Solutions for the implementation of a sensors network for border surveillance.

Mohamed Lamine Laouira

$N°$ d'Ordre: 01/2022 – D/INF

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie HOUARI-BOUMEDIENE

Faculté d'Informatique

THÈSE DE
DOCTORAT EN SCIENCES

Présentée pour l'obtention du grade de Docteur

En: INFORMATIQUE

Spécialité: INFORMATIQUE

Par: Mohamed Lamine LAOUIRA

S U J E T

Solutions pour la mise en œuvre d'un réseau de capteurs pour la surveillance de frontières.

Soutenue publiquement, le **02/03/2022** , devant le jury composé de:

M. N. BADACHE, Professeur à l'USTHB	**Président**
M. A. **ABDELLI**, Professeur à l'USTHB	**Directeur de thèse**
M. J. **BENOTHMAN**, Professeur à Supélec Paris-France	**Co-directeur de thèse**
M. H. **BENKAOUHA**, MCA à l'USTHB	**Examinateur**
Mme. L. **MOKDAD**, Professeur à l'UPEC Paris-France	**Examinatrice**
M. B. **DJAMAA**, MCA à l'EMP/Alger	**Examinateur**

D E D I C A T I O N S

I dedicated this modest work to :

- The memory of my dear father OMAR allah yarhmou, who died on that terrible night of Thursday January 28, 2021 in skikda city and buried when i was in stay in Paris-France,
I can never express my great sorrow in your absence my father,
I would have liked you to be by my side today,
But what can we do, in front of God's judgment and destiny ?
May this work be a prayer for the rest of your soul and make you happy and proud,
One more time, ALLAH YARAHMEK my dear father, I'll never forget you.

*- **My very dear mother NOUARA**, God protect and extend her life*
who have not stopped encouraging me and praying for me,
- My brother ABDOU,
- My sisters :AMEL, SABRINA, MOUNIA, DALLAL, IMEN,
- My wife,
- My son MEHDI,
- My three daughters AMINA, HIBET EL RAHMANE and ZAHRA,
- My very dear friend MOUNIR, considered as brother.

A C K N O W L E D G M E N T S

At the end of this work, it is with emotion that I would like to thank all those who, directly or indirectly, have contributed to the realization of this project.

Firstly, I would like to express my sincere gratitude to my advisor and thesis director Mr. ***Abdelkrim ABDELLI****, Professor at USTHB for the continuous support during all the time, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. In one sentence, it was a real pleasure to work under his supervision. I would also like to express my sincere thanks to my thesis co-supervisor, Mr.* ***Jalel BEN-OTHMAN****, Professor at CentraleSupélec Paris-France for his invaluable comments, ideas, encouragement, and guidance have provided a good basis for the present thesis.*

A special thanks to Ms. ***Lynda MOKDAD****, Professor at UPEC, Paris-France and the entire administration of UPEC for having accepted to welcome me at the Laboratory of Algorithms, Complexity and Logic during my entire scientific stay in Paris-France.*

I would like to thank the members of the jury for agreeing to evaluate this work and who kindly invested their precious time to read my thesis. Their comments allowed me to improve and finalize the thesis manuscript.

Finally, I thank my parents, all my family and my friends, for having supported and encouraged me during all my studies and especially during this long and very difficult period.

M.L. LAOUIRA.

A B S T R A C T

Today, new security challenges, such as terrorism, transnational crimes, drug and arms trafficking, necessarily require a new strategies to address cross-border security. For a long time, conventional techniques such as human patrols, installation of barriers, construction of insulation walls and trenching, were used for securing borders over the world. However, those conventional techniques suffer from some issues such as intensive human involvement and high deployment cost, especially when the border line is very large. To overcome these issues, the use of technology for border surveillance was pushed fastly. Hence, technologies such as Wireless Sensor Networks, radars, camera sensors and Unmanned Aerial Vehicle (UAV) were introduced to enhance the border surveillance process. However, the use of any single of those technologies separately may lead to concerns such as a high rate of false alarms and line of sight limitations. Even though combining those technologies to obtain a hybrid architectures is highly recommended in the literature, still some key challenges like energy saving and load balancing need further improvement. The research work carried out in this thesis contributes to a large project which aims to define an operational framework for securing the Algerian land borders. To do that, a multilayer framework to detect and track any border intrusion with minimum human involvements was proposed based on the combination of several technologies such as multimedia sensors, radars, UAVs,...

As a part of this thesis contributions, a detailed deployment scheme for each layer of the proposed architecture was also addressed. For energy saving, load balancing and redundancy elimination, an activation scheduling strategy was proposed also. In this thesis we studied also the effectiveness of adapting some technical parameters on the network lifetime. Finally, for energy supply in border surveillance architecture based on the combination of radars with mobile camera sensors that are embedded in UAVs, we proposed a Wireless Power Transfer (WPT) system based on rectennas to supply wirelessly UAVs batteries with power during their flight. To manage the access of UAVs to the WPT system, we implement an active UAVs scheduling strategy based on an improved Weighted Round-Robin (WRR) algorithm. All our contributions in this thesis were evaluated through a deep process of several simulations.

Keywords : *Wireless Sensor networks (WSN), Energy consumption, Network lifetime, Border surveillance, Camera sensors relevance, Scheduling strategy, Radars, Unmanned Areal Vehicles, network architecture, nodes deployment.*

Table of contents

List of figures

List of Tables

List of Acronyms

General Introduction

Topic of Focus

Given the current geostrategic changes and the proliferation of cross-border crimes, such as terrorism, drug and arms trafficking and illegal immigration, securing physical borders becomes a critical demand that all the governments over the world consider as a primary concern. Furthermore, the integrity of physical borders has become a critical issue, especially when geopolitical changes combined with economic turmoil are redrawing the world map.

It is noteworthy that there exists no one-size-fits-all solution for an effective border surveillance technique because of the difference between borders in terms of terrain, climate, profile and degree of threat. In fact, a single length of borders can often require different approaches, technologies and techniques in order to ensure an optimal security posture. For this reason, each government tries to adopt its own strategy of securing their frontiers according to their own requirements.

Recently, the need to strengthen security levels is more and more felt in various fields of activity and today, no one can deny that video surveillance is omnipresent in many sectors of activity (banking, transport, industry, ...etc) and even in our surrounding everyday life (buildings, offices, collective facilities,...etc). It is therefore a question of ensuring the surveillance of small areas of interest which do not exceed a few kilometers with a considerably low degree of threat. Therefore, from a technological point of view, video surveillance has been more and more trivialized and mastered in several areas, which is not the case for border surveillance tasks. The latter aims to secure continuously without stop (24H/7D) thousands of kilometers spread over inaccessible areas, in a severe climate and under a very high level of threat. Besides, the task of securing borders is a defense forces responsibility, it requires to control movements of enemy forces or intruders far away from the borders in order to have enough time to take the proper decision at the appropriate moment.

In the current thesis we deal with the problem of border surveillance by proposing

solutions adapted to different parts of the Algerian borders. Note that this work contributes to a large project of the Algerian Ministry of Defense, that aims at defining an operational framework for securing Algerian land borders.

Objectives and motivations

Nowadays, the use of communication technologies in border surveillance has become inevitable. As a result, several technologies have been proposed in the market and each country adopted the appropriate one according to the nature of the ground, the climate and the threats surrounding its territory. To overcome the issues such as false alarms, line of sight limitations and some other operational requirements, border surveillance techniques have shifted from classical methods conducted by humane patrols such as installation of barriers, construction of insulation walls and trenching to the use of new technologies, such as implementing Wireless Sensor Networks (WSN), Radars, Cameras towers as well as UAV. These new technologies allow the integration of hundreds of cameras, seismic and infrared sensors, UAV, satellites and radar coverage. The goal of these networks is to monitor borders and create a virtual fence [6].

When taking a close look at the literature, border surveillance technologies have been used separately and sometimes combined with each other. Although, the use of WSN as a technology to secure small areas of interest has been widely addressed, using WSN alone to protect borders can never reach the desired operational requirements, because of their very limited detection radius, that can reach tens of meters for individuals detection and hundreds of meters for vehicles. In addition to that, most authors do not distinguish between surveillance of an area of interest (commonly called video surveillance) and border surveillance, the latter is much more complicated because the area to be monitored can reach thousands of kilometers. Furthermore, border surveillance is a non-stop(24H/7D), critical application where we do not have the right to error, since it is an armed forces responsibility. Therefore, it is crucial to know what is happening in miles away to take the appropriate decision at the appropriate time. For example, in wartime or in some critical situations, we need to control movements of enemy forces or armed vehicles far away from our borders in order to have the required time to launch countermeasures.

At this point, it is important to mention that through the in-depth reading of the literature that we have carried out throughout the period of preparation of this thesis, we found out that there is a big difference between the research works related to the border surveillance and practical systems deployed at physical borders of different countries over the world. In research work (the theoretical side), we often talk about the use of scalar or multimedia sensor networks, whether alone or combined with other

types of technologies such as UAV, unlike what we find in the practice, wherein radars are often combined with multimedia sensors to secure borders, as it is the case for a part of the Algerian borders. According to a report published in 2016 by FLIR company (specialized since 1978 in the development of high performance infrared imaging systems dedicated to border surveillance), despite the diversity of border surveillance technologies on the market, the two primary technologies used to detect threats are radars and imaging systems. Radar manufacturers would often have you believe that radars alone are enough to secure borders. On the other hand, manufacturers of long-range imaging systems tout their ability to outperform radar at certain crucial tasks, and do so at a lower cost. But these bold assertions only beg more questions. What kind of radar ? Certainly all radars are not created equal, so which radar technology is best suited to a border surveillance role ? The same can be said of cameras : which sensing technology, resolution, and lens configurations are the most effective when trying to secure a border[7] ? All those questions and concerns are discussed in the different chapters of this thesis, to provide an optimal combination of these technologies for an efficient and fault tolerant border surveillance system.

Thesis main contributions

As aforementioned, the research work carried out in this thesis contributes to a large project which aims to define an operational framework for securing the Algerian land borders. The major contributions of this thesis can be summarized in the following points :

— First, we carried out a deep reading of the literature related to this field of research, to clearly identify the key problems. Such a study has led to understand the concept of border surveillance, elaborate an up-to-date state of the art on border surveillance technologies, and finally surround the operational challenges we can reveal ;

— Due to the vastness of Algerian borders and some other specificities such as the geographic diversity, the fluctuating human densities and the different types of threats surrounding these borders, we opted to divide the area of interest into two essential parts. The first part called *part*01, concerns the north-west and the south-west border strip (from the Wilaya of Tlemcen till the Wilaya of Naama). Borders in this part are shared with Morocco, Western Sahara and Mauritania (more than 2000km). The second segment as for it, keeps the extreme-south border strip (from the Wilaya of Tindouf till the Wilaya of Illizi), shared with Mali, Niger and a part of Libya (more than 2500km). Hence two different solutions are

thus proposed for each part, accordingly.

— Once a clear statement on the real issue of border surveillance is identified, we propose a new hybrid wireless sensor network architecture for border surveillance. The goal behind this multilayer framework is to detect and track any intrusion with minimum human involvements. To ensure a better fault tolerance and reliability, we consider it useful to re-enforce the *part*01 by additional equipments such as Unattended Ground Sensors (UGS) and UAV, comparatively to the *part*2.

— A detailed deployment scheme for each layer of the proposed architecture (for both *part*01 and *part*02) is addressed in this thesis. This scheme will allow us to determine the required number of each equipment to deploy to achieve an optimal coverage. The proposed deployment scheme reflects the real organization of the Algerian Border Guard Forces (ABGF), responsible of border security in Algeria ;

— For energy saving, load balancing and redundancy elimination, activation scheduling strategies are proposed for both part 01 and part 02 of the borders. One of these strategies implements the way scalar sensors and multimedia sensors are activated in *part*01 of the borders, while the other strategy implements the way multimedia sensors are activated in *part*02 of the borders.

— To highlight the efficiency of the proposed scheduling strategy for both parts of our borders, we compare our solutions to other existing methods and we give the simulation results that confirm that our solution outperforms the other schemes by extending the network lifetime while maintaining its efficiency. It should be noted that contributions related to *part*01 of the borders have been gathered in a journal paper which is the subject of a publication in the IEEE Transactions on Sustainable Computing journal, while our contributions for *part*02 of the borders is being considered for submission for a Journal.

— We studied also in this thesis the effectiveness of adapting the activation period of scalar sensors and multimedia sensors on energy consumption and the network lifetime. Obtained results show that this period should be reduced in crisis time to enhance the fault tolerance of the network while it should be augmented in peacetime to extend the network lifetime. This contribution was published in the IEEE Globecom conference in December 2019. Moreover, we design a second mechanisms to overcome a serious issue which is deploying and energy supplying system for UAV.

— For energy supply in border surveillance architecture based on the combination of radars with mobile camera sensors that are embedded on UAV, we proposed a WPT system based on rectennas to supply wirelessly UAV batteries with power during their flight. To manage the access of UAV to the WPT system, we implement an active UAV scheduling strategy based on an improved Weighted

Round-Robin (WRR) algorithm. To evaluate this scheduling strategy, simulation results are presented and discussed. This contribution was published in the IEEE Globecom conference in December 2020 ;

- Publications list

During the period devoted to this thesis, three one publication and two conference papers were published.

International conferences

- **ML. LAOUIRA**, A. Abdelli, J. Ben othman and K. Hyunbum, "An adaptive activation scheduling strategy for a border surveillance network". IEEE Global Communications Conference (GLOBECOM), 9-13 Dec. 2019, Waikoloa, HI, [8] USA.
- **ML. LAOUIRA**, A. Abdelli and J. Ben othman, "Wireless energy supply scheduling strategy in a combined border surveillance architecture". IEEE Global Communications Conference (GLOBECOM), 7-11 Dec. 2020, Taipei, Taiwan.[9]

International journals

- **ML. LAOUIRA**, A. Abdelli, J. Ben othman and K. Hyunbum, "An efficient WSN based solution for border surveillance". IEEE Transactions on Sustainable Computing journal, ISSN : 2377-3782, DOI : 10.1109/TSUSC.2019.2904855, 12 pages March. 2019.[10]
- **ML. LAOUIRA**, A. Abdelli, and J. Ben othman **CAMRAD BORDER-GUARD :** A new collaborative camera sensors and radars based solution for detection and tracking intruders in border surveillance applications. *Paper is being submitted to the International Journal of Sensors, Wireless Communications and Control.*

Thesis outline

To properly present all the contributions discussed above and in order to achieve the outlined objectives, we have opted to structure our manuscript into four (04) chapters in addition to a general introduction and a general conclusion.

— In the first chapter, an introduction to the technology of wireless sensor networks is given.

— An introduction to border monitoring and a detailed state of the art about borders monitoring techniques are addressed in Chapter 02.

— Our main contributions is discussed in Chapter 03 of this thesis, where a New network architecture as well as a detailed deployment scheme and activation scheduling strategies are discussed.

— Additional mechanisms to our primary solution are presented and evaluated in chapter 04.

Finally, the General Conclusion concludes this document and highlights the perspective researches.

Chapitre 1

WSN for border surveillance : Overview and challenges

1.1 Introduction

In the last twenty years, the field of WSN was receiving a lot of attention in the networking research community and as an area of interdisciplinary interest. Today, WSN are becoming increasingly economical, low-power, multifunctional and viable due to the latest technological advances in wireless communications which enabled the development of wireless sensors with low energy consumption. These small devices are interconnected with each other to form a wireless sensor networks and are then deployed to an area of interest to handle specific tasks [11]. In their first implementations, the sensors were deployed to detect specific events in their sensing area, such as forest fires, animals movements, humidity rate, ... etc. Moreover, sensors have been investigated in military field to detect the presence of some substances such as biological, chemical, nuclear and explosive. Nowadays, sensors play a primordial role in the technological advances of the new concept of Internet of Things (IOT), where Machine to Machine (MtM) communication enables machines, physical devices, and electronic devices to communicate via the internet without human intervention[12, 13]. In this chapter, we will try to address WSN in the context of border surveillance systems, by giving an up-to-date presentation on the main aspects related to this field.

1.2 Physical architecture of a sensor node

A sensor node is generally defined as a device that produces a measurable response to a change in the physical or chemical state of its environment. More specifically, a sensor node is a device which responds to an external stimulus (such as heat, light, pressure...etc.) and which produces a signal which can be measured or interpreted. Further, sensor nodes are defined as small wireless devices capable of responding to one or more stimuli, processing data, and transmitting it over a short distance typically using radio communication[14]. Sensor nodes architectures are almost identical. As shown in Figure 1.1, a sensor architecture is composed of four basic units, a detection unit, a processing unit, a transceiver unit (Transceiver or transmission) and a unit of energy. Sometimes, according to the type of application we require additional components, such as a positioning system, a power generator and a mobilizing.

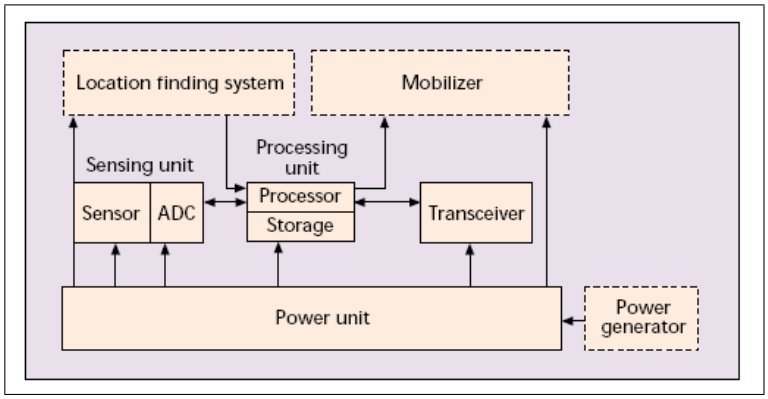


FIGURE 1.1 – Basic architecture of a sensor node.

— *The detection or acquisition unit* (sensing unit) is composed of a sensor taking measurements on environmental parameters and an Analog-to-Digital Converter (ADC) converting the data recorded into digital data in order to send it to the processing unit.
— *The processing unit* consists of two interfaces : one interface for the acquisition unit and another for the transmission unit. It receives the information from the acquisition unit and sends it, possibly after processing, to the transmission unit. This unit is made up of a processor on which a specific operating system runs.
— The transmitting unit is responsible for all transmissions and receptions of data via the radio communication medium.
— The power unit is the most important component of the collector, the functionality of this unit can be provided by techniques such as solar cells.
— The localization unit is sometimes necessary to determine the position of sensor nodes as long as they are deployed in a random manner in the area of interest.

— The energy generator, as its name implies, has the role of supplying energy to the node when needed.
— A mobilizer is needed to move a node to perform a specific task.

1.3 Generalities on WSN

A WSN consists of spatially distributed sensor nodes to monitor physical or environmental conditions. The WSN is built of nodes from a few to several hundreds or even thousands, depending on the scale of the monitored area. The data collected between sensor nodes is sent to a specific node, generally referred to as the *sink node*, which forwards directly or through a gateway node the received data to the analysis center for processing. The basic WSN architecture is depicted in Figure 1.2, [15].

According to [16], WSN technology is now a stable technology supported by a vast amount of researches, applications, and hardware platforms. Most of the current research and deployments strategies assume a certain level of redundancy. Indeed, 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, to reduce the end-to-end delays, to prolong network life using duty cycles, and to enable fault tolerance, and so on.

The sensor nodes can be deployed in a deterministic or random fashion (dropped from an aircraft, autonomous flying machine or other), depending on the nature of the application, the type of the sensing field and the deployment cost.

Recently, borders monitoring became one of the most popular application for WSN. In fact, A WSN can provide an accurate detection and tracking of intrusion with a minimal human involvement. In the literature and according to the type of application, WSN can be classified into two main categories :

— **Homogeneous WSN :** A WSN is said to be homogeneous, if all its nodes have the same technical characteristics such as storage, processing, sensing, energy and communication capacities. This kind of network is characterized by a low cost deployment and can be used only for sensing small areas of interest.
— **Heterogeneous WSN :** A heterogeneous WSN consists of two or more kinds of sensor nodes with different technical characteristics, combined together to insure the required tasks. Border monitoring is one of the applications of heterogeneous WSN.

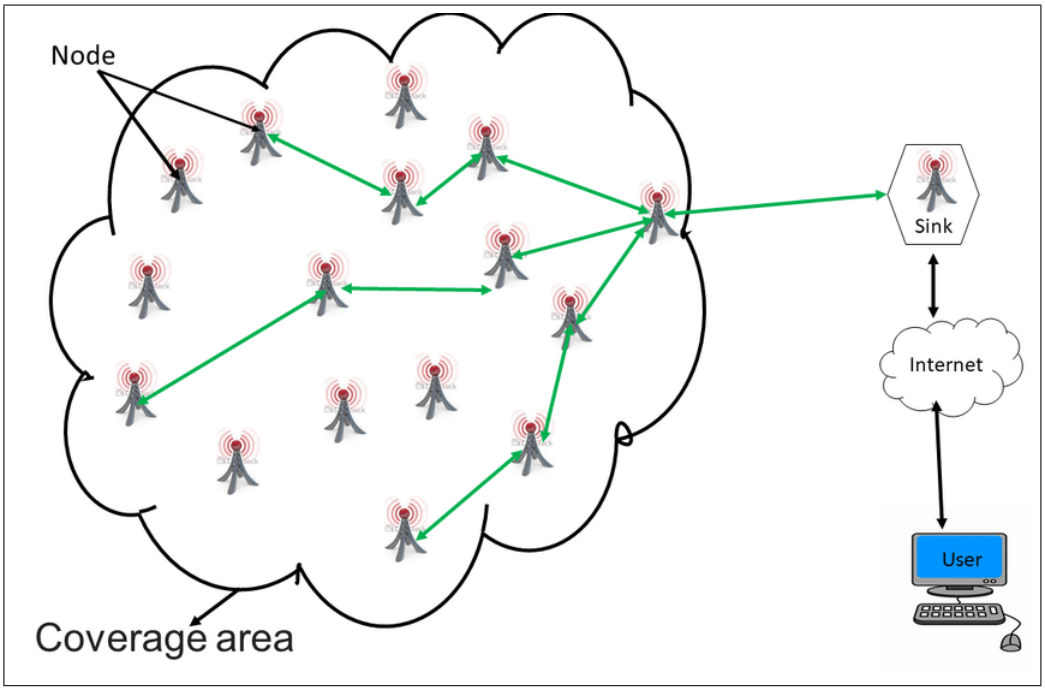


FIGURE 1.2 – Basic WSN architecture.

1.4 Characteristics and constraints of WSN

Due to the imposed manufacturing costs and miniaturisation requirements, sensors are becoming small and light. They are generally characterized by strong limitations in terms of computing power, communication range and especially energy consumption. The main characteristics and limitations of WSN are discussed hereafter [17] :

- No infrastructure requirement : As WSN are a part of Ad hoc mobile networks, they are distinguished from other networks by the absence of pre-existing fixed infrastructure ;
- Large density : Sensor node density in WSN is higher than in other networks. The number of sensor nodes can reach millions to allow better granularity of monitoring as well as fault tolerance ;
- Communication model : Nodes in WSN communicate using the many-to-one paradigm. Indeed, the sensor nodes collect information from their environment and send it to the processing center ;
- Interference : Radio links are not isolated ; two simultaneous transmissions on the same frequency using close frequencies can interfere ;
- Dynamic topology : In some situations, the sensor nodes can be attached to mobile objects which move freely and arbitrarily, thus making the topology of the network changing. It should be noted that this case is very rare ;
- Limited physical security : WSN are more affected by the security setting than

traditional wired networks. This is justified by physical constraints and limitations, which means that the control of the transferred data must be minimized. In addition to that, the sensor nodes themselves are points of vulnerability in the network because they can be reprogrammed, replaced or removed ;

— Limited bandwidth : One of the essential characteristics of networks based on wireless communication is the use of a shared communication medium, which limits bandwidth availability to the nodes ;

— Scaling up : WSN can contain thousands of sensor nodes. Such a large number of nodes generates a lot of inter-node transmissions and requires that the collector node (sink) must be equipped with a large memory capacity to store the received data ;

— Energy constraint : Energy is the most important constraint to which sensors are subject, as the lifetime of the network is directly related to the autonomy of the sensors. For most of the applications, physical access to nodes is often impossible to renew or to recharge their batteries. For example the surveillance of forest fires or military zones in which the sensors are disseminated by air, or the surveillance of urban infrastructures such as the bridges, the sensors being incorporated into the structure itself. Much of the research is therefore naturally oriented towards the economical management of this precious resource, or techniques for harvesting it. The proposed management solutions intervene at all levels, by enforcing low-consumption transmissions and light routing protocols, as well as adapting the solutions and the frameworks to different contexts and environments. Mechanisms for periodically falling asleep, reducing the size of the data exchanged : everything has been redesigned to reduce energy consumption[11]. Because of the paramount importance of energy consumption in WSN, we devote a separate section to address this issue.

— According to [18], WSN is the backbone of IoT, without which the concept of a smart city cannot be realized. Sensors and actuators are the elementary devices, which interact with the physical world and impose the changes. Under an heterogeneous environment, a large number of devices are connected together using sensors and generate large amount of data. This data is stored and analysed to derive the information and support decision-making. For all of those reasons, the challenges facing IoT today, are also facing the WSN. Some of those challenges are interoperability, scalability, management of large volumes of data, security, privacy and integrity, dynamic adaptation, reliability, and latency (transmission delay).

1.5 Energy consumption in WSN

In a WSN, the network lifetime depends on the service availability provided by its nodes, which relies strongly on energy availability. Therefore, energy conservation and power management are very important in WSN. In this context, recent research is focusing on designing energy efficient protocols and algorithms for sensor networks. The main task of a sensor node is to detect events, perform local data processing, and then transmit the data. Energy consumption can therefore be considered at three levels : detection, communication and data processing [17].

- **Detection :** During this period the energy consumption depends directly on the application type in question. Sporadic detection consumes less energy compared to a continuous monitoring of an event. In addition to that, the complexity of event detection plays a crucial role in determining power consumption, this complexity is influenced by the ambient noise [17].
- **Communication :** During data transmission, sensor nodes spend much energy. In this context, we do not consider only the operating energy, but also the energy consumption in the Transceiver during the start-up operation.
- **Data processing :** During this phase, energy consumption is much less compared to the communication cost. Local data processing is crucial to reduce energy consumption in a multi-hop WSN. It has been shown that the energy required to transmit $1KB$ of data over a distance of $100m$ is approximately the same as executing $3million$ instructions per second [17].
- **Power saving mode :** This consists of switching off the communication module as soon as possible. For example, MAC protocols based on the Time Division Multiple Access (TDMA) method offer an implicit solution since a node only exchanges messages within the time slots allocated to it. It can then keep his radio off during the other slots. As we pointed out previously, it must be only ensured that the energy gain obtained by putting the radio module on standby is not less than the additional cost generated by restarting this module.
- **Event mode :** The idea behind this technique is that the source can perform a preprocessing. So event programming seems well suited to sensor networks. Only significant changes in the environment should cause packets to be sent over the network. In the same spirit, a great collaboration is expected between the sensors of the same region due to their high density, since the observations rarely vary between very close neighbours. Therefore, this strategy can significantly reduce the network traffic.
- **Exchanges organization :** This process consists of limiting retransmission problems due to collisions. The extreme solution is to use the TDMA medium

access technique, collisions are thus greatly reduced.

