sensors can be carried without affecting the AC link. Moreover, in this application, sensors are attached to the power source, which gives the advantage of recharging sensors when needed. This draws the attention of researchers from energy saving to QoS. However, research is needed to ensure proper communications protocols and architecture to improve the QoS and reduce the maintenance and installation cost [9] .

1.5 Challenges Introduced by LWSNs

After reviewing the features of LWSN applications, several challenges related to the optimisation of such networks are identified. First, the application area, e.g., international borders, is vast and requires different node capabilities to cover such a distance. Deploying resource-rich nodes is essential, as resource constrained nodes can not cover such an area. However, the difference in capabilities between nodes creates additional complexity to the system. Therefore, *a new network architecture is needed to coordinate the variable nodes resources*. In addition, the new network must be cost-feasible and capable of being deployed in the real world.

Second, LWSNs can be accomplished by deploying sensor nodes on the monitored area in order to perform the desired task. This installation would be particularly valuable along likely avenues of detection to provide early warning. In practical terms, this means increasing the *width* of the WSN. This installation raises questions of how to determine the required network *width* and node *density*, how to calculating the minimum number of sensor nodes required in a given region, how to determine if a region is indeed covered, and the factors that affect coverage.

Third, nodes in such systems has very long transmission paths to the final destination. The shortest route will not only save energy, but also enhance network performance. The existing routing protocols were designed for networks with higher density, i.e., path redundancy, and far shorter paths than the network in border monitoring. Therefore, *a new routing protocol is required to take advantage of the linearity in the system.*

Forth, such applications do not exhibit many events, and most of the energy is spent in idle time. However, timely data is also important due to the critical nature of the application. Therefore, we *need a Medium Access Control (MAC) protocol that balances these two conflicting requirements*: saving energy during the idle periods by sending them to sleep and ensuring continuous coverage as well as timely data delivery.

Fifth, one vital limitation of WSN sensors is the battery, which is small and has a limited life. Once the battery power is drained, then that particular node will no longer participate in the network. In addition, the loss of one node could create a coverage hole in the network, especially in low density deployments such as LWSNs. Therefore, a MAC Protocol designed not only to control the access to the medium but also to deal with the mentioned challenges above is required. Nevertheless, different applications have different requirements, which adds further challenges to designing a MAC Protocol that suits a variety of LWSN applications.

1.6 Motivation

The design specifications of classical WSN protocols and algorithms makes them ineffective when deployed in border monitoring or other applications that has linear topology [12]. Many assumptions made in the design of classical networks, e.g., node redundancy, are invalid in LWSNs. Therefore, applying protocols that makes such assumptions to LWSNs would be over specifying the system, i.e., adding overhead to deal with problems that no longer exist. On the other hand, the exploitation of the new features introduced by the topological linearity will increase system robustness and performance. However, to achieve this, there is a need for developing a new generic framework for LWSN deployments, which consists of novel network architecture, novel deployment strategy, required network density, and novel communication protocols.

Applying WSN technology for monitoring large-scale areas, e.g., hundreds of kilometres, is another challenge, especially when the physical formation of the landscape pose geographical challenges to the use of sensors [27]. The architecture of such a system, which is characterised by linear topology, has to address a new set of challenges that does not exist in classical WSN deployment. This necessitates the development of a generic framework to respond to the new challenges faced by this class of deployment.

There are many challenges facing WSNs technology; one of the main challenges is reducing energy consumption [28]. The source of energy wasting has to be identified. According to [29] the following node/networks functions have been identified as the main sources of wasted energy: collision, overhearing, control packet overhead, and idle listening. Ye et al. [29] claim that most energy is wasted during node idle listening, i.e., nodes listen to an idle channel for a possible data transmission between nodes. For these reasons, this research investigates the development of a new duty cycle mechanism that exploits the linear nodes topology as a method to save energy in LWSN systems [28].

LWSNs low node redundancy, long transmission distances and strict timeliness constraints imposes special requirements and challenges that make the available communication protocols infective when applied to them. Therefore, there is a need to design a new cross-layer communication protocol that addresses the special challenges of LWSNs and avoids unnecessary complexities in existing communication protocols. For instance, some sources of the energy waste mentioned earlier do not exist and/or has small impact in linear WSNs applications. One example is collision avoidance; collisions are rare in linear topology as nodes have a limited number of neighbours. Therefore, having complex collision avoidance algorithms in a LWSN communication protocol will add unnecessary complexity to the network and extra energy waste.

A crucial aspect of building a linear WSN is the calculation of its width and node density. These important measurements have a direct impact on the network lifetime and a high influence on the energy used for reporting a certain event to the sink. Network lifetime is the continuous time duration for which all the targets in a given area are monitored by the deployed sensors. The goal is to maximize the lifetime of the network, which, on the other hand, should consume minimum resources and produce the necessary coverage. Coverage and connectivity are two crucial issues for the quality of service and performance in the WSNs, which are highly dependent on each other.

Coverage can be defined as to what extent each point of a deployed network is under the vigilance of a sensor node. Coverage gaps should be eliminated to boost monitoring capacity. Efficient coverage can be defined as the network lifetime by describing features like sensing ability and energy consumption by sensing nodes. Special algorithms are considered in this thesis in order to derive the minimal number of wireless sensor nodes required to supervise a given area during a given period.

As mentioned earlier, another important aspect is the connectivity, which has a direct relation to the coverage itself. In a reliable network data processing and transfer between

the nodes and from them to the base station run reliably and with a high quality. LWSNs are used to monitor long linear critical structures such as pipelines, rivers, railroads, international borders, and high power transmission cables. Due to the importance of these structures, the LWSN must be designed with high reliability considerations. However, one of the main challenges of LWSN design is the connection reliability among the nodes.

Unlike in WSNs in where gateway or sink node is reached over several existing routes, which can be exploited to improve the reliability, very few substitute routes are usually available in LWSNs [8]. Defects in a few adjacent nodes in a LWSN may result in creating holes in the network. Nodes located on both sides of a hole may lose their connectivity with each other, which will lead to multiple isolated segments in the network. Consequently, sensor nodes that are positioned between holes may perhaps not transmit their data, which have negative impact on the network's sensing coverage. In addition, the fact that nodes are not placed in equal distance from the sink results in unbalanced energy consumption, which is another issue to solve.

Bearing in mind all these considerations, this report addresses innovative architecture that tackles the mentioned challenges and proposes a solution that is more performant and reliable. To address difference in capabilities between nodes creates additional complexity to the system, we proposed, *a new network architecture to coordinate the variable nodes resources* along with rapid deployment technique to ease the deployment stage. To determine the required network *width* and node *density*, to determine if a region is indeed covered. To achieve this we attempt to answer three important questions:

1. What is the minimum number of sensor nodes that must be deployed to achieve k-barrier coverage in a given belt region?

2. Given an appropriate network density, how do we determine if a region is indeed

k-barrier covered?

3. What are the factors that affect barrier coverage?

To address the long distance delay problem, we develop a new routing protocol to segment the network and to find the best route to the base station. To save energy we developed a MAC protocol to balance energy among nodes, also to apply efficient duty cycle mechanism.

1.7 Thesis Contributions

Aiming at the adoption of the existing WSN technology to the application of border monitoring and surveillance, the research efforts in this project focus on the design of a large-scale LWSN system that solves all the major challenges imposed by the requirements and restrictions of this specific deployment. The main contributions in the thesis are as follows:

1. The development of a flat, modular system architecture for the deployment of LWSN applications.

2. Defined a mechanism to estimate the minimum number of sensor nodes that must be deployed to achieve k-barrier coverage in a given belt region.

3. Development of a method to determine if a region is indeed k-barrier covered, given an appropriate network density.

4. Investigation and identifying the factors that affect barrier coverage, including network density, objects movement models and network width.

5. The development of general-purpose network segmentation protocol to optimise data transmission over long geographical distance with best QoS and minimum

amount of energy consumption.

6. The design and implementation of a MAC protocol that utilises adaptive control of radio transmission power to reduce message transmission cost and reduce radio interference.

7. Development of a shifted duty cycle mechanism that is part of the MAC protocol created in Contribution 6 to further prolong the network lifetime.

8. The design and implementation of a link selection mechanism to achieve load balancing and improve the QoS of the LWSN, particularly in terms of end-to-end delay.

9. The evaluation and verification of the efficiency of all protocols and mechanisms proposed above through simulation using real-life parameters.

1.8 Thesis Outline

Chapter 1: Introduction and Motivations

This is an introductory chapter to border monitoring and WSN technologies. It furthermore defines the term of LWSN and presents some common LWSN applications. Then challenges introduced by LWSNs are discussed leading to the motivations behind this project. This followed by thesis contribution and this outline.

Chapter 2: Literature Review

This chapter presents a survey of the most common border surveillance systems used for detecting cross-border crossing to identify their limitations and show how such limitations can be addressed by the WSN technology. Then, the challenges and requirements of a new general-purpose LWSN system is discussed. It also reviewed the

LWSN specifically designed MAC protocols. It presents a new network architecture that is designed specifically for border monitoring. The need for a new framework is described. Then, suggestions for a deployment technique that responds to the new architecture and calculation of the required network density are addressed. A detailed discussion will made for the technical challenges of the new architecture.

Chapter 3: A Routing Protocol for Border Security and Surveillance Using WSNs

Chapter 3 provides a mechanism for calculating the minimum number of sensor nodes required to achieve k-barrier coverage in a given belt region, how to determine if a region is indeed k-barrier covered, and the factors that affect barrier coverage.

Chapter 4: A MAC Protocol for LWSN Segmentation and Duty Cycle Management

Chapter 4 presents a solution to the problem of unbalanced energy depletion across nodes in a network segment. The problem results from the specifics of the LWSNs architecture where nodes are placed in a linear manner, which means that some of them are closer to the base station while other are further away from it. To achieve this, a general-purpose cross-layer communication protocol is presented. It uses a special algorithm to assign nodes in a given segment to various network levels depending on their distance from a monitoring tower. Then, these levels are used to calculate the path to the sink with the lowest possible cost. In addition, an efficient duty cycle is defined in the MAC protocol, which extends the network lifetime by saving energy instead of keeping the nodes in idle listening mode.

Chapter 5: Implementations and Evaluation

This chapter presents the performance evaluation results of our proposed solution (LDG routing protocol and our modified Line-MAC protocol) under diverse conditions and network densities. The performance of LDG is compared against the well-known Dynamic Source Routing (DSR) routing protocol.

Chapter 6: Conclusion and Future Work

Conclusions are drawn and further work suggested

CHAPTER 2

Literature Review

The chapter addresses the technical capabilities of the existing and proposed surveillance systems that are designed for border monitoring purposes. These systems assist border authorities with more effective and reliable decision-making support. Such systems vary in terms of the technology used, accuracy, continuous monitoring, and ability to detect various types of intruders. This chapter studies the effectiveness of these systems, as well as what infrastructural support required for their implementation and their ability to cooperate with external monitoring systems. It also provides a brief overview of the rising issue of illegal crossings in the EU, a survey the most used border surveillance systems, especially those used for detecting border crossing, discusses their limitations, and studies border surveillance challenges and requirements. The discussion section presents the argument for the need for a new border monitoring system.

2.1 Introduction

Firstly, continuous monitoring of international borders has become a necessity in recent years due to the steady increase in organised crime, terrorist threats, and smuggling activities [1-3]. Terrorists, smugglers, and illegal immigrants are a serious security threat when they penetrate international borders. As a result, border surveillance is a hot topic, and a serious issue for many countries. Any gaps or loss in monitoring along a border may cause severe damage to the security of a given country. However, continuous border surveillance is a challenging and expensive task, and its processes and systems require a high degree of accuracy. In this chapter, key challenges in border security and possible emerging solutions to the issues raised are addressed in detail. The section 2.2 presents existing border surveillance systems and their limitations. Then section 2.3 discusses the need for a new system the challenges facing border surveillance systems. We present the argument that WSNs are particularly well-suited to dealing with modern day border breaches.

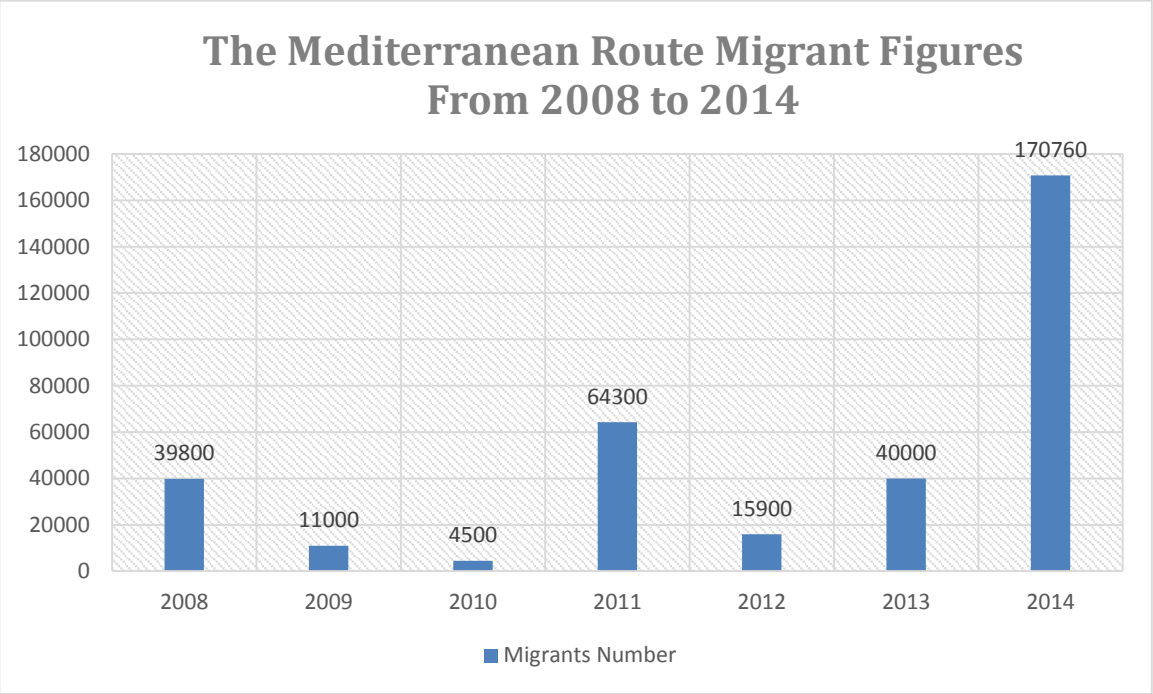
Secondly, more than two decades after their introduction, WSNs remain an active research topic due to their wide ranging applications in areas such as healthcare, military, monitoring, and surveillance systems. In most applications, sensor nodes are constrained in energy supply and communication bandwidth. Therefore, novel techniques to reduce energy inefficiencies and for efficient use of the limited bandwidth resources are essential. Such constraints combined with dense network deployment pose several challenges to the design and management of WSNs and require energy-awareness at all layers of the networking protocol stack. For instance, at the Data-Link layer, low duty cycle MAC protocols trade off latency for energy efficient operation. In this chapter, we present a survey of state-of-the-art low LWSNs MAC protocols. We present a comprehensive survey of the most prominent recent LWSNs MAC protocols (in Section 2.4). Section 2.5 highlights open research problems in MAC layer for WSNs.

Thirdly, the challenge of developing a new WSN framework for border monitoring starts by defining a suitable architecture that is feasible in the real world. The new architecture must consider all environmental terrain types, such as forest, desert, mountain, etc. The network topology is another essential factor in the new framework. Based on these two factors, node density can be measured to ensure sufficient network coverage. The section 2.6 present the existing LWSN architecture, node hierarchy, and network topology. Then the chapter discusses the technical challenges in LWSNs deployment and the new framework objectives.

2.2 Border Surveillance Systems and their Limitation

The Central Mediterranean route has become a concern to the EU state members [30]. This route refers to the North Africa flow towards the EU through the Mediterranean Sea. Smugglers overload migrants on old fishing boats without sufficient sailing equipment, fuel, and navigation heading for Italy or Malta [31].The route was important for illegal migrants in 2008, as 40,000 were detected attempting illegal crossing. This almost stopped in 2009 after the Italian-Libyan agreement. After the eruption of civil unrest in 2011 in Libya and Tunisia, the number has increased rapidly reaching more than 64,000. The migrants' numbers have increased every year since, and in 2014, 170,000 migrants arrived in Italy [30]. Table 2.1 presents the illegal migrants using the Mediterranean Sea between 2008 and 2014.

Table 2.1 Illegal migrants to the EU through the Mediterranean Sea



Another border which is currently of great concern is that of the Eastern Europe Union (EU) [5]. The most recent statistics show an increase in the number of threats caused by illegal activity in this location [4, 5], including illegal crossing and smuggling of tobacco, vehicles, petroleum products, and drugs. For instance, there has been tobacco smuggling worth 15 million euros [4], and, in another incident, 4 million cigarettes were smuggled over the Russian-Finnish border [4]. According to a recent FRONTEX report [5], there was a 24% increase in 2014 in illegal border crossings reported, compared with 2013. These crossings were conducted between checkpoints. Latest figures show that 45% of detected land crossings on the Eastern Mediterranean side of the EU are at the Bulgarian-Turkish border.

The EU's Ukrainian border is one of several key 'trouble spots' allowing illegal crossing to the EU, and, according to the FRONTEX report [4], it is "the central transit and origin of irregular migration at the common borders." In addition, Ukraine is the main transit area for Afghan, Eritrean, and Somalian illegal migrants. The EU's Ukrainian border is made up

of about 24,000 square kilometres of land.

There is emerging interest in developing intelligent border monitoring systems to help countries protect their citizens. The best form of border surveillance involves minimal human intervention [32]. Systems that currently exist for border monitoring range from simple fence-and-wall systems to very complex systems. Intelligent border monitoring systems are increasingly desirable because they augment operational efficiency, but, simultaneously, reduce costs [33]. Modern monitoring systems face considerable challenges and demands, however [34]. Large, busy, and complex landscapes must be dealt with, and, sometimes, there is the problem of integrating heterogeneous technologies. Real-time acquisition and interpretation of evolving events, and instantaneous identification of potentially critical situations in all weather and lighting conditions can be problematic. Real-time monitoring of a landscape involves taking into account a variety of topographies, including coastal plains, high mountains, dunes, and large deserts. In this chapter, we advocate WSNs as a solution to modern and evolving challenges in the field of border surveillance. WSNs are spatially-distributed autonomous sensors, which can monitor physical and environmental conditions, detect motion in the vicinity, and respond to pertinent changes accordingly.

The Subsection 2.2.1 briefly presents some of the current systems used to monitor international borders, in particular land and sea borders. It is important to note that there is a general lack of resources with detailed information about current systems due to their sensitive military nature. Thus, we present the relevant systems using the best available resources. Despite the lack of literature, problems pertaining to these systems are readily identifiable; therefore, we identify gaps in current methods. Then, the limitations of those systems are further investigated in subsection (2.2.2).

2.2.1 Existing Border Surveillance Systems

The first class of border surveillance is the image processing based surveillance systems.

The essential technology being used monitors the border from the sky using various technologies such as satellites, Unmanned Aerial Vehicle (UAV), and Closed-Circuit Television (CCTV) then compares it to the recorded images.

The first satellite-based system is called Change Detection Phenomena-based Monitoring [35]. This type of border monitoring system involves capturing and recording images of and information about a particular place from two different locations. This is mostly done using a satellite that monitors activity in a place constantly and records any difference that has occurred in the environment during a fixed time-period. This model is recommended by the European Union for use along the border of Ukraine for preventing any illegal movement. The working principle of this system is that images of an area must be captured at different intervals. For accuracy, the calibrations of instruments, and the resolution of imaging devices must be kept constant when taking images across two different periods. Image processing, voice signal threshold, and modulation activities must be performed to refine the images and voices that are recorded [36]. This system was designed with the demands of monitoring different geographical areas in mind. One challenge for this system concerns differentiating between changes that occur naturally and changes that might occur due to humans crossing the border. This system is also susceptible to natural conditions, such as cloud cover and other weather changes, which can also affect the accuracy of the results.

With regard to satellite-based systems, EUROSUR is the European external border surveillance system [37]. This system is engaged for surveillance across the Schengen borders using Satellite data to track vessels and smugglers' movements. The purpose of EUROSUR is to reduce the movement of illegal immigrants across borders, providing the common technical framework required to facilitate cooperation and round-the-clock communication between Member State authorities, and foster the use of cutting-edge technologies for border surveillance. A key concept underpinning EUROSUR is the aim of supporting Member States in their efforts to reduce the number of illegal immigrants in

Europe, migration being a significant issue in the current political sphere. EUROSUR's limitations emerge from the complexity of technical operations and maintaining coordination.

With the aim of improving decision-making and diplomatic approaches to solving immigration matters concerning the European maritime border, DOLPHIN was designed [38]. The main objectives of DOLPHIN are to prevent or reduce the death toll of illegal human trafficking through increased rescue operations, to eliminate illegal immigration by sea, and to increase EU security. DOLPHIN is governed by what is referred to as EUROSUR, outlined above, to control any type of immigration along the EU coast [39]. Being a sea-based border system limits its use to maritime borders only. In addition, the system was designed only for EU maritime use [38].

A CCTV based monitoring system was established in 2001, EVPU Defence [40], which is dedicated to designing and developing products for both mobile and fixed monitoring systems. Moreover, the firm is involved in a number of predefined projects, such as deploying pans or tilts, which are intended to provide customers with optimal short-range surveillance through managing surveillance in the azimuth and in the elevation. This system is governed by a complex project solution that delivers high overall quality. The target areas are borders, airports, and other areas of interest. As a surveillance system, EVPU is intended to achieve the objectives of effective stationary and mobile multi-sensory systems by acting on targets quickly and flexibly to achieve the required goals. Using new SAMBA technology increases security levels and protects areas from unwanted encroachment by trespassers and illegal crossers. This system is, unfortunately, tied to the Czech Republic, and, as such, is not open to other nations. In addition, the newly introduced SAMBA technology may be erroneous to some extent [40]. The main drawback of EVPU, as for other systems presented here, is the intensive human involvement required in operating the system.

The second class of border monitoring system is the multi technologies systems. These systems use more than one technology (CCTV, radar, fibre-optic cables, etc.) to achieve better surveillance results. However, these systems are designed to operate independently and cannot offer integration with other systems.

Helios, a Distributed Acoustic Sensor (DAS), was created by a British company called Fotech Solutions [41] and consists of CCTV, fibre-optic cables, lasers, and detectors. Helios is being implemented, and is proposed for surveillance across southern Arizona's borders specifically, and in other parts of America as well. It has a number of features that distinguishes it from other existing border surveillance systems. It minimises the hassle of wires, has a considerably larger scale than other systems, and offers greater accuracy (up to 1 meter) of intruder detection using G.P.S. However, interfacing with mobile communication and the internet for remote monitoring is a major flaw as most of the borders are out of coverage.

The WESTMINSTER surveillance system [42] was designed to assist in the provision of high-quality services pertaining to fencing and other physical mechanisms for preventing border encroachment. The system features bespoke surveillance and border-cross detection (for land, sea, and air). WESTMINSTER thus offers control along borders made up of different terrains, which is ideal for curbing illegal immigration and human trafficking [42]. The system uses solar power to illuminate remote borders, and makes use of radar, UAVs, drones, sonar, and Small Craft Detection systems to detect illegal crossings [43]. The main drawback is the design of this system does not allow cooperation with other technologies. Moreover, there are additional installation costs above those of lesser systems, and human involvement is minimal to operating the system, which has implications in terms of training and salaries.

The third class is the hybrid border surveillance systems that are compatible and able to integrate with other systems to provide continuous monitoring using multiple resources.

These systems use technologies such as sensor nodes, UAV, fibre-optics, and drones.