— **Energy consumption balancing :** Network clustering can be considered when the network is comprising a very large number of sensors, as it promotes a better distribution of energy consumption. Indeed, in the case of direct transmission to the observer, the remote sensors will run out of energy more quickly. On the contrary, in the case of a hop transmission, the nodes close to the observer will quickly be out of battery because they will be more used to relay the messages than others. The solution is to prioritize the exchanges by dividing the observation area into clusters.

1.6 Wireless sensor networks deployment

In general, the design of a WSN architecture must meet two important challenges which are the low cost deployment and the high coverage rate. Deployment in a WSN is the way in which nodes are physically placed in the area of interest. In the literature we identify several deployment techniques in a WSN. In application such as border surveillance, because of the immensity of the area to be monitored, a large amount of sensors and equipments may be required to cover the full area, resulting on prohibitive costs. Therefore, a carefully controlled deployment strategy is needed to achieve an acceptable compromise between cost constraints and coverage requirements. In terms of deployment density, WSN deployment techniques can be divided into two classes : a dense deployment and a sparse deployment. A dense deployment has a high number of sensor nodes in the given field of interest while a sparse deployment would have fewer nodes. Sensors can be placed in a deterministic way, where we have a prior knowledge about the surveillance area. On the other hand, in the situations where the monitoring area is hardly accessible (hostile zone) or of a large size, we recourse to random deployment. Therefore, the choice of deployment technique depends highly on the WSN applications, the surveillance area where the sensor nodes are to be deployed and the type of sensor node to be considered [19].

1.6.1 Deterministic deployment :

This type of deployment can be found in control, multimedia and body surveillance applications. A deterministic deployment in this case becomes too recommended because the measurements must be precise, relevant and of quality. This therefore imposes an appropriate location of the sensors. This is also the case for the collector nodes which

should be located near the sensors in order to achieve the acquisition, the integrity and the processing of these measurements with a minimal cost.

1.6.2 Random deployment :

Unlike the deterministic deployment, the random deployment is adopted in situations where the sensing area is not accessible. Node sensors can be deployed, for example, by dropping them from an aircraft, especially in outdoor and environmental surveillance applications characterized by high network size. Indeed, the number of node-sensors to deploy is too large and the cost of placing each in a planned manner is prohibitive. This type of deployment is highly recommended in large application scenarios where sensor nodes need to detect events, such as : a fire in a forest, a flood, an earthquake, an intrusion,. ..etc, and which can happen any time and anywhere.

In this kind of scenario, the sensor deployment will never be optimal, add to that, it can result in very dense, less dense or even disconnected areas.

In borders surveillance applications, a deterministic (manual deployment) can be used in some accessible areas, while random deployment is highly recommended in inaccessible perimeters. However, due to the sensitivity of border surveillance applications, deploying more redundant sensors (scalar and multimedia sensors), to replace failing nodes is more than a necessity [19].

According to [16], WSN applications such as international border surveillance, railway track monitoring, gas/oil/water pipelines leak detection have a common topological structure that is inherently linear. This is a result of an exhaustive and a semi planned deployment of sensor nodes to closely track the monitored environment, which is linear in nature. This class of networks as called Linear WSN or Linear Wireless Sensor Networks (LWSN) which are defined as any form of WSN that can be limited between two long parallel lines. From the author's point of view, a WSN is considered linear if all the nodes are aligned on a straight line, strictly forming a line or 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 LWSN. LWSN can be seen as a new category of WSN where nodes are placed in a strictly linear or semi-linear form.

1.7 Application areas

Nowadays, many WSN applications are at the origin of the advent of the IoT. WSN applications can be classified into two categories, conventional (old) applications and new applications (See Figure 1.3). In this section, we discuss the most important applications of WSN accordingly.

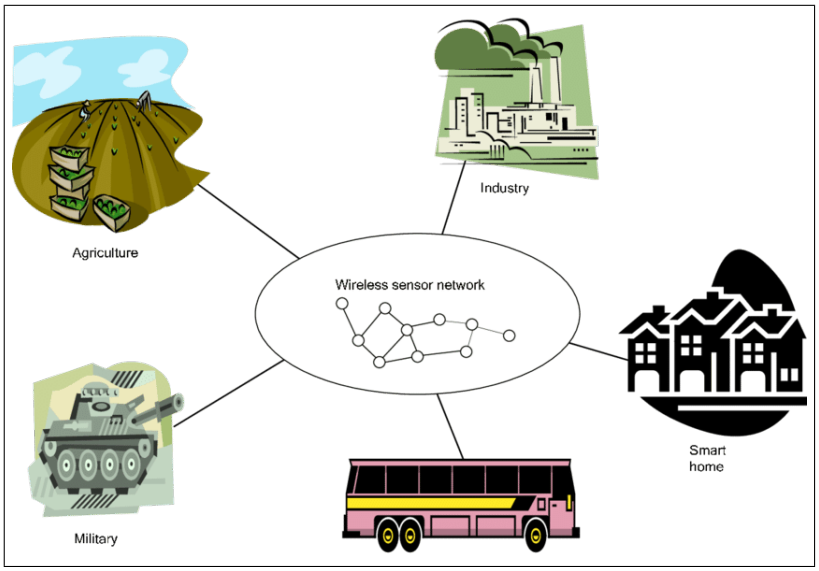


FIGURE 1.3 – WSN Applications [1].

1.7.1 Conventional applications :

-A) Medical applications : In healthcare sector, WSN provide communication interfaces to disable people, to integrated patient monitoring, to drug administration in hospitals, as well as remote monitoring of physiological data of humans.

- **Remote monitoring of human physiological data :** Physiological data collected by sensor networks can be stored for a long time, and can be used for medical exploration. Sensor networks can also monitor and detect the behaviours of the elderly people. This gives these people more freedom of movement and allows doctors to identify previously predefined symptoms. "Health Smart Home" was designed at the Medicine Faculty of the university of Grenoble-France to validate the feasibility of such a system (See Figure 1.4).
- Monitoring and control of doctors and patients in a hospital : Each patient is equipped with one or more small sensors. Each sensor performs a specific task, for example controlling the heartbeat while another controls the blood pressure.

Doctors can also be equipped with sensors to facilitate their localization inside the hospital [17].

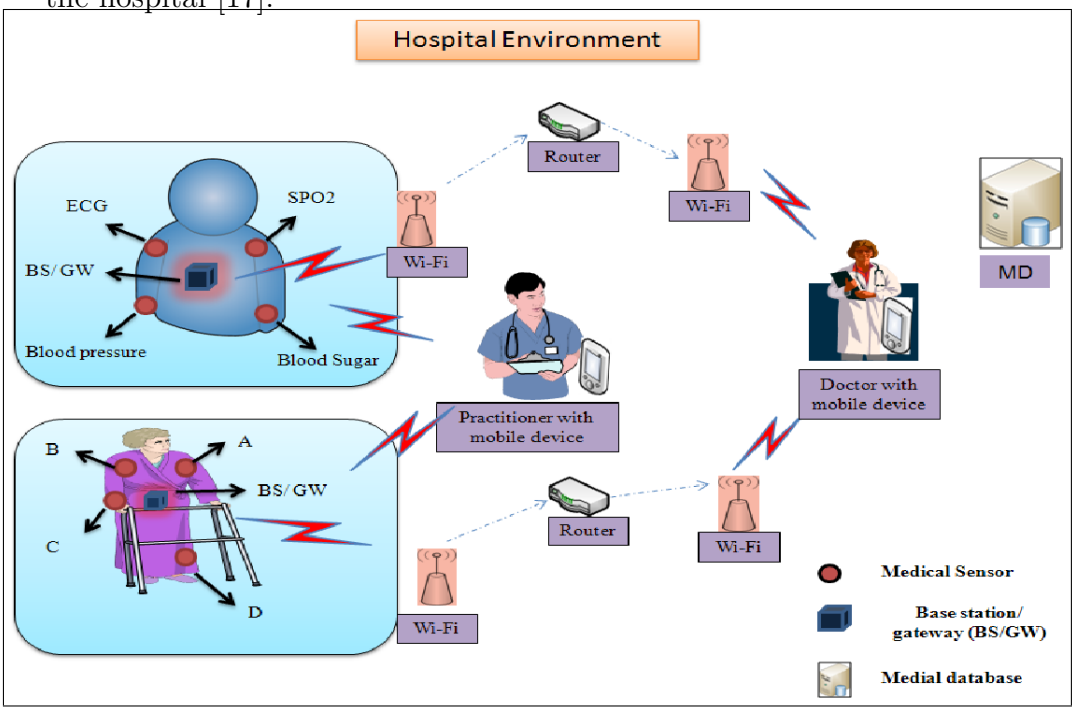


FIGURE 1.4 – Patient monitoring using a wireless medical sensor network in a hospital environment[2].

-B) Home applications : This represents the most WSN applications :

— Home automation : As technology advances, sensor nodes can be placed inside household appliances such as microwaves, vacuum cleaners and refrigerators. These sensors can communicate with each other or with external networks via the Internet or the phone network. This makes it easier for users to manage these devices locally or remotely.

— Elegant environment : Sensors placed inside household appliances can thus communicate with each other or with a room server managing all the available services, (exa : printing, faxing, and scanning). This server can communicate with other room servers. This type of applications has been implemented in the Risedential Laboratory at the Georgia Institute of Technology-USA [17] (See Figure 1.5).

-C) Military Applications : WSN are an integral part of military commands, control, communication, reconnaissance, and military intelligence (See Figure 1.6). Rapid deployment, self-organization and fault tolerance makes WSN the most widely used in battlefields. Among the military applications of WSN, we can quote : the control of friendly forces (equipment, munitions) ; monitoring of the battlefield ; reconnaissance of the terrain, control of enemy forces (positioning and equipment).

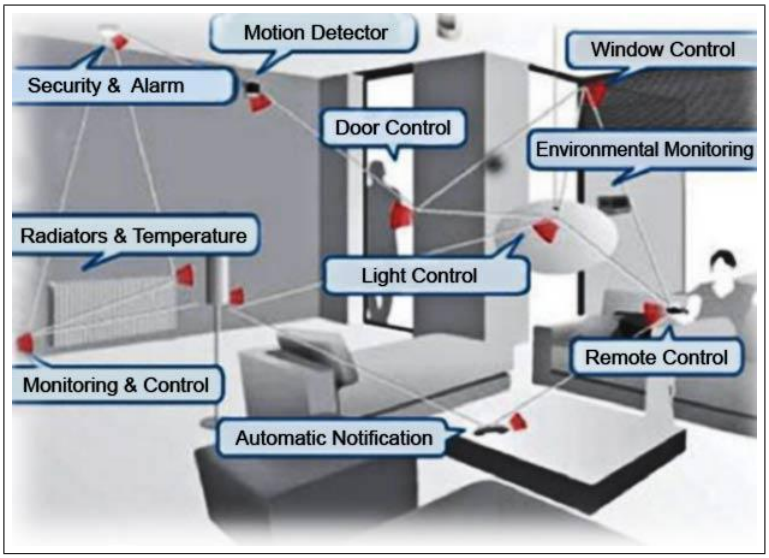


FIGURE 1.5 – Home applications of WSNs [3].

— *Friendly forces monitoring(equipment and ammunition) :* Force commanders can at any time monitor the state (conditions and availability) of friendly troops, by using a WSN. Each vehicle, important equipment can be equipped with a sensor which provides information to the responsible node (Sink) that forwards the information to a command center.
— *Battlefield monitoring :* Critical terrain and roads can be quickly covered by sensor networks. Close monitoring of the activities of opposing forces is possible. As operations are variable and renewed, operational plans may be prepared, new networks of sensors can be deployed at any time for battlefield surveillance.
— *Reconnaissance of the terrain and enemy forces :* Knowing in advance the terrain to be occupied by the enemy forces, this allows wireless sensors to be deployed in order to control all its activities and movements in real time.
— *Battlefield loss assessment :* Just before or after attacks, sensor networks can be deployed in a target area to collect battle loss assessment data [17].

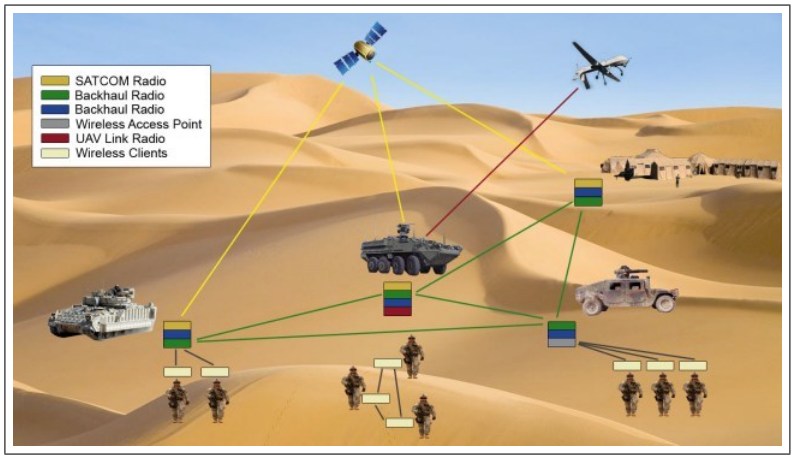


FIGURE 1.6 – Military Applications of WSNs [3].

-D) Commercial applications : Among the commercial applications of WSN, we can quote : the product quality control, the construction of intelligent office spaces, the monitoring of the environment in offices, monitoring of disaster areas,... etc.

- *Environmental control in an office :* The air conditioning and temperature in most buildings are centrally controlled. Therefore, the temperature inside a room can vary by a few degrees ; one side may be warmer than the other. As the airflow from the central system may not be evenly distributed, a WSN can be installed to monitor the airflow and the temperature in different parts of the room. Such technology can reduce energy consumption.
- *Interactive museums :* Thanks to WSN, an interaction is created between objects and the public in museums. An archaeological object will be able to respond to a person who touches it. Additionally a WSN can provide the location inside the museum. An example of such museums is the Exploratorium (a science and technology museum) in San Francisco-UAS.
- *Vehicles stealing control :* Sensor nodes are deployed to detect and identify vehicles stealing in a geographic region and report these threats to users through the Internet or satellite. In addition, wireless sensors can be deployed in a vehicle to remotely locate and track a stolen vehicle [17].

1.7.2 New applications :

-A) Recent Applications in industry :

- **Oil and gas Industry :** The oil and gas industry is perhaps one of the most

prevalent industries for the application of WSN. These applications most commonly cover monitoring of near real-time process control, safety, regulatory, and production performances. As depicted in Figure 1.7, the core applications center around : (i) Tank Levels (wireless transmitter head is paired with a level sensor based on the application requirements, process fluid, and whether or not a water interface level is required) ; (ii) Pressures (tubing pressures are monitored by pairing a wireless transmitter with a pressure transducer.) ; (iii) Flow (Flow measurement in the oil and gas industry covers everything from well injection to custody transfer) ; (iv) Valve Actuation (Emergency Shutdown valves can be wirelessly automated to shut-in a well in the event of abnormal process conditions preventing a spill or catastrophic environmental incident.),...etc.

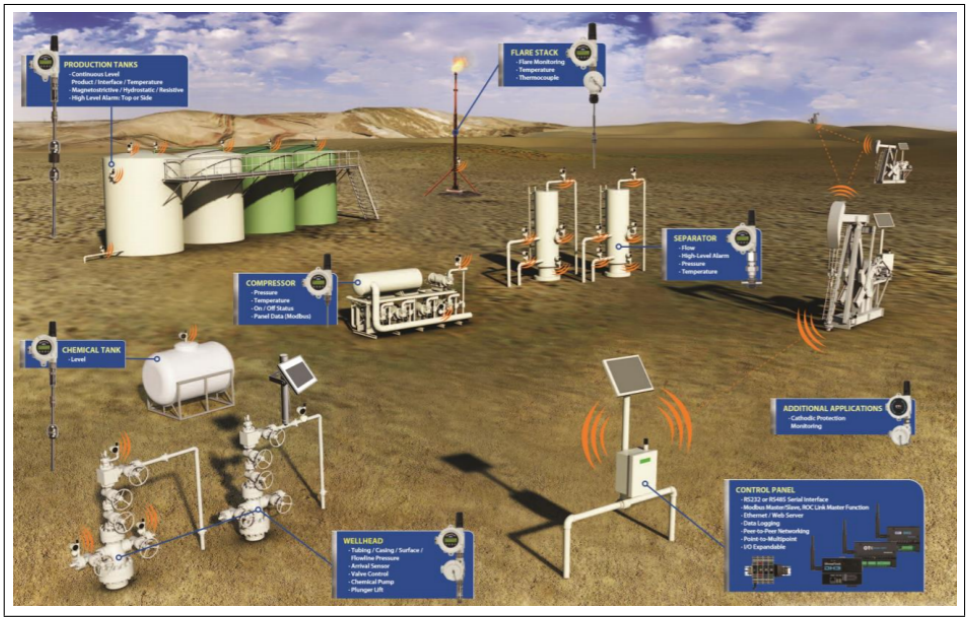


FIGURE 1.7 – WSNs Oil and gas applications.

— **Robotics :** Generally, in such applications, WSN are combined with mobile robots (in most of the case jumping robots). These robots mounted with sensors and wireless communication devices are able to enter into dangerous and unfriendly environments to execute their missions. With the capabilities of quickly overcoming obstacles and avoiding risks, jumping robots can be applied in many fields such as space exploring (See Figure 1.8).

— **Smart cities :** In this field, the key word is IoT which means the connection of physical devices and objects used in daily life to the Internet network (See Figure 1.9). IoT network in the case of a smart city must be scalable as there can be requirements of adding new devices and deleting old devices, any time and anywhere. Due to the wide application areas using different technologies, IoT integration is raising many challenges, as : interoperability, context awa-

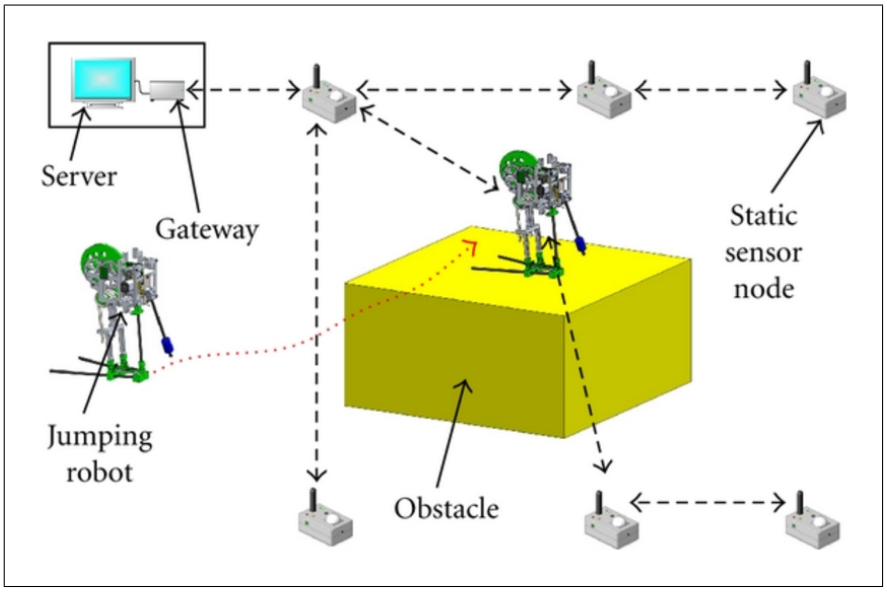


FIGURE 1.8 – WSN combined with jumping robots[4].

reness, scalability, and management of large volumes of data, security, privacy and integrity, dynamic adaptation, reliability, and latency. Among smart cities applications, we can quote : traffic monitoring and tracking, car parking management,...etc.

1.8 Towards Wireless Multimedia Sensor Networks

With the miniaturization of certain multimedia capture devices, such as cameras and microphones, WMSN have emerged. In these networks, the sensors capture and process multimedia streams (sound, image, video) widening the field of WSN applications a little further. In addition to the ability to capture multimedia contents, WMSN can process and fuse multimedia data from heterogeneous sources in real time and thus interact with the physical environment. The notion of wireless multimedia sensor networks stems from the fusion of two concepts : wireless sensor networks and traditional surveillance systems, thus providing the flexibility of one and the efficiency of the other.

FIGURE 1.9 – WSN applications in smart cities [5].

1.8.1 Basic architecture of WMSN :

As illustrated in the Figure 1.10, a reference architecture for WMSN is presented, where users connect through the Internet to a deployed multimedia sensor network. The functionalities of the various network components are summarized as follows :

- **Standard video and audio Sensors :** These are generally low resolution sensors, they can be arranged in a one tier network, as shown in Figures 1.10.a, 1.10.b or in a hierarchical structure, as shown in Figure 1.10.c.
- **Scalar Sensors :** These are generally devices with limited resources in terms of storage and processing capacity and energy. They are used to capture scalar data, such as : temperature, humidity, pressure, vibrations, in order to send it to a base stations (sink).
- **Multimedia processing hubs :** These devices have relatively large computing resources and are suitable for aggregating multimedia flows received from sensors. They are integrated in the WMSN to reduce both the size and the amount of data transmitted to the SINK and storage devices.
- **Storage hubs :** Depending on the application, multimedia flows can be exploited in real time or after additional processing. These storage platforms have extraction, data mining and function algorithms to identify the important cha-

racteristics of the event before the data is transmitted to the end user.

— **Sink :** As in WSN, the Sink is responsible for communicating user requests to the network and returns the filtered parts of the multimedia streams to the end user. Several sinks may be necessary in a large heterogeneous network.

— **Gateway :** It uses a geographical coverage map of the sensing area to distribute the spots to the appropriate sinks for the transfer of the captured data.

— *Users :* They are identified by their IP addresses. They are the initiators of the requests sent to the network which returns back the obtained results.

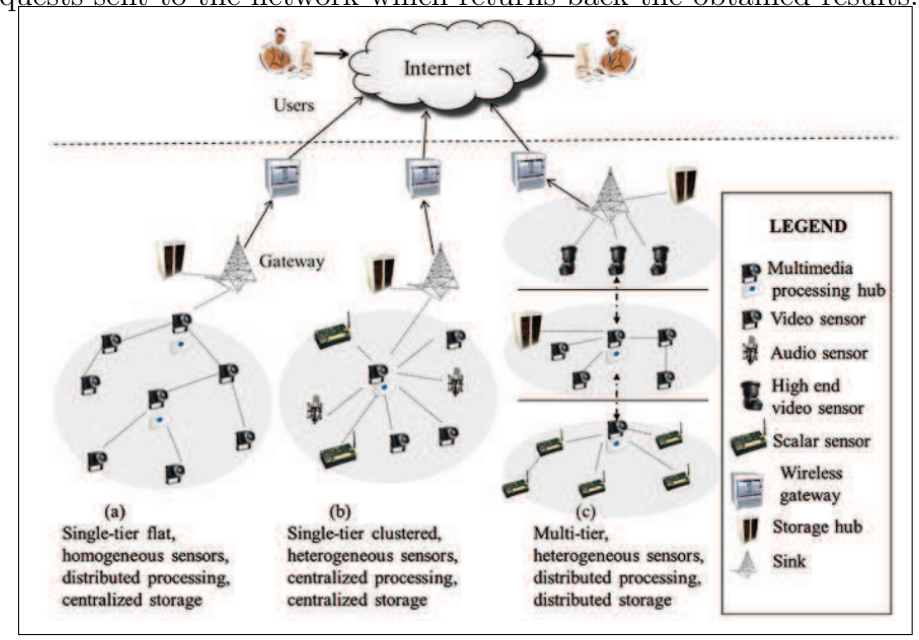


FIGURE 1.10 – Basic architecture of WMSN.

1.8.2 Some WMSN restricting aspects

In addition to classical WSN constraints that have been already discussed, such as energy constraints, WMSN suffer from very specific constraints mainly linked to the manipulation of multimedia data. Among these constraints we can cite : bandwidth limitations and fluctuations, specific Quality Of Service (QoS) requests, real time constraints, multimedia encoding, etc. Thereafter, we discuss the main factors generating the specific constraints related to WMSN [11].

— **QoS requirements** : All the applications envisaged in WMSN are facing different requirements associated with the scalar and the multimedia contents to be delivered. Therefore, high level hardware and algorithm requirements are needed to provide the required quality of service. These requirements can affect several areas, namely : delays, reliability, data distortion, or even the lifetime of the

network.

— Image capture and processing : According to [11], in conventional surveillance systems, image processing, information extraction and compression are performed locally at the source itself. Although these actions are basic and sensitive in the context of WMSN, given their limitations in both hardware and energy capacities.

— Memory requirements : While encoding simple scalar data requires only few bytes (generally no more that 1 to 8 *bytes* depending on the sensor), encoding an image or a video consumes a huge amount of data. The memory size required depends on both the resolution and the video format. An 128×128 pixel image will use $4times$ more memory space than a 64×64 image [11].

— Multimedia data transmission : As aforementioned, data transmission is one of the most energy-consuming actions in WSN. The use of suitable communication protocols is therefore necessary. In conventional sensor networks where simple scalar data is captured, the data can be merged and sent into a single packet. For multimedia data, the task becomes more complicated if we consider the size of the images. Indeed, a single image must generally be fragmented into several packets in order to be sent.

1.9 WMSN in a border surveillance architecture

Depending on the area specificities, several types of sensors can be considered to design a sensor network architecture dedicated for a border surveillance application. Sensors can be used separately (only one type of sensor is used in the architecture) or combined. According to the literature, we have observed the use of the following types of sensors in the identified securing borders solutions.

1.9.1 Scalar sensors

Scalar sensors called also non-imaging sensors, are components that directly convert the physical state of its environment (such as temperature, pressure, moisture,... etc.) into a digital information, existing in various sizes and forms. This kind of sensors implement several sensing technologies. They are called *passive sensors* as they are deployed at the area of operation, for detecting, classifying and reporting target information via wireless links to a remote control center.

In the literature, the most popular scalar sensors are :

— UGS which can combine several detectors such as seismic detectors, used to identify ground vibration caused by vehicles or pedestrians ;

— Magnetic detectors that monitor movement of metal objects such as weapons or vehicles ;

— Acoustic sensors that are used to detect targets by specific acoustic signatures (noise of engine or tracks) [20] ; and

— InfraRed (IR) sensors which can measure certain characteristics of its surroundings. It does this by either emitting (we talk about active IR sensors) or detecting infrared radiation (we talk about passive IR sensors). IR sensors are also capable of measuring the heat being emitted by an object and detecting motion.

Note that this kind of sensors were widely used by the US army in its security programs in order to secure a part of U.S-Mexico borders. The operating mode of this kind of sensor is that when an intrusion in the borders is detected, an alarm is triggered and transmitted automatically by radio to a central monitoring point in order to analyse the threat and hence take the appropriate decision. The most popular and efficient scalar sensors available on the market and dedicated for border surveillance, are :

— The Remote Detection and Classification (RDC) seismic sensor node, shown in Figure 1.11, is manufactured by the British company Digital Barriers. This kind of scalar sensor can be used to monitor a perimeter or a linear deployment area around facilities, as well as along a border or a distributed high-value infrastructure, such as a pipeline [21].

— The RS-U (Radiobarrier System) seismic sensors node manufactured by the Russian company POLUS-ST. This kind of sensors could be installed in such a way that their detection zones overlap and create a continuous and concealed protection line along the entire zone of interest, as shown in Figure 1.12, [22].

— The E-UGS Expandable Unattended Ground Sensors provided by the american company ARS, which offers innovative technologies and solutions to safety and security problems. E-UGS are disposable seismic sensors that are able of sensing for up to six (06) months, and capable of an early detection of an intrusion of pedestrians or vehicles.

  Their controller/receiver unit operates with a PC that shows maps with sensor locations and status alerts once they are activated (See Figure 1.13). Since 2010, ARS has released more than 40,000 first generation E-UGS sensors to the U.S. Military [23].

FIGURE 1.11 – The RDC Seismic Sensor Node.

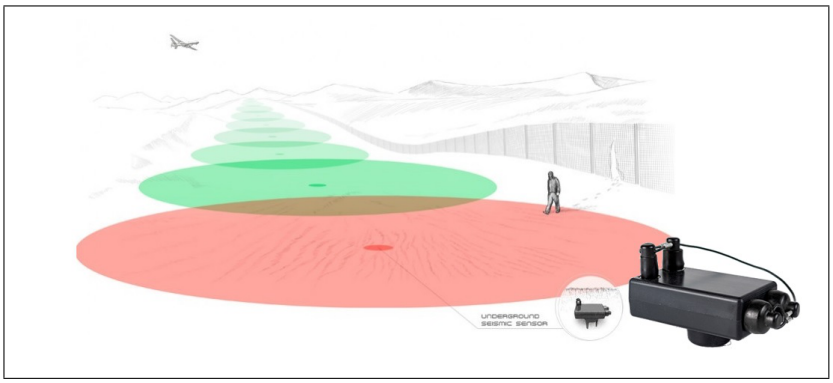


FIGURE 1.12 – The RS-U Seismic Sensors Node.

Advantages

The major advantages of scalar sensors can be summarized as follows (non exhaustive list) :

- Wireless sensors are one of the new technologies that is revolutionizing our world and our way of life, especially with the important role that wireless sensors is playing in the advent of the IoT (Internet of Things).
- Theoretically, scalar sensors have often been proposed in the literature for the monitoring of areas of interest ;
- Network setups can be carried out without a predefined infrastructure ;
- Low cost deployment in almost all cases ;
- Suitable for unreachable areas, such as mountains, deep forests and harsh rock areas ;
- In addition to that, WSN are discreet (constraint required by certain military

FIGURE 1.13 – The E-UGS Seismic Sensor Node.

applications), light (easy to transport and deploy), they are also characterized by their low energy consumption (this requires the implementation of certain rationalization mechanisms of energy consumption) ;

— In terms of data security, WSN do not suffer from this constraint because in most cases (except certain military applications), the data exchanged is not very critical and their interception does not represent any danger.

Disadvantages

The major disadvantages of scalar sensors are (non exhaustive list) :

— Limited detection range, which makes them operationally unsuitable for securing large areas ;

— Scalar sensors generally suffer from a high rate of false alarms, which requires their reinforcement with another type of sensors to reduce the effect of this issue ;

— The communication can be easily disturbed by the environment and interferences (climate, microwave, attenuation phenomenon in general, ... etc.) ;

— The power supply and consumption of the sensor nodes remains the major challenge in any sensor networks application.

1.9.2 Ground radars

As aforementioned, border surveillance is a task that must be carried out continuously, 24 hours a day, 7 days a week, with no interruptions or a reduced vigilance in

the service. Additionally, securing large borders requires reliable, long distance detection and positive identification of potential threats day or night and in all weather conditions. These requirement cannot be achieved without using radars[7]. Called also scanning sensors, radars or Ground Surveillance RAdio Detection And Ranging (RADAR) are a specific kind of high range active sensors.

According to a report published by the INRS in November 2020, entitled "ELECTROMAGNETIC FIELDS", a radar is designed to detect a stationary or a moving object using electromagnetic fields, by providing information about that object such as its distance, direction and speed. For this purpose, a radar exploits the reflection property of high-frequency electromagnetic waves on objects (Doppler effect). A radio wave produced by a transmitter (oscillator and amplifier) is sent to an antenna via a wave guide is emitted in the ether. When it encounters an obstacle, the signal is then reflected. The measurement and the comparison of the latter with the transmitted one make it possible to provide information about the target object[24].

In border surveillance context, the radar operates on a sector scan. indeed, some areas of interest may be better monitored by using radars than others and conversely some areas may be skipped or not monitored at all, depending on type of landscape and the efficiency of the radar detection. This is the case for areas behind the border (our forces or friendly forces) or which are masked by a mountain range in the axis of the sensor. Radars can operate with or without supervision depending on the command decision (see Figure 1.14).

On the market, a variety of radars using different technologies are offered to secure borders as for example :

— The Blighter which is designed and built by the mobile satellite British company Inmarsat, to provide continuous and persistent surveillance at borders, boundaries and perimeters. This kind of radar can detect moving targets over both land and water, covering a wide area (see Figure 1.15). It could be mobile or man-portable. Blighter scanning radars entered service with the United Kingdom Ministry of Defense in 2008 and are now operational in more than 10 other countries over the world, including the USA, France, Poland, Australia, South Korea, Qatar, Saudi Arabia, the Czech Republic and Oman.
— The Ranger R20SS is another popular radar which is manufactured by the US company FLIR. The R20SS is a ground and coastal radar specifically designed to detect and track personnel, vehicles, and watercraft at ranges up to 60km (see Figure 1.16).

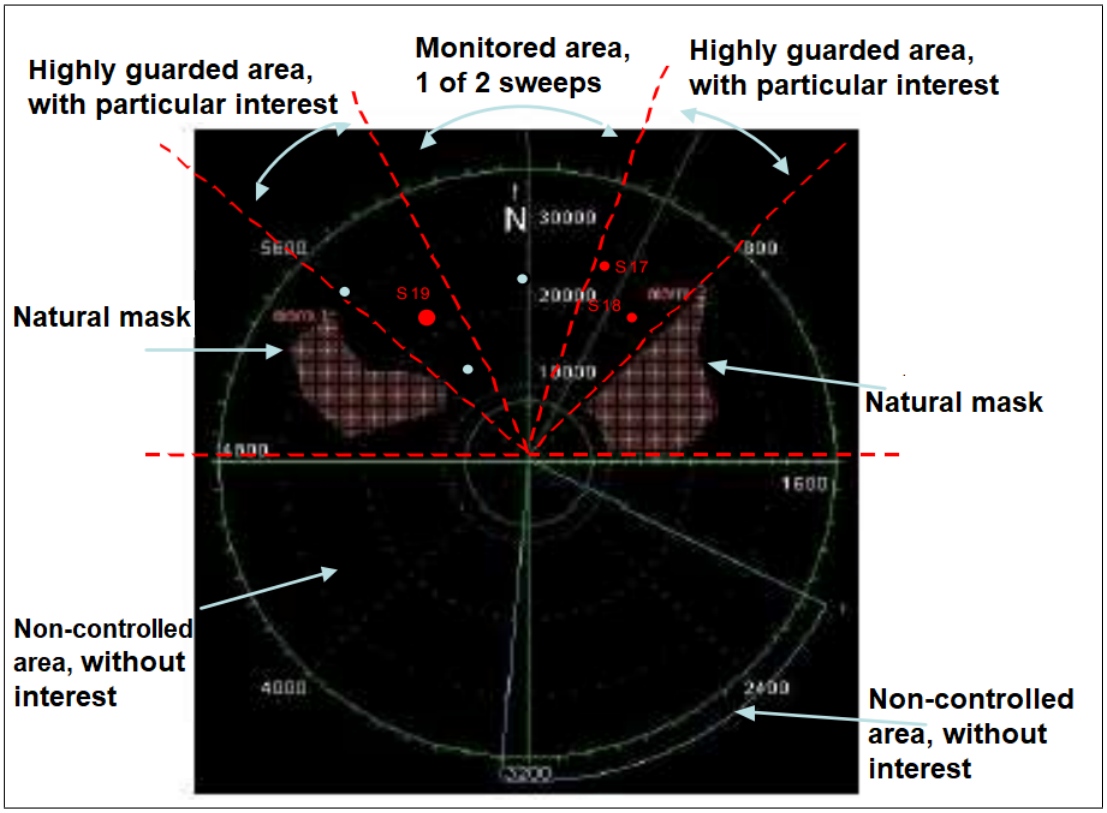


FIGURE 1.14 – Radar detection principle.

Advantages

We discuss hereafter the main advantages of using ground radar :

- One of the most important advantages of radars is that they have a long detection range compared to the other kinds of sensors ;
- Radar does not require any special lighting conditions and is not dazzled by ambient lighting unlike some other type of sensors[25] ;
- Unlike other type of sensors, the radar offers detection, classification and identification of intruders with a very low rate of false alarms ;
- Radars can detect intruders even those hidden behind obstacles or other objects, unlike multimedia sensors ;
- Suitable as a border security solution in both peacetime or wartime thanks to its large detection range which informs us of what is happening faraway from the borderline ;
- Its energy autonomy is higher as it is generally supplied by the vehicle on which it is mounted. Therefore it provides a continuous surveillance on 360 ° space direction.

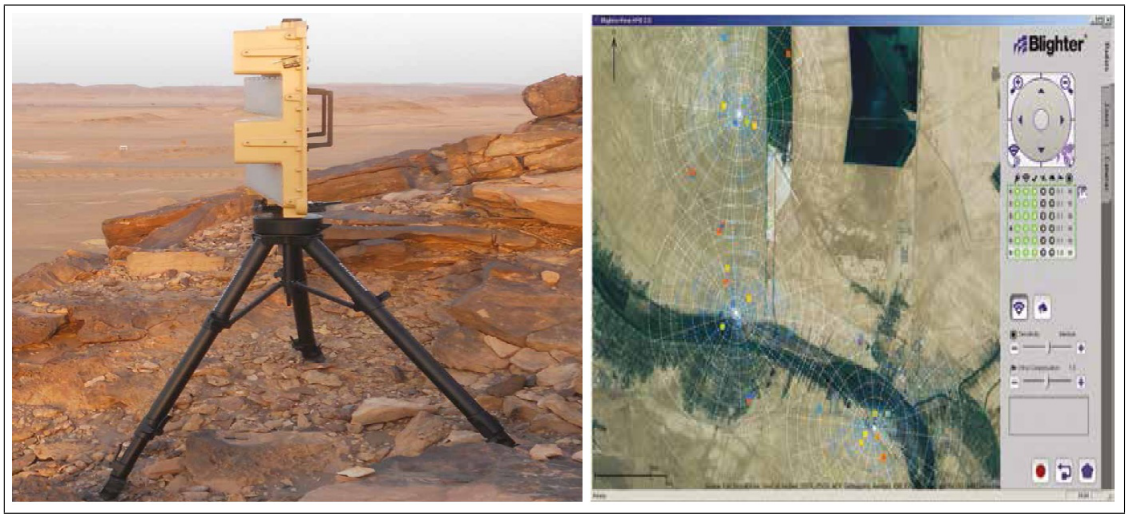


FIGURE 1.15 – The Blighter radar.

Disadvantages

However, radars can suffer from classical issues :

— Even radars inform you on what's happening in their range, they can never distinguish between friend forces and enemy forces, for this reason they should be combined with other technologies to ensure an efficient border surveillance ;

— Requires special preparation of the infrastructure that will house the radar (protection, power energy,...etc) ;

— Characterized by an expensive deployment.

— In addition to that, radars can lose their efficiency in certain rough terrain, as they suffer from the problem of interference.

1.9.3 Multimedia sensors

Also called "imaging sensors", "optronic sensors", "visual sensors", or "Optical Surveillance Systems (OSS)". These type of sensors are equipped with cameras and microphones to produce multimedia content such as images, videos and voices. On the technical side and according to [26], camera motes have different capabilities, whether in resolution, processing power, storage, and other features. They enjoy different functionalities and play different roles in the area where they are deployed. For example, low resolution cameras can be used at the lower-tier of multi-tiers network for simple object detection task to exploit their low-power consumption feature that allows them to be turned on most of the time (or in duty cycle manner). Cyclops, CMUCam3, and eCam

FIGURE 1.16 – The R20SS radar.

are examples of low-resolution cameras. Intermediate and high resolution cameras can be used at higher-tiers of the network for more complex and power-consuming tasks, such as object recognition and tracking. These types of cameras consume more power and hence there are only woken up on-demand by lower-tier devices. Web-cams, attached for example with Imote2, can be considered as intermediate-resolution cameras, while Pan-Tilt-Zoom (PTZ) cameras are an example of high-resolution camera. Figure 1.17 shows commercial product examples of camera mote platforms used in WMSN for controlling areas of interest.

Almost all of the solutions dedicated to the surveillance of borders, cameras are mainly used for identification of detected targets. They are remotely controlled by the operators of the command center who manipulate them during the tracking process.

From a functional point of view, we can distinguish between two categories of multimedia sensors that are : the day optronic sensors and the optronic sensors for night vision.

— *Day optronic sensors :* work according to the same principle of the human eye. However, the camera shoots 24 frames per second which creates the illusion of

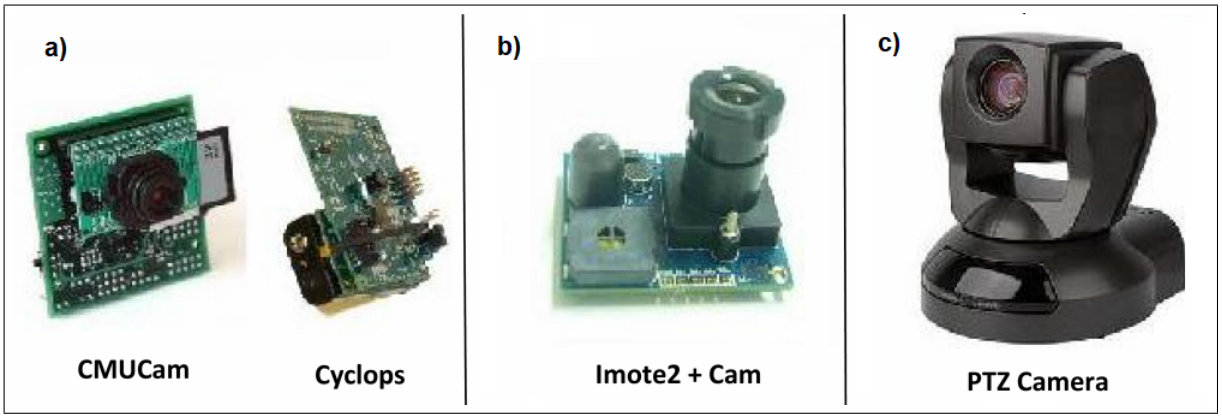


FIGURE 1.17 – a) : Low-resolution Camera ; b) : Intermediate-resolution Camera ; c) : High-resolution Camera.

movement. Whether it is the eye or the camera, these detectors must receive sufficient light. Otherwise, they cannot produce an image. In dark environment or at night time, these cameras are not operational unless an artificial light is emitted.

— *Optronic sensors for night vision :* This type of cameras provide infrared cameras and thermal ones. IR radiation is an electromagnetic radiation of the same nature as visible light. However, its wavelengths are too long to be visible by the human eye. This is because our vision is limited to a very small portion of the electromagnetic spectrum, while thermal energy has a longer wavelength than that of a visible light. It is thus possible to see all the objects having a temperature above absolute zero because they naturally emit heat. The infrared detection therefore makes it possible to see beyond the visible. That is, to form images when light in the visible part of the spectrum is rare or absent [27]. These cameras are completely different to usual day cameras. In fact, we call them "cameras", but in the truth they are sensors, they produce images from the heat given off, and not from the visible light. Heat and light are both part of the electromagnetic spectrum, but a camera capable of detecting visible light is not capable to pick up thermal energy, and vice versa. Thermal camera is used to measure the thermal emissions of a target and can detect temperature failures on an electrical installation, insulation defects and thermal leaks on a building, as well as the presence of individuals in a secure perimeter, or the source of a fire in a dense forest.
The infrared camera is mainly used in a dark environment with additional lighting to film night scenes intended for television, for instance. They can also be found in the market as infrared light cameras, they try to generate their own reflected light by projecting a beam of near infrared energy, which becomes no-

FIGURE 1.18 – Combined day and night optronic system.

ticeable when reflected back from an object. The Figure 1.19 -a) shows an image taken by a thermal camera. On the other hand, the Figure 1.19 -b) shows an image taken by a camera with an infrared flash.

In the following, we discuss the main advantages and disadvantages of using imaging sensors in border surveillance architecture.

Advantages

- Used in most border surveillance architectures deployed around the world as a means of identifying intruders ;
- By identifying the intrusion, multimedia sensors achieve to reduce the number of false alarms observed when using scalar sensors ;
- Thanks to the advantages of advanced thermal imaging, night cameras can provide images / videos in poor lighting conditions or even in poor weather conditions ;
- Can be easily embarked (embedded) on Unmanned Aerial Vehicles or land vehicles which gives them the option of mobility, a very important concept in a border surveillance architecture ;

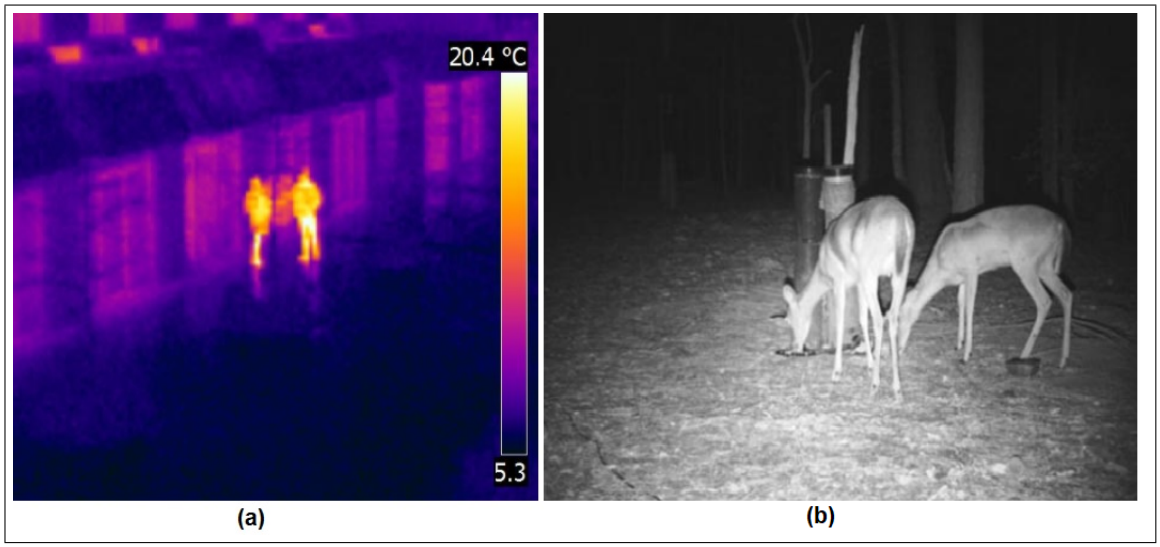


FIGURE 1.19 – a)- Image taken by a thermal camera ; b)- Image taken by a camera with infrared flash.

Disadvantages

- They depends on other types of sensors to ensure the first important task of a border surveillance solution which is the early detection of an intrusion ;
- Their cost is higher than for scalar sensors.
- Suffer from certain challenges such as the quality of service (resolution of the images / videos provided) and the transmission of multimedia data which is a serious issue in terms of network bandwidth ;
- In addition to that, multimedia sensors suffer from other major disadvantages which are the reduction of visibility in bad weather conditions and the limitation of the field of vision in certain situations.
- Like radars, this kind of sensors require special preparation of the infrastructure that will house them such as protection, power energy supply,...etc.

1.9.4 Unmanned Areal Vehicles

In accordance with the definition given by the International Civil Aviation Organization (ICAO), an UAV, commonly called drone, is simply an aircraft without a human pilot on board (See Figures 1.20,1.21). Even though they were reserved for military and defense applications for a long time, civilian drones have been appearing for the past ten years. From a simple toy to a powerful tool for aerial photography, drones are multiplying and diversifying. Innovation makes it possible to create drones

that are useful in many areas such as trade (delivery), helps in disasters, journalism, agriculture, ... etc. According to a report published by the Congressional Research Service in July 2010, there are two different types of UAV : drones and Remotely Piloted Vehicles (RPV). Both drones and RPV are pilot-less, but drones are programmed for autonomous flight. RPV are actively flown remotely by a ground control operator. UAV are defined as a powered aerial vehicle that do not carry a human operator. They uses aerodynamic forces to provide lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry lethal or non lethal payloads. Both types of UAV have played key roles in recent conflicts over the world[28]. In border surveillance architecture, UAV have been deployed to ensure an automatic detection and to track illegal border crossing.

In most of the existing border surveillance solutions, UAV are often combined with other types of sensors such as UGS or cameras to provide a reliable border surveillance architecture. Regarding the different categories of drones, there are many types of aircraft that differ according to several criteria such as weight, speed, steering system, flying autonomy and propulsion.

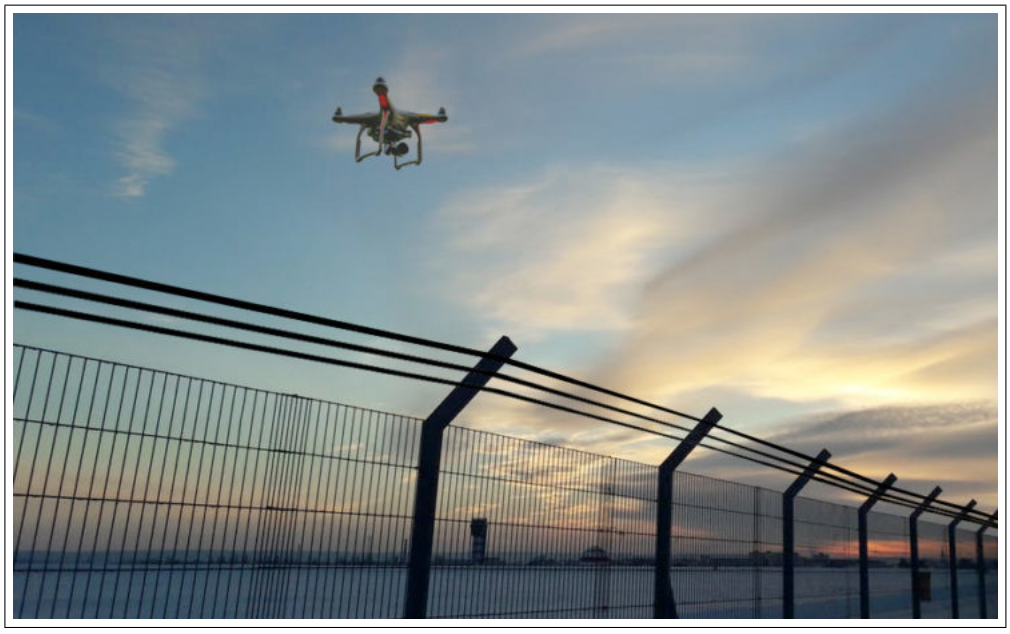


FIGURE 1.20 – UAV over a border-line.

We discuss hereafter the main advantages and drawbacks of using UAV in a border surveillance system.

Advantages :

- One potential benefit of using UAV is that they could fill a gap in border surveillance by improving coverage along remote sections of borders, especially when vast areas are to be monitored ;
- With their onboard sophisticated cameras, drones can provide precise and real-time multimedia content to a ground command center operator, who considers this information to take appropriate decisions, like deploying a border patrol quickly to the area of interest ;
- Some UAV, such as the "Predator B" used along the southern US border can fly for more than 30 hours without having to refuel, compared with a helicopter's average flight time of just over 2 hours ;
- Can reach a high altitude to avoid obstacles such as towers, antenna masts, ... etc without affecting its communications capabilities.

Disadvantages :

- UAV are hardly operational in inclement weather conditions ;
- As the distance with the command center may be important, the loss of connectivity as well as signal interferences which can disturb the communication ;
- Surveillance drones suffer from a major problem relating to the regulations which prohibit the flight in urban areas or near sensitive sites, in order to avoid affecting certain citizens freedoms, in France for example, the General Direction of Civil Aviation (DGAC) has banned night piloting for drones, which prevented the SNCF from being able to monitor its railway lines against night stealing and materials damage ;
- Most of the drones available on the market, suffer from the common issue of batteries power supply during the execution of the overflight mission, which requires them to comeback to the base station when their batteries level decreased.
- UAV are more subject to damage and failures.
- Drones can be hacked or used to hack other electronic devices, a hacker can hack a drone and use it for his own purposes, in addition to that, he can take an entire control of the drone.

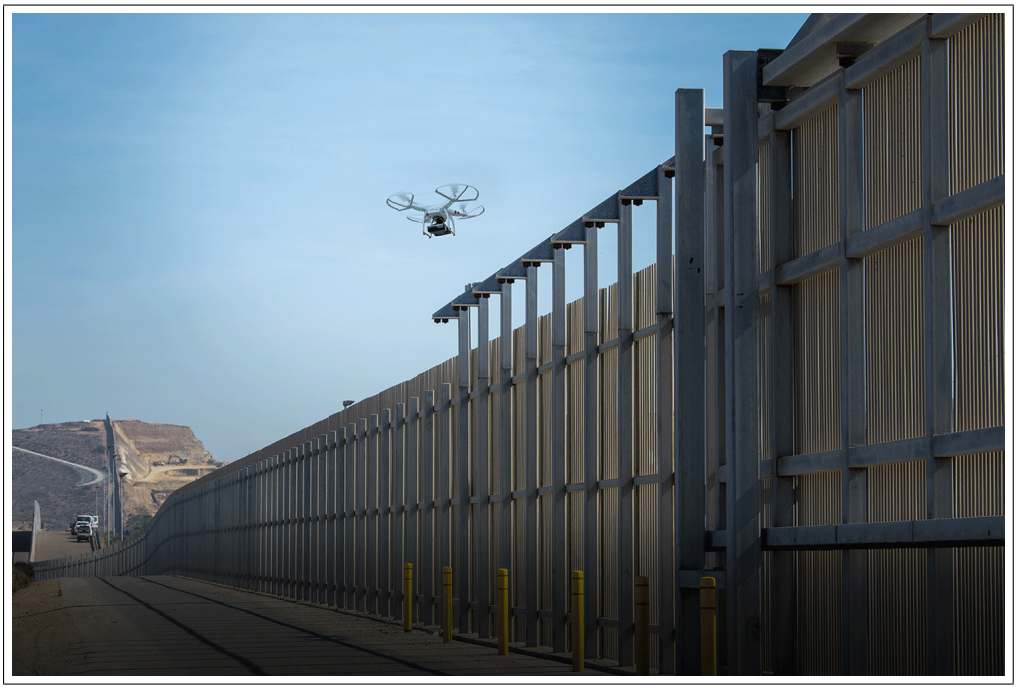


FIGURE 1.21 – UAV patrol over a part of the US border.

1.10 Conclusion

In this chapter, we have defined and described the basic physical architecture of a WSN and its functionalities. Besides, we discussed their characteristics and the constraints and the challenges they are facing, with a specific regard on energy consumption. The different deployment strategies in WSN have been presented, as well as a classification of their different dedicated applications. An overview has been given on the WMSN as well as their different aspects. We have then focused on the different types of sensor nodes used in WMSN in the context of border surveillance applications. The next chapter details further the concept of border surveillance by surveying the related works.