BorderSense [44] is a good illustration of hybrid surveillance systems. It makes use of various existing technologies, such as sensors, UAVs, and monitoring towers. One of the key advantages of BorderSense is that it requires minimal involvement from humans– ideal for cost-cutting, and for surveillance of inhospitable terrain. The technologies embedded in the entire system constitute multimedia and sensing devices, under-the-surface sensing devices, and mobile nodes. The system provides beyond-the-line-of-sight detection, i.e. even if a target is covered by some kind of material, it can still be properly detected, allowing for tracing and eventual interception. Visibility is considered a point of weakness in many border systems. For this reason, the underground sensing capability of BorderSense is one of its key selling points. Although it incorporates existing technologies, the architecture of BorderSense is slightly different from existing monitoring techniques. An assortment of heterogeneous nodes are operationalised in this form of surveillance system, which increases range as well as accuracy, and reduces the degree of false alarms where, for example, a naturally tree movement triggers a monitoring alarm at the same time. Another major advantage of this system is the compatibility with aerial surveillance systems. Since BorderSense is a hybrid system, it has the capacity to easily absorb other systems' features into itself and, thus, is the most capable of contemporary systems [44]. However, the system requires complex installation and has not been examined in detail.

Another project that combines compatibility with other systems is Cassidian [45] Border Solution technology developed by Airbus Defence and Space. This system is specially adapted for highly-integrated border surveillance in order to meet customer demand. Cassidian deploys an artificial intelligence system that is capable of gathering, aggregating, and evaluating data from numerous sources [46]. The system uses encrypted communication subsystems to provide a high level of security. There is a set of predefined fixed and mobile command centres that provide the system with decision-

making tools, helping it to conduct the required operations effectively [45]. However, such capabilities come at a cost. The key disadvantage of this system is its expensive infrastructure.

An important example of hybrid systems is FLIR [47], which is a compatible border surveillance system providing solutions for land border protection, maritime monitoring, and airport security. The system combines a variety of sensors, such as thermal cameras, radars, and a host of other sensors, in order to achieve the best available degree of detection and surveillance. FLIR operationalises reliable and cost-effective equipment, claiming low false-alarm rates, and a low life-cycle, which allows it to survive in all weather conditions. The main advantage of this system is that it curbs the perpetual false alarm rate experienced in most border security systems [48]. It is observed that the agency is too capital intensive to install the equipment, as opposed to other agencies, and the false alarm rates of FLIR are higher [47].

As far as hybrid systems are concerned, Thales group producing a compatible border surveillance system [49] designed to improve basic control and border management, since security levels are worsening daily. The system offers an impressive and high-quality service using standalone equipment such as sensors, and the firm aims to customise services for the purposes of logistic support, as well to provide training tools and services to support the use of its system [49]. Thales system is designed to ensure that present security levels are evaluated and appropriate preparations for the future are made. It tweaks response times, makes detections, has excellent reception, and the company maker says Thales system makes optimal use of resources whilst still achieving satisfying results. Additionally, Thales' makers have tailored current operations to securely conform to present IT hardware and software, and the system comes with a complete and modern turnkey Integrated Border Management System [50]. Nevertheless, the system has some flaws; the firm works on the assumption of partnerships between neighbouring countries, but co-operation is not automatic and

should not be assumed. Furthermore, thicker and denser areas of terrain may be impenetrable to the system, hindering operations, as some radars may not re-route information back to the head office.

OptaSense [51] is a hybrid cost-effective border monitoring system whose makers claim robust protection. The system features a maturely-set software technology, which is able to work with monitoring systems such as UAVs. OptaSense is chiefly intended to monitor access routes for a more secure border environment, both along roads and in forests. The system tries to alter the asset deployment schema and offer not just portable, but also effective systems aiming to improve on the inadequacies of existing systems [52]. Fibre installation and configuration along the border allow the system to work with other assets, such as cameras, and offer a secure means of providing data. The system also extends total coverage, capturing more, and greater, remote areas, and aiming for utmost security in the long term. The major drawback of this system, however, is that it requires deployment along an entire border, which entails a substantial pre-engineering cost. In addition to this, the software platform used requires user training, and, several times, OptaSense equipment has raised a number of false alarms, making it unreliable in the event of a genuine threat to a border [51].

Another hybrid system discussed here is the Integrated Surveillance Intelligence System (ISIS), which is managed by the Department of Homeland Security (DHS). ISIS delivers the latest technologies, e.g. drone-powered monitoring, sensors, and Remote Video Surveillance (RVS). Its key goal is to detect and prevent illegal crossing to the United States of America [53]. Essentially, the objectives of this project are to offer more advanced RVS and physical sensors for detecting migration in the target areas. The system can only monitor a targeted area of interest, however, and cannot provide coverage of the full border [54].

The last system reviewed here is the sensor based monitoring system Radiobarrier [55].

It is one of the surveillance systems introduced by POLUS-ST Ltd for line monitoring of the international border. Radiobarrier makes use of all the latest technological advances. Furthermore, POLUS-ST Ltd seeks to develop rapidly installable perimeters and critical infrastructure security. As a result, Radiobarrier is the perfect system in urgent situations where rapid intervention is needed. Generally, the objective of the company is to find solutions for any unresolved gap on a monitored border. There is, however, a lack of information provided about the Radiobarrier system so it is difficult to judge its actual performance in the field. The main limitation of Radiobarrier is the intensive involvement of humans, which is required from installation right through to decision-making [55].

The advantages and disadvantages of the systems mentioned above are summarised in Table 2.2. This summary provides the basis for suggestions made for improved border-monitoring solutions.

Table 2.2 Summary of Advantages and Disadvantages of Systems Reviewed in this section

Product Name/ Technology	System Description	Objectives	Limitations
Change Detection Phenomena	Captures and records images and information from a particular place at two different times.	Designed with consideration of monitoring different geographical areas.	Susceptible to natural conditions such as cloud cover.
EUROSUR	Satellite-based monitoring system facilitates cooperation and 24/7 communication between Member State authorities.	Supports authorities in reducing the number of illegal immigrants.	Complex coordination and technical operation.
DOLPHIN Surveillance	Decision-making, and diplomatic resolution. Governed by EUROSUR.	Aims to stop cross-border crimes, drug trafficking, and reduce death toll of immigrants.	Sea-based border system and for the EU use only.
EVPU Surveillance	Customer-driven design and product development for mobile and fixed monitoring systems.	Designed for short-range surveillance, reliable, monitoring of borders and airports.	Czech Republic only; Prone to error; Intensive human involvement.

Helios	Consists of fibre-optic cables, lasers, and detectors.	Distributed acoustic sensor relies on the phenomenon of optical backscattering for its operation.	Only covers a maximum of $50km$.
WESTMINSTER	Impenetrable security solutions to prevent border encroachment, and high-quality service.	Prevents or reduces the death tolls of illegal human trafficking through increased rescue operations, eliminates illegal immigration by sea, and increases EU security.	Accuracy issues; Border-sensitive areas only.
BorderSense	Hybrid system makes use of the technologies and facilities available.	Minimal human involvement, under-the-surface sensing devices, mobile nodes, use of heterogeneous nodes.	Requires complex installation.
Cassidian	Customer demand-based highly-integrated border surveillance.	Offers border sensitive networks, secure and encrypted end-to-end communications, artificial intelligence system, and mobile command systems.	Expensive infrastructure required for deployment.
FLIR	The system is portable and cost effective, and can be used anywhere.	Uses the latest technologies and offers a 360 degree system.	Capital intensive. False alarms.
Thales Border Surveillance System	Offers wide-ranging border surveillance systems such as standalone equipment, sensors, logistic support, training tools and services.	Offers a secure IT line, modern, complete turnkey, and integrated border management system.	Assumption-based cooperation with neighbouring countries; Thicker and denser areas may be impenetrable; Re-routing problems.
OptaSense Border Security	Cost-effective, mature software technology for working with monitoring systems.	Eliminates existing fibres and covers larger areas.	Difficult to master; Unreliable alarms.
ISIS	Approved by the Department of Homeland Security. Makes use of Integrated Surveillance Intelligence System (ISIS), drone-powered monitoring, and remote video surveillance (RVS), and can be impenetrable in places.	Provides advanced remote video surveillance, physical sensors, underground sensors, uses the seismic waves principle and seismic-powered sensors, and offers migration cover in targeted areas.	Not designed to provide coverage to the full border.
Radiobarrier Security System	Governed by POLUS-ST, rapidly installable perimeters, and critical infrastructure security.	Creates solutions to unresolved glitches, and can be deployed rapidly.	Intensive human involvement.

2.2.2 Limitations of Current Systems

The majority of existing border monitoring techniques or systems reviewed in the previous section can only claim robustness and reliability in limited scenarios, with limited networks of sensors, with limited video footage, limited fault tolerance, and for a small variety of landscapes. Not all present solutions build complex models of the observed spatial and temporal evolution of a scene. Another limitation of existing surveillance systems is the degree of accuracy and range of coverage that they each provide. In addition, newer surveillance systems experience false alarms that occur due to natural factors, such as wind and animals.

Current systems solve these problems from different angles depending on their individual applications. The focus is on applications' perspectives rather than on developing general solutions that suit applications sharing the same deployment features. There is a need for new surveillance systems to close the gap between the existing systems and their limitations. A technology must be developed that can combat the shortcomings summarised in Table 2.2.

The use of insidious methods for detection and surveillance, for instance WSN technology, makes this task more intriguing. The installation of surveillance devices under the ground or in a hidden location can make them more effective because they are concealed from the naked eye and, so, their processes cannot be disrupted. Usually, borders constitute a large geographical area that is a combination of both rough and plain terrain, and it is preferable to use devices that are more solid, long-lasting, effective, and compatible with those already in place. LWSNs, if added to a border monitoring setup, can take the surveillance process to another level entirely since the sensor networks directly reduce human dependency, and work on an embedded artificial neural network. A fully-embedded WSN possesses all the essential components needed for successful border monitoring, and combats or does not exhibit many of the

disadvantages of the systems outlined in Table 2.2.

2.3 New Border Surveillance System Needs and Challenges

Similar to border monitoring, other applications, such as pipeline monitoring, railway monitoring, Alternating Current (AC) link monitoring, etc., require high levels of security. The aforementioned applications share the same linear infrastructure that can run over up to 1000 kilometres. Any interruption to these applications might affect public and national security. An interruption could lead to severe financial crises and major security threats. This could happen even in a very secure country, such as the United Kingdom, which suggests even higher probabilities of such events in developing countries, and this applies even more so in cases of countries facing war or revolution. For instance, in late April 2014, a gang of thieves managed to steal thousands of gallons of diesel from Britain's most important pipeline that runs the 130 miles from Fawley refinery to the West Midlands [56]. A similar incident happened in Nigeria when some community members stole oil from the national oil pipeline, and the spiralling cost of oil theft in 2013 was one billion pounds a month [57]. This not only disturbed the security forces and energy prices, but also had an impact on the environment, causing significant pollution. Another example is railway disruption, which can lead busy nations into massive interruptions when a break in the main railway links occurs.

These examples highlight the importance of having very secure infrastructures that are able to stop any disruption that might occur, or even prevent it–something that an ideal border solution should also do. They also highlight a number of challenges. The infrastructures mentioned are national property, and they are costly with respect to development. However, such expensive property is the vital backbone of public need in any modern society. Such important systems require high-capability security monitoring systems that allow on-time surveillance at a minimum cost. This raises the necessity of developing a complete generic system that is able to provide a satisfactory level of

security in many contexts, and the same principles apply to borders.

An integrated framework for border monitoring should adaptively employ various approaches to border monitoring in order to maximise the amount and quality of monitoring information whilst minimising resource utilisation. By providing this standardised framework, we anticipate promoting interoperability and information integration. The best border monitoring system should integrate various technologies to achieve high performance and accuracy. Implementing WSNs will assure systematic coverage that fills the gap in other surveillance systems–their numerous disadvantages listed in section 2 warrant this conclusion. It is worth mentioning that WSN systems can utilise various types of sensors to detect different variables such as acoustic variables, vibrations, chemicals, environmental changes, weather factors, humidity, flow, position, angle, displacement, distance, speed, light, etc. In addition, WSN technology can be deployed to raise early alarms to prevent potential threats to a border rather than flagging an incident when it has already happened.

The new framework can also be used in all other WSN applications. This chapter focuses on these applications because they raise a number of challenges for future research in this area. There are many approaches for addressing these applications; however, they are rather expensive, unreliable, and difficult to implement. We believe it is more feasible to deploy WSNs in these areas in order to achieve easier installation, better quality of service, and energy savings.

There are five surveillance factors that must be considered when designing border monitoring, according to Giompapa et al. [1]. These are:

1. There is a high number of potential threats that could be irregular
2. Surveillance operations occur during peace conditions
3. Many environmental elements can lead to confusion and cause distraction

4. Threat detection and identification can be made more complicated by the use of camouflaging techniques
5. The monitored area is typically vast and requires a large and heterogeneous sensor network [1].

Many of these characteristics are common in most LWSN deployments. These five aspects, if taken into account when creating border solutions, can ensure a better monitoring system and, hence, more secure borders. They also address possible vulnerabilities as well as the identification of components of the system. An area of importance is highlighted by the study, which states that these surveillance operations normally occur during normal situations across borders, and, so, the information thus gathered during phases of normalcy is being used by countries in the longer term. LWSN systems are subject to various forms of threats such as signal jamming, etc. The most common approach to defend against such attacks is to use covert passive ground sensor system.

Current systems are subject to the physical presence of humans, and the actual intervention and supervision of humans as well. They also require huge capital investment resources. Moreover, full coverage of the monitored area is an important aspect of any surveillance system. The coverage must be combined with on-time delivery of information, as late data delivery will result in the failure of the surveillance mission of the system [58].

Another major challenge is the line-of-sight factor that curtails functioning, and prevents monitoring behind walls or, in fact, behind or through any type of physical obstacle. Many existing systems suffer from this defect, and it reduces performance not just in terms of long-range detection, but also in terms of the expenditure incurred due to repetitive installation of surveillance elements. All these factors call for an effective and dynamic surveillance system, which will enable more accurate monitoring that is less dependent

on human intervention, and is much more effective in terms of range and accuracy.

There is a need to make border surveillance systems independent of the physical presence of human patrolling, as this costs money, time, and management and training resources. Moreover, some terrains hostile to humans require monitoring, and people simply cannot go there (e.g. very cold regions). As such, there is a need to establish new surveillance systems that are compatible with and versatile in variable circumstances. Such a system should be modelled in such a way that adjustments can be made without disrupting an entire project, or completely reconfiguring a surveillance device. Monitoring devices must be multi-hop communication enabled, which supports network scalability. Sensor nodes have a serious constraint that imposes the need for a monitoring system that can extend the lifetime of sensor nodes without risking overall throughput. Energy consumption is a hot topic in the monitoring of remote areas where nodes can not be maintained or replaced at regular intervals, so, for this reason, any incumbent devices should be energy efficient. LWSNs are the key to an effective border surveillance system. They incorporate the current methods, tools, and techniques that are effectively secure, and facilitate a significant decrease in trespassing across borders as well as all other undesired processes.

Deploying WSNs at international borders for surveillance and security has significant advantages over current systems while raising some challenges at the same time. An effective remote surveillance system must take into account the following major issues for successful WSN deployment for border surveillance:

1. Reliability of the system
2. Power efficiency
3. Appropriate maintenance for reducing downtime
4. Deployment technique that is achievable in large, unmanned areas
5. Architecture that limits the need for over-constructor resources

6. Efficient routing techniques for effective data transmission [59]
7. Efficient MAC protocol that adopts duty-cycle technology

Efficient MAC protocol is one of the methods being developed and employed to support border surveillance purposes. Two main challenges must be addressed in the MAC protocol: energy savings and on-time data delivery. Maximising node lifespan can be achieved by applying a suitable duty cycle MAC protocol while assuring prompt data delivery and power conservation.

New deployment strategies specific to WSNs are needed to fill the gaps in existing knowledge and technology. The aim of this deployment method is to support heterogeneity, scalability, and energy efficiency. A network must adopt heterogeneous node deployment that allows for different nodes' capabilities and functionalities. For instance, some nodes sense emotions, while others might sense temperatures. Any new system should be energy efficient, scalable, reliable, cost-efficient, and independent of human intervention. Given the disadvantages of current approaches, it seems that a new border security framework is required.

2.4 LWSNs Specifically Designed MAC Protocols

In this section, we review the relevant MAC protocols designed to improve the data delivery, throughput, and power efficiency of linear/chain-type large-scale WSNs networks.

A real-time MAC protocol with realistic assumptions has been proposed for LWSN random deployment in Watteyne et al. [60] . The protocol aims to ensure packet delivery within the period limit given. The protocol has four stages: initialisation, switching, unprotected, and protected mode. The initialisation stage organises the nodes and groups them into cells to allow the nodes to communicate with all the nodes in two neighbouring communication cells. The sink sends a *CC(i)* message to create cell *i*. All nodes that receive this message will forward the *CC* according the $backoff_{initialisation}$ that is coordinated to their distance to the sender. The farthest cell will start sending first. Nodes in backoff time will record the number of *CC* messages that have been received, the reception time of the last one, and the last created cell number. A node will start $timer_{last}$ while sending the *CC* message. If the $timer_{last}$ expires before receiving a new message, the node will be set as the end node of the network, and it will send an *END* message to inform the sink that the initialisation stage has finished. All nodes will know their cell and their location within the cell by the end of this stage.

The network will start unprotected mode of transmission offering good message speed to the sink. Once collision occurs, the network can switch to protected mode offering collision-free protocol. The idea of this protocol is based on using signalling messages to reserve five cells towards the sink from the source node. After reserving, the ALARM message can be sent through in unprotected mode. However, no new ALARM can be generated at this time, which is a serious drawback in this protocol.

The sink can switch to unprotected mode based on the rate of the arriving alarm; it is not congested when receiving fewer alarms. The protocol uses a JAM message to physically switch between modes. Nodes generate a JAM message if collision occurs or they are hearing a JAM message. The hybrid approach performed well in the simulation, which quantifies the protocol speed [60].

Karveli et al. [61] developed a collision free Directional Scheduled MAC protocol (Dis-MAC). A directional antenna is used to achieve the following advantages: increase the spatial reuse, achieve higher gains, and realize longer ranges between communicating nodes. The collision is avoided by directing the radio beam in a specific direction. DiS-MAC was specifically designed for motorway surveillance. Each node is equipped with one transceiver and a directional antenna. The antenna can point its high gain beam in a particular direction while its lower gain back lobe covers the opposite direction. There are two-channel accesses in DiS-MAC with time duration of T_1 and T_2. In phase 1, nodes allocated on $2n-1$ can transmit for T_1 time interval while the rest of the nodes $(2n)$ are set in receiving state, where n is the node location in the topology. The opposite procedure is carried out in phase 2 and by this, the network completes its scheduling cycle.

In contrast with contention-based protocols, Dis-MAC uses directional antennas to solve collision and hidden terminal problems without using RTS/CTS packets. In addition, there is no backoff mechanism in the protocol; therefore, per hop latency is minimised and can be calculated by $2T$. DiS-MAC addresses throughput rather than delay; therefore, it has been examined under the following conditions:

1- First node acts as source,
2- Packets are generated by all nodes, and
3- Probability *q* defines the final destination to which all packets are forwarded.

Simulation results show a reliable communication link among nodes[61]. On the other

hand, error rate increase with large packet transmissions, for which the authors suggested considering the incorporation of channel coding and data fragmentation techniques with Dis-MAC.

Long-Chain MAC (LC-MAC) protocol is a duty cycle protocol that uses advance booking for relay nodes and transmits packets in a burst manner [62] . The aim is to reduce end-to-end delay in long linear deployment while maintaining low energy consumption. LC-MAC applies the three following phases:

- Initialisation phase where relay nodes detect their neighbouring relay node. A relay node with only one neighbour will set itself as the end point R_n of the network. The relay node R_n will send a Location Detection Package (LDP) message containing its location address to the neighbouring relay node. The LDP message will travel through all the relay nodes until reaching the sink, and every relay node will add its address before forwarding the message. At the end of this phase, the sink node sends LDP containing a table address along the route to confirm relay node locations.
- In the second phase, relay nodes create a Staggered Wakeup Schedule (SWS) to pass a super synchronisation message (SSYNC). Relay nodes do not need to use RTS and CTS mechanisms to avoid collision, instead following SWS to transmit SSYNC. There are two parts embedded in the SSYNC message, transmission and registration. The first part contains the duty cycle and address information, the second part is split into n fractions for n relay node. A fraction has p bits space to record the number of packets ready to be sent. The length of the SSYNC message is fixed once the confirmation from the end point is received. By this step, all relay nodes have packets of information assigned to each relay node, and set an accurate time schedule.
- The last phase is transmitting data in bursts.

The examination of the protocol performance was carried in comparison with the traditional duty cycle S-MAC with adaptive listening mode [63] . The simulation outcome indicates that LC-MAC achieved better data delivery improvement with 99% compared to S-MAC. In addition, LC-MAC has better traffic load throughput in long linear deployment. However, the power consumption is not much improved compared to S-MAC.

Zimmerling et al. [10] used IEEE 802.11 standard RTC/CTS mechanisms in the CSMA/CA algorithm in LWSN. The CSMA/CA approach increases the throughput of the medium sharing among nodes. Hidden terminal problems are avoided by applying RTS/CTS. The protocol operates as follows: the sender node transmits RTS first; once a receiver node sends CTS without backoff, then the sender node will transmit immediately. The receiver will send an acknowledgement (ACK) confirming a successful packet transmission. There is a trade-off in CSMA/CA between the required time to send RTS/CTS and the packet length. Therefore, small packet transmission does not benefit from RTS/CTS functions.

The authors proposed a *leaky shift register* model for the packet to transmit from left to right. However, some frames could be lost in the following cases: FIFO overload, exceeding of retransmission limit, and medium overload. Simulation figures recorded less packet loss and queue load with RTS/CTS, while delay increases slightly.

Another approach is an on demand CMAC-T protocol application designed to monitor crop-growing [26]. The sink node periodically sends beacon messages to the nodes for channel access and synchronisation with the adjacent nodes. Nodes in wake up mode receive beacon messages and can access the channel with the specified time slot. A node will switch to sleep after transmission, or if the node was not giving channel access. The data frame has node ID and alarm information. A real life deployment in a greenhouse provides a satisfactory level of reliability, and low power consumption.

Another approach is the synchronised duty cycle contention based protocol called Multi

transmission MAC (MFT-MAC) [64] . The aim of this protocol is to reduce the end-to-end delay by using control frame PION to forward multiple data frames over multiple hops in one duty cycle. One duty cycle in MFT-MAC has the following three stages: SYNC, where a precise synchronisation is set among nodes; DATA, where the source node sets up a forwarding path using the control frame to win channel access in order to send its message to the sink; and SLEEP, where the data transmission occurs between the source and next hop node while the rest of the nodes are in sleep mode. A node wakes up from the sleep mode at the specified time (SYNC) to receive the multi frames then goes back to sleep, unless it has a packet to send or received a packet from a neighbouring node to be transmitted. A comparison with DW-MAC [23] and R-MAC was carried out [64]. The authors claim that MFT-MAC performs better in regards to throughput, end-to-end delay, and average power consumption.

In Li et al. [65], the authors proposed an Adaptive Coordinated MAC protocol based on Dynamic Power Management (AC-MAC/DPM). AC-MAC/DPM was designed to reduce the number of transceiver state switches in order to achieve high throughput, less power consumption, and low delay in high traffic load applications. The DPM mechanism is used to reduce power consumption by controlling the transition between sleep/wake modes. It uses the sensor's traffic load to measure the new duty cycle. A comparison of the results with S-MAC in linear topology shows that AC-MAC/DPM achieves better performance in term of energy efficiency and end-to-end delay.

The last MAC protocol to be reviewed is the synchronous contention free MAC protocol for a chain-typed application called WiWi [66]. Similar to DiS-MAC, WiWi avoids interferences between simultaneous transmissions by alternating transmissions between adjacent nodes. One difference is that WiWi uses bidirectional communication over a single RF channel instead of using a directional antenna. Nodes in this protocol do not require explicit addressing as there is only one receiving node within the transmission range. The authors claim that predictable throughput and latency in the

two directions are achieved using WiWi. The main shortcoming of this approach is not considering the power consumption.