Chapitre 2

Border monitoring : An Overview & State of the art

2.1 Introduction

Today, detection of border intrusion and illegal activities becomes a crucial concern for any country or organization over the world. Indeed, governments have to facilitate travelling and trade so that economies continue to grow while preventing the entry of dangerous entities such as drugs and firearms. The mission of securing borders becomes even more difficult if the area of interest is rough and large. When we take a look at border surveillance techniques, we find that methods based on technology such as WSN, radars, ... etc, have quickly replaced conventional approaches based on trenches, walls insulation, ... etc. A reliable border intrusion detection system should provide a large coverage, lower energy consumption, real time crossing detection, and use efficient tools to report crossing information and tracking intrusions. The basic principle of any border surveillance solution is that each sensor node regardless to its type, has the ability to monitor the nearby area and to collaborate with other nodes to provide information of interest to the command center for decision making. Like other countries in the world, Algeria is today confronted to many security problems at its borders such as fighting terrorism, smuggling and organized crime. Therefore, a huge effort has been invested in the last decade by the Algerian authorities to ensure the protection of their entire borders against any type of threat. In this chapter, we discuss the key features and challenges to consider to design a border surveillance architecture, then, we give a short overview about Algerian borders, which is considered as our area of interest. At the end of this chapter, we give a detailed classification of border surveillance approaches, this

classification represents a broad exploration of the literature in this field. We close this chapter by reviewing the different activation strategies used in the context of border surveillance systems.

2.2 Key features for a border surveillance architecture

Whatever the architecture of the system dedicated to border surveillance, there are some functionalities that should be ensured by the designed architecture [29]. Those functionalities are ensured by a combination of a set of software and hardware components. As a reminder, the main objective of this thesis is to contribute to the reinforcement of the already deployed solution for the Algerian border surveillance. The goal is achieve an almost immediate and precise detection of suspicious elements trying to enter Algerian territory. The solution must allows to identify and to intercept any intrusion as soon as possible in order to be able to control it under the best possible security conditions. In this section, a detailed description of all the needed features for border surveillance architecture is discussed.

- **Data acquisition :** When designing a border surveillance architecture, data acquisition represents a key step that can affect significantly the reliability of the solution. Data acquisition can be either achieved by different types of sensors such as scalar sensors, multimedia sensors, radars,...etc. A detailed description of each kind of these sensors was given in the previous chapter. For data acquisition, two main purposes must be reached, which are observation and early detection. Observation assistance corresponds to the provision of means that can improve short and medium range observation capabilities, in day as in night time. The most popular observation means are cameras, day and night individual binoculars, thermal goggles. In case of intruder presence, an alert is triggered by the sensors in charge of controlling the area in question in order to be sent to the system supervisor.
- **Data classification :** Once the target is detected, sensors used for border surveillance must offer an important functionality which is classification of the detected target. An example of classification, sensors can filter and classify detected objects such as vehicles, peoples and animals, or distinguish between friendly and enemy forces.
- **Data compression :** Multimedia data such as images and video clips represent a large amount of data to be transmitted through the network. Sending a video

clip may require up to 165 megabits of bandwidth. A single recording video for a day requires 07 gigabytes of disk space. This is why the multimedia data must be compressed or fused using specific algorithms in order to reduce its size.

— **Data transmission :** The data captured by the sensors must be transmitted to the processing, recording and viewing systems. This transmission can be done by cable or through air. Wired transmission predominates widely in video surveillance systems. It offers a large amount of bandwidth and reliability than wireless connections. However, wireless data transmission is sometimes required as a solution, for example in the case of monitoring large perimeters such as borders, where the wiring installation could be too expensive, or when areas to be monitored are impossible to reach by cable.

— **Data processing :** Before the sensed information is submitted to a higher level node for decision-making, some treatments are necessary such as fusion of the data coming from several sensor nodes, analysis, retrieval and extraction of useful data from the video sequences. Besides, some treatments can be performed on the content to ease its interpretation. Depending on the application, these processing operations can be either carried out at the sensor level or at the base station level.

— **Data displaying :** The data can be displayed on a map at the end user in case of scalar data, or displayed on screens when videos are captured by multimedia sensors. In this case, usually much of the captured videos are archived and rarely screened. They are reviewed if necessary following an incident or an alert triggered by a radar or a scalar sensor (such as vibration or seismic sensors).

— **Data archiving :** The video-surveillance data archiving period varies according to the needs of the application, ranging from a few days to a few years. On average, organizations retain, video evidence between 30 to 90 days. Although the cost of recording media has dropped considerably in recent years, archiving is often an important part of the infrastructure spending in a video-surveillance architecture. Two types of storage solutions exist : Internal storage : This is the most common form of archiving, it is carried out on hard drives integrated to the sensing devices. Some **ip!** (**ip!**) cameras have a memory card or **usb!** (**usb!**) disk to record hours, some times days of video. Attached or external storage : Archiving is done on external devices to sensor nodes. These systems are **nas!** (**nas!**) or **san!** (**san!**), providing shared storage space between different devices of the architecture.

2.3 Border monitoring challenges

Till today, border surveillance architectures have many challenging features that should be taken into consideration when designing such solutions. These challenges are magnified especially when the technology was involved in critical applications, such as border surveillance. In the sequel, we discuss the main challenges for a border surveillance architecture.

- **Early detection :** In border surveillance, observation and detection are the two first key features that should be achieved by the designed architecture. The latter should ensure a reliable long-range threat detection all day, all night, and in all conditions. Whether the primary targets are people, vehicles or trucks crossing borders, the system should give us an early warning and threat assessment that we need to respond efficiently and effectively. These key features can be achieved by deploying extensively sensors on the area of interest
- **Reliable identification :** Detecting a potential threat is just the first step of the process. Once an intrusion is detected, it must be identified, and its threat level assessed. Without a visual identification of the threat, operators can never discern between false alarms and those that require intervention. For this reason, when designing a border surveillance architecture, it is important to consider tools for identification of intruders such as day and night cameras. It should be noted that some types of cameras can perform the two features (detection and identification of intruders) at the same time.
- **Energy efficiency :** A primary issue that we should consider in the design of any WSN is its power consumption requirements and the supplying sources for energy. Border surveillance applications, require the deployment of sensors in an extended geographical area, which necessitates the deployment of a low-power sensor based architecture that must be fitted with low and long time power consumption components, especially when we are dealing with rough terrain where the accessibility is difficult, which make batteries replacement too costly, if not impossible. To overcome this issue, energy harvesting techniques were largely explored in order to provide energy to battery nodes by extracting this energy from the surrounding environment such as solar power, temperature variations, wind, mechanical vibrations, magnetic fields, ...etc. One of those techniques of energy harvesting called WPT was proposed in this thesis in order to supply UAV batteries during their flight. More details are available in the section reserved to this aspect.
- **Full area coverage :** Designing a border surveillance architecture that ensures a full area coverage is one of the main challenges to achieve. In order to reduce

coverage overlap between sensors, optimization methods should be considered to select the best placement of the sensor nodes in the field [15]. In the literature, several distributed algorithms to optimize sensor nodes deployment were proposed in order to minimize the cost of a full coverage along the area of interest.

— **Moderate deployment cost :** Unlike video surveillance applications designed to monitor limited surface areas such as banks and some sensitive sites, border surveillance requires more resources due to the huge areas to be monitored. This requirement calls the implementation of an efficient, low cost deployment methodology of sensor nodes with the assurance of an acceptable rate of coverage. Another criterion that impacts the cost of deployment is the choice of the technology to be implemented (which kind of sensor should be used,...), which depends on the sensitivity of the designed application. Moreover, in border surveillance applications, the degree of threat varies from one region to another. For example, at the Algerian borders, the north-western border with Morocco represents both an economic and security threat. Economic threat due to smuggling of gasoline and other grocery goods and security issue due to illegal immigration, weapons and drogues trafficking especially. When designing a border surveillance architecture, we need to adapt the deployment and the technology to the type of threat and its level. Such a design vision has been neglected by most of the architectures that we have reviewed in the literature.

— **Low false alarm rate :** Whatever the advanced technology used to monitor borders, most of border surveillance architectures suffer from the issue of false alarms when detecting intruders. Sometimes false alarms are generated due to climatic conditions such as wind and rainfall. However, sometimes the system deployed does not distinguish between two different targets such as an animal and a human or between friendly and enemy forces. In such situations, we talk about target classification issue. This problem should be taken into account when designing an architecture for border surveillance in order to achieve a moderate false alarm rate.

2.4 Algerian borders : an overview

The work conducted in this thesis is a part of a project that aims to secure Algerian borders. Through a deep reading of the literature related to this area of research, we found that each architecture or border surveillance solution is supposed to be deployed in a particular area depending on some environment characteristics such as surrounding threats, climate conditions and topography. As these features must be taken into account when designing any solution for border surveillance, we give in the sequel a

brief description of Algerian Borders specificities.

2.4.1 From a geographical point of view

Algeria, which was already the largest country in the Mediterranean area, has been promoted as the largest country in Africa after the partition of Sudan. This vast country by area occupies **2,310,210** Km^2, 14% of which represents the north zone which the denser in terms of population, whereas as the largest part 86% is a desert area where located in the south. The total population is over 45 million inhabitants with a density of 89% in the north and a concentration of 11% in the south. The land borders are spread over more than **6343** km of which 25% constitutes the north border strip and 75% is the south border strip. Due to the high threat concern, the primary priority for Algerian government, is to secure the north-west, south-west and the extreme south borders of the country. The north-east and south-east parts of Algerian borders are geographically similar to the north-west and the south-west parts respectively. In this case, countries that share the same borders are : ***Morocco***, ***Western Sahara*** and ***Mauritania*** for the north-west and the south-west borders. ***Libya* for the south borders**, ***Mali*** and ***Niger*** for the extreme south borders. Border districts (called Wilayas) of Algeria involved in border area of interest are : ***Tlemcen***, ***Naama***, ***Bechar*** and ***Tindouf*** for the north-west and the south-west borders, ***Adrar***, ***Illizi*** and ***Tamanrasset*** for the south and the extreme south borders.

The geographical location of Algeria has seen the emergence of phenomena such as smuggling, drug trafficking, falsification of documents and human trafficking. These phenomena are likely to create difficulties and troubles for the Algerian state. Moreover, the events in the Arab world (called the Arabic spring) since 2011, including the fall of the Libyan regime of Kadhafi that triggered the free flow of arms and unoccupied mercenaries, only served to strengthen the security vacuum in the sahelo saharan zone. This security vacuum that emerged after the crisis in northern Mali particularly aggravates the security risks due to djihadists and transnational criminal terrorist networks, fragile states and ethnic and religious conflicts [30].

As Algeria is a one of the leading countries in the Maghreb and Sahel, the developments in the sahelo-saharan region have become one of their biggest challenges in terms of national security. Indeed, Algeria becomes a transit country for the trafficking of human, weapons, drugs or combatants. Therefore, it is directly or indirectly concerned and affected by this security crisis. The North West, South West, South East and extreme south borders of Algeria are particularly affected by these scourges.

Algerian legislation related to fighting against smuggling has been strengthened by the arrival of the ordinance No. **05-06** of 23 August 2005 related to fighting against

smuggling. This ordinance stipulates the establishment of preventive measures, better supervision of cross-sectoral coordination, the introduction of specific rules for prosecution and repression and an international cooperation scheme. It should be noted that, long years ago, the Algerian-Moroccan border security was reinforced by digging trenches in order to fight against drug trafficking, smuggling and illegal immigration. But, the Algerian government has understood that trenches alone is not enough, a technology based architecture must be deployed to improve the situation.

2.4.2 Characteristics of Algerian borders

The land borders of Algeria stretches over 6343 km, the north-west and south-west borders extend over 2064 km (1559 km with Morocco, 42 km with western Sahara and 463 km with Mauritania). The south and the extreme south borders extend over "3314 km (982 km with Libya, 1376 km with Mali and 956 km with Niger). So, the total length of the area of interest is 2064+3314 = **5378** km. *This information will be useful to estimate the total number of different kinds of sensors needed to cover all the borders.*

This border strip is characterized by rugged and mountainous terrain in the north part and by an extensive desert sand or rock ***Hamada***,***Erg*** in the south part.

According to [31], for several years, Algeria has become a country of destination and transit for nationals especially of African countries. This phenomenon (illegal immigration) has grown on the north-west part (with Morocco) and also on the southern and the extreme southern part of the borders (with Libya, Mali and Niger). Smuggling (groceries, gasoline, etc) and drug trafficking spreads on the north-west borders (with Morocco). It should be noted that, gasoline and groceries go from Algeria to Morocco. However, drugs come from Morocco to Algeria. Finally, weapons and human trafficking spread on the southern and the extreme southern part of the borders, see figure. 2.1. According to the annual report of the Algerian Ministry of National Defense for 2020, published in Jan 2020, more than 70 tons of cannabis resin was seized in Algeria during 2020, of which more than 46% in the North-West part of Algerian Borders and more than 3.6 million of psychotropic tablets. The total quantity of drug seized in 2015 by the Algerian army (People's National Army (ANP)) was more than 128 tons with the arrest of $1,514$ drug traffickers according to the annual activity report of Algerian Army. According to the same report, 314 pieces of weapons (machine guns, semi-automatic rifles, automatic pistols, rocket-launchers and shotguns) were seized during the same year. With regard to smuggling, the same report indicates that more than 2451 tons of grocery goods, more than 1.3 million liters of fuel and 186 metal detectors were seized. In addition to that, 3085 illegal immigrants were arrested by the ANP detachments and border guards of the National Gendarmerie in the context of illegal immigration,

as long as Algeria is considered as a gateway to the European Union countries.

Regarding climate, according to [29], the north west border is characterized by a Mediterranean climate (at the wilaya of Tlemcen) and a continental climate (at the wilaya of Naama). the south-west and the extreme south borders are characterized by a desert climate (Saharan). The Mediterranean climate is characterized by a dry summers and a mild, moist winters, winter temperatures vary between 8 and $15°C$, they climb to $25°C$ in May to get an average of $28°C$ to $30°C$ in July and August. The continental climate is characterized by a cold winter and a warm summer, in the winter, temperature vary between -12 and $07°C$, in summer it vary between 25 and $38°C$.Finally, the desert climate which is a hot, dry in summer and very cold in winter, it is also characterized by exceptional and very irregular rains . They often fall with a bang, destroying and burying everything in minutes. Daytime temperatures reach 45 and even $50°C$ in summer, in winter, nights are very cold, when it freezes often.

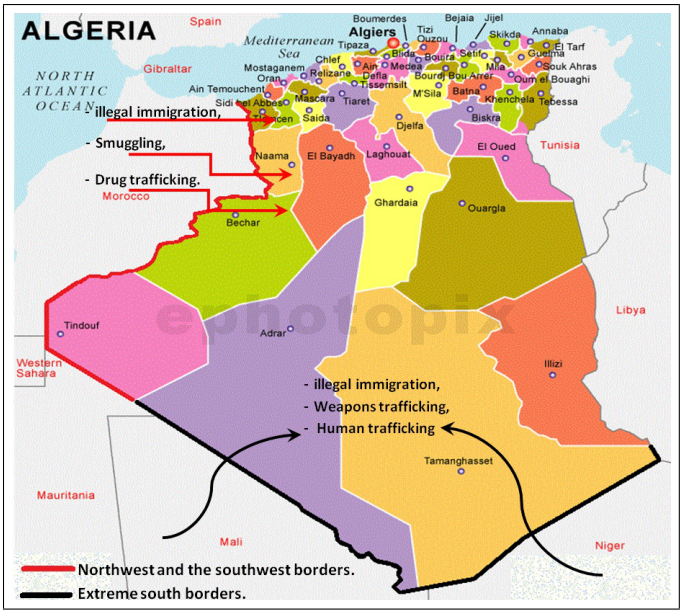


FIGURE 2.1 – Algerian borders and the various surrounding threats.

2.4.3 Principal threats surrounding Algerian borders

Compared to neighbouring countries, Algerian borders are concerned with more polarizing threats that principally touch two primordial sectors which are security and economic. Most of bibliographic references in this subject talk a lot about the security issue at the Algerian borders and ignore the negative impact of this phenomena on the national economic. In the following we will try to address the most important kind of

threats surrounding Algerian borders, which are : transnational terrorism, smuggling and drug trafficking.

— **Transnational terrorism :** The cross-border fight against terrorism has always been at the heart of the Algerian state's priorities. The deterioration of the security situation in neighbouring countries has put the borders of Algeria in a very worrying situation, requiring a great vigilance from the ANP forces to guarantee the security of the country and protect the integrity of the national territory. In May 2014, General Boualem Madi, director of communication of the staff at the Ministry of Defense, said that the key factors in the fight against cross-border terrorism include the means available to the elements of the ANP whose priority is the fight against terrorism and organized crime, and in cooperation and coordination with the security services of neighbouring States [32]. In particular, and in this context, the Libyan crisis on the eastern border of Algeria worries the public powers, they fear the incursion of armed groups from Libya. The main obsession of the Algerian state is to protect the gas installations that are on the Algerian-Libyan border. The state wants at all costs to avoid the scenario of an attack on the model of that which occurred at Tiguentourine-In Amenas, in January 2013 (a massive hostage-taking led by a dissident Islamist armed group of AQIM), which explains the intense deployment of the Algerian army around these facilities. But according to official sources of the Algerian government, the real weakest security link in the region is Tunisia. The Algerian government absolutely wants to prevent its neighbour from falling into a logic of civil war and terrorism as the case of Syria or Iraq. It would then be feared that major Algerian cities at the border are within reach of attacks by terrorists from Tunisia, and the Algerian state wants absolutely to avoid this scenario. That is why there is intense cooperation between the security authorities of both countries[33]. This observation was confirmed by the huge activity of the armed forces of the two countries where we have registered several joint operations, among which, the one resulted in the neutralization of three (03) terrorists by the National Gendarmerie of Algeria after they had fled the Tunisian territory in 2017's summer. *Given this situation and given the geographical spread of Algerian borders shared with the countries of the Sahel region (more than 3,000 km of borders), Algeria needs a powerful mechanism for controlling and monitoring its borders.*

FIGURE 2.2 – The gas facility of Tiguentourine, victim of a terrorist attack by AQIM in January 2013.

— **Smuggling :** At the Algerian borders, smuggling is a phenomenon that is not recent but is growing every year. This phenomenon mainly targets fuel and consumer food products. It is important to note that this phenomenon affects products subsidized by the Algerian state (fuel, milk, olive oil, ...). But for the Algerian government, the smuggling of fuel is the real headache. According to former Algerian Interior Minister Dahou Ould Kablia, 25% of national fuel production is wasted and illegally exported to the borders. In an official statement, the former **ceo!** (**ceo!**) of the national company of marketing and distribution of petroleum products (Naftal), Mr. Hocine Rizou indicated that the smuggling of fuels, all types, makes lose Algeria two (02) million tonnes of these products annually. According to conclusions of a new Atlantic Council study on fuel smuggling, quoted by the British newspaper The Guardian, nearly 660,000 Moroccan and Tunisian vehicles consume Algerian fuel, nearly 13% of the total fleet in these two countries. I remember that during a working visit that i made to the city of Tlemcen in June 2012 (located in the north-west of Algeria) it was difficult if not impossible to find an open fuel station after 09 o'clock in the morning, the entire amount of fuel allocated to this city is sold at the first hours. To deal with this scourge, the Algerian government has taken a series of precautionary measures such as the significant increase in fuel prices during the drafting of the 2017 finance law, where a liter of diesel costs 20.63 Algerian Dinar, against one (01) Euro in Morocco and 0.7 Euro in Tunisia. These show that this increase is insignificant compared to the cost of the gasoline in neighbouring countries which motivates smugglers to engage in this type of illegal activity.
As a result, the Algerian government has recently adopted a battery of measures to strengthen the protection of its long land borders. According to 2016's National Gendarmerie activity report(published in a press release), the number of

smuggling cases was **5249** cases, which resulted in the arrest of **1875** people, the most affected cities are : **El tarf**, **Souk ahras**, **Tebessa** (eastern border zone), **Tlemcen** (western border zone), Tindouf, Tamanrasset, Adrar, El Oued et Illizi (southern border zone). The table 2.1 summarizes the activity of the National Gendarmerie in the fight against fuel smuggling (2016's activity report of the National Gendarmerie).

City	**Seized quantity (liter)**	**Percentage**
$Tebessa$	629538	46.27%
$Tlemcen$	284248	20.90%
$Soukahras$	144181	10.60
$ElTarf$	83611	6.14%
$Adrar$	135920	9.99%
$Tamanrasset$	69160	5%
$ElOued$	9227	0.67%
$Illizi$	3750	0.27%
$Tindouf$	1020	0.16%

TABLE 2.1 – Fuel smuggling :2016's activity report of the National Gendarmerie.

Table 2.2 summarizes the activity of the National Gendarmerie in the fight against products smuggling (2016's activity report of the National Gendarmerie).

Product	**Seized quantity**
$Food\ stuffs$(tonnes)	2683,862
$Cigarette(packages)$	323385
$Alcoholic\ beverages(bottle)$	51143,18
$livestock(head)$	4445
$Clothingeffects(Article)$	230179
$Electronics(Article)$	21360
$Cosmetics(Article)$	969832
$HardwareProduct(Article)$	11629940
$Vehicles(Unit)$	834

TABLE 2.2 – Products smuggling :2016's activity report of the National Gendarmerie.

— **Drug trafficking :** Due to its high security reinforcement, the Algerian-Moroccan border is probably the least unstable of all Maghreb borders. However, this part of border remains the vector par excellence of drug trafficking. According to an

article published in May 2009 by the Algerian daily Refexion, Tlemcen, Naama and Adrar, border regions with Morocco, have become an important axis for inter-Maghreb drug trafficking. Moreover, the last years Algeria has moved from being a transit country to a drug consumption market. Pointed the finger, Morocco does not seem particularly concerned about the activities of drug traffickers on its borders with Algeria. Rabat rarely announces arrests of traffickers trying to smuggle drugs across the border. However, the Royal Gendarmerie has arrested many drug traffickers and is seizing large quantities of cannabis resin destined for the European market. Algeria has recently adopted a battery of measures to strengthen the protection of its land borders with Morocco. In addition to the strengthening of border guards forces by the deployment of additional number of Gendarmes, the Algerian government has launched the construction of trenches along the border strip with Morocco, parallel to the famous fence wall built by Morocco and funded by the European Union to curb the flow of illegal immigrants.

According to the communications officer of the National Gendarmerie, no less than 80 breaches are opened, including eight in Maghnia, by the drug traffickers to pass the fence wall, for the trenches they use planks of a length of six (06) meters to transgress borders. According to 2016's National Gendarmerie activity report, 4127 cases of drug trafficking which represent 28.10% of organized crime, were recorded in 2016. In this context, more than 79 tons of treated kif, 517,056 psychotropic tablets and more than 43 kg of cocaine were seized in the same year, which resulted in the arrest of 6284 people. The wilayas of Tlemcen (33,523 tons), Naama (9,555 tons) and Bechar (8,702 tons) are the most affected by this phenomenon. To cope with this situation, the Algerian government finds itself forced to deploy more sophisticated means in terms of technologies to monitor efficiently its borders.

2.4.4 Organization and deployment of Algerian border troops

Due to the huge length of the Algerian borders, Border land control and surveillance are carried out by the contribution of four institutions each within the scope of their prerogatives and in coordination with each other. Those institutions are : the National People's Army ANP, the Nationale Gendarmerie National Gendarmerie (GN), the police, and the Algerian Customs. However the ANP and the GN are the two institutions that address the various threats such as terrorism, illegal immigration, smuggling and all kinds of cross-border crimes. Police, and the Algerian Customs ensure in generally the management of check points (controlling passengers). In this section we discuss the organization and the deployment of the ANP and the GN groups responsible for

securing borders.

— **National People's Army :** The missions of the Algerian army cover the aspects related to National Defense for surveillance and border control. This mission is affirmed by article 82 of the Algerian Constitution specifying that the ANP has a permanent mission to safeguard national independence and sovereignty, to defend the unity and territorial integrity of the country. The ANP participates in border surveillance through the Border Guard Units (BGU) of the land forces. These units give the necessary help to the National Gendarmerie border guards. BGU can make arrests in their areas of competence. They carry out an intelligence monitoring mission along the land borders. To improve its missions, the Algerian army opts for a strategy reconciling its modernization and professionalization [31]. Due to threats such as the proliferation of what is called AQIM which became more active in the Saharan region, in addition to illegal immigration, smuggling and drogue traffic through the north-west Algerian borders with Morocco, the ANP has introduced a new military strategy designed to restrict movement through the volatile border regions that Algeria shares with Morocco, Niger, Mali and Mauritania. Algeria has practically doubled the number of soldiers deployed in these areas. Algerian military forces in these regions fall under the command of the 6^{th} and the 3^{rd} military regions, headquartered at Tamanrasset and Bechar respectively.

FIGURE 2.3 – Algerian National People's Army.

— **National Gendarmerie Border Guards :** According to [34], the participation of the National Gendarmerie in the surveillance and the control of the borders is done through the Border Guard Corps (CGF). It was created by decree number : 109/77/SG/A1/S of 17 November 1977, and attached to the Command of the National Gendarmerie by Decree No. 91-04 / PR of 8 January 1991. Its missions

and its organization were fixed and specified by decree number :$91 - 05/pr$ of January 8, 1991. Following the Decree number $143/09/pr$ of April 27, 2009, the Border Guard Corps has undergone a change in its official name to be called : CUGF. It is responsible for preserving the country's land borders. As such, it carries out defense and police missions. With regard to the defense mission, the CUGF is responsible for : Permanent monitoring of border areas ; the collection and transmission of information of any kind for the benefit of the military authority ; the observation and detection of any incursion likely to affect the integrity or security of the territory ; prohibition and neutralization of any movement tending to undermine border security ; and the preservation of the elements of the land materializing the boundaries. In terms of police mission, the CUGF is responsible for : the control of people and goods circulating in the border area ; the prevention and repression of illegal immigration ; smuggling activities and drug trafficking. Finally, the CUGF is organized in the form of a regional commandment, groups and squadrons deployed in advanced posts. These groups no longer use, as in the past, traditional means but electronic surveillance devices have been installed on a stretch of nearly 1,000 km of the Moroccan borders. New identification systems such as the **afis!** (**afis!**) is in use.

FIGURE 2.4 – A deployed squadron of CUGF.

2.5 Classification of border surveillance approaches

In the recent past, conventional methods were used over the world for border surveillance. These methods call the use of : *physical obstacles* such as (trenches, fences and walls (figures 2.5) and 2.6), *human patrols* (pedestrian or in vehicles), *permanent or temporary immigration checkpoints* (to detect illegal aliens, drug, and other illegal activities), and finally *manned aircraft*. Such techniques can be used separately or combined to provide a high level of border security, depending on the type of threat, the sensitivity and the geographical nature of the area. However, they require the deployment of an extensive human resources especially when the borders are very large and subject to intrusion and contraband activities. Years ago, the proliferation of cross-border crimes over the world, has pushed quickly the use of technology to secure borders. For this reason, conventional methods were progressively abandoned and being replaced by new technologies which are either used separately or combined to achieve border surveillance requirements.

FIGURE 2.5 – Example of conventional border surveillance methods.

When taking a look at the literature related to border surveillance, we can distinguish between two principal categories : the first one is the researches such as journal and conference paper publications that a big amount among them haven't been implemented in practice ; the second category is border surveillance systems deployed in real

world and implemented to secure borders of a particular country. In this chapter, we give a non exhaustive list about both recent researches in the field of border surveillance as well as border surveillance systems that already have been deployed by army forces over the world.

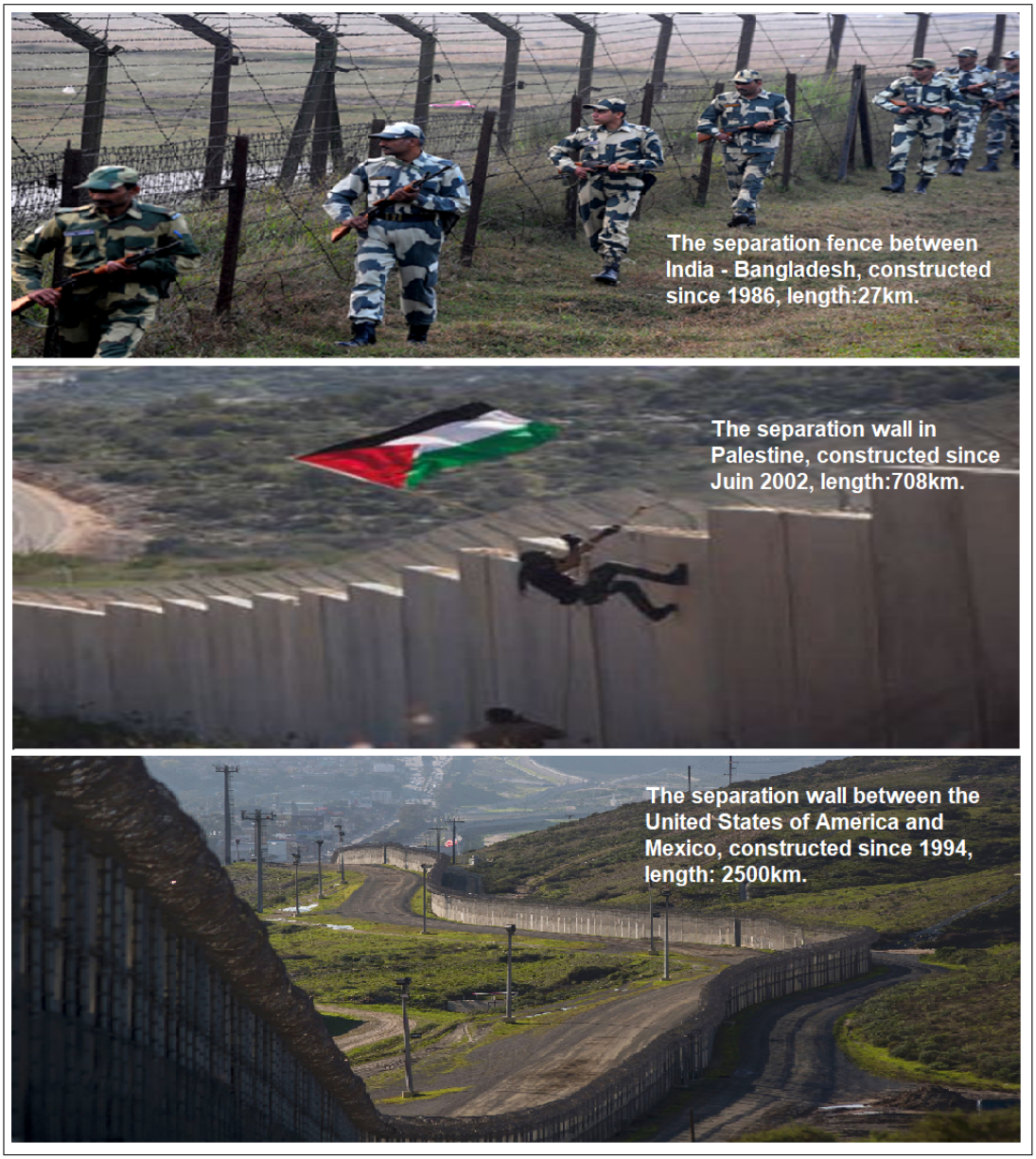


FIGURE 2.6 – Another example of conventional border surveillance methods.

In the following we will try to give a detailed classification of border surveillance approaches. For organizational reasons, we classify them into five principal categories, which are :

— (i) Wired sensors based technologies(such as fiber optic sensors) ;

— (ii) Wireless Scalar Sensor based technologies ;
— (iii) Wireless Multimedia Sensor based technologies ;
— (iv)Radars based technologies ; and
— (v) Combined technologies (hybrids).

In the following, we discuss the related works of each category that includes only theoretical research works published in the literature. Such works have not necessary been deployed in practice to secure the borders of a particular country or the perimeter of an organization. Border surveillance solutions (systems for border surveillance) that have been deployed in practice are addressed in the next section.

2.5.1 Wired sensors based technologies

This is an old method for securing borders. The most popular wired based technology for border monitoring is the one based on Fiber Optic Sensing technology or sometimes called distributed fiber optic sensing. This technology exploits the physical properties of light when it travels along a fiber to detect changes in temperature, strains, and some other parameters. According to a report recently published by the *viavi solutions company* on its website, fiber optic sensing utilizes the fiber as a sensor to create thousands of continuous sensor points along the fiber. A fiber optic cable can act as the communication path between a test station and an external sensor, which is known as extrinsic sensing. However, when the fiber itself acts as the fiber optic sensing system, this is known as intrinsic fiber sensing. The devices measuring the fiber itself are generally called interrogators. Temperature and strains are measured using Raman and Brillouin Distributed Fiber Sensor techniques. This kind of technology was used in several domains such as oil and gas stations, pipelines, electric utilities, telecoms cables and even in border surveillance.

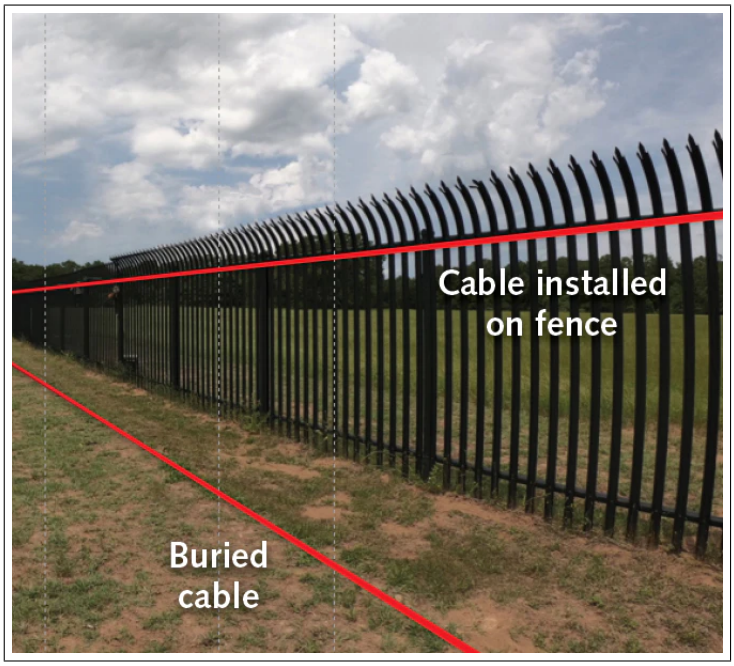


FIGURE 2.7 – Fiber-Optic sensing technology.

- In [35] a technology based on Buried **fos!** (**fos!**) to secure borders was proposed. Seismic sensors that can measure pressure waves in the earth caused by intruders were used. Seismic sensors were one of the first sensor technologies to be considered 40 years ago.

- In [36], a technique called OptaSense was proposed to detect intruders crossing an area of interest. This technology based on a **das!** (**das!**) system is an acoustic and seismic sensing technology that uses simple fiber optic communications cables as a sensor. It provides sensitivity to strain on commercial cables by measuring the change in length and index of refraction of the fiber induced by the acoustic or seismic waves around it. As depicted in figure 2.7, fiber optic cable can be installed on fences or buried underground. *However, the implementation of such system requires the deployment of a single wire along the border to ensure sensors interconnection with the command center. Therefore, the occurrence of any single point-of-failure can affect the communication. Moreover, deploying wired sensors a long borders is very expensive and difficult especially in harsh environmental conditions. Also, the use of fiber optic seismic sensors alone without other technologies can generate a very high amount of false alerts. Finally deploying this kind of technology for border surveillance can never reach the principal operational requirement which is the early detection, since this kind of technology detect the intruder when he crosses borderlines, which is too late for decision making.*

2.5.2 Wireless Scalar Sensor based technologies

- In order to support the ability to track the position of moving targets in an energy-efficient and stealthy manner, a ground surveillance system based on the detection of the magnetic field generated by the movement of vehicles and magnetic objects was proposed in [37]. According to the author, the main goal of this work is to alert the military command and control unit in advance to the occurrence of events of interest (presence of moving vehicles) in hostile regions. To reach this goal, a 70 tiny sensor devices, called $MICA2$ *motes* are deployed along a 280 feet long perimeter in a grassy field that would typically represent a critical choke point or passageway to be monitored. Each of the motes is equipped with a $433MHz$ Chipcon radio with 255 selectable transmission power settings. The sensed information is routed to a base station attached to a portable device which is mainly used for visualization. Sensors that detect the same event join the same group and report sensed information to the leader of their group. Tracking is ensured by allowing each mote that has sensed an event to report its location and other relevant information about the event to the base station. The base station can then filter out the false alarms and infer the location of the event from the genuine reports (complex processing is deferred to the more powerful base station instead of the sensor itself).

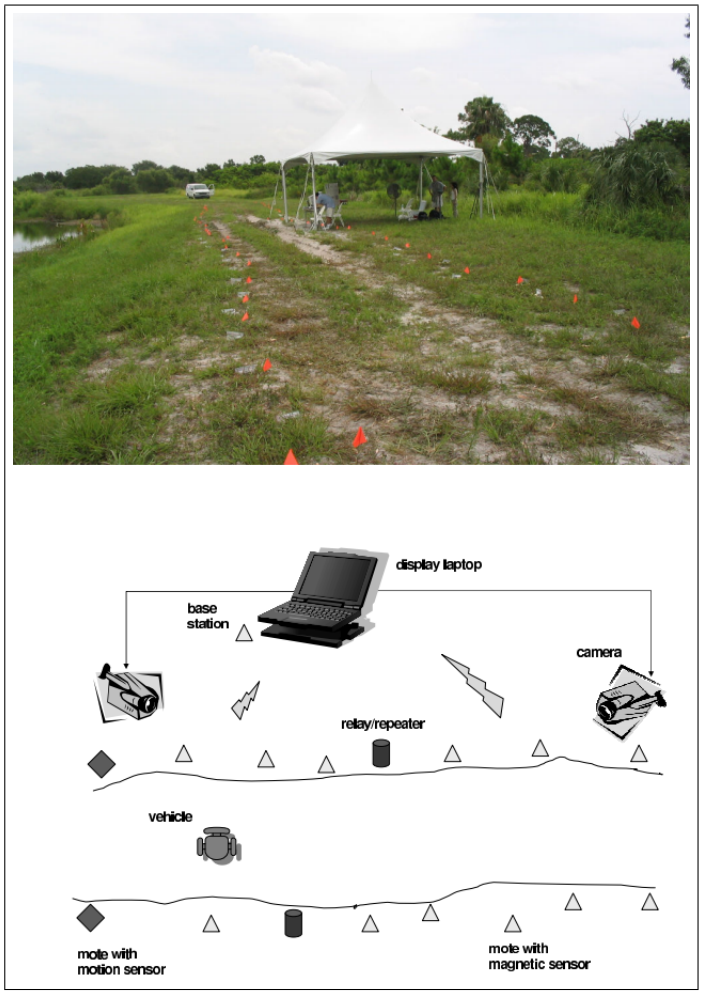


FIGURE 2.8 – Magnetic wireless sensor network for border surveillance.

Even though experiment results show that these sensors can sense a small magnet at a distance of approximately 01 ft and slowly moving passenger vehicles at a distance of approximately 08-10 ft, this detection ability is not practical at all, because of the late detection (at 10 ft) which does not give the required time to take the appropriate decision. Add to that, detection of individuals is not addressed in this study as,only vehicles detection is considered. Finally, the author state that the their solution uses cameras controlled by a laptop (see figure 2.8) when triggered by the sensor field. However, no details were given in the paper about this collaboration.

- To detect, identify and distinguish people crossing borders from other targets such as animals, three kind of scalar sensors namely Acoustic, Seismic and Ultrasonic sensors were considered in [38]. Acoustic sensors are for formants and footstep detection, they are used also to estimate the cadence of walking animals and discriminate between animals and people when a human voice is not detected. Seismic sensors are used for footstep detection and classification of humans and animals. Human detection is achie-

ved by phenomenological features extracted from human voice and its characteristics and also from sounds generated due to footfalls and their cadence, in these cases acoustic sensors are used. Seismic sensors are used to detect footfalls of humans walking within the receptive field of the sensor. Ultrasonic data is processed to count the number of targets in the vicinity using the energy content in various bands of Doppler returned from animals and human (animals Doppler are quite different compared to those from humans). Detection and classification are achieved by Dempster-Shafer fusion of data coming from the sensors. In order to evaluate the different algorithms, 26 scenarios with various combinations of people, animals, and payload were enacted.

Even though the reported results show that the probability of detection for either acoustic or seismic data does not exceed 0.7*, whereas that resulted from fusion of acoustic and seismic information is higher (about* 0.85*), the author does not show how the proposed solution can reduce the rate of false alarms generated by the acoustic and the seismic sensors. Moreover, the short detection range of the sensors used in this work represents a real problem from an operational point of view.*

- In [39], a four layer nodes architecture and a deployment strategy for border surveillance are proposed. The first layer of nodes, called ***bsn!*** *(**bsn!**)*, is in charge of detecting the presence of an event or an intruder. When an intrusion is detected, a BSN reports the data to the nearest node in the superior layer, called a ***drn!*** *(**drn!**)*, that forms the second hierarchical layer of the network. The main role of a **drn!** is to collect the data received from different **bsn!** and forward it to the appropriate node in the higher layer of the hierarchy, called *Data Dissemination Node (DDN)*. The main role of a DDN is first, to pre-process and fuse the received data before forwarding them to the *Network Control Center (NCC)* for analysis and decision making.

Even though this deployment strategy provides mathematical control models to evaluate the performances of the network regardless connectivity and coverage, the proposed architecture is based only on using scalar sensors which may yield many false alarms in certain cases. Indeed, while the deployment of UGS is not costly, the efficiency of UGS based systems is often limited due to the high rate of false alerts and classification errors. More works related to using Unattended Ground Sensors for border surveillance are available in [40]. - In [41], a new coverage, called one-direction barrier coverage, which has a great efficiency on directional detection, was addressed. The key problem discussed in this paper is how to let a sensor network know an intruder's direction, if this intruder is an illegal one while ignoring legal intruders. *Unfortunately, some practical difficulties in deploying sensors have not been addressed. The details of the proposed model have not been given too. Add to that, the authors did not report experimental results related to the reduction of false alarms and the determination of the direction of*

crossing.

- In a recent work [42], the authors proposed a solution to provide a round the clock video-surveillance at the places where human deployment is not possible due to geographical, climatic or some other reasons.

To this aim, they combined two kind of sensors which are : Infrared sensors and Ultra-sonic sensors respectively. An IR sensor can measure the heat of an object as well as to detect the motion. This type of sensors measures only infrared radiation, rather than emitting it, that is why it is called a passive IR sensor. Usually, in the infrared spectrum, all the objects radiate some form of thermal radiation. These types of radiations are invisible to our eyes, and can be detected by an IR sensor. The emitter is simply an IR Light Emitting Diode (LED) and the detector is an IR photo-diode that is sensitive to IR light of the same wavelength as that emitted by the IR LED. When the IR light falls on the photo-diode, the resistances and the output voltages will change in proportion to the magnitude of the IR light received. The second type of used sensors (Ultra-sonic sensors) provides very short ($2cm$) to long-range ($4m$) detection and ranging. According to the authors, this sensor provides precise, stable non- contact distance measurements from $2cm$ to $4meters$ with very high accuracy. The sensor transmits an ultrasonic wave and produces an output pulse that corresponds to the time required for the burst echo to return to the sensor. In addition to that two kind of sensors, a POWER SUPPLY, RASBERRY-PI (a small single board computer that can be used for real time Image/Video Processing, IOT based applications and Robotics applications), BUZZERS(mechanical, electromechanical, or electronic transducer) were also used. The system can provide a multiple responses depending upon the position of the intruder with respect to the border fence.

In this solution, the authors discussed three possible scenarios. The first scenario considers a potential intruder in the other side of the border fence and not in the sensor proximity. In this case, the camera just keeps observing without moving itself and no other action is taken. The second scenario assumes a potential intruder in the sensor proximity but not yet crossing the border. In this case, the sensors generate signals which decide the movement and positioning of the surveillance camera such that the potential intruder movement can be recorded. The third and the most critical scenario considers an intruder who finally crossed the border. The video cameras are installed at a distance to continuously keep an eye on the border area and if any movement is detected, the camera positions itself according to the signals sent by the sensors and it is checked whether it is a human or an animal. In case, it is found to be a human the camera starts taking snapshots of the live video. An alert message along with the images is sent to the controller.

In this solution, the authors consider using cameras but no description was given. Add to that, no details were given about the collaboration between the camera and the other kinds of sensors. Finally, the authors consider that 4 *meters is a long detection range for border surveillance applications which is far to be true realistic.*

- In a more recent work, a Mobile Sensor Network (MSN) was proposed to provide a $k - barrier$ coverage probability which can be considered as the intrusion detection probability of an intruder when the latter follows different paths with different angles relatively to the shortest path to cross the region of interest. In addition to that, the effect of different network variables such as node density, sensing range, intrusion path angle and the ratio of sensor to intruder velocity on intrusion detection probability were also investigated. The deployed MSN consists of independently and uniformly deployed mobile sensors having a random direction mobility pattern to monitor and detect illegal intruders. In this solution, the authors assumed that the intruder follows a straight-line path at a well known angle to cross the Region of Interest (RoI). Mobile sensors have a random direction mobility pattern and they are spread in a rectangular RoI, following a Poisson distribution. As far as $k-barrier$ is concerned, it means that all the intruder routes crossing the RoI are cumulatively detected by at least k distinct mobile sensors. In this case, an intruder may take a zigzag path, a curved path or a highly complex movement pattern to avoid its detection or to maximize the detection time during its journey inside the RoI. Intruders are assumed to be a point object that tries to cross the RoI, moving with a constant speed at a particular angle. To evaluate the system, the effects of different network as well as system variables on intrusion detection probability were experimentally and theoretically analyzed. For simulation results, a rectangular RoI having 100×50 square units of area was considered, where number of mobile nodes having homogeneous sensing range, identical mobility pattern and energy resources are uniformly and independently distributed. Among the analyzed system variables, the influence of k required mobile sensors on $k - barrier$ coverage probability in a Poisson distributed MSN has been investigated. It was observed that the $k - barrier$ coverage probability decreases with the increase of required k at a particular intrusion angle. It is found also that the $k-barrier$ coverage probability improves by increasing the intrusion angle at a given required k. This is because an increase in the intrusion angle makes the intruder cover larger distances, and hence spends more time inside the RoI which augments the probability of its detection. Another variable that was also analyzed in this paper is the effect of movable sensors count and the intrusion route angle at a given value of required k. It is observed that the $k - barrier$ coverage probability in an MSN improves with the increase in movable sensors count for a particular intrusion angle at a given value of required k. *This work aims to calculate the* $k-barrier$ *coverage probability for an intruder travelling inside the RoI from one parallel boundary to another in a MSN. However, no details were given about the sensors mobility inside the RoI, also, the author did not give any specification about the kind of mobile sensors used. Finally,*

the major issue of WSN which is energy saving, has not been addressed at all in this work.

2.5.3 Wireless Multimedia Sensor based technologies

Due to the limited information provided by scalar sensors, multimedia sensors have been used to provide high accuracy in human detection and keep false alarms to a minimum [43]. This includes inter alia surveillance towers equipped with video monitors and night vision scopes, wireless cameras or thermal imaging cameras. *However, using this technology typically requires human interaction to determine the type of intrusion. Moreover, it is assumed that the targets are within the line of sight. If the monitoring area consists of obstacles such as rocks, brushwood, or trees, the failure rate can be important. And last but not least, the use of this technology requires the implementation of a robust mechanism that guarantees energy saving and load balancing to extend the network lifetime. To overcome these issues, this technology must be combined with some other technologies.*

2.5.4 Radars based technologies

In the literature, radars are often used for maritime surveillance, radar based ground border surveillance solutions are addressed only in few works. Among important works in this field, we can quote the work proposed in [44], where a deployment strategy of a bi-static radars network for intrusion detection was introduced. The authors considered that deploying the radar transmitter and receiver separately is more favorable than a mono-static radar to achieve an optimal coverage quality, the goal is to maximize the worst-case intrusion detectability. The proposed optimal placement strategy was compared with a mono static radar network deployment. The vulnerability of a line segment H under the optimal placement of bi-static radars was compared to that of a mono-static radar while varying the number of transmitters and receivers. Numerical results show that the advantage of bi-static radars is significant, which demonstrates that the flexibility to place transmitters and receivers separately is highly beneficial for barrier coverage. *However, this deployment strategy seems to be very difficult to implement, in addition to that, according to the literature, bi-static radars suffer from poor coverage at low altitude because several sites must be on sight.*

2.5.5 Combined technologies

A hybrid technique called **BorderSense**, which is based on three types of sensor nodes was introduced in [45]. Those sensors are : Multimedia sensor nodes (video cameras or night vision scopes) ; scalar sensor nodes (vibration/seismic sensor) ; and finally mobile sensor nodes. *The authors reported that this technique achieve to reduce significantly the rate of false alarms. However, because of the complex underground channel characteristics, the use of underground sensors in this architecture requires a new physical layer to handle signal propagation so that to implement reliable communications. Add to that, to deal with the unidirectional sensing of the cameras, the authors have suggested the use of a rotating mechanism to direct them, but the feasibility of this solution has not been discussed. Also, we report a lack of a coordination between the cameras and the ground/underground sensors. Indeed, the latter need to report the intrusion information directly to a random camera tower that covers the field without running any selection process beforehand that can help to manage the energy of the available cameras while ensuring a load balancing. Finally, this solution suffer from a principal issue which is the limitation of the detection range of the sensors (few hundreds of meters), which is not practical for a border surveillance mission, that requires earlier detection information.*

In [46], an heterogeneous architecture that combines UAV with UGS was addressed. When the UGS detects an intrusion, it sets off an alert, then an UAV is directed to the site subject of alarm. Similar architectures for border surveillance techniques using UAV and UGS are presented and discussed in[47, 48]. *The use of UAV and UGS in border patrolling, can make the control process independent of human intervention. However, this kind of techniques suffers from some issues such as a low rate of reliability and availability of the system especially when UGS are subject to failures. Therefore, the need of a strict deployment strategy in this case is more than necessary.*

In a recent work presented in [49], a system called Smart Border surveillance system was proposed to insure border intrusion detection. Based on infrared sensors and camera sensors, when an intrusion is detected by the infrared sensors which are installed on the border fence, a signal is sent to position an appropriate surveillance camera in the direction where intruder has been detected. *Although the proposed system reduces human involvement in border surveillance process, many technical constraints have not been discussed. For example, the lack of a deployment plan which is very useful in case where one of the components of the solution breaks down (either the infrared sensors or the surveillance cameras). In addition to that, energy saving for infrared sensors and surveillance cameras which represents a decisive factor in this kind of solution, has not been addressed at all.*

In this section, several borders surveillance techniques are discussed, some techno-

logies were used separately, while others were combined with others. However, most of them if not all, ignore some operational key requirements for border surveillance and also the effect of certain criteria that should be taken such as climate conditions, topography and dangers surrounding the area, that can affect significantly the entire architecture. Next section talk about border surveillance systems deployed over the world that consider these aspects.

2.6 Some deployed systems and solutions over the world

In this section, a brief presentation of some border surveillance systems already deployed over the world is given. It should be noted that due to the military and security nature of this type of systems, a lack of details about some aspects related to systems functionalities was noticed. Some other similar technologies were intended to sea borders securing, pipeline security and perimeter protection issues, however they could be easily adapted to border surveillance context.

- Among the deployed systems and solutions over the world, we can quote the combination of UGS with Remote Video Surveillance (RVS) cameras (which are not cued to the sensors), to patrol the US borders with Mexico. According to [50], the US government announces that some $7,500$ sensors were acquired between 2003 and 2007, to create a movement detection perimeter. UGS can pick up moving heavy vehicles (such as tanks) from a distance of 500 meters and walking humans from 50 meters[51]. In its report issued in December 2005, the Department of Homeland Security (DHS), indicates that the probability of false alarm of the system is very high (between 34 and 96% of the sensor alerts) and the probability of detection is very low (between 1% and 57%). So this confirms that this kind of systems suffer from some issues that was already discussed.

- Eurosur[52], is another example of deployed solutions for border surveillance. Image processing based borders surveillance technique is a new trend border surveillance technology which relies on using satellites in addition to other equipment like UAV,UGS ...etc. The captured images are compared to the reference ones to detect any changes in the scenery. This kind of detection is called *digital change detection*. The EUROSUR is an example of using satellite technology (see Figure.2.9) . This system is operational since *December* 2013. However, its global cost amounts to 244 *million* for $2014 - 2020$. In addition to this higher cost, the major limitation of EUROSUR emerges from the complexity of technical operations, maintaining coordination and the dependency to the satellite connection.

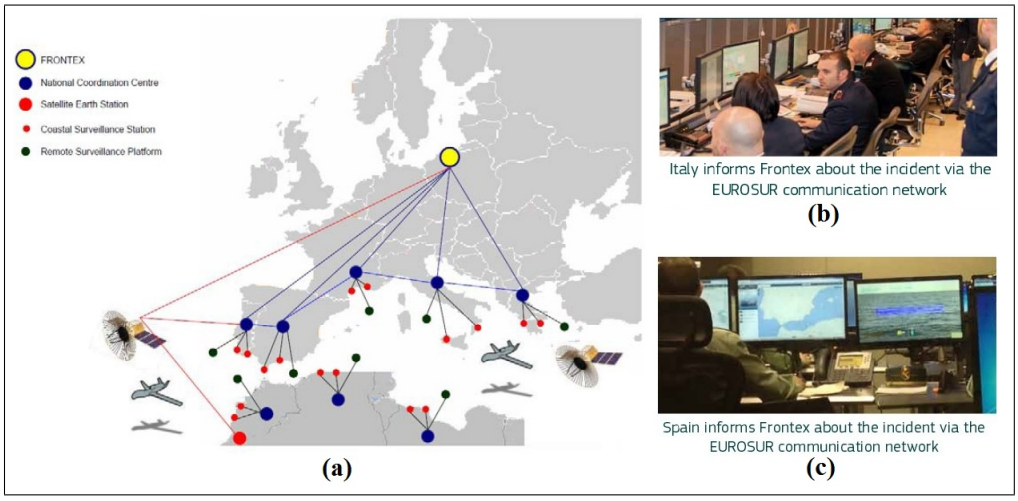


FIGURE 2.9 – (a) : Architecture of Eurosur system, (b) : EUROSUR National Coordination Centre, Rome, (c) : EUROSUR National Coordination Centre, Madrid.