Table 2.3 Summarises the features of the reviewed LWSN duty cycle MAC protocols

MAC Protocol	Target Application	Key Design Points	Features
Real-Time MAC	-LWSN random deployment	-Using three stages (initialisation, switching, protected and unprotected modes) -Usage of backoff to wait for possible alternate route -A sink can switch based on the arriving alarm	- Ensure packet delivery within the period limit given -Hybrid approach
DiS-MAC	-Specifically designed for motorway surveillance	- Node equipped with directional antenna	- Increase the spatial reuse - longer range between communicating nodes -Collision avoidance and reduction in hidden terminal problems
LC-MAC	-Designed for long linear deployment	-Uses advance booking for relay nodes -Transmits packets in bursts	-Reduces the end-to-end delay in long linear deployment
CSMA/CA	-Designed for linear applications	-uses RTC/CTS to avoid hidden terminal problems -*Leaky shift register* for packet to transmit from left to right	- Fewer packets lose applying RTS/CTS -Less queue load
CMAC-T	-Designed for crop-growing application	- Uses beacon messages for synchronisation and channel access	-On demand -Good level of reliability -Low power consumption
MFT-MAC	NO TARGET APPLICATION?	-Contention based -Use PION to forward multiple data	-Reduces end to end delay using control frame -High throughput, end-to-end delay, average power consumption
AC-MAC/DPM	-Designed for high load traffic applications	-Uses Dynamic Power Management (DPM) - Controls the transition between sleep/wake modes	-Reduces power consumption -Better end-to-end delay
WiWi	-Chain-type applications	- Alternating transmission between adjacent nodes -Uses bidirectional over single RF	-Avoids interferences between simultaneous transmissions

2.4.1 LWSNs MAC protocols Analysis and Discussion

The existing general-purpose duty cycle MAC protocols designed for classical WSNs dramatically decrease the overall network throughput when applied to LWSNs. Researchers focused on power saving as a priority above all requirements. All previously reviewed methods suffer from some serious limitation when considering time critical applications. The real issue is to improve the network latency without sacrificing the energy. In classical WSNs, many factors, e.g., nodes mobility and network density, affect the protocol timeliness [67]. However, nodes mobility and high network density do not exist in static LWSNs deployments. Therefore, problems related to these factors, such as collisions, can be simply ignored when designing protocols for LWSNs.

Most of duty cycle MAC protocols reviewed here are designed without considering the impact of the network layer on the overall system performance. In addition, some LWSN specific protocols have attempted to solve some of the challenges specific to LWSNs from an application specific perspective. Therefore, there is no such work that addresses all the mentioned challenges. For instance DiS-MAC [61] was designed specifically for motorway surveillance application using directional antenna for message transmission in one direction. This approach does not suite applications that have transmission flow in both directions as the case in most linear applications. Some other approaches improved the network throughput at the expense of high power consumption, e.g. LC-MAC [62] and WiWi [68]. Other approaches such as CSMA/CA [10] and DiS-MAC have not considered the time critical applications.

Oliver and Fohler [67] claimed that bounding end-to-end delays can be achieved in real deployment only ‘When the network enforces deterministic behaviour on each communication layer’, or in “perfect” or “fixed” network topology. The key problem with this explanation is that the network will have over-constrained properties, which contradict with the nature of classical WSNs and LWSNs. End-to-end delay can be improved at MAC

layers when using neighbour synchronisation and periodic sensing, however this is expensive in terms of energy consumption. Application requirements can affect the trade-off between the network resources and network overall performance. For example, to achieve timeliness in high priority message, networks should allow the extra usage of transmission in order to get the message to the sink faster. Using two different nodes capability along with the appropriate communication and segmentation methods can overcome these issues. Therefore, our new work is proposing a new communication protocol to deal with time critical applications without sacrificing the power efficiency.

Based on our review, we observed that asynchronous MAC protocols are more scalable than synchronous MAC protocols. Frequent re-synchronisation results in higher energy consumption. When global synchronisation is necessary, the cost of re-synchronisation may exceed the cost of keeping the nodes on at all times. Many of the problems present in existing MAC protocols, e.g., congestion, collisions, end-to-end delays, etc., are a result of the dense node deployment. In LWSNs, the overhearing, interference and collision problems are far simpler than those in classical WSNs. Therefore, developing an effective LWSN MAC protocol can simply be a problem of optimising an existing general purpose protocol, i.e., the complexity of MAC protocols for classical networks is to deal with problems that are less severe, or even do not exist, in LWSNs.

2.5 Related Work

Current WSN systems for area monitoring and surveillance can be classified into two categories: flat and layered. Flat systems are comprised of a set of sensor nodes with similar hardware capabilities that collaborate to detect and report events. In layered systems, additional resources, such as unmanned vehicles or drones, are deployed to carry out computationally intensive tasks.

The authors would like to draw the attention of readers to a major problem they identified while conducting their literature survey, which is the presence of a large number of poor quality papers presenting border security and surveillance solutions. Often, these papers carry misleading titles and contain tremendous claims that are not verified or tested. In this section, we limit our literature survey to internationally peer-reviewed research that has no referencing concerns and includes some evaluation results to confirm some or all claims. Many papers present immature work on border surveillance published by undergraduate students in locally managed open-source journals. Felemban [69] presents a short survey paper of border intrusion detection and surveillance systems using WSNs; out of the seven papers reviewed, only three papers are post 2010 and the rest are basic experiments with technology that has advanced significantly since their publication

In Hanjiang et al. [70], one of the early experimental deployments of WSNs for border surveillance is presented. This deployment relies on resource-rich nodes to run resource-intensive tasks and to cover non-line-of-sight terrain. For instance, each video assessment node supports up to three video cameras and a two-way audio capability. The authors rely on the assumption that the highest value implementation of this capability would be in non-line-of-sight areas (behind hills, in trees, in low areas, such as dry riverbeds, etc.). However, it can be argued that the rough terrain can be helpful in reducing cost, since such areas will be inaccessible, and hence sensor nodes need not be

deployed there. The paper focuses on the hardware architecture that forms their multi-layered system so data communication and processing are not discussed.

Recently, Sun et al. [44] described the concept of a hybrid WSN architecture for border patrol systems similar to the one proposed in Hanjiang et al. [70]. The authors suggest the integration of multimedia- and underground-WSNs with Unmanned Aerial Vehicles (UAVs) and robots. The resulting hybrid system is expected to reduce the number of false alarms and lower the event detection miss-rate. This is achieved by passing any detected event through multiple phases, where sensors from various layers are activated to verify an event. The main contribution of this chapter is to outline techniques from the literature to calculate node density and determine the number as well as the location of monitoring towers. However, as in Hanjiang et al. [70], the cost of such a system could be extremely high and its multi-phase sensing could introduce significant reporting delays. The collaboration between sensors in different layers requires complex coordination techniques. Furthermore, the integration of the multimodal data is not a trivial task. Finally, it is not clear how the underground sensors can be deployed on very long stretches of borders.

More recently, a border intrusion detection system that aims to enhance coverage quality and detection accuracy has been proposed in Yang et al. [71]. This chapter reproduces some of the ideas published in Sun et al. [44]. A model to calculate the amount of redundancy required to guarantee the quality of sensing coverage is presented. The proposed model may be difficult to implement in practice, for example, having the nodes located in a belt with two coverage levels is difficult to achieve with node deployment from the air. The scheme offers reduced false alarms, determination of crossing direction, and high detection accuracy, although these claims were not verified experimentally.

A maritime border surveillance system was proposed in Hanjiang et al. [70]. The research

focuses on distinguishing between ship-generated waves and ocean waves using spatio-temporal correlations of an intrusion. A three-tier system to detect intruding vessels is proposed. The node-level detection involves sampling events and extracting features to be transmitted to a local head node. Cluster-level classification applies more resource intensive tasks, such as regional data fusion. Clusters are formed on a geographical basis. Sink-level detection involves processing the data received from cluster heads, and the final decision will be reported to the end user via satellite or other means. The main limitation of this study is that it requires a dense network to achieve a low miss-rate, especially with small vessels because of the high level of noise in the sea. Additionally, it is based on a grid network topology, which is difficult to achieve in real-world deployments, such as dropping buoys from a plane.

The work in Dong et al. [33] presents an energy-aware routing protocol for WSN-based border monitoring and surveillance. For this purpose, the authors propose a routing algorithm that splits sensor nodes into a number of scheduling sets and keeps track of the energy level of each sensor node. This algorithm is based on the routing algorithm published in Yan et al. [72], which addresses the m-coverage and n-connectivity problem under border effects. Border effects in this context are defined as “a phenomenon that the difference between the network property of nodes that are closer to the network boundary and the network property of nodes that are further from the boundary is distinguishable.” Dong et al. [33] confuse the border effect with the borders that demarcate the geographic boundaries of a political territory. Despite this, the routing algorithm published in Yan et al. [72] considers the scenario where the heterogeneous sensor nodes are randomly distributed in a circular region, which renders it unsuitable for border surveillance applications.

In Sharei-Amarghan et al. [73], a set of well-known routing protocols (AODV, DSR, and OLSR) are simulated using OPNET. DSR was found to perform better than other protocols in border surveillance applications. The authors propose a minor modification to DSR to

achieve better energy management in border surveillance applications; however, the proposed modification does not achieve significant energy gains and is not hardware platform specific. The study focuses on energy consumption without giving any attention to any quality-of-data or quality-of-services aspects.

FleGSens [74] is a simple system developed for region observation using only simple and passive infrared sensors to discover intrude. This system focuses on ensuring integrity and authenticity of reported events in the presence of an attacker who may compromise a limited number of nodes. It also implements a node failure-detection protocol, which notifies the sink if a node fails to reply for an identified period. This protocol was demonstrated in Dudek et al. [75] on a small scale, i.e. a small stretch of border or perimeter of private property. Below the application layer, FleGSens architecture employs a hop-based routing network layer and an IEEE 802.15.4 link layer. The hop-based routing ignores load balancing among nodes and links reliability, which is critical in hostile environments and could have considerable impact on the packet delivery ratio and timeliness. Moreover, the grid topology is impossible to achieve for international border applications. Relying on such assumptions limits the scalability of the system.

In Mishra [76], Artificial Neural Networks (ANN) are used to discover distinct patterns that describe an intrusion event across a border. ANN running at the central sink uses gathered sound and light readings to identify events that can be classified as intrusions. For data collection, the Collection Tree Protocol (CTP) [20] is used. CTP builds and sustains minimum-cost trees to nodes that advertise themselves as tree roots. The proposed system manages to reduce the number of false alarms. Besides the high cost of central data collection, the system introduces response delays due to centralised processing of large volumes of data. The proposed model is designed and tested with only two data modalities, light and sound; introducing new data modalities requires the addition of new models that analyse and integrate the received data. Finally, CTP is designed for traditional nonlinear topologies and it does not provide end-to-end

reliability. The authors do not give the CTP implementation details, such as the timing for routing and forwarding packets.

It is evident from the literature survey that there is no systematic approach to WSN application to border security and surveillance. Most reviewed systems are built with narrow application objectives in mind. There is no serious attempt to address the fundamental challenges imposed by large-scale border security and surveillance at the topological level. The linear structure of the network topology necessitates new solutions not only at the application level, but also at the data link and application levels. As the network infrastructure becomes more complex, it needs to accommodate several applications. These applications have many, and potentially conflicting, requirements, such as timeliness, reliability, data accuracy, and energy efficiency. It is important to accommodate these requirements before a generic architecture for linear-based WSN that covers a wide spectrum of application is realised.

Monitoring applications, such LWSN border/pipeline surveillance, are concerned with current sensor values, and, therefore, require real-time data collection. They also have low false alarm rates; dispatching a patrol or maintenance team in response to a false alarm could cost thousands of pounds. Similarly, most applications require continuous coverage to avoid missing any events. Another common feature among these applications is the large stretch of area they cover. Often, multi-sense modalities are measured and fused to detect events of interest. As they are mostly deployed in hostile environments, it is also necessary to use the on-board power supply efficiently. Most of the systems reviewed above address one or two of these requirements, while ignoring others. Furthermore, most of these issues need to be addressed in the communication layers to provide an effective solution. Yet, the communication aspects of such systems are only touched upon, leaving open problems of how and when to communicate information. In this study, we contribute a routing protocol for topologically linear WSNs. We attempt to provide a scalable solution that can deliver accurate data across reliable

links at a low cost. This protocol does not need resource-rich nodes; it only utilises flat network topology to deliver data to the base station

2.6 LWSN Architecture and Node Hierarchy

This section describes the existing types of commonly used nodes within the classical WSN networks. Networks may have different hierarchies depend on the application and the size of the network. In classical WSNs, nodes are divided into three categories: Basic Sensor Nodes, Data Relay Nodes, and Data Dissemination Nodes. The relation between nodes is shown in Figure 4.1. The following node hierarchy is presented in [9, 77]:

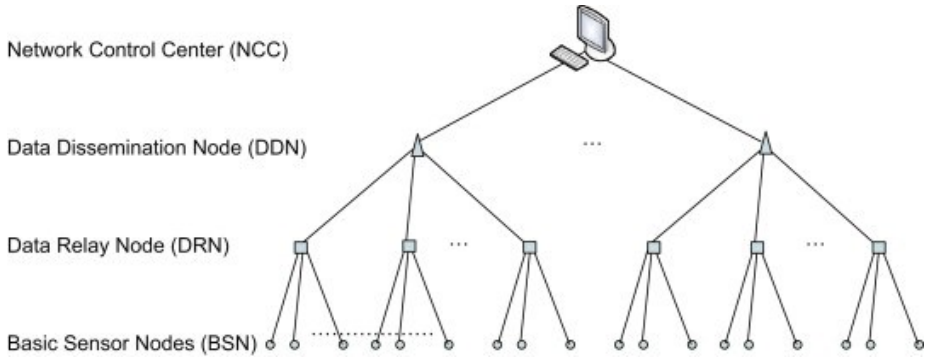


Figure 2.1 LWSNs' General Hierarchy from BSN to the Base Station [9]

2.6.1 Node Types

2.6.1.1 Basic Sensor Nodes (BSNs)

These nodes are mainly capable of three functions: sensing (can vary, i.e. sensing air pollution or emotion recognition), computing, and communicating. They have limited lifetime due to the size of their battery. These nodes can make a complete network themselves, or they can be configured with other high transmission nodes depending on the needed application. It is worthwhile to mention that BSNs are the main component of any WSN.

2.6.1.2 Data Relay Nodes (DRNs)

These types of nodes are responsible for transmitting the data received from the BSNs to either DDNs or the base station. DRNs will compress and transmit the data received; they are also responsible for aggregation and routing. In other words, they are generally performing cluster head duties. However, in our deployment, DRNs are not required as they are an additional complication to the network and an extra cost.

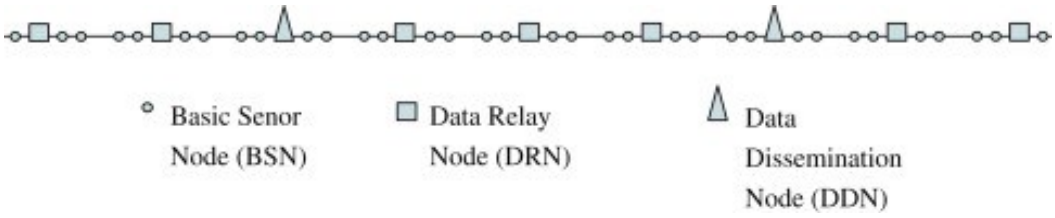


Figure 2.2 Demonstrate BSNs, DRNs, and DDNs in real deployment [9]

2.6.1.3 Data Dissemination Nodes (DDNs)

These nodes are always in direct link with the base station or network control centre to transmit the data received from DRNs. Additionally, transmission technology within these nodes may vary, as these nodes should have rich resources of power, such as electricity or solar energy. Figure 4.2 presents a flat deployment of the three types of nodes.

2.6.2 Network Topology of LWSNs

Nodes, which are usually located randomly throughout the observation, can each collect data and route the data back to the gateway, “the end-user”. Data is transmitted via multi-hop network architecture. The gateway node must be able to have direct communication with the task manager, possibly via Internet or satellite. This can be divided into three categories from a topological point of view: *Thin, Thick*, and *Very Thick.*

2.6.2.1 Thin Hierarchy

It is the basic level of deployment where all sensor nodes are deployed one by one in a linear structure as a one-dimensional form. This form is ideal to monitor many important applications such as motorway light and speed management or water/gas pipelines [78]. The advanced knowledge of the network layout allows improvement in network efficiency and power conservation [79]. Based on node hierarchical types, thin networks can be divided into three categories: thin one-level LWSNs, thin two-level LWSNs, and thin three-level LWSNs

- **One-level LWSNs:** This is the basic form where the network contains only BSNs, in which all nodes have the same duty of sensing and delivering data to the sink node through other BSNs. This form of deployment is suitable for small-scale applications that have a short network distance. However, this type of network is very vulnerable as nodes might be relocated by natural or manmade causes. For instance, if *S* number of BSNs moves out of range, this will result in network cut, which would make it unreliable. Figure 2.3 illustrates one-level thin LWSNs.

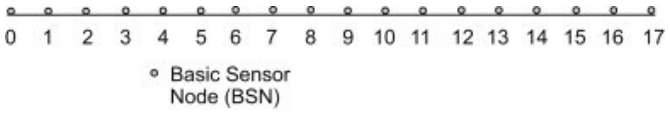


Figure 2.3 Demonstration of one-level thin LWSNs

- **Two-level LWSNs:** This is the form of LWSN deployment where a network contains two types of nodes: BSNs and DRNs. Each set or segment of BSNs gathers their data to one local DRN. DRNs in this network are responsible for transmitting data from BSNs to the base station via neighbouring DRNs to the sink. In such a network, BSNs are expected to have a longer lifetime compared to one-level as DRNs perform routing and aggregation tasks [80]. This is suitable for medium length networks, and it has more reliability compared to a one-level network.

- **Three-level LWSNs:** This network has all three types of sensor nodes: BSNs, DRNs, and DDNs. In this form of deployment, DDNs transmit the data received from a group of segments to the base station (BS) as demonstrated in Figure 4.4. One segment failure will not affect the rest of the network, which improves the robustness and the scalability of the network. Having the benefit of DDNs will ameliorate the network performance due to the direct communication with the BS. Additionally, this model reduces the number of routers used along the path; hence, the end-to-end delay is reduced. The major drawback is many gaps in the sensed area may occur if any node dies. This sensing gap in the network is a major disadvantage in some applications, such as border surveillance. This model can be used in some large-scale applications, including pipelines, roads, etc. [9].

2.6.2.2 Thick Hierarchy

In this model, just DRNs and DDNs are deployed in a line, while BSNs are deployed randomly. In addition, BSNs can have different dimensional distributions. A thick LWSN is ideal for monitoring a geographic area, such as an international border.

- **One Level**: Only BSNs are distributed randomly in a two-dimensional fashion between two parallel lines as showed in Figure 2.4 BSNs are responsible for all network operations from sensing to transmitting to the base station.

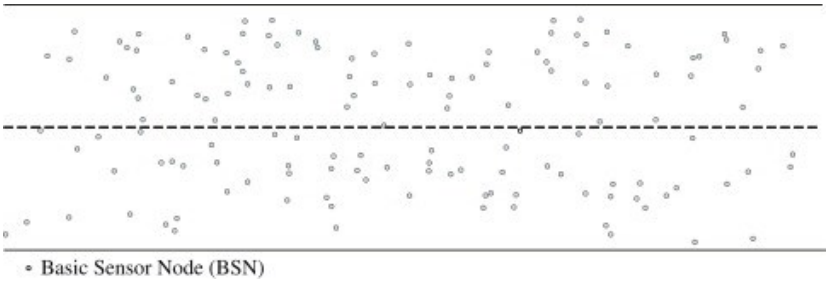


Figure 2.4 Demonstration of one-level thick LWSNs [9]**.**

- **Two and Three Levels:** In these networks, the two high level nodes are scattered in a linear fashion; however, the BSNs can be scattered randomly in two or three dimensions. The main difference between two levels and three levels is the existence of DDNs. Figure 2.5 presents two-levels thick LWSNs.

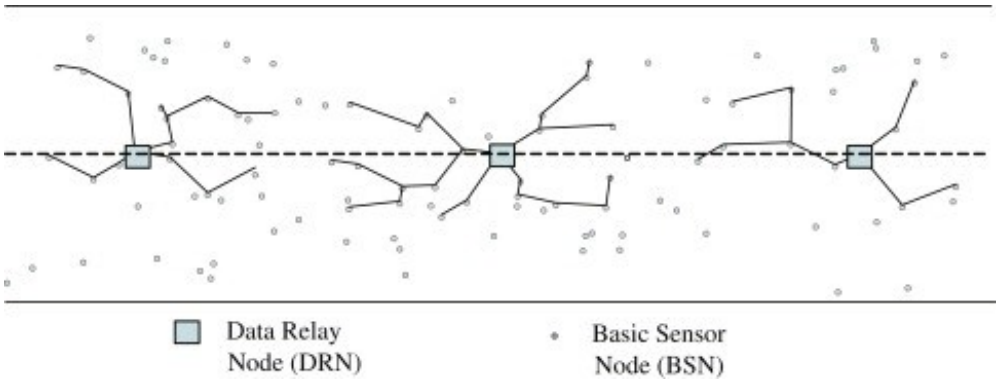


Figure 2.5 Demonstration of two-level thick LWSNs [9]

2.6.2.3 Very Thick hierarchy

A very thick hierarchy is a linear structure where nodes at all levels are randomly deployed; however, all nodes must be located between two lines over a long distance. One level does not exist in the very thick network as it has been categorised in the thick network.

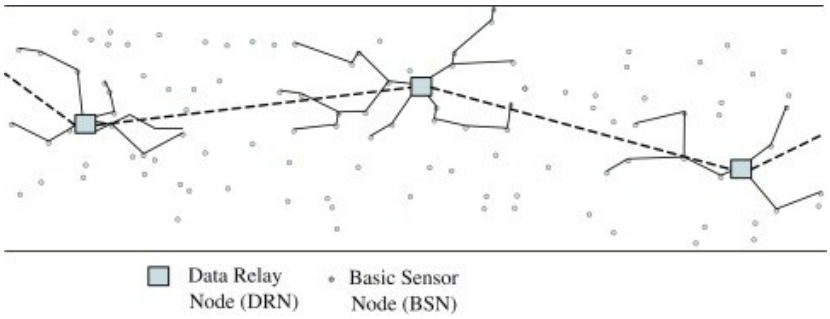


Figure 2.6 Demonstration of very thick LWSNs [9]

- **Two Levels:** BSNs and DRNs are scattered in this network in a two-dimensional

style as demonstrated in Figure 2.6.

- **Two and Three Levels:** In this network, only DDNs are deployed in a one-dimensional structure, while BSNs and DRNs are in multi-dimensional form.

2.7 Possible Technical Challenges in LWSN Deployments

LWSNs inherit many characteristics that are common to the general types of WSNs. However, LWSNs operate in conditions that are more severe due to the constraints of resources [81]. These include the restriction in energy supply, small bandwidth, scarcity in power for computation, and the reduced capability supply. In addition, LWSNs have extra restrictions created by the linear topology and the scares deployment [82], including sensor data aggregation, inter node communication, control commands and the long range flow for sensing data. These extra restrictions come with several challenges, all of which must be considered when developing new operation schemes for LWSNs. The levels at which these challenges are addressed will have an overall impact on the performance of system.

The first challenge faced by these LWSNs is the development of a deployment architecture that is energy efficient and scalable [83]. Such an architecture has the ability to enable the network of sensors to have a long life and an overall lower cost of deployment. The design of the architecture is generally influenced by the following characteristics [84, 85]: sensor nodes' deployment in a linear fashion and a network dimension that stretches over a long distance.

The next challenge is the necessity to develop a communication protocol that is energy efficient [86]. The communication protocol enables communication between sensor nodes and between the sensor nodes and their base stations. The uniqueness of the linear typology restricts the number of communication paths that exist between the sensor nodes with a directional transmission through the distribution path of the LWSNs.