- EdgeVis Shield is the integrated surveillance platform provided by the **uk!** (**uk!**) company Digital Barriers, one of the world leaders in visually intelligent solutions for the global surveillance, security and safety markets in United Kingdom. This platform provides a real-time video streaming and early warning intrusion alerts for remote locations by using a combination of radar, sensors (RDC low-power ground sensor), high-specification cameras (optical and thermal) and video analytics to give a complete site security solution, even in the most remote locations. As is depicted in Figure.2.10, the architecture of this system is based on three key levels, which are : Detection (by RDC sensors, Cameras and Radars) ; Transmission (over wireless network) ; and Responding [53]. The key technology of this system is the use of a real-time video-distribution technology, called Transport Video Interface (TVI) which is video codec technique that can deliver videos over wireless networks with under 0.5 second latency and can also, stream real-time video over wireless networks at under $10kbits/s$. According to [53], EdgeVis Shield was developed for the highly demanding world of defense, border surveillance and critical infrastructure protection, it is now the proven choice for customers in more than 30 countries worldwide. In addition, RDC sensors can detect and classify a potential intrusion threat, identifying whether it is a person or a vehicle. It can be rapidly deployed with exceptional power efficiency, allowing them to be used in areas where communications and power infrastructure are limited. However, deploying, ground sensors, cameras and radars at the same time turns out that this solution is too costly, especially for countries that suffer from economic crisis.

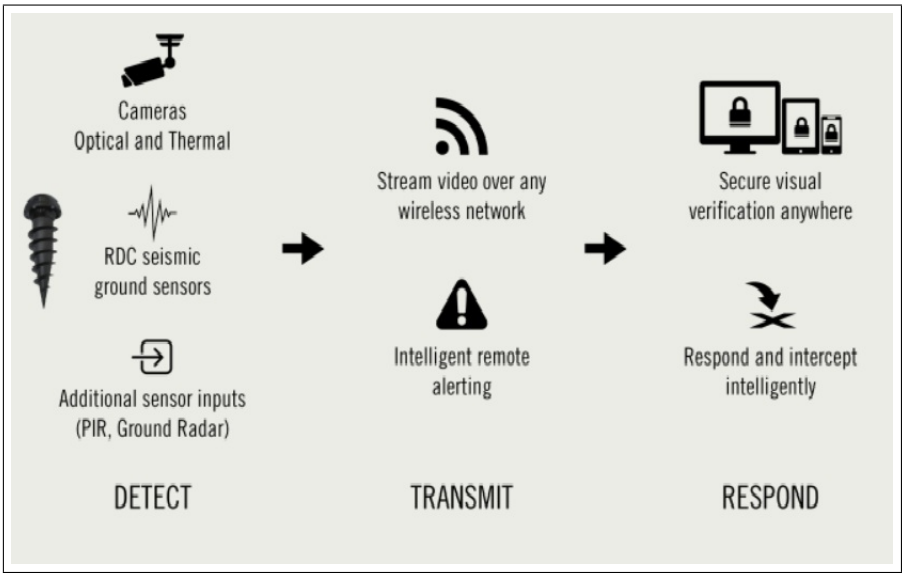


FIGURE 2.10 – Architecture of the EdgeVis Shield platform.

-In May 2015, the Czech Company ***EVPU Defence*** presented the ***BMS-MIRA 42*** system in the IDET2015 (International Defence and Security Technologies Fair), which is a low cost solution for monitoring and surveillance of area of interest such as boundary lines, airports, coastal areas and other areas with increased demands for flexible protection against penetration of intruders during day or/and night time. As illustrated in Figure.2.11 It can be easily and quickly integrated on standard vehicle. The based configuration of this system comprise Pan/Tilts, sensor container with uncooled IR camera, daylight Charge-Coupled Device Television (CCDTV) camera and as optional laser range finder, operators console and power supply pack[54]. This mobile monitoring system communicates by radio with Command Center, patrols and intervention elements. In addition to, it affords the combination of the camera system with the radar system, which increases the operating efficiency of the whole system. However, since it is embarked on a vehicle, it requires human involvement for car driving. In addition, for rough roads some times it is difficult if not impossible to access with cars.

FIGURE 2.11 – The BMS-MIRA 42 system mounted on a Skoda car.

- The Spanish company Indra, provides an ***Integrated Border Surveillance System*** to protect all kind of border areas, both land and maritime in the fight against different types of intruders. According to [55], this system is fully adapted to each particular environment, and can integrate all type of sensors from any manufacturer, besides Indras' technology itself. It provides also command and control capabilities and integrating state-of-the-art technologies in radar, electro-optical systems, underground sensors, as well as other type of sensors, physical barriers and integrated communications. This border surveillance system consists of one or multiple Command and Control Centers (CCC) and a set of Sensor Stations forming a hierarchical architecture. The sensor stations are deployed across the surveillance area and can be fixed or mobile, as illustrated in Figure.2.12. This system has been installed in several locations of the coast of Spain and in different islands of the same country as part of the **sive!** (**sive!**) Project. Besides the **sive!** project, Indra's Border Surveillance systems have been deployed at : Hong Kong SAR CSS, Latvia CSS, Bulgaria Green Border Surveillance, Romania CSS(SCOMAR Project), Portugal CSS (SIVICC Project) and Poland National Vessel Traffic System. However, this system is based on a rigid architecture (CCC and SS) required by the manufacturer, this architecture can be not useful in certain cases.

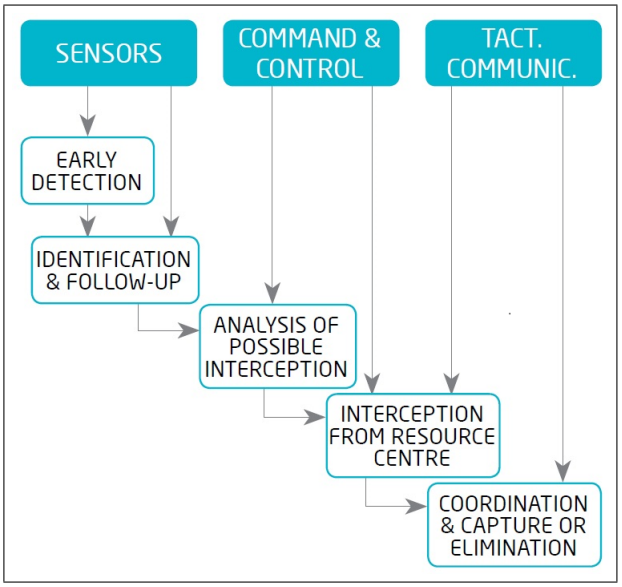


FIGURE 2.12 – Main architecture of Indra's Integrated Border Surveillance System.

- Helios Distributed Acoustic Sensor provided by the British company Fotech Solutions is a border monitoring system. According to [56], Helios provides security personnel with location details of an event or intrusion and helps other surveillance and security measures to be directed to the right place exactly when they are required. This technology is based on laser pulses transmitted through fiber optic cables buried in the ground that respond to movements on the surface above. A detector at one or both ends of the cable analyzes these responses as is illustrated in figure 2.13 (a). It is sensitive enough to detect a dog and can discriminate between people, horses and trucks. The system can be set to avoid being triggered by small animals, and can also tell if people are running or walking, or digging, and in which direction.

In 2010, Lowell Institute for Mineral Resources assisted by the National Center for Border Security and Immigration of the University of Arizona, leaded the project of deploying Helios as a tool for border surveillance [57]. Figure.2.13 (b) shows a screen shot of the Helios system output captured while two horses ran across the buried fiber optic cables. The red traces are clearly visible, unlike those made by a small dog, and are also quite distinct from the traces created by humans, cattle or trucks. However, some challenges with this technology are the difficulty of deploying the cable when the solution is dedicated in an extreme topography. In addition, when digging up the cable and cutting it this causes system stopping.

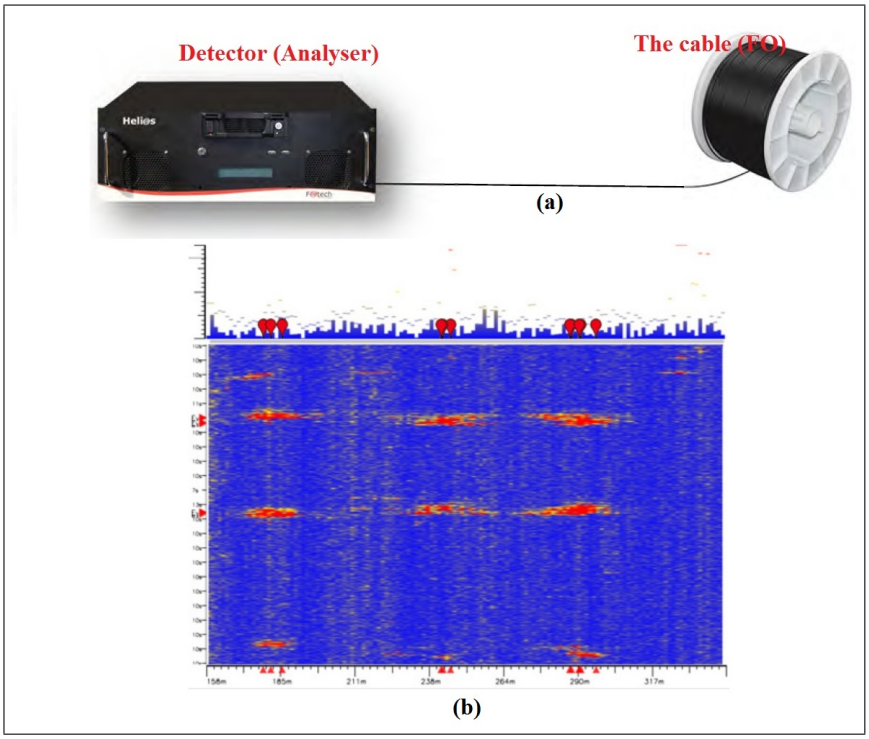


FIGURE 2.13 – (a) : The two main parts of Helios , (b) :Screen shot of Helios system for two horses ran across the buried fiber optic cables.

- Rheinmetall's Vingtaqs II Long Range which is a target acquisition and border surveillance system that includes a thermal camera, a ground surveillence radar, a laser range-finding and a laser target pointer as depicted in Figure.2.14 (a). The Vingtaqs II accurately determines target coordinates at long distances from the vehicle forward observer position. A standalone system, the Vingtaqs II can be integrated at low cost into a wide variety of vehicles. The system also accommodates instrumentation for laser-designated targeting, enabling it to support forward air controller operations. In November 2011, DEFTECH of Malaysia placed a 36 $million Euro$ order for Vingtaqs II surveillance systems to equip its $AV8$ armored vehicles. Vingtaqs II Long Range, can compute target coordinates up to 20 $kilometers$, maximum detection ranges are 48 km (Radar), 17 km (Day Camera), 15 km (Thermal Imaging Module). The positioning system consists of the **ins!** (**ins!**) and a **gps!** (**gps!**) [58]. However, the accessibility issue to rough roads and terrains can be a big challenge to this system since it is installed on vehicles.

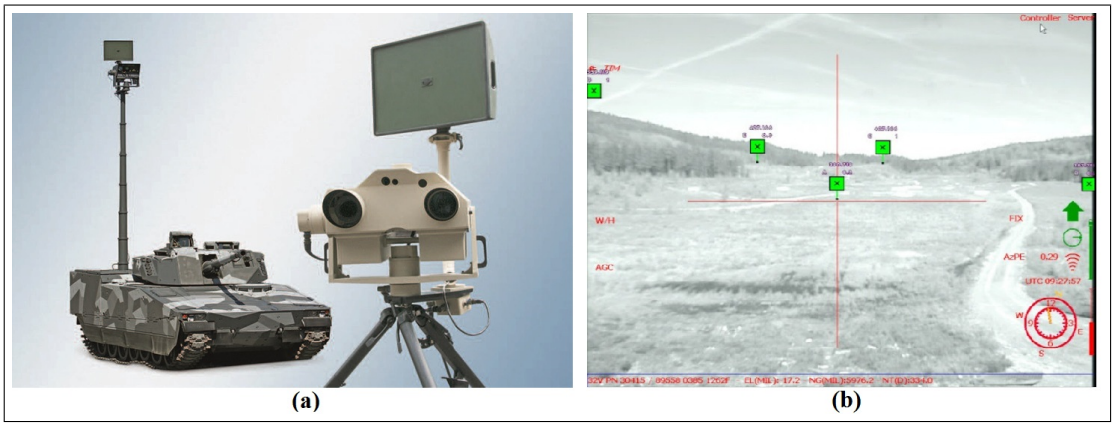


FIGURE 2.14 – (a) : Vingtaqs II Long Range, (b) :Radar images of Vingtaqs II.

- Another surveyed border surveillance system is the ***Radiobarrier Autonomous Perimeter Security System*** designed by the Russian company called POLUS-ST LLC. This system is a battery operated wireless intrusion detection system for area surveillance and perimeter protection of zones with no power and communication infrastructure. The entire system consists of three main parts : Sensors ; controlling and receiving units ; and the video sub-system. Sensors are considered as detection devices, POLUS-ST LLC commercializes three kind of sensors (RS-U seismic sensor, RS-L microwave sensor and RS-IK infrared sensor). In the International Exhibition of National Security and Resilience (15 to 17 March 2016 - Abu Dhabi, United Arab Emirates) [59] this company presented its new RS-N sensor which detects foot-borne intruders and/or vehicles based on the seismic signature they produce. The sensor is deployed underground to the depth of 30 to 50 *cm*. The sensor is powered by 05-year battery and communicates with command and control system wirelessly. The detection zone is circular (approx 100 meters in radius) and split into 04 equal sections. The sensor displays the sections in which the target is located in. When the target moves from one section to another, the operator sees an arrow indicating direction of movement. Command and Control Units are KOPR control receiver, MPO operator's console and C2 software. Video Subsystem, can be either PTV portable TV receiver, RS-TV wireless camera or RS-TP thermal imaging camera as illustrated in Figure.2.15. The main advantages of this system is that sensors allow the operator to see the direction of border crossing. In addition, sensors have a long mission life up to 05 years on a single battery, perfectly suits the most sophisticated border surveillance project. However, instead of being used largely for securing borders, it was used extensively by major players of the oil and gas industry(to protect pipelines infrastructures) for crime prevention and anti-terrorism activities.

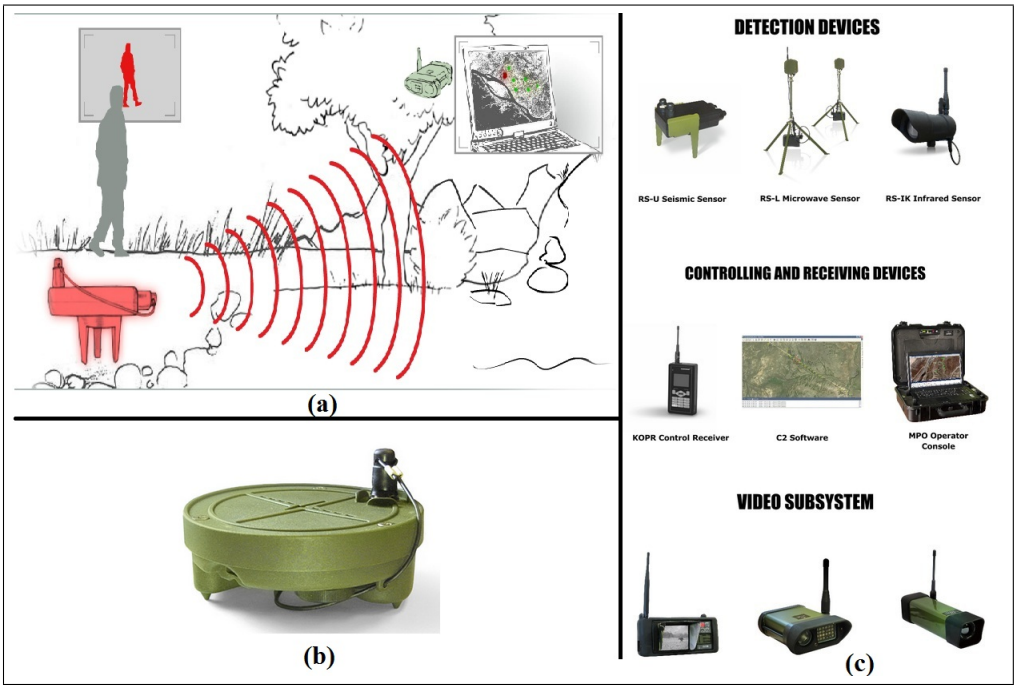


FIGURE 2.15 – (a) : Architecture deployment (an example), (b) :RS-N Directional Seismic Sensor, (c) The three main parts of the system.

- UAV for aerial surveillance have been used to ensure an automatic detection and to track illegal border crossing. According to [60, 61], the use of this technology UAV was adopted by the United States Customs and Border Protection (CBP) after being tested in 2004, to patrol the US international land border. In addition to the large coverage provided by this technology, Electro-Optical cameras can identify an object the size of a milk carton from an altitude of 60.000 feet.

- One of the Radar based implemented solutions is the Blighter radars surveillance technology, which are a modern electronic scanning radars. They are designed and built to provide continuous persistent surveillance at borders, boundaries and perimeters. They detect moving targets over both land and water, covering a wide area. They could be mobile or man-portable. Introduced by ***Inmarsat***(the mobile satellite company), Blighter scanning radars entered service with the United Kingdom Ministry of Defense in 2008 and is now operational in more than 10 other countries, including the **usa!** (**usa!**), France, Poland, Australia, South Korea, Qatar, Saudi Arabia, the Czech Republic and Oman. As depicted in Figure 2.16, this kind of radars, employ electronic rather than mechanical scanning which provides the highest possible levels of system availability and reliability. In addition to, there are no lifed items such as drive belts and there are no moving parts or rotating joints to lubricate, replace or service. Finally, Blighter can detect very slow moving targets, down to $0.4km/h$. This ensures

that targets moving almost tangentially to the radar can still be detected[62]. However, this kind of radars depends on the global satellite communications network called **bgan!** (**bgan!**) (an Inmarsat's service) which obliges the users of Blighter radars to pay an extra cost for being subscribed to this satellite network.

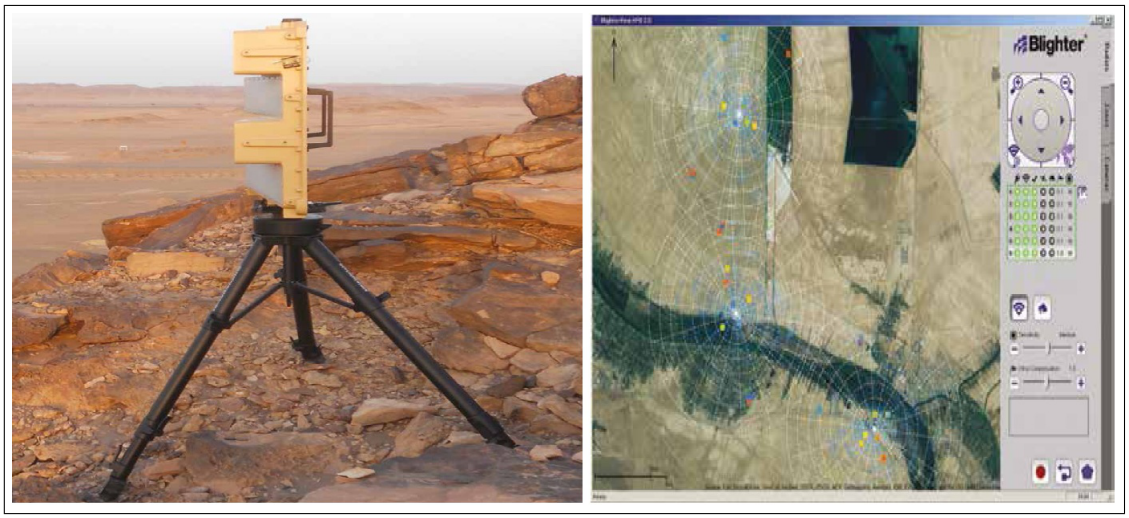


FIGURE 2.16 – Blighter scanning radar.

- The second Radar based implemented solution that we survey is the ***SQUIRE***, ground surveillance radar which is a man-portable medium-range ground surveillance one that can detect and classify moving targets on, or close to, the ground at ranges up to $48km$. This radar transmits in the band and has a very low output power of one (01) watt, making its detection difficult. The Squire radar can detect a person at a range of $13km$ and a helicopter at ranges of $19km$ (ten nautical miles) [63]. It can include an integrated infrared optronics system, plus a mini Unmanned Aerial Vehicle detection mode. To determine target speed, Squire uses **fmcw!** (**fmcw!**) architecture with Doppler filtering. According to *Gerrald Korenromp*, marketing and sales manager for ground surveillance radar activities, the Squire "can be used in both a stand-alone and vehicle-mounted configuration." This radar was commercialized by the french company Thales, and more than 400 units have been sold to armed forces all over the globe. Thales signed a contract for the delivery of 44 Squire radars, to be deployed by the Norwegian Armed Forces, the first 10 systems were delivered in the second half of 2013, the last delivery was scheduled for the beginning of 2017. The Egyptian Army has also acquired the Thales Squire man-portable ground-surveillance radar as it is shown in Figure.2.17. Moreover, Squire can be used to detect drones which is increasingly becoming a real threat to the security of the countries. However, the major challenge is the inability to distinguish between small, slow-flying drones and birds.

FIGURE 2.17 – (a) : Squire radar deployed in a mountainous area. (b) Egyptian army showing their Squire radars.

- The third Radar based implemented solution over the world is the ARSS which is a man-portable ground-surveillance radar that can be controlled locally or remotely. Manufactured by the US company Telephonics, it is capable of detecting a pedestrian at $12km$ and a large vehicle at $30km$, it can also detect aircraft such as a hovering helicopter at a range of $15km$[64]. ARSS is a pulse-Doppler radar featuring Track-While-Scan (TWS) and pulse compression technology providing high-performance and Wide Area Surveillance (WAS) capability to search, detect, acquire and track targets (See Figure.2.18). The system operates in X-band with eight user-selectable operating frequencies and is tested to and complies with the requirements of measurement for electro-magnetic interference characteristics. The ARSS is a Low Probability of Intercept (LPI) system employing non-linear waveform and low-power consumption. ARSS consists of three main parts : an antenna unit, a tripod unit and a remote control and display unit. The ARSS is used by US CBP on the US Southern Boarder, it was used also by the US armed forces to protect Forward Operating Bases in Afghanistan and Iraq. Over 1200 systems have been deployed globally, supporting a wide range of applications including : border security, force protection, battlefield surveillance and critical infrastructure protection. Similar radars for border surveillance were manufactured by Telephonics, for example : RaVEN-M (Mobile Surveillance System for a wide range of terrains) ; RaVEN-P (Man-Portable Surveillance System for borders, ports and harbours surveillance ; and RaVEN-F (Integrated Fixed Tower Surveillance System). Comparing with SQUIRE presented above, ARSS has a Lower detection range (up to $30km$) against $48km$ for the SQUIRE radar.

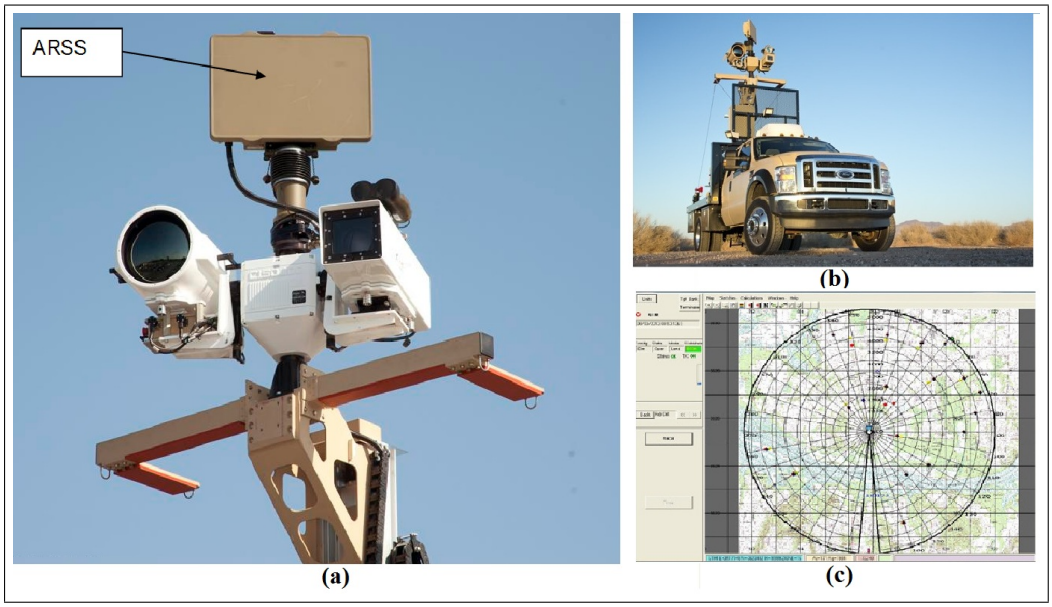


FIGURE 2.18 – (a) : ARSS radar integrated with surveillance cameras, (b) : ARSS integrated on Telephonics'RaVEN-**msc!**, (c) : ARSS Interface showing the 360° coverage.

It should be noted that through the in-depth readings of the literature that we have carried out on border surveillance systems implemented around the world, we have found that almost all the countries over the world uses Radars as a part of their border surveillance system. According to a report published in August 2020 by Globe Newswire (provides press release distribution services around the world, primarily in North America and Europe), the surveillance radars market is projected to grow from USD 8.0 *billion in* 2020 *to* USD 11.5 *billion by* 2025. *However, industry experts believe that* $COVID-19$ *could affect surveillance radar production and deliveries by* 3% *to* 5% *globally in 2020.*

After presenting some of the deployed border surveillance systems and solution over the world, Table 2.3 summarizes some useful information such as technology used, advantages and disadvantages of the surveyed border surveillance systems. This summary may be useful for making suggestions to improved border-monitoring techniques and solutions.

Product/System Name	**Manufacturer**	**Technology used**	**Strengths**	**Limitations**
EUROSUR	European Commission (EU).	Satellites, Helicopters, Drones.	- Border related information is shared between individual member states, partner organizations and surveillance gadgetry, - Each state of the EU has its own National Coordination Center for Border Surveillance.	- High cost, - Complexity of technical operations and maintaining coordination.
Blighter	Inmarsat (United Kingdom).	Electronic scanning radar.	- Employs electronic rather than mechanical scanning, - Detect, recognize and identify targets, - Low False Alarm Rate(01 false alarm/day).	Depends on the global satellite communications network **bgan!**, - Needs to be combined with other technologies such as UAV, UAV to improve intruders detection.
BMS-MIRA 42	EVPU Defence (Czech republic).	Pan/Tilts, sensor container with uncooled IR camera and daylight CCDTV camera	- Low cost solution, - Configuration varies according to customer needs .	- Requires human involvement (embedded in vehicle), - Difficult to use in rough roads and terrains.
SQUIRE	Thales (France).	Ground Surveillance Radar.	- Wide detection range (up to $48km$) , - Very low output power(01 watt), - Can be used to detect drones.	- Difficult to distinguish between small, slow-flying drones and birds.
EdgeVis Shield	Digital Barriers (United Kingdom).	Radar, low-power RDC sensors, optical and thermal cameras.	- Using real-time video-distribution technology (**tva!** (**tva!**)), - RDC sensors can detect, classify and identify intruders.	- High cost for deployment.
ARSS	Telephonics (United States).	Man-portable ground-surveillance radar	- Capability to search, detect, acquire and track targets, - LPI.	-Low detection range (up to $30km$) comparing to SQUIRE.
Integrated Border Surveillance System	Indra (Spain)	Radar, electro-optical systems, underground sensors, physical barriers, and integrated communications	- Can integrate all type of sensors from any manufacturer, - Sensor stations can be fixed or mobile.	- Based on a rigid architecture (CCC and SS)
Helios DAS	Fotech (United Kingdom).	Laser pulses transmitted through fiber optic cable connected to a detector	- Can detect a dog and discriminates between people, horses and trucks, - Can be set to avoid being triggered by small animals.	- Difficulty to deploy in an extreme topography areas.
Vingtaqs II Long Range	Rheinmetall (Germany).	Thermal imager, Ground surveillence radar, Laser range-finding and laser target pointer	- Can be integrated at low cost into a wide variety of vehicles, - Wide detection ranges (48 km for Radar, 17 km for Day Camera, 15 km for Thermal Imaging Module.	-Accessibility issue to rough roads and terrains since it is installed on vehicles
RADIOBARRIER-AUTONOMOUS PERIMETER SECURITY SYSTEM	POLUS-ST LLC (Russia).	Sensors, controlling and receiving units and video sub-system.	- Give the direction of border crossing, - Long mission life for sensor's batteries up to 05 years.	- Used extensively by major players of the oil and gas industry instead of being used largely for securing borders.