These communication protocols are supposed to determine the duty cycle of nodes, and this leads to lower energy consumption and the coordination of the transmission of data between the nodes and the towers.

The final challenge that should be addressed for the new deployment of the sensor networks is the development of a duty cycle MAC protocol that enables seamless communication among the sensor nodes all the way to the towers. The MAC protocols for the classical WSNs are designed based on the assumptions that the nodes have the ability to transfer data to other nodes and to the base station directly or through cluster head, and the deployment of the sensor nodes in a fashion that is distributive and concentrated in three-dimensional or two-dimensional regions of interest [87, 88]. The linear typology requires directional transmission for the nodes' communication. Moreover, the sparsely populated network in terms of distance between nodes, the number of neighbours of each node, and the total network density makes traditional MAC protocol techniques inapplicable to LWSNs. For instance, some MAC protocols, e.g. such in [11], rely on resource redundancy to achieve their goals. Some protocols use multiple paths to multiplex traffic to achieve load balancing or communication details. At the same time, sparse node deployment means that many problems that exist in standard WSNs due to network density, such as long MAC scheduling waiting times, frequent collisions or communication interferences, are now less severe. The new MAC protocol should also support the nature of the applications that are event-driven, giving priority to the design scheme to provide prompt data delivery. It should also be free of functions, which mostly introduce delays and extra communication/computation cost, to deal with problems that no longer exist.

2.8 New Framework Objectives

In order to make the right assumptions in the design of the desired LWSN framework, we need to understand the behaviour and objectives of this surveillance system. The border

monitoring application is a very large system that could span several thousands of kilometres. The main objective of border surveillance is to detect any personnel and vehicle intrusions across the monitored area. This application scenario includes collaboratively interacting and detecting various entities in the monitored environment, including terrorists, smugglers, and illegal immigrants, illegal vehicles crossing, patrol movement, nearby residents' movements, etc.

Border monitoring is selected because of its generality and sensitivity among other applications with large linear topology, e.g. pipelines, rail track, AC power line monitoring, etc. We believe that WSN technology can be optimised to provide real time intelligence on illegal border crossing. Deploying effective LWSNs for border monitoring can help to ensure a high level of remote border security and management. In addition, it is more cost effective and environmentally friendly than traditional border patrols. Border surveillance application includes a mixture of node capabilities to cover the long border distance. This approach is a practical contribution towards linear large-scale network applications.

Any proposed solution must address the challenges and conditions required by border monitoring. Therefore, this provides a perfect situation to examine the new LWSNs protocol. The scenario created in this project highlights the motivations for using the new LWSNs protocol to overcome the presented challenges and to enable an energy efficient system. The new general framework will be designed according the identified requirements. Finally, the framework will be tested in a real world application to measure its performance.

2.9 Summary

There is no perfect technology; each technology has specific features that work well in certain situations. The authors believe that a carefully designed WSNs can reduce risks in border surveillance systems. Hybrid systems that encompass the features of various available systems would serve the purpose of border monitoring more efficiently. Taking the positive features of all systems to complement their respective drawbacks will enable the building of a hybrid system, which is not just efficient, but functions according to the needs of the hour in terms of border surveillance. The hybrid system should work independently of natural changes in the form of rain and storms, and be compatible with deserts and other barren border locations.

In this chapter, we reviewed MAC protocols designed for LWSNs. The focus of the study was on protocols that apply a duty cycle mechanism to reduce energy consumption. Most of the current work focuses on the theoretical architecture of the network, or the deployment of nodes creating either a system with high vulnerability, which undermines its mission, or high resource requirements in the deployment [91]. It does not solve the long-range communication problem, which is the main concern in these applications. Moreover, none of the existing work has provided a realistic generic framework considering the lack of resources, low node redundancy and time sensitivity of the application. Any new LWSN-specific MAC protocol should take advantage of the features of the linear network topology to meet the application requirements, achieve high-energy savings and timeliness data delivery in low-density networks. Such requirements are essential to all mission critical LWSN applications.

This chapter also introduced existing WSNs deployment architectures and different types of nodes used in their implementation, namely: BSNs, DRNs, and DDNs. The next chapter will study the network deployment technique for efficient and rapid establishment of the network, also will focus on the calculation of the required network density.

CHAPTER 3

Network Deployment, Architecture, Density and Barrier Coverage

This chapter suggests an effective and scalable network architecture specifically designed for border surveillance. The given solution satisfies the basic challenges concerning the implementation of a LWSN framework, i.e., the deployment of an architecture that is energy efficient and scalable. Also addresses crucial considerations referring to the LWSNs deployments such as network width and node density. It also defines a method of determining the minimum number of sensor nodes necessary in a certain deployment in order to achieve k-barrier coverage in a given belt. In addition, it tackles issues such as determining if a region is indeed k-barrier covered and discovering of any coverage gaps in a certain belt of sensor nodes. The results obtained by the described method can be used to estimate the required network density to provide complete border coverage.

3.1 Introduction

The challenge of developing a new WSN framework for border monitoring starts by defining a suitable architecture that is feasible in the real world. The new architecture must consider all environmental terrain types, such as forest, desert, mountain, etc. The network topology is another essential factor in the new framework. Based on these two factors, node density can be measured to ensure sufficient network coverage. The current research in LWSNs addresses problems as they arise from a narrow application perspective. For instance, many routing protocols were proposed for pipeline monitoring applications. In such systems, data collection is typically accomplished through specialised mobile or power-rich nodes. In border security, this is not always possible. For example, in wild forests, it is infeasible for an unmanned vehicle to bypass large natural obstacles. Therefore, there is a need to tackle the problem fundamentally at the topological level. This chapter contributes a mechanism for calculating the minimum number of sensor nodes required to achieve k-barrier coverage in a given belt region, how to determine if a region is indeed k-barrier covered, and the factors that affect barrier coverage

The rest of this chapter is organised as follows. Section 3.2 discusses the deployment technique of border surveillance systems. Section 3.3 proposes a new system architecture for border surveillance. crossing path coverage levels of the new architecture. Section 3.4 investigate node density and barrier construction designed for LWSN applications to insure coverage and connectivity. Section 3.5 analysis crossing path coverage levels of the new architecture.

3.2 Deployment Techniques

In WSN border intruder detection applications, system engineers place nodes along a narrow line ensuring adequate level of sensing coverage and radio connectivity.

Therefore, quality of such systems is highly dependent on the deployment method of sensor nodes and their density. The challenge is how to reach maximum performance using the minimum number of nodes. Achieving uniform node deployment is a complex task in such a large geographical area (several hundreds of kilometres). Moreover, environmental barriers, such as mountains and forests, makes access to the monitored area more difficult and high objects may cause communication and sensing coverage gaps.

Currently, using an aircraft to drop the sensors might be the only achievable methods to deploy sensors in vast areas. However, dropping sensors from the air is not expected to have uniform deployment as the environmental factors might affect the process of landing. Figure 4.8 demonstrates a random airdropping of sensor nodes using a chopper.

Figure 3.1 Random deployment of sensor nodes using aircraft

Theoretically, it is impossible to deal with such a large distance as one WSN due to limited node capabilities and high application QoS demands. Therefore, it is necessary to divide the system into a smaller group of networks, which work cooperatively to monitor the full monitored area. Therefore, two types of communication nodes are required, BSN and DDN. The basic idea is to divide the network into a number of segments, where each segment consists from two DDN nodes and the BSNs between them. In real-life deployment, a segment two ends is the monitoring tower, which are normally built at

regular distances or in sensitive locations. Monitoring towers are normally occupied by border guards and host long-range radio facilities that allows communication with central control and command centres. BSNs will be placed between two towers in a linear fashion. By default, nodes are homogeneous. In Figure 4.8, the network consists of a set of segments where BSNs are positioned on narrow and long belts with sink nodes at each end of the segment. A BSN is responsible for collecting data in its range and delivering it to the sink directly or through neighbouring node.

As nodes will be deployed along a virtual line, we can assume a two-dimensional area having a long and thin rectangular shape. This area has the length and width of l and w, respectively. All nodes are static since landing and their location are known. Figure 3.2 demonstrates the area of deployment.

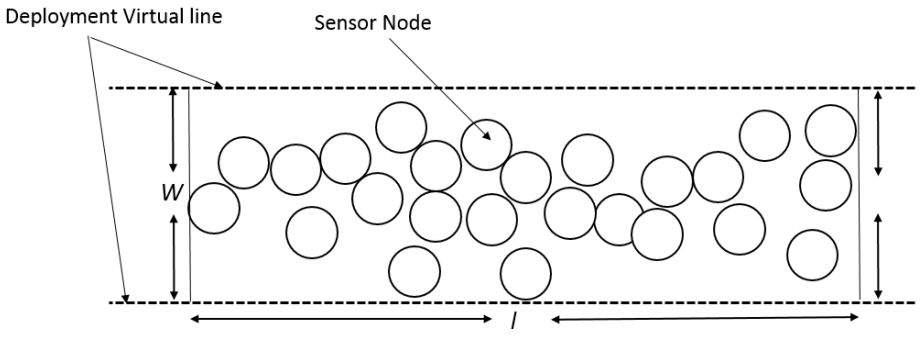


Figure 3.2 Overhead view of sensor nodes deployment area

Saipulla et al. [89] calculates the location of a node during deployment process. If the coordinates of a node is (y, x), then, the Probability Density Function (PDF) which describe the relative likelihood of a deployed node to take on a given location variable, can be calculated as follows [89]:

$$f(y,x) = \begin{cases} \frac{1}{lw}, 0 \le y \le 1, 0 \le x \le w \\ 0, otherwise \end{cases}$$

where l and w are the length and width respectively of the rectangular shape that represents the virtual line where node are deployed.

Any crossing is detected by at least one sensor node. A crossing counts when an intruder has passed the two width lines of the rectangle, also called the crossing path. As in Saipulla et al. [89], an event occurs with high probability when its probability tends to 1 as $n \to \infty$.

3.3 System Architecture

Most of the current WSN systems for area monitoring and surveillance can be described as multi-layered systems. In multi-layered systems, additional resources, such as unmanned ground vehicles or UAVs, are deployed to carry out data collection and computationally intensive tasks. As explained in Section 3.4, multi-layered systems offer many benefits in terms of improved performance and lower energy consumption. However, the integration of multiple technologies is a complex task. More importantly, the success of a border security system relies on timely data delivery; therefore, periodic data collection using mobile unmanned vehicles or drones is not appropriate. In many deployments, mobile vehicles cannot reach or could get stuck in rough terrain border stretches, e.g. hills, trees, and riverbeds; consequently, stopping the critical flow of data. The operation of mobile vehicles and drones requires human involvement and intervention. The initial cost of these devices added to their operation and maintenance cost significantly increases the overall expense of the system. Finally, WSN systems are often deployed in response to emergency situations; border security and surveillance are no exception. In multi-layered systems, the deployment of the top layer nodes requires physical access to the field, time, and planning. This prevents rapid deployment of a WSN-based system for border security and surveillance applications.

To overcome the drawbacks of multi-layered systems, we propose a flat architecture. Flat

systems are comprised of a set of sensor nodes with similar hardware capabilities that collaborate to detect and report events. This class of systems can be rapidly deployed in conflict areas to respond to emergencies at a low cost and with minimal setup. It has been suggested by domain experts that the highest value implementation of this capability is along likely avenues of intrusion or in non-line-of-sight areas. The use of sensors with overlapping coverage and both local and central data fusion can achieve a high detection rate with fewer false alarms. This work adopts a flat, modular system architecture to offer timely, mission centric event detection. The system is open to any hardware platform and does not assume any sensing modality. The modular system architecture allows easy integration of potential hardware and software technologies. This flat architecture permits monitoring and control of sensors scattered throughout a large stretch of border and interfaces with existing command and control systems.

a b c

Figure 3.3 a. Border monitoring tower [90]. b. LMV armoured vehicles used by border guard units in Europe [91]. c. Tactical manpack antennas are suitable for handheld and man-portable applications [92]

Conventional border surveillance systems rely on fixed checkpoints, monitoring towers, and mobile vehicles with border troops. Border guards could be equipped with manpack antennas. Figure 3.3 shows the three main actors in conventional border surveillance systems. The proposed network architecture accommodates the existing border surveillance infrastructure. The unattended ground, possibly underground, sensor nodes provide higher granularity for monitoring. These nodes are resource-constrained, low-power devices that perform sensing tasks and send their information to a local

processing hub or to the base-station for network-wide processing. These devices also communicate with neighbouring nodes using low-power, low-rate, short-distance radio. Each sensor node offers multi-hop routing capability to its neighbours. In this work, the Boolean sensing model is adopted, in which every sensor has a certain sensing range, r. A sensor can detect intruders only within its sensing area. A location is said to be in a covered region if it lies within that sensor's sensing area. A vacant location is not in the sensing range of any sensor.

Stationary and mobile (e.g. armoured vehicle dispatched to incident location) surveillance towers collect and route data to the wired network. Surveillance towers can host powerful and reliable multimedia sensors, i.e. radars, cameras, and sensors. Information from the sensor nodes and the multimedia sensors can be fused at the surveillance tower to reduce the false alarm rate. After the surveillance towers confirm an intrusion detected by sensor nodes, they report the intrusion location to the remote control and command centre. Data fusion is outside the scope of this work; Mishra et al. [76] and Hanjiang et al. [70] present solutions for data fusion to reduce false alarms.

Due to coverage considerations and to reduce the miss-rate, the number of deployed sensor nodes is very large. Hence, the network is divided into several segments. A segment comprises a surveillance tower and the nodes to its left and right, which transmit their data to it. Similarly, surveillance towers coordinate with each other to improve the detection rate. The details of the segmentation process are given in Subsection 4.2.2.1. Figure 3.4 sketches the described network architecture. It shows two stationary surveillance towers, where the left tower is equipped to deliver data over the internet using satellite communication. The two towers can also communicate with each other. Each tower collects data from the sensor nodes around it. The armoured vehicle on the right depicts a scenario where a mobile tower is dispatched in response to an alarm.

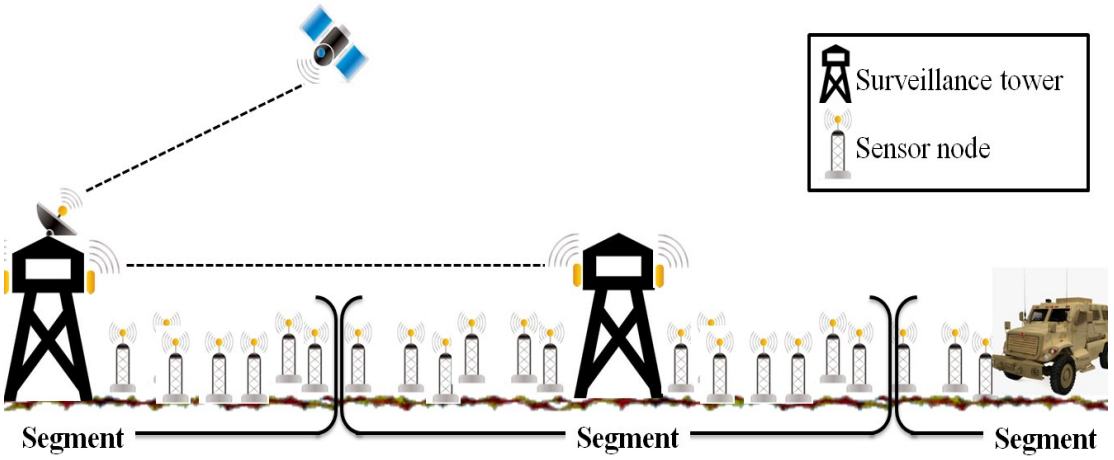


Figure 3.4 A sketch of the system architecture adopted in this work

3.4 Node Density and Barrier Construction

In border surveillance, there is a need to notify border guards with advanced warning of intruder activity, which, if geopolitical conditions allow, can be accomplished by deploying sensor nodes on the other side of the border. This installation would be particularly valuable along likely avenues of intrusion to provide early warning before intruders reach the borderline. In practical terms, this means increasing the *width* of the WSN. This installation raises questions of how to determine the required network *width* and node *density*. This problem is sometimes referred to in the literature as the m-coverage and n-connectivity problem. Coverage is a crucial metric to determine the capacity of monitoring. Connectivity ensures that the data can be delivered to the base-station with the specified quality-of-service guarantee. The use of sensors with overlapping ranges and both local and central data processing is essential to achieve a high detection rate with low false alarms and nuisance.

The m-coverage and n-connectivity problem for border surveillance has been studied in the literature before [33]; however, considered research scenarios assume nodes to be distributed in a *circular* region. In the context of intrusion detection, this problem is formulated as the *k*-barrier of a belt region [33, 93-95]. When sensor nodes are deployed to detect intruders, they form a logical barrier for such intruders. If a barrier does not contain coverage gaps, then it is called a strong barrier. A crossing path is a path that connects one side of a belt region to the opposite side, i.e. the entrance point and the exit point exist on two opposite sides of the region [94]. For border surveillance applications, it is assumed that the intruders attempt to cross the width of the belt. A belt is a region bounded by two approximately parallel curves. In border surveillance applications, the deployment for barrier coverage is very long and thin belts. Often, in barrier coverage, sensor nodes are deployed in regions of an irregular long belt shape. A given belt region is said to be k-barrier covered if all crossing paths through the region are k-covered. A path is called k-covered if at least one node is covering the path. K-coverage can be contrasted with full coverage, where every location in the deployment area is covered.

The aim of the proposed border surveillance WSN system is to detect intruders before they have crossed the border as opposed to detecting them at every point in the crossing path. Therefore, reporting data on full coverage is often an excess. This makes the established research work on full coverage unsuitable to apply directly to k-barrier coverage in a belt region. In this section, we attempt to answer three important questions:

1. What is the minimum number of sensor nodes that must be deployed to achieve k-barrier coverage in a given belt region?

2. Given an appropriate network density, how do we determine if a region is indeed k-barrier covered?

3. What are the factors that affect barrier coverage?

Early research described how to construct barriers to detect intruders travelling along crossing paths in rectangular areas. In the following, we give the number of disjoint open crossing paths that exist in each rectangle. As in Huang and Tseng [3], we construct a bond percolation model to obtain the number of disjoint barrier sections crossing the length of the segment. Initially, the area is divided into equal size squares, where the length of each edge is $\mathrm{l} = \mathrm{r}/\sqrt{2}$, where r is the sensing range of a particular sensor. The probability that a square contains at least one sensor can be reached by changing the sensor node density δ:

$$P = 1 - e^{-\delta l^2}$$

A square is said to be open if it hosts one or more nodes; otherwise, it is said to be closed. Since $l = r/\sqrt{2}$, an open square will be completely covered by a single sensor. Consequently, if two adjacent squares are both open, the sensing coverage of nodes located in these sensors will overlap leaving no gaps for an intruder to cross without being detected. This structure can be further refined by the discrete bond percolation model by drawing horizontal and vertical edges to partition the square into four equal portions. This gives a grid of connected edges, where a series of linked edges form a crossing path. A path that consists only of open square edges, an open path, acts as a barrier that can detect any intrusion event. Therefore, the strength of strong barrier coverage, a barrier with no gaps, depends on the number of disjoint open paths in the network. We define a two-dimensional belt of length s, with $\left(\frac{1}{s}\right)$. If $\left(\frac{1}{s}\right) = \varphi(\log \mathrm{s})$, then A can be divided into horizontal belt regions $\mathrm{R_s}$ of size $s \times \mathrm{cr}\log \mathrm{w}$, where $\mathrm{w} = \frac{\mathrm{s}}{\mathrm{r}}$ for some $\mathrm{c} > 0$. The result is $\frac{\left(\frac{1}{s}\right)}{\mathrm{crw}}$ rectangles. In the bond percolation model, each rectangle $\mathrm{R_s}$ is of network size $\mathrm{w} \times \mathrm{k}\log \mathrm{w}$. Let $L(i)$denote the set of all crossing paths congruent to i. According to Kumar et al. [93], the belt region is said to be k-barrier covered with

high probability if

$$\forall_i \lim Pr\left[\forall_j \in L(i): j \; is \; k - covered\right] = 1$$

Lemma 1 presents the number of disjoint open paths that cross each section. The proof of this lemma is the same proof of Theorem 3 in Huang and Tseng [3].

LEMMA 1. For any $\mathrm{k} > 0$, if $\frac{\delta > 2\left(\log 6 + \frac{2}{c}\right)}{\mathrm{r}^2}$, there exists a constant $|\chi(\delta \mathrm{l}^2, c)|$ such that with high probability there exist $\chi c \log \frac{s}{r}$ disjoint barrier sections that cross each R_n from left to right.

The total number of disjoint barrier sections is linearly proportional to the width of the region and is calculated as $\frac{\chi}{\mathrm{s.r}}$. If intruders are known to move in groups, where they follow virtually congruent paths, weak barrier coverage will guarantee detection with high probability. To provide weak barrier coverage in a belt region with high probability, a considerably smaller number of sensors is needed than that required for strong barrier coverage with high probability. Finally, if the sensor nodes are covert, then having weak barrier coverage with high probability may be effective to detect all intruders.

3.5 Crossing Path Coverage Levels

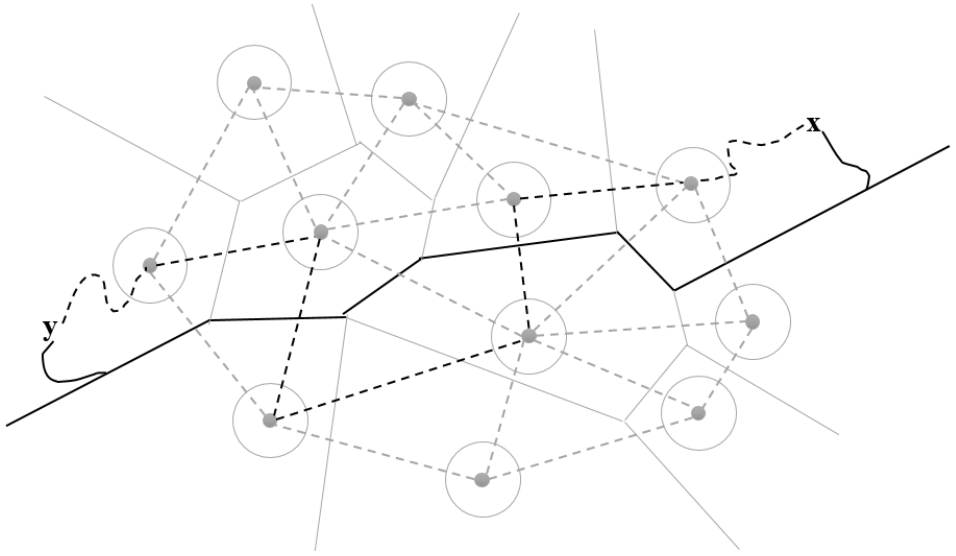


Figure 3.5 MBP and MSP examples. The segments drawn in bold lines denote maximal breach and support paths. Sensor nodes are represented as circles with a large dot in the centre. The continuous bold line segments are the edges of the Voronoi Diagram, and the dashed lines are the edges of the Delaunay triangulation.

In the domain of WSNs, most existing research on the area coverage problem aims to cover the entire region of interest [72]. Meguerdichian et al. [96] quantify the quality of worst-case coverage by identifying the Maximal Breach Path (MBP). The MBP is the path with the lowest observability among all the possible paths from a specific starting point to a specific destination. The lowest observability is due to every point on the path being the most distant from the deployed sensor nodes. Likewise, the best-case coverage describes the path, called the Maximal Support Path (MSP), with the maximal observability or support along all the possible paths between the two given points. Figure 3.5 shows the MBP and the MSP in a small WSN. In this section, we build on these definitions to define a method for discovering any coverage gaps in a belt of sensor nodes. The results obtained by this method can be used to estimate the required network density to provide complete border coverage. This can be achieved by calculating the probability of an object crossing the border with or without being detected.

A WSN can be modelled by a directed communication graph $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ where V is the set of sensor nodes with $\|\mathrm{V}\| = \mathrm{N}$ and N is the total number of sensor nodes. For a type i node u and a type j node v, there is a directed edge (u, v) in E if and only if v is within the radio range of u. The degree of u, denoted as $d(u)$, is the number of neighbours of u. The degree of a communication graph G is denoted as $dm(G) = min\forall u \in V\{d(u)\}$. Let the sensor nodes be represented as a set of n sites, S, in a two-dimensional field. The Euclidean distance between two nodes n_i and n_j is denoted as $\|n_i, n_j\|$. The distance between node n_i to a set of nodes I is the smallest distance of n_i to all nodes of I; this is denoted as $d(n_i, I) = min_{n_j \in I}\|n_i, n_j\|$. Accordingly, the smallest distance from n_i to all points on an edge uv is denoted as $d(n_i, uv)$. The coverage-distance between node set U to another node set W is the maximum distance of every $u \in U$ to V, i.e. $cover\ (U, V) = max_{u \in U} dist(u, V)$.

Let $P = T(x, y)$ be a crossing path of an object travelling from a starting point x to an ending point y inside S. The observability in terms of how well the path is covered by sensor nodes is defined as *coverage-distance* $= max_{x \in P} d(x, N)$. The breach-distance of P is defined as $min_{x \in P}\ d(x, S)$, which describes how far the path is from all sensor nodes. Meguerdichian et al. [96] proved that a best coverage path exists in the WSN that connects x to its nearest sensor node u_x and connects y to its nearest sensor node u_y. Without loss of generality, we focus our study on the path connecting the start and end points to u_x and u_y, respectively.

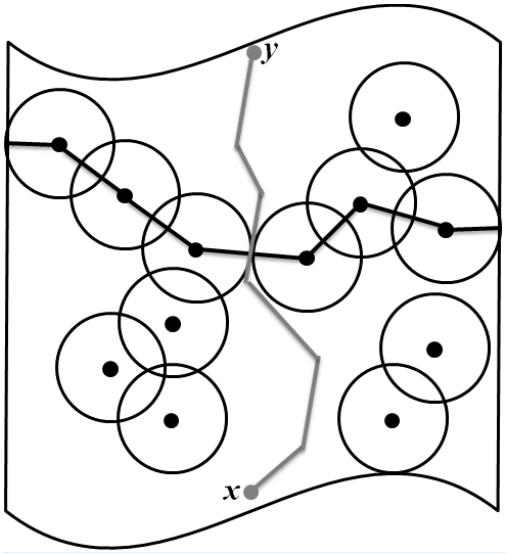


Figure 3.6 The relationship between the MBP (grey line) and the MSP (black line)

To discover coverage gaps in a belt region, we use the growing disk concept explained in Meguerdichian et al. [96]. Assume that each sensor node initially has a disk centred at its location with radius 0 and all disks start growing with the same speed. Define $D(S,r)$ as the region covered by all disks centred at nodes of S with radius r. $\overline{\mathrm{D(S,r)}}$ is the complementary region of $D(S,r)$ in the sensing field. Subsequently, the best coverage problem can be stated as follows: what is the smallest sensing radius value r such that there is a path, inside $D(S,r)$, connecting points x and y (see Figure 3.7). Similarly, the worst sensing coverage problem can be stated as follows: what is the largest sensing radius value r such that there is a crossing path, inside $\overline{\mathrm{D(S,r)}}$, connecting points x and y?

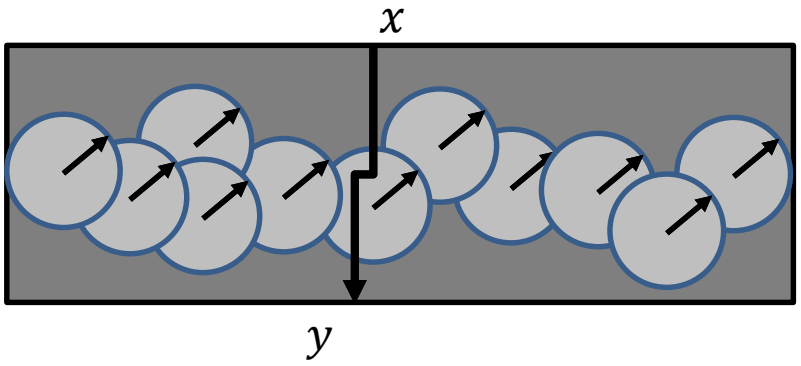


Figure 3.7 Schematic representation of the sensor deployment. The light grey area show $D(S, r)$ and the dark grey area shows $\overline{\mathrm{D(S,\ r)}}$

Based on the growing disks concept described above, we observe that there is a two-way relationship between the MSP and the MBP, i.e. an optimal algorithm for best-case coverage can be applied to find wors-case coverage. To illustrate this relationship, we show a belt region in Figure 5.2 with a crossing path from x to y. From the figure, it can be seen that finding the distance for the worst-case coverage (grey line) of the MBP from x to y is the complement to finding the MSP from the start of the end of the barrier section (black line).

There are many algorithms in the literature for finding the best- and worst-case coverage, e.g. Meguerdichian et al. [96]. Most of these are centralised algorithms with time complexity $O(N \log N)$. We propose applying any of these algorithms concurrently and independently in each network segment. This segments the problem to reduce its complexity to $O(N_s \log N_s)$, where N_s is the number of nodes in a single segment. The performance can be further improved by stopping the MBP process when an edge on the path intersects with any barrier section; this indicates that there are no coverage gaps in that barrier section.

Our goal is to find a path connecting x and y such that every point on the path is covered by a sensor node. The other variation is to find a path with the smallest total travelling distance among all optimum paths with the best coverage distance. To search for this path, we can use the property proved by Zhang and Hou [71] that if radio range $\mathrm{r_r}$ is at least twice as large as sensing range $\mathrm{r_s}$, full sensing coverage implies network connectivity. To conserve energy, the overlap of sensing disks of active nodes is minimised by sending redundant nodes to sleep. The model they propose is that, in the ideal case, the centre points of the three closest nodes form an equilateral triangle with side length $\sqrt{3r_s}$. Based on these observations, we suggest searching for an MBP at intervals that are r_s wide. This search can be started in parallel at the two end points of the segment.

If an MBP exists, this means that the barrier is weak. If the distance between two adjacent MBPs is $g \leq \frac{r_s}{2}$, then the barrier is strong. If the distance between two adjacent MBPs is $g > r_s$, this means that there is a coverage gap.

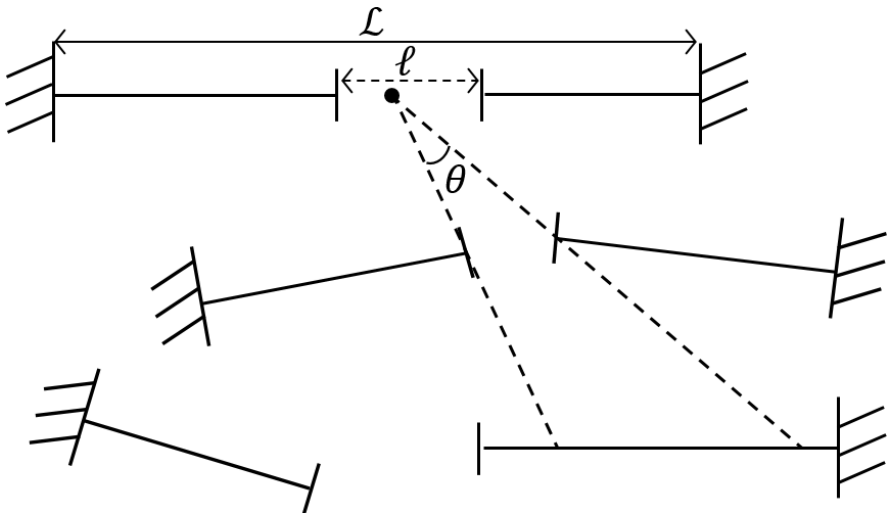


Figure 3.8 A belt with several weak barriers. The top level shows a coverage gap of size ℓ in a belt of length $\mathcal{L}$.

In real life deployments, a belt contains multiple weak barriers distributed at different levels as shown in Figure 3.8. Assume that there exists a randomly moving object, i.e., objects with nondeterministic mobility patterns, that is equally likely to hit any point on a belt of length $\mathcal{L}$. The probability of the object passing through the gaps formed between weak barriers at the same level is $\Pr[l_1] = \sum \frac{\ell}{\mathcal{L}}$. This crossing scenario is illustrated in the top level of Figure 5.3. From any location in the gap, the probability of passing through a gap between two weak barriers at the next level is $\Pr[l_n] = \frac{\theta}{\pi}$, where θ is the acute angle between the lines connecting the end points of the gap segment to the object's current location. The total probability of an object passing through all gaps along a specific route within a belt is:

$$\mathrm{T}_{Pr} = \frac{1}{\ell} \int_{\ell} \frac{\theta(\ell)}{\pi} d\ell$$

Due to many factors, such as hardware cost and topography, it is very difficult to guarantee strong barrier formation in every segment. However, it is important to note that in the presence of a small number of reasonably small coverage gaps, the intrusion detection performance is not greatly affected. This is because intruders, most of the time, cross the borders in groups, and it is very likely that at least one entity in the group will trigger an alarm. Moreover, sensors may be deployed covertly making it very difficult, without having an advanced wireless signal and sensor mapping devices, to find a way to navigate around these devices to avoid detection. Finally, sensor nodes are normally equipped with multiple sensors, e.g. sound and motion, each with a different sensing range. This increases the probability of detecting activity. Therefore, application specific factors such as these must be considered at deployment to decide node density and what sensing modalities to deploy.

3.6 Summary

This chapter focus on the design of a new, effective, and scalable network architecture explicitly designed for border surveillance. It consists of surveillance tower, which have a direct connection to the base station and BSNs. The BSNs, on the other hand, are connected to the surveillance tower using lower level neighbours. Moreover, the architecture allows the accommodation of additional BSNs and surveillance tower when necessary making the model easily expandable. The problems left to be solved are determining the routing scheme of the BSNs and fixing the unbalanced energy consumption. Additionally, this chapter defines the node density required to have sufficient barrier insuring full coverage at low cost possible. Also, it is explained what k-barrier coverage is and how it can be implemented to its maximum by giving a mechanism for calculating the minimum number of sensor nodes required to achieve k-barrier coverage in a given belt region and for determining if a region is indeed k-barrier covered. It also describes which factors can influence the level of barrier coverage. In addition, the chapter gave a definition for the crossing path term and a method for discovering any coverage gaps in a belt of sensor nodes. The results can be used to estimate the required network density to provide complete border coverage.

CHAPTER 4

A MAC Protocol for LWSN Segmentation and Duty Cycle Management

This chapter describes a mechanism to assign nodes in a given segment of the suggested architecture to various network levels depending on their distance from a monitoring tower. A cross-layer communication protocol then makes use of these levels to calculate the data delivery to the sink at the lowest possible cost and with the smallest amount of energy, which also results in the smallest delivery delay for such an operation. The network initialisation and the communication processes are explained in details. In addition, new effective sleep/wake cycle is introduced to further increase the network life and performance.

4.1 Introduction

Our proposed LWSN system architecture uses multi-hop communication in order to transfer data from the sensor nodes to the base station. In such architecture, nodes closer to the sink perform more transmissions to overlay the data of other nodes in higher levels of the network. This raise a new challenge to address balancing workload across nodes in the same network segment? Resolving this problem is important since communication is the most expensive operation in LWSNs and a possible solution would decrease the over-all network energy consumption and its lifetime as well. The chapter gives such a solution to the described problem by the implementation of the Level Division Graph (LDG) algorithm, which implements a sleep scheduling, where nodes enter low-power sleep modes during idle times. This chapter p a routing protocol that is tailored to address the requirements of LWSNs. We apply our protocol to border security and surveillance as it presents a complex set of challenges that are generic enough to cover most LWSN applications. Communication is the most power hungry process in WSNs. Routing deals with issues such as data reliability, timeliness, error rate, network lifetime, and system scalability; these determine the success of any WSN system. The main contribution of this chapter is a novel routing protocol designed specifically to address the communication needs and link reliability for border security and surveillance applications.

4.2 Network Segmentation and Inter-cluster Communications

In the directed communication graph $\mathrm{G} = (\mathrm{V}, \mathrm{E})$, each sensor node in the network is depicted as a node in G and a link between two nodes represents their ability to communicate with each other. An initial connectivity graph is built by the base stations, in our architecture surveillance towers, during the network configuration phase. Occasional connectivity updates are used to deal with temporal changes in the wireless channel.

Nodes in the network are assigned to various logical levels in a breadth-first order depending on the connectivity graph. Each local base station is assigned level 0. In effect, the level of a node is directly proportional to the minimum number of hops to reach the base station with which it associates itself. L_k denotes the set of nodes in level k. The maximum number of levels in the network is denoted by h.

The amount of energy consumed by each node varies relative to the node's location from its base station. Nodes in the lowest network levels suffer greater power consumption, because data from higher levels travel through them to reach the base station. This results in unbalanced energy depletion across nodes in a given network segment. In addition, in border surveillance, urgent events are occasional, but require immediate notification of time sensitive information. Since nodes in the highest network levels, the farthest from the base station, experience the longest delays, we focus our analysis on the delay for these nodes.

In this section, we describe a general purpose cross layer communication protocol that deals with the aforementioned requirements of an LWSN system. Communication protocols determine the path that a datagram should follow from the source to the destination. In the design of our LWSN routing protocol, we aim to eliminate any defects, which can result in unbalanced energy consumption as a result of aggregating and forwarding data of nodes further away from the base station. We also aim to maintain timely and reliable event notification.

4.2.1 Energy Balancing by Limiting Distances

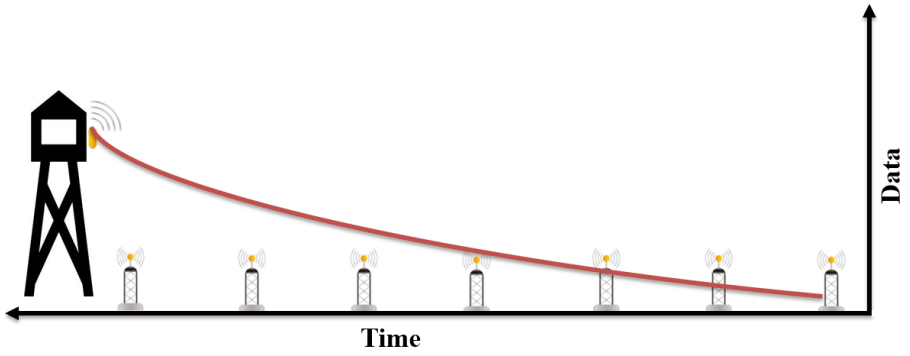


Figure 4.1 Data transmission distribution in nodes relative to their location from the base station

Nodes at different locations in the network send and receive different amounts of data. In multi-hope communications, nodes closer to the base station transmit more data than nodes located further away in the same segment. Figure 4.1 illustrates the amount of data transmitted by nodes with transmission direction from right to left. In the depicted network segment, nodes are equally spaced and transmit equal size messages. The transmitted data grows in size as it moves closer to the base station. This is because more data is collected on the way. Regardless of the payload, nodes closer to the base station are expected to perform more transmissions to overlay the data of other nodes in higher levels of the network.

Balancing energy consumption among nodes in such architecture is a challenging problem. Motivated by the fact that communication is the most power-hungry operation in WSNs, we propose applying transmission power control techniques to achieve significant energy savings in lower network levels. We aim to balance energy consumption across a network segment by dynamically adjusting the transmission power based on the level of the node. Ammari et al. [97] proved that by increasing the distance travelled at each hop, the end-to-end delay decreases at the cost of higher power consumption. For a shorter per-hop transmission distance, less energy is consumed due to lower transmission

power, while end-to-end delay increases linearly in proportion to the number of hops on the path to the sink. Therefore, limiting the transmission distance/power of nodes in lower network levels is expected to reduce their energy expenditure enough to compensate for the high-workload they incur. Similarly, sensor nodes in higher network levels transfer data over longer distance to reduce end-to-end delay.

A node transmission power model needs to consider the hardware design of a node and the requirements of the communication standards. The power of a certain signal of interest is calculated as

$$p = \rho S_0 d^{-\alpha} E$$

where ρ is the fixed transmitter power, S_0 is the channel gain between typical Tx-Rx, d is the distance between source and destination, α is the path-loss exponent $(\alpha > 2)$ and E is some real valued constant.

The proposed variable power link quality control technique is expected to enhance the overall network performance and data delivery. This technique can be used by MAC protocols to detect when a certain link's reliability is below a specific threshold; then, the protocol increases the transmission power to improve the probability of successful data transmissions. Moreover, only nodes that share the same space will contend to access the medium, which decreases the number of collisions in the network. This improves network bandwidth utilisation, reduces the hidden and exposed terminal problems, and reduces end-to-end delays. At the physical layer, using a higher transmission power allows coding and modulation methods with a higher bit/baud ratio. This is particularly beneficial because adjusting the bandwidth based on the current workload increases energy savings.

4.2.2 Configuration Phase

In our proposed system architecture, sensor nodes gather data from the environment and transfer it to their base station through multi-hop communication. The base station aggregates multiple streams of data and transmits it to the end-users directly through a WAN connection.

Network initialisation is started when the base stations advertise their presence to nearby sensor nodes. The advertisement message contains the sender's network level and the cost of the path to reach the base station from the sending node. These two values are initially set to zero. Upon receiving the advertisement message, each sensor node calculates the cost of the link to reach the sender (defined in Subsection 6.2.2.2) and stores it in its local table. Then, they increment the received network level value by 1 and update the received link cost parameter with the calculated one. The modified message is broadcasted to all neighbouring nodes. Each node down the communication tree proceeds in a similar way, i.e. it increments the received level value by 1 and adds the cost of its link to the received cumulative path cost. Using the received level and path cost information, each sensor node determines which network level it belongs to and joins the network segment formed by the base station that can be reached over the most effective path. The cost metric defines the effective path as the shortest, most reliable, and energy efficient path.

The cost metric that estimates the link quality accommodates the effects of communication interference resulting from simultaneous transmissions, because the base station advertisement messages are being transmitted concurrently at multiple paths. Therefore, the path cost metric gives a better approximation of the actual link quality. Using the path cost stored locally at each intermediate sensor node, the path selection algorithm allows nodes to select the path(s) with the lowest delay, least energy consumption, and least interference (link quality). Information about link quality is provided by the

MAC layer of the network. The MAC layer can provide a variety of link quality indicators in terms of bit error rate, interference, etc.

The data routing tree is built based on the quality of the link and the residual energy of all nodes up the tree, which are dynamic over time. The paths offering high energy level but poor link quality or vice versa, are given very low weight. This is because paths with high link quality and low residual energy are likely to create a coverage/communication hole in the network, which leads to network partitioning. Similarly, paths having high residual energy and poor link quality suffer from high bit error rate, which leads to increased retransmissions causing energy waste and high end-to-end delay.

In the following subsections, we provide the initial configuration phase details of the proposed communication protocol. Particularly, we give the details of our segmentation algorithm. Then, we present the link cost metric used to build the communication tree within each network segment.

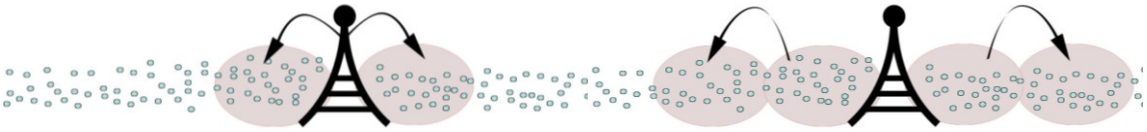
4.2.2.1 Levels Division Graph (LDG)

This section describes the Level Division Graph (LDG) algorithm, which is used to organise nodes into network segments with a sequence of logical levels. Generally, multi-level communication is expected to improve the overall network performance, because system designers can select suitable communication algorithms for each level. During the initial discovery phase, nodes execute the LDG algorithm to determine their network level relative to the base station. The main objectives of the LDG algorithm are:

1. To organise sensor nodes into network segments;
2. To allocate sensor nodes according to a communication cost and reliability into smaller manageable levels; and
3. To establish the shortest/most cost-efficient/most reliable link to the base station.

We assume that each base station is equipped with two directional antennas, left and right. Messages are labelled left or right depending on which transceiver they are transmitted over. The LDG algorithm is initialised by each base station broadcasting beacon messages (called *level_msg*) containing its ID, direction (left or right), and the network level. The network level value in the initial *level_msg* is set to 0, as base stations always have their level assigned to 0.

The initial broadcast transmission power is limited to r_i, where r_i is the maximum radio range of a sensor node. All nodes that receive the initial *level_msg* set their level to L_1 or R_1 depending on the label of that message. Nodes in levels L_1 or R_1 can communicate with the base station directly. Having several direct links with the base station provides fault tolerance and load balancing.



(a) Initial LDG broadcast (b) Next level LDG broadcast

Figure 4.2 Shows the initial level division using LDG

Sensor nodes deploy a backoff mechanism to halt any actions on the received *level_msg*. During the backoff time, sensor nodes wait to receive all potential *level_msg*. At the end of the backoff time, every sensor node chooses the 'best' *level_msg* it received and sets its level to L_{i} or R_{i} depending on the content of that message. The source of the best *level_msg* is recorded as the next hop to the base station. The best message is the one that provides the shortest and most reliable link to the nearest base station (see Section 4.2.2.2). Then, each node increments the level value in the original message it received before it re-broadcasts it to its neighbours. Figure 4.2 shows the process of assigning nodes to levels using the LDG algorithm. The *level_msg* broadcast process continues until the left direction of the base station at one end of the segment meets the right direction

of the base station at the other end of the segment. Nodes located at the level where the two directions meet will choose to join the nearest base station over the most reliable link. A node that chooses between l_i or R_i does not re-broadcast any *level_msg*. Such nodes form the boundaries of the left and right segments. The full LDG algorithm progress in the left direction is described in Algorithm 1. The progress in the right direction is similar to Algorithm 1.

Algorithm 1 LDG Routing for the Left Direction

1. base station broadcasts *level_msg*$(Sender\ ID, L_0)$
2. node receives *level_msg*$(Sender\ ID, L_0)$
3. $level = l_1$
4. $next\ hop = base\ station$
5. broadcast *level_msg*$(Sender\ ID,\ L_1)$
6. node receives *level_msg*$(Sender\ ID,\ L_i)$
7. start backoff time
8. $level = l_{i+1}$
9. $next\ hop = ID$
10. continue listening
11. *level_msg*$(Sender\ ID',\ L_i')$ arrives:
12. **if** $L_i' < L_i$
13. **then** $level = L_{i+1}'$
14. $next\ hop = ID'$
15. **if** $L_i' == L_i$ and $Cost(node, ID') < Cost((node, ID)$
16. **then** $next\ hop = ID'$
17. *level_msg*$(Sender\ ID'',\ R_i)$ arrives:
18. **if** $R_i < L_i$
19. **then** $level = R_{i+1}$
20. $next\ hop = ID''$
21. **if** $R_i == L_i$ and $Cost(node, ID'') < Cost((node, ID)$
22. **then** $next\ hop = ID''$
23. *level_msg*$(Sender\ ID^{\circ},\ R_i')$ arrives:
24. **if** $R_i' < R_i$
25. **then** $level = R_i'$
26. $next\ hop = ID^{\circ}$
27. **if** $R_i' == R_i$ and $Cost(node, ID^{\circ}) < Cost((node, ID'')$
28. $next\ hop = ID^{\circ}$
29. end backoff time
30. broadcast *level_msg*$(Node\ ID, level)$

4.2.2.2 Link Selection in LDG Algorithm

During the configuration phase, sensor nodes receive multiple *level_msg* advertisements. To improve the overall performance of the system in terms of energy consumption and end-to-end delay, sensor nodes use a cost metric to choose the 'best' base station and the 'best' parent to reach that base station. From each node perspective, the proposed cost metric incorporates the following attributes: residual energy level of the potential parent, distance to the potential parent, and the quality of the link connecting the two nodes. The weight of the link used for sending 1 bit from node i in level L_i to node j in adjacent level L_j can be calculated as follows:

$$\omega(i,j) = \frac{d(i,j)}{L_q(i,j)} \times \frac{E_i}{E_j}$$

where $d(i,j)$ is the distance between nodes i and j, L_q is a quality indicator of the link between nodes i and j, and E_i and E_j are the residual energy of nodes i and j, respectively. The $\frac{E_i}{E_j}$ is introduced to increase the communication cost with nodes with low residual energy level.