TABLE 2.3 – Comparative summary table for some deployed border surveillance systems.

2.6.1 Sensor scheduling strategies in border surveillance systems

In this section we review the most interesting sensor scheduling strategies used in context of border surveillance systems. Several recent works have discussed the design of country border surveillance systems based on sensor scheduling strategies. According to [65], the most commonly used approaches to ensure a high level of coverage and energy efficiency of the monitored area, is to select a subset of nodes to be active and keeping the remaining ones (redundant nodes) in the sleep mode.

- In [66], a tracking scheme called Border Cooperative Predictive Tracking Scheme was proposed. This scheme is a three-step process, in the first step, the target is detected as soon as it enters the strip. In the second step, the appropriate sensors are waked-up to follow the crossing target while predicting its next positions. In the final step, the exit time and the exit point (or segment) are estimated. The main goal of this work is to reduce the energy consumption of the tracking processes by reducing properly the number of sensors to wake up for tracking. The process of tracking is iterative. When a sensor detects a target at a given time, it determines the positions of the target at the following time slots until the latter leaves its sensing area. Then, then sensor builds a message containing the type of the detected target, the two last observed positions, the new position and the time duration of observation, and sends it to the sink node and to its neighbours located out of its tracking range, so that to determine the next node that should track the target. This solution aims to reduce energy consumption at the tracking level only. However, the energy consumption during the detection phase is not discussed.

- To track moving objects (abnormal behaviour of conductors) on a traffic scene (Highway), an active camera scheduling strategy was proposed in [67], as a part of multi-camera tracking system. Two kinds of camera are used to design this framework, static cameras which are wide field-of-view that can only deliver low-quality information of the supervised scene ; and active cameras that can get high resolution images of the objects of interest, representing the suspicious vehicles. The appropriate active camera is selected according to a function, called camera relevance computation, which defines the relevance of a camera i to observe a vehicle j. The camera relevance function is calculated by the combination of six factors such as camera-vehicle distance, frontal viewing direction,...etc. According to the reported simulation results, the proposed camera scheduling strategy can track a maximum number of vehicles as long as possible, however power saving issue has not been addressed at all, and the camera sensor were activated during the entire surveillance period. Add to that, the threat degree of the

vehicles was not taken into account, and the possibility of grouping intruders into a single group is not offered(each individual vehicle requires a dedicated camera).

- Finally, a strategy to schedule the activities of sensor nodes in critical surveillance applications was proposed in [65]. To do that, a distributed algorithm that enables each node to extract its cover sets by organizing its neighbours into non-disjoint subsets, each of which overlaps its Filed of view. This algorithm is executed in rounds and the algorithm operates after the nodes construct their cover sets. The status of every multimedia node is tested in rounds. At each round, every node decides to be active or not according to the activity messages received from its neighbours. According to the reported simulation results, the proposed algorithm gives a high level of coverage and an acceptable percentage of nodes in cover and guarantees the set cardinality (the number of cover sets per sensor). However, the algorithm does not take into account certain important parameters, such as the energy issue. The algorithm only seeks to find the cover set of a node and checks if the active nodes belongs to the cover sets of that node. The later goes to sleep mode even if some of the active nodes have low energy level. In other words, there is no load balancing mechanism to keep the energy consumption balanced between the different network nodes.

2.7 Conclusion

In this chapter, we have first provided an overview of key features and challenges specific to border monitoring. Besides, a detailed overview related to Algerian borders was presented and discussed as an area of interest for this study. Then, a non exhaustive list of border surveillance techniques and systems has been reviewed and discussed. This survey stands to be useful when it comes to build our new multi-level architecture for securing Algerian Borders. It should be noted also that other similar technologies were intended to sea borders, pipeline security and perimeter protection issues, those techniques could be easily integrated in the border surveillance context. At the end of this chapter, we surveyed some interesting activation strategies defined in the context of border surveillance. Next chapters introduce our contributions.

Chapitre 3

Proposed network architecture for border surveillance

3.1 Introduction

Nowadays, the use of communication technologies in border surveillance has become inevitable. For this reason, several technologies have been proposed in the market and each country adopted the appropriate one according to the nature of the ground, the climate and the threats surrounding its territory. When taking a look at data-sheets of any border surveillance system, the manufacturers endeavour to design their systems holistically as a full package. However, as each technology has its own strengths but may enjoy also limitations. For this reasons, we will try in this chapter to discuss and propose the most appropriate architecture for securing Algerian borders.

3.2 Proposed network architecture for border surveillance

In the literature, the type of WSN architectures for video surveillance to consider depends on several factors, previously discussed. This is why borders control systems vary from a country to another, but the basic components and operational activities of the systems are practically similar. When designing a border control architecture, certain parameters must be taken into consideration such as the sensitivity of the area, the type of threat and the geographic nature of the area. Therefore, combining two or more

technologies seems to be the right way to provide the appropriate technique for border surveillance. Such an approach is used by the CBP to secure the US-Mexico frontiers where an **ift!** (**ift!**) system which includes radars and day-night cameras mounted on a series of towers is implemented along the borders.

As aforementioned, this thesis has to be put in the context of a large project that aims at defining an operational framework for securing the Algerian borders. As it was mentioned earlier, Algeria which is the largest country in Africa enjoys huge segments of borders (6511 km) that are shared with 7 countries in addition to an access to the Mediterranean sea along 1600 km of coasts. The border areas cover different landscapes and reliefs. However, the most important part is located in desert area (1376 km with Mali ; 982 km with Lybia ; 461 km with Mauritania ; 41 km with Western Sahara and 956 km with Niger). Algeria is facing different threats along its borders, drugs and goods smuggling, arm trafficking, illegal immigrations and more seriously intrusions of AQIM (Al-Qaeda in the Islamic Maghreb) and **isis!** (**isis!**) groups from Lybia, Mali and Niger sides. As it is the primary priority of the Algerian government, our area of interest concerns the north-west, south-west and the extreme south borders, the north-east and south-east parts of Algerian borders are almost geographically similar to the north-west and the south-west parts respectively.

Faced with this immensity of land borders, the geographic diversity, the different distribution of the population and the different types of threats surrounding these borders, it seems difficult, even impossible, to use the same architecture and the same components to secure all the Algerian borders. Consequently and as already evoked, we considered it useful to divide the area of interest into two (02) essential parts. The first part (called $Part01$), includes the north-west and the south-west border strips (from the wilaya of Tlemcen till the wilaya of Naama), and are shared with Morocco, Western Sahara and Mauritania. The second part, called $Part02$, includes the extreme-south border strip (from the wilaya of Tindouf till the Wilaya of Illizi), shared with Mali, Niger and part of Libya (more than $2500km$). Hence, the real challenge is how to choose the most suitable and efficient architecture for both parts of our area of interest. There exists no one-size-fits-all solution to secure these borders as they are different in the terrain, threat profile, communication facilities, ...etc. In fact, a single length of border can often require different tactics, technology, and techniques to ensure an optimal security posture, which is the case for the Algerian borders.

According to a report (titled 21^{st} Century Border Surveillance) published in 2016 by the FLIR company, using cameras and radars in border surveillance is sufficient to detect most of intrusions. Cameras can be used in a relatively narrow field of vision. Reciprocally, radars can offer a persistent 360 degree coverage every second out of a distance up to 40 km. However, the latter can neither distinguish between friendly and enemy forces, nor determine the intent of what it is detected. Undoubtedly, combining two or more technologies seems to be the right way to provide the best solution for

border surveillance. Table 3.2 compares both parts of the borders in terms of terrain, facilities and risk of intrusion.

	Part 01	**Part 02**
Demography	Crowded area	Less crowded
Weather type	Mediterranean/Continental	Saharan
Type of threat	Illegal immigration/Smuggling/Drug trafficking	Illegal immigration/Weapons trafficking
Terrain's nature	Rough and mountainous	Flat and clear
Communication means(*)	Optical fiber/Dedicated military network(FH)/Mobil network (4G)	Optical fiber(unavailable in some areas)/Dedicated military network(FH)/Mobil network (4G)
Energy sources	Electric power	Electric power in some areas/Solar power
Population density at the border strip(inhabitants/Km^2)	between 400 and 700	Less than 20
Priority degree	Very high	High
Intrusion rate observed	Very high	High
Temperature (° C)	Between 11.7 and 23.1	Between 20.92 and 35.99
Precipitation (mm)	686.6	38.1

TABLE 3.1 – Comparative table between the two border segments.

(*) : Although almost the same type of communications are available in both parts, the network coverage rate is greater in part01 compared to part02. As far as we are concerned, the Algerian government has already opted for the implementation of a basic architecture using radars and cameras to secure all the land borders. Our goal here is to reinforce this basic architecture by adding the appropriate software and hardware, when needed, in order to meet specific operational requirements. Therefore, in our study radars and cameras are both considered in securing $Part01$ and $Part02$. Radars are used for early detection, while cameras are for identification, tracking of intruders are ensured by both of them. However, taking into account the nature of $Part01's$ terrain of the borders which is rough and mountainous in most cases (especially with the Moroccan neighbor), which make radars communications difficult even less reliable. Add to that the population density in this part is more important comparatively to $Part02$ of the

borders and this high risk of intrusion and hence false alarms. Indeed, these lands require a high network coverage in response to the nature of the threat surrounding this area which is in most cases the penetration of fuel smugglers and drug dealers as well as arm trafficking that could be detected at the border strip by using scalar sensors when radars are not operational or when their reliability is challenged. Therefore, we consider UGS as a detection mean beside radars, and UAV to perform virtual tracking in impassable areas at $Part01$ of our borders. Such additional features are not considered in $PART2$ as the cost of their deployment is very high and the facilities are not always available is such no-man's-land areas. Besides the risk on intrusion is lesser and scarce and does not worth to implement a high level solution as it is recommended in $Part01$. Indeed, $Part02$ is a Saharan zone, flat, clear and less populated which makes it desirable for the activity of radars. It is characterized in some of its parts by a very high terrorist activity especially with trucks and heavy vehicles as well as a significant activity of weapon trafficking. The use of high detection radars combined with long range cameras, can achieve a good solution with a minimal cost, providing that deployment and activation strategies are well designed. In other respects, using satellite imaging has been excluded in our architecture because this solution is very expensive. In addition to that, satellite induces a high latency in the decision making which is not affordable in some critical military situations that require complex technical operations and coordination. Finally, bad satellite images due to cloudy sky or bad weather conditions can easily affect the reliability of this solution. For military duties, especially in wartime or in some critical situations, it is essential to have information about the capabilities and movements of enemy forces as earlier as possible. Unfortunately, this information is often available miles away from the borderline. To the best of our knowledge, this need, have never been addressed by the border surveillance techniques available in the literature. All the reviewed solutions are considering small areas of interest, with hundreds of meters near to the borderlines.

3.2.1 Algerian Border Guards hierarchy

It is noteworthy that, when designing a border surveillance architecture, it is strongly recommended to adapt the latter to the hierarchy of the forces in charge of this mission. Adapting the proposed architecture to the hierarchy of the ABGF, which are responsible for securing Algerian land borders, was a real challenge. As illustrated in Figure 3.1, **bgg!** (**bgg!**) is responsible for several (02 to 03) **bgs!** (**bgs!**), the latter itself is responsible for several (03 to 04) **abgp!** (**abgp!**). The transverse front of a **bgg!** extends from 50 to $60km$ in the north part of the country and some times from 180 to $220km$ in the south part of the country. It is located at 30 to $50km$ from the borderline. A **bgs!** has a transverse front from 20 to $30km$ in the north part of the country and

from 60 to 90km in the south part of the country. It is located at 03 to 05km from the borderline, while an **abgp!** can reach 10 to 15km of the transverse front in the north part of the country and 20 to 30km of the transverse front in the south part of the country. **abgp!** is generally set up almost at the borderline.

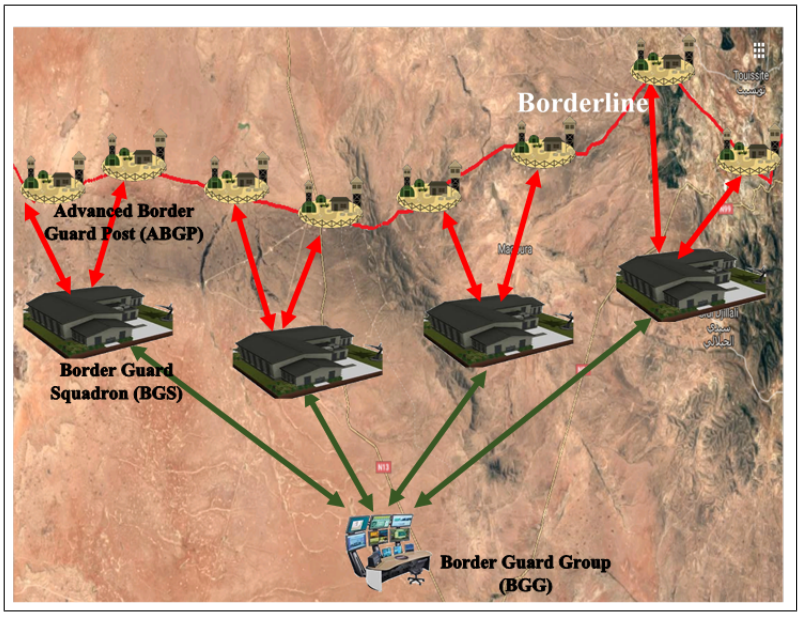


FIGURE 3.1 – Algerian Border Guards hierarchy.

3.2.2 Global network architecture for part 01

Unlike homogeneous WSN, heterogeneous WSN have various kind of sensors that have different capabilities in terms of storage, processing, sensing, and communication. It is clear that heterogeneous WSN have the advantage of increasing network reliability and lifetime. The proposed multilayer architecture for *Part*01 of the Algerian borders is based on three main layers, each layer contains several types of sensor technologies.

As illustrated in Figure 3.2, the hybrid three layers architecture for *Part*01 is composed of UGS, radars, cameras and UAV. UGS and radars are used for intrusion detection, while cameras are used for visualizing and identifying the nature of the intrusions. UAV are considered to substitute to human patrols for tracking intruders or for performing virtual air patrols when the latter cannot be deployed in hostile areas as it is the case in this part of the borders. As pictured in Figure 3.3, the three layers of the proposed architecture are : The basic layer called **Detection layer** ; the intermediate layer called **Visualization and the identification layer** ; and finally the upper layer called **Decisional layer** (the Commend and Control Center 3C). In addition to that, more

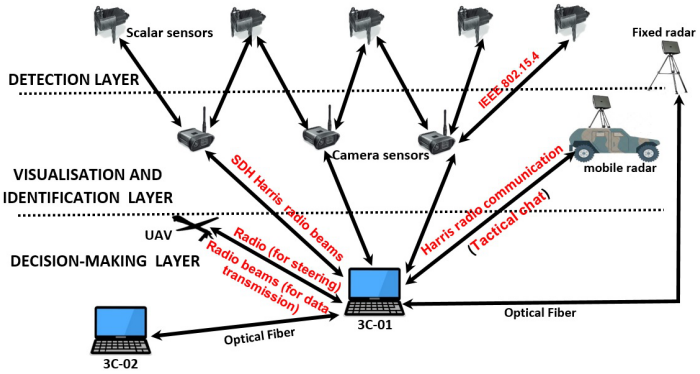


FIGURE 3.2 – Global hierarchy among the three layers for *Part*01.

nodes that can ensure tasks other than sensing, like data filtering, fusion and transport, are deployed at the intermediate level.

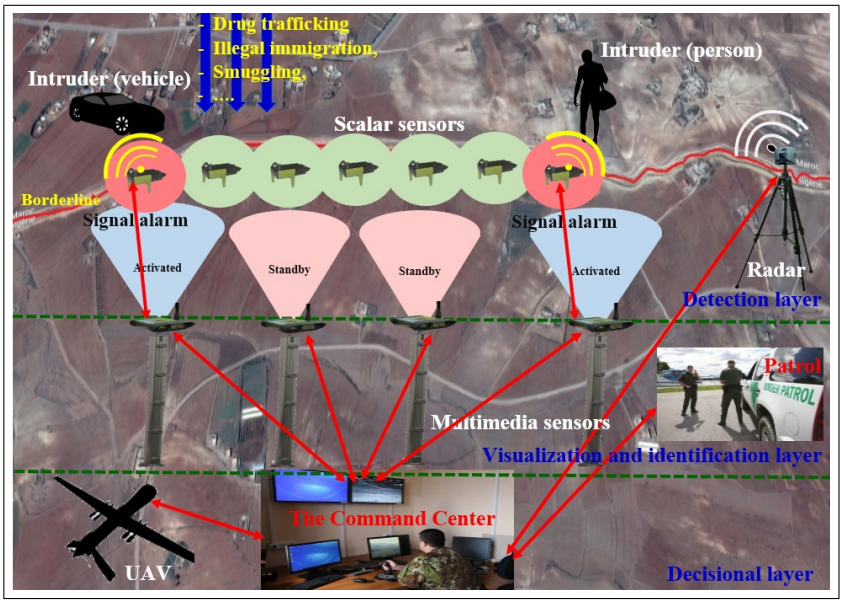


FIGURE 3.3 – Proposed network architecture for *Part*01 of the Algerian borders.

Communications between layers

Technically, the three layers could communicate via several technologies, as the 802.15.4 standard, 4*G* mobile networks, WIFI or satellites. However, although 4*G* mobile network can be a good solution it is not deployed in most of Algerian border areas because of the low concentration of the population in some areas. Moreover, as the border security is the army forces responsibility and for the high confidentiality of the task,

it is recommended to use the traditional military communication networks that consider specific secure radio beams (FH). In the layer I, the IEEE 802.15.4 standard is considered to connect UGS with the different antennas set at camera towers. This standard provides low-rate, and low-power consumption, which typically fits the requirements of border surveillance applications. The IEEE 802.15.4 standard uses three license-free frequency bands. In our case, we consider the $2.4GHz$ (16 channels with data rates of 250 kbps), band since its operates worldwide, contrarily to the other frequencies which are adopted only in Europe, North America, and Australia. For radars, fixed radars are connected to the nearest 3C by optical fiber. For mobile radars, a specific radio channel is established using two Harris stations of type $AN/PRC-150(C)$, one is installed on the car holding the radar and the other at the 3C. The interaction is done via an application called *tactical chat*. For communication between the antennas of layer 2 and the 3C, we use specific radio beams. In practical case, the *Harris Stratex Networks*, already deployed in Algeria, is considered. This network is based on the *Truepoint system* of Harris which has been enriched since 2004 by the Eclipse range developed by Stratex. This technology enjoys quite remarkable characteristics of robustness and reliability and is optimized for a topology of mesh IP radio beams network, offering much better IP traffic routing performance to those obtained using the best routers. Eclipse also allows achieving a solid SDH backbone of 155 Mbit/s. For interconnection between 3Cs, an optical fiber network is considered to provide more security and reliability. For UAV transmissions, the 3C use two radio beams modes. The first one is for the UAV control, the second one is for video transmissions.

- Detailed description of the architecture

1. **Detection layer :** This layer is responsible of sensing (intrusion detection) the area of interest and sending the information to upper layers. To accomplish these tasks, the detection layer calls on scalar sensors and radars.

   (i)- **Scalar sensors** (UGS) which are the elementary nodes, represent the big amount of sensors used in the architecture of $Part01$. The main task of UGS is to perform seismic or vibration measurements. This kind of sensors was described in details previously, so for more details, refers to Chapter 1. The use of UGS is to substitute to radars (in case of a loss of detection), and to assist the camera sensor in targeting the intrusion. As UGS are cheaper they can be deployed in full extent to cover the area unlike radars and camera sensor. In addition, their need in terms of energy is very low comparatively to other devices, and can be replaced easily in case of damage or battery repletion. We assume that each scalar sensor is correlated with a number of cameras that can communicate with. When a scalar sensor is activated it starts sensing continuously the area of interest. If the sensed

seismic pattern is similar to human steps or to vehicle movements, an alarm signal is generated and sent to activate the most appropriate camera for intrusion identification and further investigations. In the practical case, we recommend the use of a seismic sensor called ***RS-U seismic sensor***, which is manufactured by the Russian company *RADIOBARRIER* and already presented in Chapter I. The main reason for this choice is that this kind of sensors can detect and classify intruders according to the perceived seismic noise. Furthermore, they can operate for a long time without recharging or battery replacement while being invisible to the enemy. UGS can communicate with cameras to which they are correlated and can be activated and put in a standby mode by the 3C. The communication is ensured by wireless antennas set on the camera towers, by using the IEEE 802.15.4 standard.

(ii)- **Radars** are also considered at this level to overcome the sensing limitations of UGS. Indeed, besides that the detection radius of the latter is limited to 100 meters for pedestrians and 200 meters for vehicles, they can not monitor the airspace surrounding the borders. For military forces, it is important to know what is happening in miles away. For example in wartime or in some critical situations we need to control movements of enemy forces or armed vehicles far away from our own borders in order to take the appropriate decision at the appropriate time. Add to that, UGS can never detect a small drone penetrating the airspace. Far from military concerns such as spying, the use of drones is become commonplace nowadays. They are used by drug traffickers as a new transportation mode to pass kilograms of cocaine in border areas. Using radars can contribute in some extent to reduce false alarms (lawful cross-border activities, such as nomads with their flocks, tourists, travelling merchant and the sovereign activities of authorities in neighbouring countries who also carry out surveillance operations in their border areas). This can be achieved by assuming that radars operate according to a sector scan (also known in military jargon by **echo extractor**). In this case, some sectors are more investigated while others may be skipped. Although tracking can be seemingly performed exclusively by radars which cover a larger monitoring field, UGS are still used because they can be deployed everywhere and are more precise to detect pedestrians at near distances of the borders. As already pointed, $Part01$ of the borders is characterized by a high population density which some times hinders the radar activity. Add to this, in bad weather conditions or in a high signal interferences, radars lose their efficiency in terms of communication availability and reliability. As an example, the inability of radars of three different countries (Malaysia, China and India) to identify the Malaysian Airlines plane crash site in march 2014 following very bad weather conditions. Radars can be either fixed or mobile, the ideal solution is to fix radars above military facilities (near the 3C), to guarantee

their energy supply. In this case, the use of optical fibers to connect the radars to the 3C is recommended to enforce reliability and security of data transmissions. As the number of fixed radars may not be sufficient to cover all the area of interest, mobile radars mounted on cars (powered by rechargeable batteries or through the car power plug), can be deployed to monitor sensitive sectors in times of security crisis. As the energy supply is not an issue, radars should be thus activated most of the time. In case of an intrusion, the coordinates of the intruder, its type, its speed and the detection time of the intrusion, are sent to the 3C to be displayed on a digital map. If needed, the appropriate camera can be activated by the 3C operator. In our architecture, we recommend the use of a specific radar, called SQUIRE (already described earlier), which is commercialized by the french company Thales. Some of its functionalities includes, intruder detection and classification up to $48km$ with a very low output power of (less than 01 watt), thus making its own detection difficult by enemy forces.

In the architecture proposed for $Part01$, radars are not correlated directly with cameras, unlike UGS, because the detection range of radars is far bigger than the visualization field of the considered camera in that solution. This is because the sight of view of cameras is often broken due the rugged and mountainous terrain. In addition, the latter become inaccessible when radars are mobile. Therefore, the decision to activate the appropriate camera or to send a UAV for identification is left to the 3C operator once the intrusion signal is geo-positioned on the map.

Additional nodes at this level that are considered to collect data from UGS, and to perform eventual processing on collected data (fusion, filtering) before sending the synthetic information to the 3C, for processing, analysis and decision making. At this level of our architecture, we can also use two specific equipments, called *MR Trunk Repeater* and *TV-R TV Repeater* manufactured by *RADIO-BARRIER*. The first one is used to provide connection between UGS sensors and to repeat signal to the 3C ; the second device is used to activate cameras after receiving signal from the 3C.

2. **Visualization and identification layer**

   When scalar sensors alarms are not sufficient to confirm the intrusion, the 3C operator needs to take a look on what is happening on the borderline to identify the intrusion threat, its nature, and estimate the level of its dangerousness. In this case, cameras provide the 3C operator with a real time snapshots and video streams of the covered area. To extend their lifetime, cameras are in the standby mode for most of the time, they can be activated by the 3C operator or when an alert is sent by the correlated UGS. To avoid the transfer of a huge amount of unnecessary data, we consider the use of the *digital change detection* technique. That means that a camera stops sensing if there are no substantial changes in the scenery. This could happen in case of false alarms induced by

scalar sensors. In practice, we recommend using specific multi-directional camera, called ***RS-TV wireless camera or RS-TP thermal imaging camera***, commercialized by the company *RADIOBARRIER*(already discussed earlier) that are energy supplied by rechargeable batteries powered by solar panels. The latter are compatible with the RS-U seismic sensor adopted at the detection layer and equipped with infra-red back-light that enables the operator to detect a camouflaged person moving against a background of vegetation. The images provided by thermal cameras are in $JPEG$ or PNG format with a 320×240 pixel resolution. The pixel denotes the temperature level instead of light density. To enhance the resolution of the received images, the Fine Resolution (FR) technique can be applied at the 3C level to improve their quality by four times, if needed. For their protection and a better coverage, we assume that the camera sensor are permanently mounted on towers. RS-TP thermal imaging camera has a detection range that can up to 200 meters. There is no need in $Part01$ to consider a higher range camera, because cameras are only correlated to UGS, detection range of which is limited to 200 meters. Besides, cameras are deployed intensively in this part of the borders. Therefore, to limit the global costs, we avoided to consider cameras with higher performances knowing that UAV can perform the visualisation task too at a very high range while tracking then intruders, when required (in case of a radar alarm). To ensure a good communication between scalar sensors and cameras, we assume that the distance between them is inside the radio range of both. Something else that we have to consider is the protection of cameras against bad weather conditions such as rain, fog, snow, smoke, sand-storm and other extreme environments. For example, cameras used in a humid areas, should be equipped with built-in heaters that prevent condensation on the lens.

3. **Decision-making layer** At this upper level which is the Decision-making layer we find the 3Cs that are monitoring and controlling the network. In each 3C, we find in addition to human operators, the necessary equipments to process and display the information ; such as workstations, large screens to display the signals sent by cameras (fixed or embedded on UAV) and radars. The 3C operator can control any equipment in the architecture. For example, he can activate or switch them into the standby mode, as he can control the zoom and the focus of a specific camera, etc. The 3C receives images or video streams from cameras upon an intrusion is detected in their field of view. Intrusion alerts sent by radars are processed before displayed on a digital map to ease their interpretation. The operator can then decide to activate the camera which is the closest to the intrusion. In addition to that, this level is endowed with the necessary logistics and the means of locomotion allowing the intervention in a timely manner. As the case may be and after assessing the gravity of the intrusion, the operator can

dispatch a pedestrian patrol or orders the UAV to perform a virtual investigation into the desired place.