The link quality approximations depend on the Channel State Information (CSI). Standard methods of CSI measurement include Packet Delivery Ratio (PDR), Received Signal Strength (RSS), and Expected Transmission Count (ETX). PDR and ETX measurements are fully platform independent and RSS is made available by most radios. In the previous decade, the RSS was considered as a poor link quality indicator, mostly because of the limitations of early hardware platforms. Recently, the research community has focused on the 802.15.4 protocol stack, which offers a much more reliable RSS measurement. In this work, we adopt the RSS as the link quality indicator. RSS is widely adopted in the

literature for this purpose. It was proven that the RSS, if higher than about −87dBm, correlates closely with the PDR [98].

The overall weight of the link, including the end-to-end delay, is calculated as

$$\omega_t(i,j) = \omega(i,j)^{\alpha} \times (L_d)^{\beta}$$

where α and β are non-negative integers and L_d is the delay incurred on the link. The link end-to-end delay can be calculated using the method described in Oliver and Fohler [99]. If all received *level_msg* advertisements do not satisfy both requirements of energy efficiency and low end-to-end delay, then the node with maximum energy with CSI value below β threshold will be selected as the next hop or the minimum CSI with energy above α threshold will be selected as the next hop candidate.

In this algorithm, the selection of parent is based on the cumulative path CSI and end-to-end delay. Considering the full path, as opposed to a direct link with the potential parent, ensures that the algorithm equalises as much as is possible the length of a segment and balances the membership of the segments. The cumulative path is the summation of the weights of individual links forming the path from the node to the base station. The cumulative path cost is given as

$$Cost(i,bs) = \sum \omega_t(i,i_p) \cdots \omega_t(j,bs)$$

where i is a sensor node to be associated with a base station bs, i_p is the parent of node i, and j is the vertex of edges connecting the last node in the path to the base station forming the path, P, from i to the bs. The cumulative cost allows nodes to ally themselves with the base station over the shortest and most reliable multi-hop path with the highest residual energy.

4.2.3 Communication Phase

In this phase, sensor nodes send event-driven notifications to their base station. In event-driven applications, such as border monitoring, data transmissions are triggered by detecting an anomaly in the monitored environment. On route to the base station, each message collects information about the residual energy levels of nodes on the path. When energy levels of any sensor node drop below a critical threshold, a local path configuration is started. This update does not cause a ripple effect on the path; only the portion from the low-power node up to the base station is updated. The low-power node sends a *path_update* message asking all neighbouring nodes to advertise their cost value. This message contains the ID of the previous node on the path (n_p). Upon receiving the *path_update*, n_p enters into a maintenance state and starts its backoff timer. All nodes hearing the *path_update* message except n_p respond by sending a *level_update* message, which is the same as the *level_msg*. Only nodes in the maintenance state read the *level_update* messages. At the end of the backoff time, n_p selects a new parent offering the best path. Path updates are not expected to occur frequently because load-balancing is one of the main design factors of the cost metric used to establish routes to the base station.

On the other end, base stations are in an active state at all times and ready to receive data generated by any node on the network. The base station aggregates and analyses the received sensor data before transmission to the end user over a high-speed WAN connection.

To prolong the network life, sensor nodes can go to sleep during the no-activity periods. In the next sub section, we present a duty cycle algorithm that can be integrated with any TDMA schedule.

4.2.3.1 LWSN Duty Cycle

An effective approach to increase the longevity of sensor networks is to implement sleep scheduling, where nodes enter low-power sleep modes during ideal times. In this sub-section, we present the design of an efficient synchronous wakeup-scheduling scheme for LWSNs that adheres to the unidirectional end-to-end delay constraints posed by large-scale border surveillance applications. We consider the lifetime-delay and power-delay trade-offs for our proposed method and show how it can considerably enhance the system performance and increase the network lifetime while satisfying the application latency constraints.

We assume the presence of a network-wide time synchronisation protocol to maintain a consistent notion of time across sensor nodes in the network. Time synchronisation in WSNs is a well-established research area and several solutions can achieve synchronisation within an μsec. Current sensor nodes are equipped with passive sensors, which make event detection possible while a node is in sleep mode. Other hardware platforms offer ultra-low-power, low-rate periodic sampling for occasional event detection. When an event is detected, the sensor node is instantly woken up (within a few μsecs) to send a notification to the base-station.

Each node at level l_{i-1} has $\mathcal{G}$ parents from level l. We denote one period of the wakeup cycle as an interval. We examine $\mathcal{G}$ consecutive intervals and associate each interval with a different level. Sensor nodes in every level apply an identical wakeup pattern in their corresponding interval and sleep in the other $\mathcal{G} - 1$ intervals. For instance, in a basic periodic wakeup pattern where $\mathcal{G} = 2$, every node is assigned two parents p_1 and p_2. If p_1 is awake, p_2 can go to sleep and vice versa. In this setup, the child node views the same pattern as in the always-up single-parent case and enjoys the same chances to send a message. Therefore, the end-to-end delay remains unchanged while sensor nodes wake up $\mathcal{G}$ times less frequently as in the single-parent case. Consequently, the formula for delay distribution is the same as in the single-parent case but the effective wakeup time

is scaled down by a factor of $\mathcal{G}$. During any interval, a sensor node may wake up several times. The effective wake up period is calculated as

$$\mathcal{T} = \lim_{t \to \infty} \frac{\mathrm{t}}{\mathcal{N}_t}$$

were $\mathcal{N}_t$ is the number of wakeups in period t. This means that sensor nodes wake up once every $\mathcal{T}sec$. In the multi-parent case, the effective wake up period is $\frac{\mathcal{T}}{\mathcal{G}}$.

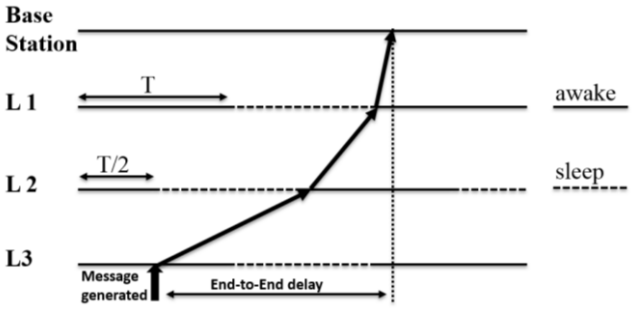


Figure 4.3 Shifted sleep/wake scheme

At the network level layer, the receive-send-sleep cycle is implemented by shifting the wakeup pattern of the nodes in even levels by $\frac{T}{2}$. T is the length of the wakeup period. In this scheduling scheme, the worst-case delay is when a message is generated by a child immediately after the wakeup of the parent of the node (illustrated in Figure 6.3). In this scenario, the first hop needs T seconds and the following $(h-1)$ hops each needs $\frac{T}{2}$ seconds. The worst-case end-to-end delay is

$$\frac{(h\ +\ 1)T}{2}$$

and the distribution of delay is

$$\mathcal{D} = \frac{h}{2}\mathcal{T}$$

This wake up shifting scheme reduces the end-to-end delay by half when compared to fully synchronised schemes, where all sensor nodes in the network wake up at the same time based on a basic periodic pattern with a fixed T. The overall distribution delay in the multi-parent case is

$$\mathcal{D} = \frac{h}{2g}\mathcal{T}$$

To ensure continuous sensing coverage, any two adjacent nodes on a weak or strong barrier cannot go to sleep at the same time. This effectively introduces a new dimension to the sleep/wake cycle, which allows nodes to utilise the sensing coverage dependencies to build a coverage overlap map.

4.3 Summary

This chapter proposed the LDG segmentation algorithm, which groups nodes into network segments with a sequence of logical levels. It is used for quick delivery of data with the objective of minimizing the time duration of delivering data to the sink, that is, minimizing the delay and thus to improve the overall network performance. At the data link layer, an effective sleep/wake scheduling mechanism is introduced to further boost the network performance and prolong its lifetime. Much emphasis was laid on the configuration and communication phase of the new architecture by considering the above mentioned optimizations.

CHAPTER 5

Implementation and Evaluation

Performance and reliability measurements are the final station of this long journey of defining and conquering the different challenges concerning the design of the suggested LWSNs architecture for border surveillance in the thesis. This chapter uses simulation and comparison methods to evaluate the proposed framework and then lists the results, advantages and achievements in this concrete architecture

5.1 Introduction

One of the most important questions addressed in this research concerns whether the exploitation of the linear topology improves the performance of the network. This chapter presents evaluation results from extensive simulation we conducted to evaluate the performance of our proposed framework under diverse conditions of network density. The performance of LDG is compared against the well-known Dynamic Source Routing (DSR) protocol.

The choice of DSR is justified by the following reasons: First, DSR has been recognised as one of the most suitable routing protocols for linear topologies in WSNs [73]. It has been shown that DSR outperforms other routing protocols in border surveillance applications [73]. Second, the design of DSR is similar to our protocol as they are both based on on-demand route discovery and maintenance to achieve data routing. This similarity guarantees better fairness in performance comparison, and makes it more credible. Third, it is widely cited in the literature, and published in a reputable journal [73, 100-103]. Finally, several trusted and well-tested DSR implementations are available on different network simulators. This allows us to reproduce the exact behaviour of the network protocol under our simulation scenarios.

Our performance evaluation experiments have been carried out using NS2 simulator. NS2 is known as one of the most reliable network simulators that have been widely adopted among research community. Simulation results demonstrated the efficiency of our proposed mechanisms to deal with specific features of linear topologies in WSNs.

The chapter is organised as follows. First, a brief description of DSR protocol is provided. Then, Section 7.3 explains in details our simulation environment as well as the methodology that we followed to undertake the performance comparison study. In

Section 7.4, the simulation results are discussed and finally Section 7.5 concludes the chapter and highlights the main findings

5.2 Overview of Dynamic Source Routing (DSR)

DSR is an on-demand routing protocol based on source routing mechanism. This latter allows the packet's originator to initiate a route discovery process in order to select the path to the destination [100]. The node, which originates a data packet (called a source node), selects the routing path based on the number of hops in every discovered route. Thus, the source node chooses amongst the discovered routes the one that contains a lower number of hops. [102]. In this way, forwarding nodes in the selected path do not need to make any routing decision for the routed packet, allowing better bandwidth utilisation by control packets [104].

In case of a wireless link failure between two forwarding nodes, a route_error packet will be generated by the node that is unable to transmit the routed packet. Upon receipt of the route_error packet, the source node will remove this link from its Route Cache and start to discover a new route to the destination. This makes DSR a self-organised and self-configured routing protocol.

Globally, DSR routing protocol is based on the following two functions:

1- Route Discovery is used when the source node *S* aims to find a route to the target destination *D*. This is only done when there is no valid route that has been previously discovered from *S* to *D.*

2- Route Maintenance is employed to maintain and re-establish broken paths. A route between *S* and *D* can be broken for several reasons such as topological changes engendered by nodes' mobility or wireless link unavailability. In this case, the routing protocol will choose a new path from the routing table, or launch a

new routing discovery process [103, 105].

5.3 Evaluation Methodology

Evaluating the performance of any communication protocol in WSNs can be done with one of the following techniques: analytical methods, testbed experimentations, or simulation. However, the inherent characteristics and complexity of WSNs often cause analytical methods to be unsuitable or inaccurate [106]. In fact, WSNs' operations are influenced by many parameters, which are highly dynamic and unpredictable, such as data traffic generation rate, a node's energy consumption, and wireless links' reliability. This makes it impossible to find an analytical model that is able to capture all these parameters for the performance evaluation.

On the other hand, real testbed experiments are intended for small-scale experimentations only, because large-scale implementations are costly and time consuming. For our case, the objective is to evaluate our protocol in LWSNs. Most of the applications using LWSNs (like borders monitoring) require a large-scale deployment. Testing LDG in small-scale testbed would not correctly reflect its performances in real-life applications.

Consequently, we believe that simulation is the most judicious technique of performance evaluation in LWSNs, allowing low cost and rapid evaluation of new algorithms and communication protocols.

5.3.1 Network Simulator NS-2

As we can find a plethora of network simulation tools that have been used in the literature, we established [107, 108] a comprehensive survey that reviews and analyses these tools for the case of WSNs environments.

Among the existing candidates, we adopted NS-2 simulator in order to evaluate our LDG routing protocol. For this purpose, we added several extensions to this simulator, such as LDG implementation and modified line-MAC protocol.

The choice of NS-2 is mainly due to its reputation as the most popular open-source simulator in the networking field research community. In fact, the protocols' implementations provided by this simulator have continuously gained positive reviews, allowing more credible and widely accepted simulation studies.

NS-2 [109] is an object-oriented, discrete-event simulator commonly used by the networking research community. This open source simulator was originally designed for wired IP networks. Afterwards, new and flexible models have been integrated into NS-2 in order to support wireless networks, and particularly energy-constrained ad hoc networks, such as WSNs. However, NS-2 still suffers from a number of limitations. Examples are presented in the following:

1. NS-2 puts some restrictions on the customisation of packet formats, energy models, MAC protocols, and the sensing hardware models, especially for the case of some application-specific WSNs.
2. It lacks realistic models in the application layer that implement complete interactions with lower network layers. This makes some simulations ineffective, especially those focusing on application and middleware protocols.
3. Protocols implementation in NS-2 cannot be directly ported to a real hardware code. Some simulators like TOSSIM [110] offer this advantage, where the same simulation code can be compiled to be run on real sensor motes without any modifications.
4. As for every open-source software, new protocol implementations that are proposed for NS-2 are made by independent developers. These implementations

may contain several inherent known and unknown bugs and need several reviews to be correctly used.

5. Finally, NS-2 coding is based on C++ and oTCL scripts. The lack of high-level simplified programming language makes it difficult to learn and limits the widespread use of this simulator.

5.3.2 Performance Metrics

The main motivation behind the design of LDG routing protocol is to exploit the topological characteristics of LWSNs in order to improve the efficiency of the routing protocol, by eliminating unnecessary overhead message exchange. Reducing the amount of overhead traffic in routing protocols contributes to enhancing the protocol's performance in terms of energy consumption. This latter is very important in LWSNs, where the deployed nodes are equipped with small batteries of limited capacity, which may be irreplaceable in some application scenarios.

However, our objective in this study is to ascertain whether the proposed improvements in LDG influence other efficiency parameters of the routing operations, such as end-to-end reliability. To investigate this issue, our simulation study considers the following performance metrics:

1. **Packet Delivery Ratio (PDR)**:
   This metric defines the reliability of any routing protocol. It is expressed as the ratio between the number of packets successfully delivered to a destination (sink nodes) and the number of packets sent by source nodes [100]. A routing protocol is more reliable as the PDR metric converges to 100%. Routing reliability represents an important metric in some sensitive applications of LWSNs, like border surveillance, where every piece of sensed data needs to be successfully delivered to the sink nodes in order to guarantee the border's security.

$$PDF = \frac{\sum Packets\ deliverd}{\sum Number\ of\ packets\ generated}$$

2. **Total Throughput:**

   It measures the number of packets successfully transmitted to the final destination per unit of time. This metric is calculated by dividing the cumulative size of all received data by the duration of simulation experiments.

$$T = \frac{number\ of\ received\ packets \times packet\ size}{simulation\ time}\ (bit/second)$$

   A good throughput is mainly required by LWSN applications needing to transmit high data traffic to the sink, such as video data. This applies to border surveillance using LWSN with video sensor motes. In this scenario, a routing protocol that causes a degradation of network throughput will prevent the whole network from achieving the intended goal of effective surveillance.

3. **Average End-to-End Delay**:

   This well-known metric reflects the average time spent in routing data packets from the source node to the base station [101]. The measured time value includes delays caused by all routing steps, such as route discovery, packet buffering, and data forwarding between intermediary nodes.

   Let us note by $Delay_i$ the time separating the transmission of a packet i from the source node and its reception at destination. Let P be the total number of packets that are correctly received during the simulation time. The average end-to-end delay is thus given by the following equation:

$$D = \frac{\sum_{i=1..N} Delay_i}{P}\ (s)$$

Delay-sensitive applications of LWSNs require this metric to be as low as possible. For example, a border surveillance sensor network requires a routing protocol with short end-to-end delays, to rapidly report any anomaly noticed in the sensed area, and take necessary measures in time.

4. **Normalised Routing Load (NRL):**

   The normalised routing load characterises the overhead traffic engendered by control packets of the routing protocol. This load is normalised to the number of useful data packets transmitted to the base station, in order to reflect the extra bandwidth consumed by routing overhead only.

   In other words, this metric can be defined as the average number of routing packets transmitted per data packet delivered to the sink node [12].

$$NRL = \frac{\sum Routing\ packets}{\sum Data\ packets}$$

5. **Average Energy Consumption**:

   As emphasised earlier, the efficiency in energy consumption represents one of the most important design objectives of the protocol in LWSNs. This is due to the highly constrained nature of these networks in terms of energy resources. In fact, sensor motes are powered by small batteries with a very limited capacity. These batteries may be irreplaceable in some application scenarios, where the network is deployed in a harsh environment that is inaccessible to humans or robots.

   The average energy consumption is one of the metrics reflecting energy efficiency and one of the most often used in the literature, e.g., [111-113]. It measures the amount of power consumed at each node during network operation. In NS-2, the calculation of energy expenditure at each node takes into account the power consumed for packet transmission and reception (communication), the one consumed during the time where the radio is in sleep mode, and

the energy consumed by the environment sensing operations (sensor boards). Thus, the average energy consumed by each node is calculated as follows:

$$Energy\_Ave = \frac{\sum Energy(I - \mathrm{R})}{n}$$

Where I represents the initial energy capacity of a sensor node, R is the remaining energy of the sensor node at the end of the simulation, and n is the total number of sensor nodes in the network.

6. **Network Lifetime**:

Similar to the previous metric, network lifetime also reflects the protocol's energy efficiency. However, instead of quantifying the amount of energy expenditure, this metric shows if the routing protocol has a good load balancing in terms of energy consumption. Some routing protocols can achieve low energy consumption, but their operations are concentrated on a limited subset of nodes in the network. This is highly undesirable since those overloaded nodes will see their energy resources depleted rapidly, which would cause a network partition that results in the network being out of service. Consequently, an energy efficient routing protocol must guarantee a good balance in energy consumption amongst all the nodes in the network. This is done by achieving a good *network lifetime*.

For our study, we define this metric as the average lifetime of all the nodes in the network. Assuming that the simulated network is composed of n nodes, this metric will be calculated as follows:

$$NL = \frac{\sum_{i=1..n} TE_i - TS}{n}$$

Where TS is the starting time of the network simulation, and TE_i is the time when node i dies and its energy level is equal to zero. If node i remains alive during the entire simulation experiment, TE_i will be set to the simulation end

time.

5.3.3 Simulation Model

To investigate the efficiency of our LDG protocol, we compare its performance to DSR via several simulation runs, and under different network densities. The simulated WSNs contain 200 nodes that are randomly scattered within a fixed area of$2000 \times 100\mathrm{m}$. As shown in Figure 5.1, the rectangular shape of the deployment area has a linear (chain) topology of the simulated network. Each sensor node in the network is represented by its position (green dot), as well as a circle with a time-varying radius that characterizes the traffic load generated by this node. Finally, the base stations are illustrated with red circles in order to be distinguished from ordinary sensor nodes.

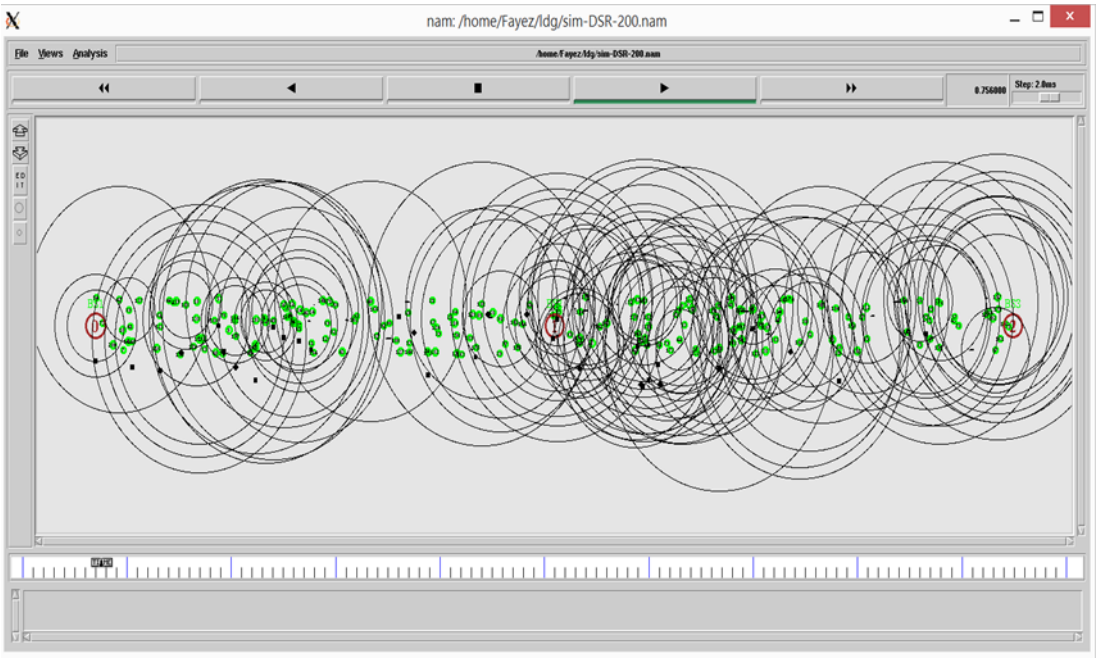


Figure 5.1 Linear WSN running on NS2 simulation

The BSNs are stationary and have a wireless transmission range of $50m$ and sensing range of $25m$, note that communication range higher than sensing range. Each simulated network contains three MTs, also called base stations. Two of them are located on both

extremities of the network chain, and one in the middle. These nodes are assumed more powerful in terms of energy capacity and wireless communication range. Their principal mission is to collect the data generated by sensor nodes, and transmit it to the end-user through satellite communication. During the simulation time of $100s$, a subset of nodes is periodically and randomly chosen to generate the data traffic load and send it to the sink nodes. The sender's traffic load as well as the data packet size are maintained constantly throughout the simulation time, and are equal to $1\ packet/s$ and $32\ bytes$ respectively. $Table\ 5.1$ Summarises the parameter settings used in our simulation experiments.

Table 5.1 Parameter settings of the experiment

Parameter	Value
Number of nodes	200
Simulation area	$2000\ m\ x\ 100\ m$
Wireless radio range (BSN)	$50\ m$
Source nodes data rate	$1\ pkts/s$
Number of base stations	3
Bandwidth	$250\ Kbps$
Data packet size	$32\ Byte$

5.4 Results and discussion

As emphasised earlier, we considered in our simulation an LWSN containing three base stations. Consequently, the resulting topology will be divided into two different segments; each one is located between two base stations. In the following, we present the simulation results of both LDG and DSR with respect to the six metrics previously defined.

5.4.1 Average End-to-End Delay

Figure 5.2 shows the variation of average end-to-end delays for both LDG and DSR protocols, as a function of simulation time t. We notice that LDG induces shorter packet

delivery delays compared to DSR, during the entire simulation time. The performance gap between the two protocols attains its maximum during the first 40 seconds of the simulation experiment. For example, when $t = 5s$, one packet transmission with DSR took $220\ ms$, while it was reduced by 95% and took $5ms$ only in LDG. This is explained by the difference in the route discovery mechanisms of each protocol. During the network initialisation phase, almost every operation of data packet transmission requires a route discovery step, due to the absence of previously discovered paths in nodes' routing tables. In LDG, this step takes into account the chain topology feature of LWSNs by dividing the network into small logical levels. The route discovery process is then executed in a localised manner within each level only, requiring a shorter time compared to DSR. In the latter, route request packets are flooded throughout the entire network, adding extra delays to the route discovery phase, and hence to the whole process of data packet transmission.

After second 40 of the simulation time, the performance gap between LDG and DSR becomes lower, but remains considerable. This is due to the difference in discovered routes quality between LDG and DSR. Adopting multi-level network partitioning in LDG allows sending nodes to discover shorter and more reliable paths to the base stations. Shorter paths induce shorter end-to-end delays due the small number of forwarding nodes in each route. In addition, reliable routes help save the time spent in route recovery phases, which considerably degrade the protocol performance in terms of end-to-end delays.

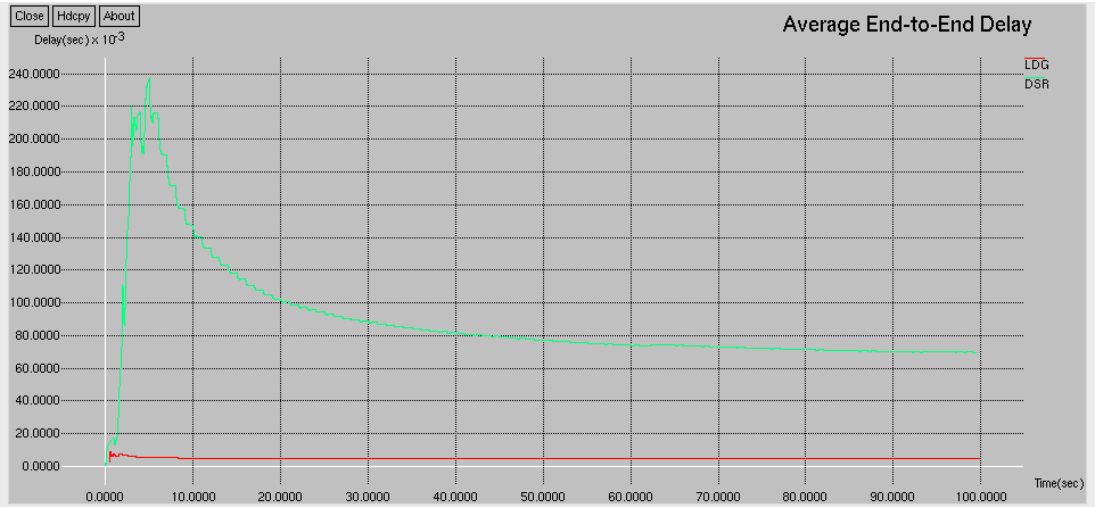


Figure 5.2 Average End-to-End delays

5.4.2 Packet Delivery Ratio (PDR)

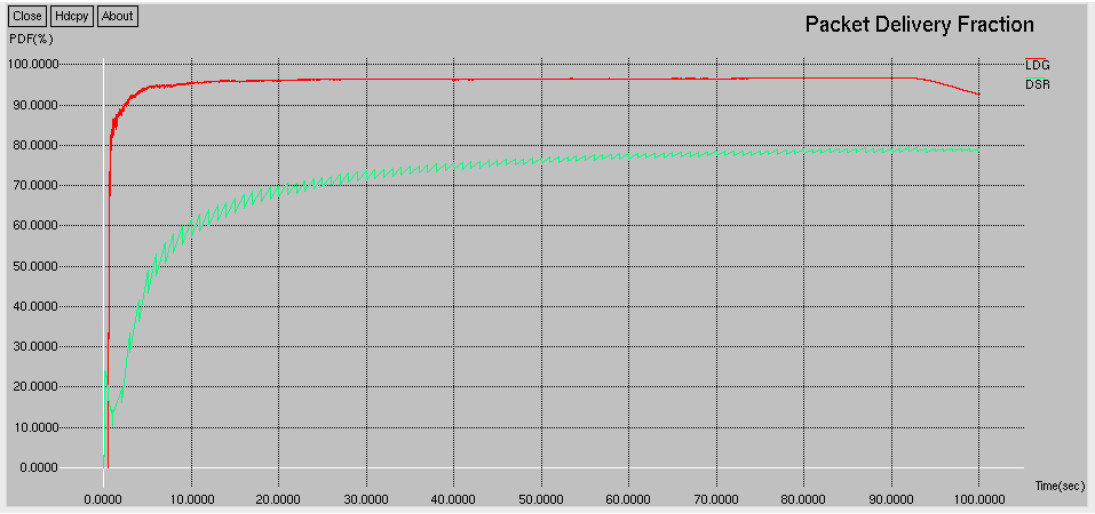


Figure 5.3 Packet Delivery Ratios for LDG and DSR

As illustrated in Figure 5.3, LDG achieves better routing effectiveness when compared to DSR, in terms of packet delivery ratio. The performance enhancement of LDG turns around the average value of 20% all along the simulation period. It can be observed also that our protocol guarantees a higher PDR since the early stage of network initialisation reaches 90% in less than 3 seconds, while DSR spends 21 seconds to reach 70%. The

high packet delivery ratio in LDG is a direct consequence of the reduced routing overhead. In fact, LDG limits the number of control messages necessary for route discovery and maintenance. Moreover, it relies on localised communication between nodes belonging to the same level, in order to establish a route between the data originator and the base station. In contrast, DSR is heavily based on flooding the network with a high number of control messages. This induces increased contention, congestion, and collisions, preventing this protocol from being able to successfully deliver more than 30% of the transmitted data packets.

5.4.3 Network Lifetime

Figure 5.4 Network lifetime results of LDG and DSR

The simulation result in Figure 5.4 highlights the lifetime duration for each sensor node in both scenarios where LDG and DSR are employed. Nodes showing the worst lifetime durations are seen when LDG is used. In fact, the plots demonstrate that the number of nodes with a lifetime under $96s$ is higher in the case of LDG, compared to DSR. This is mainly caused by the multi-level communication adopted in our protocol. Although this technique considerably minimises the routing overhead, it may sometimes cause the overuse of some nodes that are responsible for routing messages between consecutive

levels. This results in fast depletion of their batteries, and shortens their lifetime.

However, for the global network lifetime, LDG slightly outperforms DSR, with a higher number of nodes that remain alive until the end of the simulation. This can be confirmed when comparing the two curves in Figure 5.4, which plot the average node's lifetime for each routing protocol. It is shown that this value is a bit higher in LDG than in DSR. This fact is also clearly illustrated in Figure 5.5, which depicts the network topology at the end of simulation time. We notice that only a few nodes remained alive when running DSR (red nodes with circles), while almost all nodes are still operational with LDG (green nodes with circles).

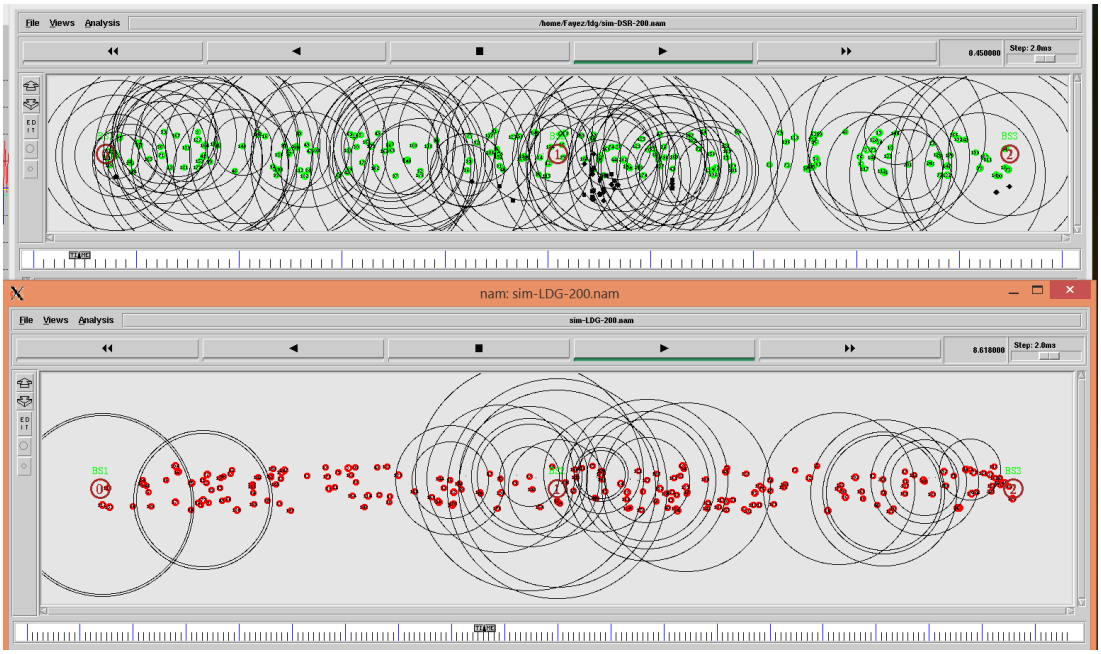


Figure 5.5 LDG and DSR routing protocols running in NS2

5.4.4 Throughput

During the network initialisation phase, LDG and DSR showed opposite behaviours regarding their throughput performance (Figure 5.6). Drastic degradation in throughput occurred with DSR during the first $5\ seconds$ of simulation time, and a minimum value

of $20kb/s$ has been measured. This bad performance is explained by the high number of route request (RREQ)/route reply (RREP) messages generated in DSR during this particular phase, which results in congestion, and enormously reduces the available bandwidth for data packet transmission. Unlike DSR, our protocol showed a better performance during this phase, where the throughput increased with a higher load of data traffic, reaching a maximum value of $100Kb/s$.

When the network attained a steady state, both LDG and DSR showed a stable throughput, with higher values for LDG that outperforms DSR with 60%. This proves the ability of our protocol to carry out routing operations in a transparent and light manner without affecting the rate of successful data packet delivery.

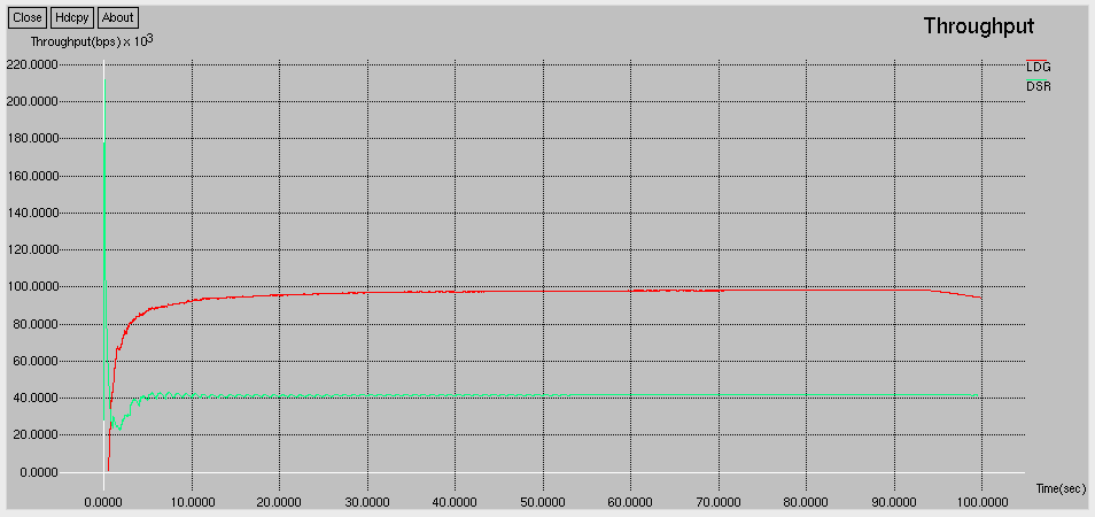


Figure 5.6 Throughput simulation results of LDG and DSR

5.4.5 Normalised Routing Load

Figure 5.7 provides the measurements of normalised routing load for LDG and DSR during the simulation time. Higher values of routing overhead are generated for both protocols at the beginning of the simulation experiments. This is quite logical since any packet transmission during this phase necessitates a route discovery process, due to the

lack of previously discovered routes in the node's routing table. However, we remark that DSR requires more routing traffic load than LDG for this particular phase. In fact, LDG recorded an NRL value inferior to 240, while this metric was superior to 260 for DSR. The reduced routing overhead in LDG is achieved thanks to multi-level network partitioning. In contrast to DSR, all routing packet transmissions are localised in our protocol and no network-wide flooding is required.

Finally, it is worth mentioning that LDG attained the NRL steady state a bit faster than DSR. By the NRL steady state, we mean the ability for a data originator to send data packets using cashed routes with a minimum or null NRL. LDG needed less than $2\ seconds$ to be able to send data packets without the need of routing messages $(NRL\ = 0)$, while DSR needed more than $5\ seconds$.

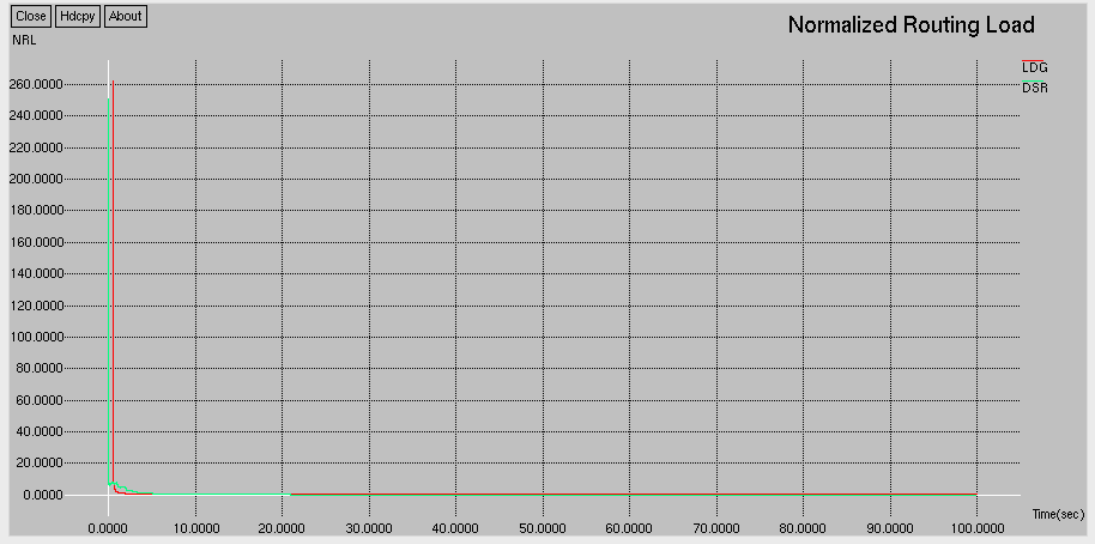


Figure 5.7 Simulation results of Normalised Routing Load for LDG and DSR

5.4.6 Energy Consumption

The plots in Figure 5.8 confirm what was concluded earlier while discussing the average network lifetime metric. Here also, the results reveal a close performance of DSR and LDG in terms of average energy consumption with slight improvement in LDG. Both

protocols consume less energy as the data traffic load decreases during the end of simulation experiments. Furthermore, the maximum value of average energy consumption ($20\ Joules$) recorded by LDG during a high data traffic load can be considered as a good performance for LWSNs.

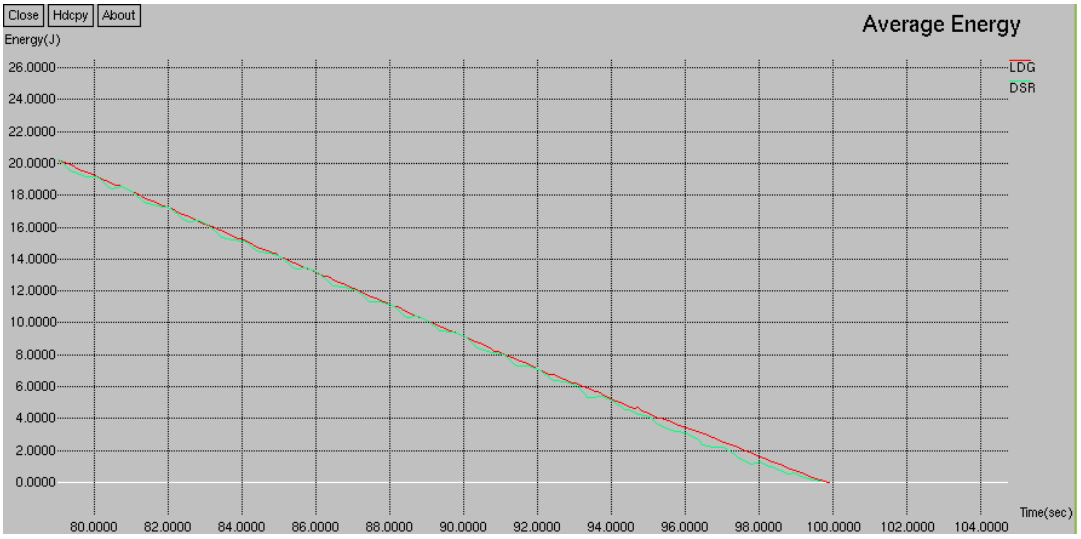


Figure 5.8 Average Energy consumption in LDG and DSR

5.5 Summary

In this chapter, the performance of our protocol has been evaluated by simulation and compared to DSR with respect to six performance metrics. The results of our simulation show an important improvement in our protocol compared to DSR, especially in terms of end-to-end delays, packet delivery ratio, and throughput. This demonstrates the efficiency of LDG routing mechanisms, which take into account the specific topological nature of LWSNs. Throughout this study, it has been revealed that the adopted network organisation into several logical levels, and the localised routing operations in LDG participate considerably in achieving a high routing performance, needed in sensitive applications of LWSNs, like border surveillance.

CHAPTER 6

Conclusion and Future Work

Nowadays, countries face unprecedented challenges in the area of border security as a result of the increased risks of terrorism, illegal movement of drugs, weapons, contraband and people. External border security is critical to a country's security and the challenges it poses are changing and likely to intensify. Securing international borders is a complex task that involves international collaboration, deployment of advanced technological solutions and professional skill-sets. Continuous monitoring of international borders has become a necessity in recent years due to a steady increase in organised crime, terrorist threats, and smuggling activities. The effects of illegal entrance in international border have result to issue of high esteem in nearly all the countries of the world. These issues need not just any solutions but it solutions that are capable of solving the problem with fault tolerance robust systems. It not always feasible to deploy border guards along the borders to combat this challenges due to the hostile topography, severe weather conditions, political and military conflicts.

There have been various means and solution put in place to counter these problems. These solutions vary from design of logical techniques, which include both manual and automated. The manual means of physical checking at border by military zones and unit is inefficient compare to the menace been done by the smugglers and terrorist that

continuously find their ways into many countries via porous and unsecure borders. This results to the design of various surveillance systems with little or no human intervention. The surveillance system ranges from simple to complex and assist border authorities with more effective and reliable decision-making support.

The limitations of the previously existing surveillance system motivates the design of new effective systems. The majority of existing border monitoring can only claim robustness and reliability in limited space, with limited networks of sensors, limited video footage, limited fault tolerance, and for a small variety of landscapes. The limited coverage range with the previously existing system makes it so difficult to counter the day-to-day challenges from different international borders. The existing system also grossly depends on the present of human being to perform so routine functions and adequate supervision before the system performs effectively. They also require huge capital investment resources to setup and maintain. However, full coverage of the monitored area is an important aspect of any surveillance system. The coverage must combine with on-time delivery of information, as late data delivery will result in the failure of the surveillance mission of the system.

The limitation in the existing surveillance system warrant the design of a more robust system that is; reliable, power efficient, appropriately maintained for reducing downtime, well-structured to limits the need for over-constructor resources, worked perfectly in unmanned areas, deployed techniques to achieve good result in large areas and deliver needed data on-time.

This thesis proposed a more sophisticated border surveillance system capable of solving the problem of illegal entrance in borders. The success of this hypothetical hybrid surveillance system is based on the robustness of the architecture. The hybrid system was design by considering the flaws and the power of the previously existing system. Working on those flaws enabled the author to design a more fault tolerance system with

the capability of monitoring borders, railway and pipeline more efficiently using the low-cost WSNs technology to provide real time illegal border crossing. LWSNs help border force to insure high level of remote border security and management at less cost. Border surveillance application includes mixture of node capabilities to cover the long border distance. LWSNs protocol help to overcome the presented challenges by enabling energy efficient system. However LWSNs operate in conditions that are more severe due to the constraints of resources[81]. The framework is tested in real world application and its performance, efficiency and flaws is noted and appropriate corrections are made where necessary.

The existing border surveillance system solve the problem of long range network by clustering however, LWSNs sensors acting as cluster head will run out of power quickly due to the difficulty of rotating the role of the cluster head. The new architecture was designed to enhance power and communication capabilities in LWSNs. This help to build a more robust surveillance system. The new effective and scalable network architecture was explicitly designed for border surveillance application, comprising of the BSNs, and MTs. The BSNs are connected to the MTs in using lower level neighbours, without any clustering involved. This regulates the use of energy among the sensor nodes to ensure a given node does not run out of energy while the others still have energy.

As advised by border experts, the proposed architecture deployment was designed before the border to provide early alert and prevent risk before it happened rather than allowing the risk to come before looking for appropriate deployment as in previous system. The models are design with the ability to expand easily when more MTs and BSNs are added to the network. The length and width of the linear structure is also adaptive to easily incorporate any additions of the BSNs and MTs, to ensure maximizing the network lifetime and balancing the BSNs duties. These are all put together is such a systematic way to determine the routing scheme of the BSNs, and to devise solution for the unbalanced energy consumption.

Most previously existing systems are designed with very expensive technology although yet operate below expectations. WSNs is a low cost technology that can provide an effective solution to the range of problems faced in securing borders effectively. The ability of a WSN to operate without human involvement and in other situations where other surveillance technologies are impractical made it favourite for deployment in hostile hazardous environments. WSNs works efficiently also in rough terrains such as forests or in severe weather conditions, where satellites or air surveillance methods are rendered ineffective.

However, WSNs can be easily integrated with existing systems to provide a common data set at every point of intervention. Data integration from multiple systems is a key feature of modern day border control and surveillance system. Also, the current research in LWSNs addressed problems that arise from a narrow application perspective. Communication been the most power hungry process in WSNs. This new architecture devises a Routing that deals with issues such as data reliability, timeliness, error rate, and network lifetime and system scalability. The main contribution of this thesis is the development of a novel routing protocol to specifically address the communication needs and link reliability for border security and surveillance applications.

In multi-layered systems, the deployment of the top layer nodes requires physical access to the field, time and planning. This prevents rapid deployment of WSN-based system for border security and surveillance applications. To overcome the drawbacks of multi-layered systems, a flat architecture was deployed to detect and report events. This class of systems can be rapidly deployed in conflict areas to respond to emergencies at a low cost and with minimal setup. The new system architecture uses sensor nodes to gather data from the environment and transfer it to their base station through multi-hop communication. The need to make border surveillance systems independent of the

physical presence of human patrolling, as this costs money, time, and management and training resources was incorporated in the proposed architecture and has successfully utilized the five factors that Giompapa et al. [1] considered as a must in terms of border monitoring.

In this thesis, we reviewed the current border surveillance systems and their limitations. We also investigate MAC protocols designed for LWSNs. The focus of the study was on protocols that apply a duty cycle mechanism to reduce energy consumption. It does not solve the long-range communication problem, which is the main concern in these applications. Moreover, none of the existing work has provided a realistic generic framework considering the lack of resources, low node redundancy and time sensitivity of the application. Any new LWSN-specific MAC protocol should take advantage of the features of the linear network topology to meet the application requirements, achieve high-energy savings and timeliness data delivery in low-density networks. Such requirements are essential to all mission critical LWSN applications. We also introduced the existing WSNs deployment architecture and the different types of nodes used in their implementation, namely: BSNs, DRNs, and DDNs.

The thesis further focuses on the design of a new, effective, and scalable network architecture explicitly designed for border surveillance. It consists of surveillance tower, which have a direct connection to the base station and BSNs. Moreover, the architecture allows the accommodation of additional BSNs and surveillance tower when necessary making the model easily expandable. Additionally, it defines the node density required to have sufficient barrier insuring full coverage at low cost possible. Also, it is explained what k-barrier coverage is and how it can be implemented giving a calculating of the minimum number of sensor nodes required to achieve k-barrier coverage in a given belt region and for determining if a region is indeed k-barrier covered. It also describes which factors can influence the level of barrier coverage. In addition, we gave a definition for the crossing path term and a method for discovering any coverage gaps in a belt of

sensor nodes. The results can be used to estimate the required network density to provide complete border coverage.

This was followed by the proposed the LDG segmentation algorithm, which groups nodes into network segments with a sequence of logical levels. It is used for quick delivery of data with the objective of minimizing the time duration of delivering data to the sink, that is, minimizing the delay and thus to improve the overall network performance. At the data link layer, an effective sleep/wake scheduling mechanism is introduced to further boost the network performance and prolong its lifetime. Much emphasis was laid on the configuration and communication phase of the new architecture by considering the above mentioned optimizations.

In conclusion, the LDG algorithm and MAC optimisations will significantly prolong the LWSN lifetime, boost its performance and make it energy-efficient. Moreover, as it was made clear throughout the thesis, these improvements are applicable in other scenarios such as pipelines, railway, motorway etc.

The thesis opens new avenues for future research including the following:

First, there is a need to evaluate the work proposed under real world condition. The work described in the thesis is currently being implemented on real hardware platform and is to be tested in real world environment. The field deployment of the proposed protocols will allow us to verify the results obtained through simulation and capture any factors missed during the design stage. For this implementation, the ESP8266 modules are being used to build a sensor node suitable for border monitoring applications. Using the NodeMCU software to program our protocols in Lua is considered to be the simplest approach. We are currently building 50 nodes with a variety of sensors. Each sensor node will cost less than £3, which makes it an ideal candidate hardware platform for real life deployment of such systems. The basic evaluation scenario is to use on board accelerometers to detect ground vibrations. The intruder detection would consist of

detecting the same vibration between two nodes, and concluding that someone had passed the ‘boundary’ between those.

Additionally, it is important to apply the proposed framework to other LWSN applications, such as gas/petrol pipelines and railway tracks, to examine its performance under different application conditions and prove that the proposed framework can serve other LWSN applications.

Furthermore, studying the effect of people movement models on the overall detection rate is an important problem. Intruder behaviours can vary, which may affect the detection rate.

Finally, integrating the WSN system with other information sources, e.g., satellite data, is a complex data fusion problem that may significantly improve the overall monitoring system performance. For instance, the WSN data may be used to direct surveillance camera to a location of potential interest.

References

1. Giompapa, S., et al., *Computer Simulation of an Integrated Multi-Sensor System for Maritime Border Control*, in *Radar Conference, 2007 IEEE*. 2007. p. 308 -313.

2. Yen, L.-H., C.W. Yu, and Y.-M. Cheng, *Expected k-coverage in wireless sensor networks.* Ad Hoc Networks, 2006. **4**(5): p. 636-650.

3. Huang, C.-F. and Y.-C. Tseng, *The coverage problem in a wireless sensor network*, in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. 2003, ACM: San Diego, CA, USA. p. 115-121.

4. *Eastren European Borders Annual Risk Analysis 2013*. Frontex [Risk Analysis] 2013 (Accessed 20/08/2015)]; Available from: http://frontex.europa.eu/assets/Publications/Risk_Analysis/EB_ARA_2013.pdf.

5. *Eastren European Borders Annual Risk Analysis 2015*. Frontex [Risk Analysis] 2015 05/2015 [cited (Accessed 18/05/2015); Available from: http://frontex.europa.eu/assets/Publications/Risk_Analysis/EB_ARA_2015.pdf.

6. *FRONTEX: The Eastren European External Borders Agency*. Frontex [Report with Evidence] 2008 03/2008 (Accessed 23/06/2015)]; Available from: http://www.publications.parliament.uk/pa/ld200708/ldselect/ldeucom/60/60.pdf.

7. Remagnino, P., et al., *Novel concepts and challenges for the next generation of video surveillance systems.* Machine Vision and Applications, 2007. **18**(3): p. 135-137.

8. Buratti, C., et al., *An Overview on Wireless Sensor Networks Technology and Evolution.* Sensors, 2009. **9**(9): p. 6869--6896.

9. Jawhar, I., N. Mohamed, and D.P. Agrawal, *Linear wireless sensor networks: Classification and applications.* J. Netw. Comput. Appl., 2011. **34**: p. 1671--1682.

10. Zimmerling, M., W. Dargie, and J.M. Reason, *Localized power-aware routing in linear wireless sensor networks*, in *Proceedings of the 2nd ACM international conference on Context-awareness for self-managing systems*. 2008, ACM: New York, NY, USA. p. 24--33.

11. Li, H. and X. Shunjie, *Energy-Efficient Node Placement in Linear Wireless Sensor Networks*, in *Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on*. 2010. p. 104 -107.

12. Jawhar, I., et al., *Monitoring Linear Infrastructures Using Wireless Sensor Networks **, in *Wireless Sensor and Actor Networks II*, A. Miri, Editor. 2008, Springer Boston. p. 185-196.

13. Jawhar, I. and J. Wu, *Qos support in TDMA-based mobile ad hoc networks.* The Journal of Computer Science and Technology (JCST), Springer, 2005. **20**: p. 797--810.

14. Hwang, Y. and P. Varshney, *An adaptive QoS routing protocol with dispersity for ad-hoc networks*, in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*. 2003. p. 10 pp.

15. Gerasimov, I. and R. Simon, *Performance analysis for ad hoc QoS routing protocols*, in *Mobility and Wireless Access Workshop, 2002. MobiWac 2002. International*. 2002. p. 87 - 94.

16. Stoianov, I., et al., *PIPENET: A Wireless Sensor Network for Pipeline Monitoring*, in *Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on*. 2007. p. 264 -273.

17. Nan, W., et al., *Research on Linear Wireless Sensor Networks Used for Online Monitoring of Rolling Bearing in Freight Train.* Journal of Physics: Conference Series, 2011. **305**(1): p. 012024.

18. Mohamed, N., J. Al-Jaroodi, and I. Jawhar, *A Cost-Effective Design for Combining Sensing Robots and Fixed Sensors for Fault-Tolerant Linear Wireless Sensor Networks.* International Journal of Distributed Sensor Networks, 2014. **2014**: p. 11.

19. Martin, K. and M.B. Paterson, *Ultra-lightweight key predistribution in wireless sensor networks for monitoring linear infrastructure*, in *Information Security Theory and Practice: Smart Devices, Pervasive Systems and Ubiquitous Networks (WISTP 2009)*. 2009. p. 143-152.

20. *The world's longest oil and gas pipelines*. 2012 (Accessed 16/05/2015); 18/10/2012:[Available from: http://www.hydrocarbons-technology.com/features/featureworlds-longest-oil-gas-pipelines-imports.

21. Carrillo, A., et al., *New distributed optical sensor for detection and localization of liquid leaks: Part I. Experimental studies.* Sensors and Actuators A: Physical, 2002. **99**(3): p. 229 - 235.

22. EPA. *Drinking Water Infrastructure Needs Survey and Assessment: Fourth Report to Congress* 2009 March [cited (Accessed 10/6/2014); Available from: http://water.epa.gov/infrastructure/drinkingwater/dwns/index.cfm.

23. Hartong, M., R. Goel, and D. Wijesekera, *Positive Train Control (PTC) failure modes.* Journal of King Saud University - Science, 2011. **23**(3): p. 311-321.

24. Aboelela, E., et al., *Wireless sensor network based model for secure railway operations*, in *Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International*. 2006. p. 6 pp.-628.

25. Lee, W., et al., *Railroad bridge instrumentation with fiber-optic sensors.* Applied Optics, 1999. **38**(7): p. 1110-1114.

26. Shafiullah, G.M., S.A. Azad, and A.B.M.S. Ali, *Energy-Efficient Wireless MAC Protocols for Railway Monitoring Applications.* Intelligent Transportation Systems, IEEE Transactions on, 2013. **14**(2): p. 649-659.

27. Akyildiz, I.F. and E.P. Stuntebeck, *Wireless underground sensor networks: Research challenges.* Ad Hoc Networks, 2006. **4**(6): p. 669-686.

28. Ameen, M.A., S.M.R. Islam, and K.S. Kwak, *Energy Saving Mechanisms for MAC Protocols in Wireless Sensor Networks.* IJDSN, 2010.

29. Ye, W., J. Heidemann, and D. Estrin, *An energy-efficient MAC protocol for wireless sensor networks*, in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2002. p. 1567-1576 vol.3.

30. *CENTRAL MEDITERRANEAN ROUTE*. Frontex 2015 [cited (Accessed 6/7/2015); Available from: http://frontex.europa.eu/trends-and-routes/central-mediterranean-route/.

31. *Mapping Mediterranean migration*. BBC News 2014 [cited (Accessed 5/02/2015); Available from: http://www.bbc.co.uk/news/world-europe-24521614.

32. Busch, C., et al. *Towards Unattended and Privacy Protected Border Control*. in *Biometrics Symposium, 2007*. 2007.

33. Dong, Y., et al., *Energy aware routing algorithm for WSN applications in border surveillance*, in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. 2010. p. 530 -535.

34. Fischer-Lescano, A., T. Löhr, and T. Tohidipur, *Border controls at sea: Requirements under international human rights and refugee law.* International journal of refugee law, 2009: p. eep008.

35. Coppin, P., et al., *Review ArticleDigital change detection methods in ecosystem monitoring: a review.* International journal of remote sensing, 2004. **25**(9): p. 1565-1596.

36. Gromek, A.a.J., M. *SAR imagery change detection method for Land Border Monitoring*. in *{Analysis of Multi-temporal Remote Sensing Images (Multi-Temp), 2011 6th International Workshop on the*. 2011. IEEE.

37. Hayes, B. and M. Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the" Smart Borders" Proposals: a Study by the Heinrich Böll Foundation*. 2012: Heinrich-Böll-Stiftung.

38. *Border Surveillance | GMES DOLPHIN*. n.d. (Accessed 11/03/2015)]; Available from: http://www.gmes-dolphin.eu/node/20

39. Margarit, G., *Operational activations of maritime surveillance services within the framework of MARISS, NEREIDS and SAGRES projects.*

40. *EVPU Defence - Monitoring and Surveillance Systems - Army Technology*. n.d. (Accessed 25 May 2015)]; Available from: http://www.army-technology.com/contractors/surveillance/evpu-defence/.

41. *DAS enabled Security Allocation*. 2014 [cited (Accessed 05/06/2015); Available from: http://www.fotechsolutions.com/index.php/products/security.

42. Marsh, L.D.J. and O.C.H.T.T. Force, *Issues Impacting Human Trafficking Collaborations: A Local Law Enforcement Perspective.* Orange County Human Trafficking Task Force. Westminster Police Department, 2007.

43. *Border Security System and Equipment, Perimeter Access Control and Surveillance*. n.d. (Accessed 10/06/2015)]; Available from: http://www.wi-ltd.com/Solutions_by_Sector/Border_Security.

44. Sun, Z., et al., *BorderSense: Border patrol through advanced wireless sensor networks.* Ad Hoc Networks, 2011. **9**(3): p. 468-477.

45. *BORDER SURVEILLANCE SOLUTION*. n.d. 15 May 2015]; Available from: http://www.defenceandsecurity-airbusds.com/pl_PL/1283.

46. AŞAN, E., *AGILE AND COLLABORATIVE SYSTEMS ENGINEERING*. 2014, MIDDLE EAST TECHNICAL UNIVERSITY.

47. *FLIR Border Surveillance Products | FLIR Systems*. n.d. 20 May 2015]; Available from: http://www.flir.com/surveillance/display/?id=64968

48. Blazakie, J. *Border security and unmanned aerial vehicles*. 2004. DTIC Document.

49. Kähloer, M., *The european train control system in thales signalling solutions.* Mechanics Transport Communications, 2008. **3**: p. 2008.

50. *Border surveillance system* n.d. 20 May 2015]; Available from: https://www.thalesgroup.com/en/worldwide/defence/border-surveillance-system.

51. OptaSense. *Border Monitoring | Border Protection | Military Road Transport*. 2014 15 May 2015]; Available from: http://www.optasense.com/our-solutions/borders-military/protecting-borders.

52. Owen, A., G. Duckworth, and J. Worsley. *OptaSense: fibre optic distributed acoustic sensing for border monitoring*. in *Intelligence and Security Informatics Conference (EISIC), 2012 European*. 2012. IEEE.

53. Customs, U., *Secure Borders, Safe Travel, Legal Trade: US Customs and Border Protection Fiscal Year 2009-2014 Strategic Plan*. 2009, Washington, DC: CBP. www. cbp. gov/linkhandler/cgov/about/mission/strategic_plan_09_14. ctt/strategic_plan_09_14. pdf.

54. *Integrated Surveillance Intelligence System (ISIS)*. n.d. [cited 2015 18 May]; Available from: http://www.globalsecurity.org/security/systems/isis.htm.

55. *Border Surveillance systems*. n.d. [cited 2015 26 May]; Available from: http://www.radiobarrier.com/border-surveillance-1/

56. Evans, M., *Fuel thieves steal 30,000 litres of diesel from major pipeline*, in *The Telegraph*. 2014, Telegraph Media Group Limited 2015.

57. Vidal, J., *£1bn a month: the spiralling cost of oil theft in Nigeria*, in *The Guardian*. 2013, Guardian News and Media Limited.

58. Felemban, E., L. Chang-Gun, and E. Ekici, *MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks.* Mobile Computing, IEEE Transactions on, 2006. **5**(6): p. 738-754.

59. Pratap, P., J.M. Kallberg, and L.A. Thomas, *Challenges of remote border monitoring*, in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. 2010. p. 303 -307.

60. Watteyne, T., et al., *Dual-mode real-time MAC protocol for wireless sensor networks: a validation/simulation approach*, in *Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*. 2006, ACM: Nice, France. p. 2.

61. Karveli, T., et al. *DiS-MAC: A MAC protocol for sensor networks used for roadside and highway monitoring*. in *Ultra Modern Telecommunications & Workshops, 2009. ICUMT'09. International Conference on*. 2009. IEEE.

62. Fang, C., H. Liu, and L. Qian. *LC-MAC: An Efficient MAC Protocol for the Long-Chain Wireless Sensor Networks*. in *Communications and Mobile Computing (CMC), 2011 Third International Conference on*. 2011. IEEE.

63. Ye, W., J. Heidemann, and D. Estrin, *Medium access control with coordinated adaptive sleeping for wireless sensor networks.* IEEE/ACM Trans. Netw., 2004. **12**(3): p. 493-506.

64. Lee, E., J.W. Jwa, and H. Kim, *MFT-MAC: A Duty-Cycle MAC Protocol Using Multiframe Transmission for Wireless Sensor Networks.* International Journal of Distributed Sensor Networks, 2013. **2013**: p. 6.

65. Li, F., et al., *An adaptive coordinated MAC protocol based on dynamic power management for wireless sensor networks*, in *Proceedings of the 2006 international conference on Wireless communications and mobile computing*. 2006, ACM: Vancouver, British Columbia, Canada. p. 1073-1078.

66. Doerel, T., *Simulation of wireless ad-hoc sensor networks with QualNet.* Technische Universitat Chemnitz, 2009.

67. Serna Oliver, R. and G. Fohler, *Probabilistic Routing for Wireless Sensor Networks*, in *Proceedings of Work-in-Progress Session, 29th IEEE Real-Time Systems Symposium 2008*. 2008.

68. De Caneva, D. and P.L. Montessoro, *A synchronous and deterministic MAC protocol for wireless communications on linear topologies.* Int'l J. of Communications, Network and System Sciences, 2010. **3**(12): p. 925.

69. Felemban, E., *Advanced border intrusion detection and surveillance using wireless sensor network technology.* 2013.

70. Hanjiang, L., et al., *Ship Detection with Wireless Sensor Networks.* Parallel and Distributed Systems, IEEE Transactions on, 2012. **23**(7): p. 1336-1343.

71. Yang, T., et al., *Energy-efficient border intrusion detection using wireless sensors network.* EURASIP Journal on Wireless Communications and Networking, 2014. **2014**(1): p. 1-12.

72. Yan, J., et al., *EECCR: An Energy-Efficient m -Coverage and n -Connectivity Routing Algorithm Under Border Effects in Heterogeneous Sensor Networks.* Vehicular Technology, IEEE Transactions on, 2009. **58**(3): p. 1429-1442.

73. Sharei-Amarghan, H., A. Keshavarz-Haddad, and G. Garraux, *Routing Protocols for Border Surveillance Using ZigBee-Based Wireless Sensor Networks*, in *Computer Networks*, A. Kwiecień, P. Gaj, and P. Stera, Editors. 2013, Springer Berlin Heidelberg. p. 114-123.

74. Rothenpieler, P., et al., *Flegsens-secure area monitoring using wireless sensor networks.* Proceedings of the 4th Safety and Security Systems in Europe, 2009.

75. Dudek, D., et al. *A wireless sensor network for border surveillance*. in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*. 2009. ACM.

76. Mishra, A., K. Sudan, and H. Soliman. *Detecting border intrusion using wireless sensor network and artificial neural network*. in *Distributed Computing in Sensor Systems Workshops (DCOSSW), 2010 6th IEEE International Conference on*. 2010. IEEE.

77. Wang, Z., X. Zhao, and X. Qian, *The application and issuse of linear wireless sensor networks*, in *System Science, Engineering Design and Manufacturing Informatization (ICSEM), 2011 International Conference on*. 2011. p. 9 -12.

78. Jawhar, I., et al., *An Efficient Framework and Networking Protocol for Linear Wireless Sensor Networks.* Ad Hoc & Sensor Wireless Networks, 2009. **7**(1-2): p. 3-21.

79. Jawhar, I., N. Mohamed, and K. Shuaib. *A framework for pipeline infrastructure monitoring using wireless sensor networks*. in *Wireless Telecommunications Symposium, 2007. WTS 2007*. 2007.

80. Banerjee, T., K.R. Chowdhury, and D.P. Agrawal, *Using polynomial regression for data*

representation in wireless sensor networks: Research Articles. Int. J. Commun. Syst., 2007. **20**(7): p. 829-856.

81. Dan, L., et al., *Detection, classification, and tracking of targets.* Signal Processing Magazine, IEEE, 2002. **19**(2): p. 17-29.

82. Warneke, B., et al., *Smart Dust: communicating with a cubic-millimeter computer.* Computer, 2001. **34**(1): p. 44-51.

83. Gupta, G. and M. Younis. *Load-balanced clustering of wireless sensor networks*. in *Communications, 2003. ICC '03. IEEE International Conference on*. 2003.

84. Raghuwanshi, S. and A. Mishra. *A self-adaptive clustering based algorithm for increased energy-efficiency and scalability in wireless sensor networks*. in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*. 2003.

85. Chen, C.W. and Y. Wang, *Chain-Type Wireless Sensor Network for Monitoring Long Range Infrastructures: Architecture and Protocols.* International Journal of Distributed Sensor Networks, 2008. **4**(4): p. 287-314.

86. Xiaobing, W., C. Guihai, and S.K. Das, *Avoiding Energy Holes in Wireless Sensor Networks with Nonuniform Node Distribution.* Parallel and Distributed Systems, IEEE Transactions on, 2008. **19**(5): p. 710-720.

87. Lindsey, S., C. Raghavendra, and S. Krishna. *Data gathering in sensor networks using the energy*delay metric*. in *Parallel and Distributed Processing Symposium., Proceedings 15th International*. 2001.

88. Bandyopadhyay, S. and E.J. Coyle. *An energy efficient hierarchical clustering algorithm for wireless sensor networks*. in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. 2003.

89. Saipulla, A., L. Benyuan, and W. Jie. *Barrier coverage with airdropped wireless sensors*. in *Military Communications Conference, 2008. MILCOM 2008. IEEE*. 2008.

90. Limited, P.N., *Border Monitoring System*, B.M. Tower, Editor. 2014, Prodeals Nigeria Limited: Prodeals Nigeria.com.

91. *French VBL to Equip Russian Border Guards?*, vbl_vasp1.jpg, Editor. 2011, Defence Update: Defense-Update.com.

92. Group, C.C., *Military Manpack Antennas*, M.M. Antennas-s.jpg, Editor. 2010, Military Systems and Technology: Military Systems and Technology.

93. Kumar, S., T.H. Lai, and A. Arora, *Barrier coverage with wireless sensors*, in *Proceedings of the 11th annual international conference on Mobile computing and networking*. 2005, ACM: Cologne, Germany. p. 284-298.

94. Liu, B., et al., *Strong barrier coverage of wireless sensor networks*, in *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*. 2008, ACM: Hong Kong, Hong Kong, China. p. 411-420.

95. Hou, Y.-T., et al. *Optimal coverage deployment for wireless sensor networks*. in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*. 2006. IEEE.

96. Meguerdichian, S., et al. *Coverage problems in wireless ad-hoc sensor networks*. in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2001.

97. Wattenhofer, R., et al., *Distributed topology control for power efficient operation in multihop wireless ad hoc networks*, in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2001. p. 1388-1397 vol.3.

98. Srinivasan, K. and P. Levis, *RSSI is Under Appreciated*, in *Embedded Networked Sensors*.

99. Oliver, R.S. and G. Fohler. *Probabilistic estimation of end-to-end path latency in Wireless Sensor Networks*. in *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*. 2009.

100. Rahman, J., M.A.M. Hasan, and M.K.B. Islam. *Comparative analysis the performance of AODV, DSDV and DSR routing protocols in wireless sensor network*. in *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*. 2012.

101. Ihbeel, A.A.S., H.I. Sigiuk, and A.A. Alhnsh. *Simulation based evaluation of MANET routing protocols for static WSN*. in *Innovative Computing Technology (INTECH), 2012 Second International Conference on*. 2012.

102. Rakesh, P., S. Amit Kumar, and S. Dr. Dharm, *DSR Routing Protocol in Wireless Ad-hoc Networks: Drop Analysis.* International Journal of Computer Applications, 2011. **14**: p. 18-21.

103. Ali, S. and A. Ali. *Performance analysis of AODV, DSR and OLSR in MANET*. in *Proceedings on Seventh International Conference on Wireless Systems*. 2009.

104. Razouqi, Q., et al. *Combined traffic simulation scenarios performance investigation routing protocols AODV, DSR and DSDV in MANET*. in *Computer Engineering Conference (ICENCO), 2012 8th International*. 2012.

105. Holter, K., *Kenneth Holter.* 2005.

106. G. Chen, et al., *Sense: A sensor network simulator*, in *Advances in Pervasive Computing & Networking*. 2004. p. 249-267.

107. Abuarqoub, A., et al. *Simulation issues in wireless sensor networks: A survey*. in *The Sixth International Conference on Sensor Technologies and Applications (SENSORCOMM 2012)*. 2012.

108. Al-Fayez, F., et al., *Wireless Sensor Network Simulation: The Current State and Simulation Tools.* Sensors & Transducers, 2013. **18**(1): p. 145.

109. McCanne, S., et al., *Network simulator ns-2*. 1997.

110. Nath, R. *A TOSSIM based implementation and analysis of collection tree protocol in wireless sensor networks*. in *Communications and Signal Processing (ICCSP), 2013 International Conference on*. 2013.

111. Pottie, G.J. and W.J. Kaiser, *Wireless integrated network sensors.* Communications of the ACM, 2000. **43**(5): p. 51-58.

112. Barati, M., et al. *Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET*. in *Computer & Information Science (ICCIS), 2012 International Conference on*. 2012.

113. Guo, Z., et al. *Energy Aware Proactive MANET Routing with Prediction on Energy Consumption*. in *Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on*. 2007.