Compared to conventional border surveillance techniques, this designed solution reduces considerably the deployment of an extensive human resources in the *Part*01 of the Algerian borders while providing a real time decision. Furthermore, the combination of several technologies such as scalar sensors, camera sensors, radars and UAV can considerably improve the reliability of the architecture which makes it operate either in peacetime or wartime. More details are given when we discuss the deployment and the activation scheduling strategies considered in this architecture to improve its energy efficiency and to extend its lifetime.

3.2.3 Global network architecture for part 02

The architecture network of *Part*2 is a basic architecture comparing to that of *Part*01. Instead of using four (04) different components, we combine only two (02) components which are radars and cameras. Indeed, cameras combined with radars stands to be the basic architecture for most if not all of the border surveillance systems deployed over the world. As aforementioned, the use of radars for detection is very effective, particularly in less populated border areas where traffic is light, which really characterizes the *Part*02 of our borders where inhabitants concentration is low (less than 20 inhabitants per km^2 according to 2020's report of the Algerian National Statistics Office). The architecture proposed for *Part*02, called CAMRAD BORDER-GUARD, is based on cameras and radars, which gives an almost immediate and precise detection, identification and tracking of suspicious elements once they try to cross borders. This solution integrates cameras and a radar coverage with high performances, comparing to *Part*01 to build a layered architecture solution for border surveillance.

Detailed description of the architecture

As illustrated in Figure 3.4, the proposed architecture for *Part*2 of the Algerian borders includes three layers, which are :

1. **Detection and Localization Layer (DLL) :**
   In military surveillance duties, detection means signalling the existence of a moving target. This is the first basic operational act that should be done in intrusion situations. This lower level is responsible for reporting the early detection and the localization of any intrusion. To accomplish these tasks, this layer implements

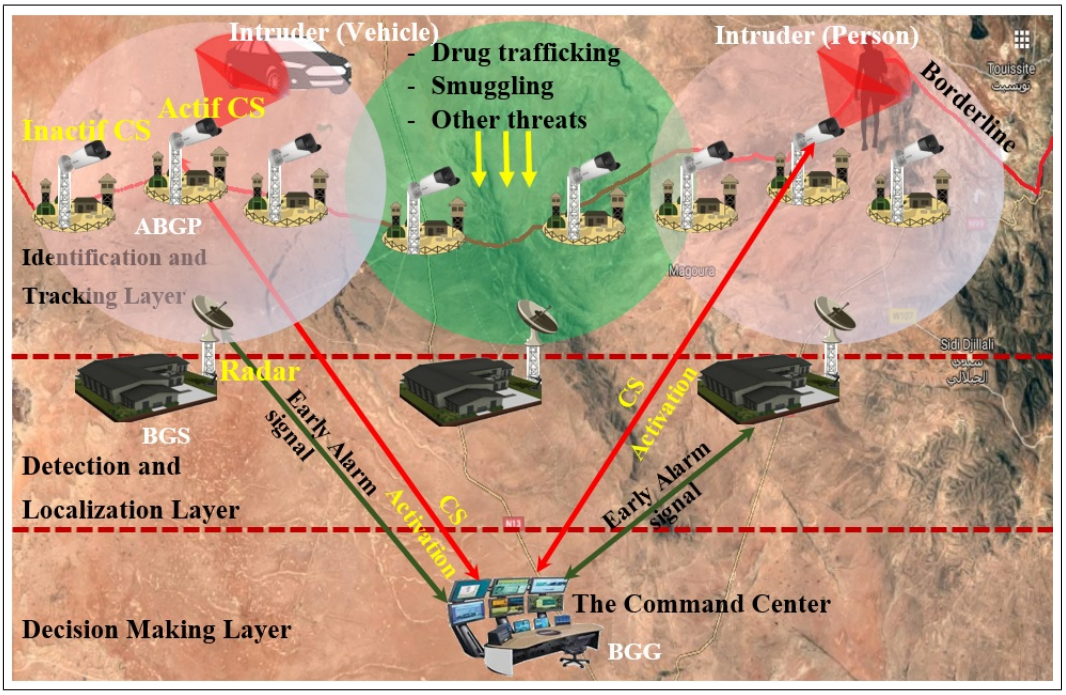


FIGURE 3.4 – Proposed network architecture of *Part*02.

radars, which are resource-rich, high-power devices with larger communication range, compared to the other devices. Depending on the nature of the area, type of treats, environmental characteristics and operational constraints, radars can enjoy long, medium or short range. In our case, we assume the use of the SQUIRE radars, as those used in *Part*01, however we adjust the detection range to $24km$ instead of $48km$ in order to meet some deployment specifications which are discussed when describing the deployment strategy adopted for this part of the borders. This type of radars provides a non stop 24/7, $n \times 360°$ coverage type around the site where they are installed. To ensure an effective detection of intruders while limiting the false alarms rate. Preliminary choices regarding the configuration parameters of the radar's extractor (called also the echo extractor) should be made for each radar and each coverage area. The detection of an element in motion is ensured by the Doppler effect. However, a momentary stopping of the intruder, causes a momentary loss of detection. To deal with this issue and to limit the "non-detection" moments by stopping the movement, we consider radars that can memorize intruders tracks. For an optimal detection and coverage and as it is in *Part*1, we assume that radars operate according to a scan by sector which means that, some sectors can be better monitored than others and conversely, certain sectors can be skipped (without interest), this is the case of the areas behind the border (occupied by friendly troops).

With regard to their implementation, it is recommended that they should be ins-

talled on infrastructures of the guard posts to be powered, secured and protected against climatic conditions and endowed in addition with solar panel energy supply to maximize their autonomy. In our solution, radars are installed on the top of the masts fixed to the BGSs as illustrated in Figure 3.4. Like in $Part01$, we assume that each radar is connected with the 3C using the same communication means. Note that radars can provide the server at the 3C level by a primary classification information about intruders (e.g. distinguish between vehicles and human) which can be denied or confirmed by the cameras once activated.

2. **Identification and Tracking Layer (ITL) :**
In some border surveillance situations, receiving alarm signals from radars is not sufficient. Sometimes, the operator at the CC needs to see what is happening in the area where the intrusion is detected in order to confirm the intrusion threat, its nature, and estimate the level of its harmfulness. This need can be accomplished by cameras deployed at this level, which are responsible for the continuous tracking and identification of any intruder. Cameras provide the operator at the 3C with a real day and night-time snapshots and video streams of the covered area. In other words, they provide a visual identification and a continuous tracking of the detected intruders, especially during periods of voluntary stops or maintenance, where radars can be blind for lack of Doppler effect. To better manage their energy, cameras are in standby mode for most of the time, they can be activated automatically by the server at the 3C when an intruder approaches their detection range or manually by the operator at the 3C in critical situations. For practical and operational reasons, the cameras used in our architecture, are in most cases installed on the top of the masts fixed near to the **abgp!** as illustrated in Figure 3.4.

   In $Part02$ we have opted for cameras with higher performances in terms of coverage range, resolution, and capabilities compared to those used in $Part01$. In the latter we have opted for a RS-TV wireless camera or a RS-TP thermal imaging camera with a detection range that can up only to $200m$ with a horizontal rotation. In order to meet the operational requirements in $Part02$, we need to upgrade the performances so that to be able to correlate cameras with radars which have a higher detection range. As the nature of the $Part02's$ terrain is flat and clear, the line of sight is rarely broken by obstacles unlike in $Part01$ therefore we have opted for a different kind of camera that is able to detect intruders from a distance up to $10km$, calibrated, with overlapping fields of view. These cameras are also endowed with a PTZ functionality : pan (horizontal rotation$(0° - 180°)$), tilt (vertical rotation), and an optical zoom. Moreover, as it is the case in $Part1$, the solution integrates additional infra red thermal cameras for night-vision. Despite, the additional cost to acquire these high performances cameras, the required number to deploy in $Part02$ is by far lesser than that

needed in $Part01$.

Moreover, as for radars and due to the lack of facilities in the $Part02$ borders, cameras are additionally energy supplied with solar panels and positioned in a standby mode. A global scheduling strategy is considered to prevent them from damage, attrition, and to streamline their energy consumption. Similarly as in $Part1$, all the data acquired at this level is forwarded to the 3C to be processed and analysed by the operator for decision making.

3. **Decision Making Layer(DML) :**
   As for $Part1$, this layer represents the higher level of the proposed architecture, which is represented by the 3C. At this level, a permanent supervision of all the activities at the borderline is centralized. The information produced by the *capture and the visualization subsystem*(radars and cameras), is transmitted to 3C via the communications network subsystem to allow the operator at this level to take the appropriate decision. According to the hierarchy represented in Figure 3.1, a 3C is considered at each **bgg!**. As it is the case in $Part1$. This level is the only one of our architecture that requires human involvement.

   As concerns the means of communications, the $Part02$) is huge in terms of area (more than 2500 km) which makes the network coverage difficult and very expensive. Therefore, we consider optical fiber network, when it is provided, as a main communication mean to connect all the architecture layers. Alternatively, we use the dedicated military network with specific radio beams FH as in $Part01$ to connect radars and cameras to the 3C.

The functioning of the architecture in $Part02$ is quite similar to that of $Part01$. Once an intruder enters the detection field of a radar, the latter sends to the 3C an early warning message to indicate the presence of an intruder. This message includes inter alia the coordinates, the speed, the size, and the nature, of the the intruder. At this stage, the tracking is ensured by the radar. The appropriate cameras at the second layer are switched to activated mode automatically by the server or manually by the operator located at the 3C level as soon the intruder enter their visual range. Therefore, to deal with the case of multiple intruders, a relevance based camera sensor scheduling strategy is implemented to allow the server to activate the appropriate cameras. This scheduling strategy allows to reduce the attrition and the energy consumption by avoiding the unnecessary activation of cameras as well as to maintain the tracking of a maximum number of intruders as long as possible.

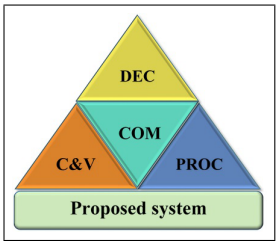


FIGURE 3.5 – Operational vision of both proposed architectures

- Operationally vision of the proposed architecture

After giving a detailed description of each layer of the proposed architectures of $Part1and2$ of our borders, now we give our vision from an operational point of view. As illustrated in Figure 3.5, our system can be seen as a set of a four (04) combined subsystems, which are :

- The capture and the visualization subsystem (C&V) : includes all the detection, the localization, the identification, and the tracking equipments materialized by radars, UGS, and fixed and embedded cameras ;
- The data processing subsystem (PROC) : represented by the processing units, which are supposed to be integrated into the servers at the 3C ;
- The communications network subsystem (COM) : including all radio communication equipments for data and video exchanges. It is responsible for maintaining communication links between the different layers of the both architectures. This can refer to the 802.15.4 network, or to the existing Harris Stratex Networks radio beams(already deployed in Algeria) or to the optic fiber networks that are used to transmit data from the different layers of both architectures to the 3C level.
- The decision making subsystem (DEC) : represented by the 3C implemented in both proposed architecture ;

3.3 Deployment strategy description

Many border surveillance architectures don't give enough importance to the deployment method that should be considered. Usually, to cover an area of interest, sensor nodes are deployed randomly. In this case, there is no guarantee that the nodes are uniformly distributed to form a reliable barrier coverage. When deploying nodes, several factors must be taken into consideration, such as the sensitivity of the application (application needs dense or sparse deployment), weather conditions (such as heat and

damp), area accessibility, etc. Recently, many WSN deployment techniques have been discussed in the literature, these depend mainly on the bandwidth efficiency, the power-saving, and the coverage rate. As far as WSN are concerned, sensor nodes can be either dropped from the air using a helicopter, in this case the number of sensors required is much higher, or deployed manually by placing the nodes in the appropriate geographic coordinates. For the impracticable and inaccessible parts of a border strip, an air dropping using a helicopter is generally conducted. A more advanced technique like using laser guns is used to shoot and place the sensors in the right position. In our solution, when it is the case, we strongly recommend a manual deployment for accessible area. For inaccessible ones, sensors like UGS can be dropped from the air. In the following, we are going to describe the deployment strategy designed for both $Part01$ and $Part02$ of the Algerian borders.

3.3.1 Deployment strategy for $Part01$

Because of the immensity of the area to be monitored ($Part01$, more than $2000km$), a large amount of sensors and equipments may be required for a full coverage, resulting on prohibitive costs. Therefore, a carefully controlled deployment strategy is needed to achieve an acceptable compromise between cost constraints and coverage requirements as well as fault tolerance.

1. **3C deployment :** This level is the only one of our architecture that requires human involvement. The number of 3C required to cover the entire $Part01$ of the borderline depends mainly on the extent of the border bungs and the organization of armed forces responsible for securing the borders. According to the hierarchy of Algerian border guards, already explained and represented in figure 3.1, the 3C of this part can be established at the level of the **bgg!** where the transverse front very from 50 to $60km$ in most of the segments of $Part01$. Often and in relation to operational requirements, the 3C must be within $50km$ from the borderlines. Each device in the architecture is affiliated and controlled by one 3C at a given time. The communication between UGS and the 3C goes through the antennas fixed on camera towers. A local database is run at this level that inventories all the equipments and devices located within the area ruled by the 3C. The status of each device and its **gps!** position is maintained in real time an the decision to activate each device is taken at this level according to the considered deployment strategy. Concretely, once a device is deployed, it broadcasts a message containing its Id, its **gps!** position and the level of its battery. Once the 3C in charge of ruling the device receives the information it updates the

database and the operator decides to activate or not each equipment according to the deployment strategy that we discuss in the sequel.

Afterwards, each device exchanges periodically with the 3C hello messages to notify that it still remains in service. Moreover, 3Cs units are continuously coordinating and exchanging data to guarantee a holistic detection process. 3Cs ensure handover in case of mobile equipments (such as mobile radars) as in cellular networks.

2. **Cameras deployment :** Cameras are assumed to be deployed near the borderline at the **abgp!** levels. To provide an efficient coverage for the architecture of *part*01, we considered horizontal-directional cameras that. The viewing field of such a camera determines an angle equal to $\alpha = 23°$, its detection range is D=200 meters, while its radio range is up to 450 meters. For practical reasons, we assume that the maximum distance between the camera and its correlated scalar sensors is d= 125 meters, which is less than the radio range of the scalar sensors. Hence, the covered area by this camera at a given time, noted W, is (see Figure 3.6.A) :

$$W = 2 \times d \times \tan(\frac{\alpha}{2}) \tag{3.1}$$

For $\alpha = 23°$ and d=125 meters, we have $W = 50$ meters, namely two times the sensing range of an UGS (see scalar sensor deployment). As the global field of view of a camera, noted $W^{'}$, is extended when it rotates horizontally, the number of scalar sensors located within $W^{'}$ is increased as well. The value of W' is obtained by considering the distance d between the camera and the scalar sensors and using the Pythagore's theorem, (see Figure 3.6.B).

$$W^{'} = 2\sqrt{(D^2 - d^2)} = 312\ meters \tag{3.2}$$

To guarantee a fault tolerant application the field of view of each camera must be also covered conjointly by its two neighbours (left and right). In case the nearest camera is down, a scalar sensor remains in the field of view of at least one other camera. Hence, we assume that the distance between two consecutive cameras is $d^{'}$=100 meters (see Figure 3.6-C). In this case, the overlapping zone between two cameras is :

$$D_{olapcam} = (W^{'} - d^{'}) = 212meters. \tag{3.3}$$

3. **Scalar sensors deployment :** The main goal of our deployment strategy is to find the minimum number of scalar sensors required to ensure a full coverage of each segment of $Part$01 with a good fault tolerance. As for cameras, scalar

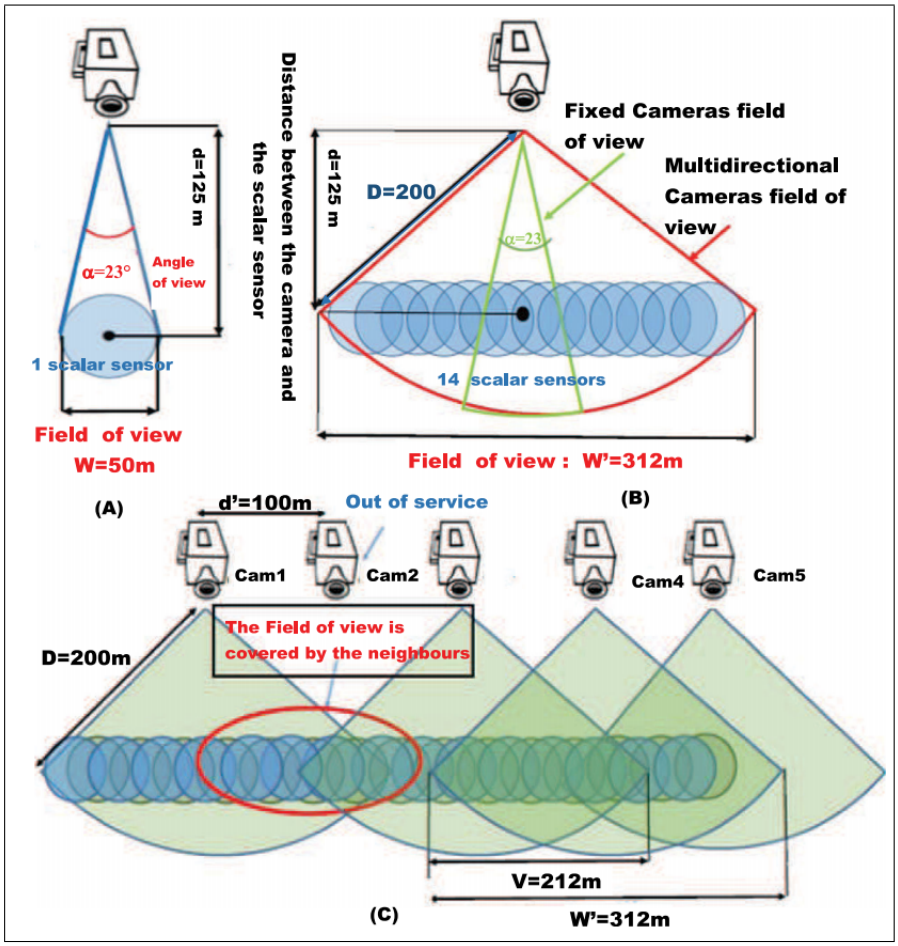


FIGURE 3.6 – (A) : Field of view of a fixed camera (B) : Field of view of a multi-directional camera (C) : Overlapping area between two consecutive cameras

sensors are deployed at the **abgp!** level on the borderline. The RS-U seismic sensor enjoys a theoretical sensing range of 100 meters, which oscillates practically between 25 and 40 meters. However, we assume that its sensing range is $R_s = 25$ meters.

Scalar sensors are deployed progressively to form one barrier along each segment so that to be within the field of view of the cameras and their radio range. To enhance the availability and increase the lifetime of the network in this part of the borders, we assume that two neighbouring sensors overlap each other with a distance $D_{olap} = 30meters \geq R_s = 25$ (see Figure 3.7). Hence, if we deploy k scalar sensors, we get $(k-1)$ overlapping areas. The length of the area covered by a single sensor is equal to 50 meters, 70 meters for two sensors, 90 meters for three sensors and 110 meters for four sensors. Hence, for k sensors, the length of the covered area L is determined by :

$$L = k \times (2R_s - D_{olap}) + D_{olap} \tag{3.4}$$

In this case, the number k of needed scalar sensors to cover an area of length equal to L is :

$$k = \frac{(L - D_{olap})}{(2R_s - D_{olap})} \tag{3.5}$$

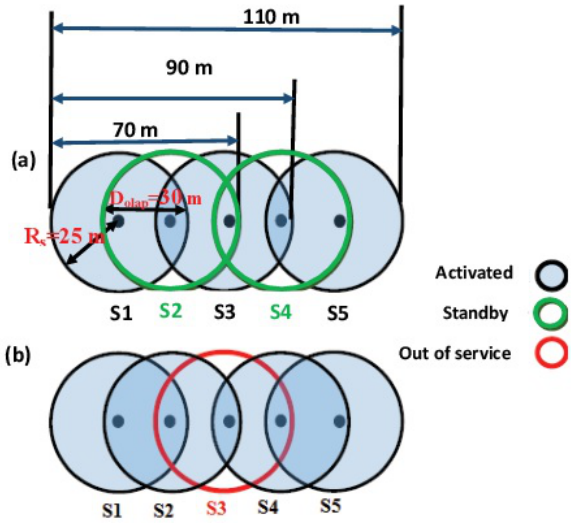


FIGURE 3.7 – (A) : Scalar sensors deployment (03 activated sensors and 02 in standby mode) (B) : If S3 fails, its area is monitored by S2 and S4.

According to equation 3.5 and assuming that $W = 50m$ and $W' = 312m$, the number of sensors covered by one camera is : $k = \frac{(50-30)}{(50-30)} = 1$ at a given instant, and $k' = \frac{(312-30)}{(50-30)} = 14$ when rotating horizontally. Moreover, the number of sensors located in the overlapping area of two neighbouring cameras ($V = 212m$) is : $k" = \frac{(212-30)}{(50-30)} = 9$ scalar sensors.

4. **Radars deployment :** As it was the case for scalar sensors, the goal of our deployment strategy at this level is to use a minimum number of radars while ensuring a full area coverage. Radars are deployed at the **bgg!** level, their number and their exact positions are determined hereafter. Generally, one is required at each **bgg!** level as the distance between two **bgg!** in this $Part01$ is around 50 to $60km$.

   The detection range of the **SQUIRE** radars we consider for this part can up to **48 km** and the overlap point between two consecutive radars should be reached at a point located at **05 km** of the borderline (see Figure 3.8). We assume that the radars are placed at a distance of $d_1 = 28\ km$ to the inside of the borderline, this determines also the position of the **bgg!**. This provides a covering area of $d_2 + d_3 = 20\ km$ towards the outside of the borders, as long as the radar range can up to 48km. We need to determine the distance D' between

two consecutive radars to estimate the number of radars required to cover the borders. As depicted in Figure 3.8, D' can be calculated using the following formulae :

$$\tan(\frac{\alpha}{2}) = \frac{(\frac{D'}{2})}{(d_1 + d_2)}; \quad D' = 2 \times (d_1 + d_2) \times \tan(\frac{\alpha}{2}) \tag{3.6}$$

The overlap zone between two neighbouring radars prevents, at best, high attenuation, extinction phenomena and cover the masks induced by mountain slopes. To obtain a distance $D' = 50km$ which is the distance separating two **bgg!** in $Part01$, the scanning width should be equal to $\alpha = 72°$

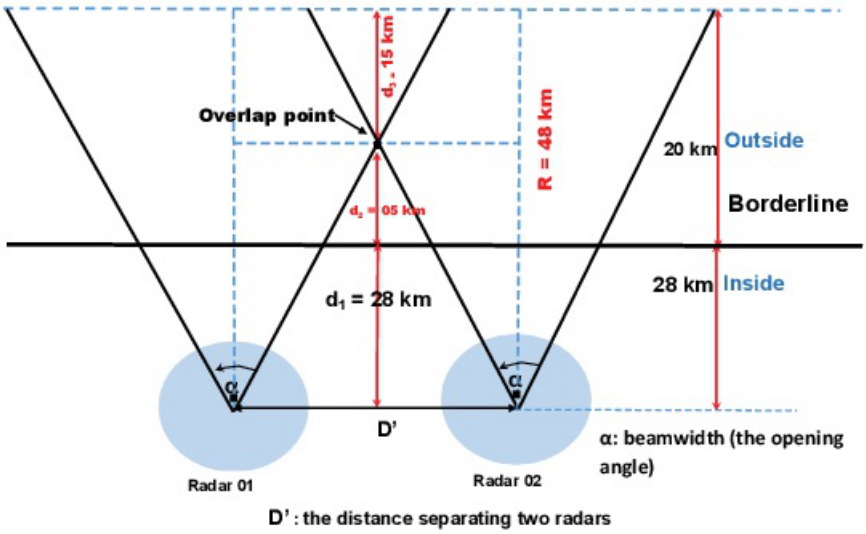


FIGURE 3.8 – Radars deployment : The overlapping area between two consecutive radars.

5. **Unmanned Aerial Vehicle deployment :** UAV are suggested to be used in this part of borders to perform virtual patrol and identification in some critical situations instead of sending pedestrian troops. It is also used for tracking intruders by providing the 3C with the necessary images about their movements. UAV are largely used to secure borders over the world. In USA and according to an article published by **the guardian** in 13 November 2014, the US government has operated about $10,000$ drones to cover about 900 miles, much of it in Texas. According to [68], the drone called Inspire 2 is the most efficient over the world. It enjoys a flight autonomy of 27min covering a maximum distance of 42km, with a maximum speed of 94km/h and a transmission range of 7km. It integrates a Zenmuse X5 camera which is able to record 4K videos with a 72 ˚ field of view at more than 1,6 km distance. Starting from the fact that the area to be monitored by an **abgp!** is equal to a maximum $(100km^2 = (5km \times 20km)$. As we

assume that at least one Inspire 2 is required to patrol a $5 \times 5km^2$ of a square land, therefore, 4 UAV are needed to patrol the area of an **abgp!**. However, to guarantee a fault tolerant tracking system, we consider the deployment of six (06) UAV at each **abgp!**. Therefore at least 24 UAV are provided to patrol the range for each radar. Notice that UAV attached to neighbouring **abgp!** can be called into rescue in case all the local UAV are not operational or already sent in mission.

3.3.2 Deployment strategy for $Part02$

For this part of the borders, our deployment strategy aims to ensure an optimal coverage of the borderline, with a good fault tolerance and considerable reducing of false alarms, only buy using radars and cameras.

1. **Radars deployment :** In the architecture of $Part2$, we recommended the squire radar as in $Part01$, however, we adjust its detection range R_{rad} to $24km$. This adjustment was required in the field to meet the operational requirements expressed by Algerian Border Guards (radar technicians and operational people), depending on several parameters such as the nature of the borderline area (open and clear terrain), the weather conditions of the region(almost always sunny) and the types of the threats that characterize this part of the borders (illegal immigration, weapons trafficking,...). Concretely, as radar is the only device used in the detection process, we need to increase their number and to adapt their positions according to the terrain and the risk level. In the $Part02$ of the borders, most of the lands are desert which seldom activities or movements. The terrain is mainly flat with an open line of sight. Therefore, tactically, it is recommended to place radars the nearest possible to the borders to monitor suspicious activities that occur far outside the borders. Hence, in case of a high intrusion risk, the cameras can be activated for identification and special troupes of **abgp!** alerted to prepare for patrolling missions.

   For radar location, unlike in $Part01$ we preferably install them on the top of the masts between each **abgp!** and the **bgs!**, at a distance of $d_{in} = 04km$ inside the borderline. This makes radars well secured, well powered and also quickly maintained. Therefore, the space to monitor outside the borders is more important comparatively to $Part01$ and dead zones are reduced. Besides, the number of required radars is sensibly increased as the distance between two radars is lesser than in $Part01$.

   As aforementioned in the radar deployment section of $Part01$, the *overlappoint*

between two consecutive radars should be reached at a point located at **05 km** from the borderline, this distance is called $D_{Olap-point}$. The length of the overlapping area between two consecutive radars is noted $d_{olap-rad}$. Now we need to determine the distance D_{2Rad} between two consecutive radars to estimate the number of radars required to cover the entire area of interest. As depicted in Figure 3.9, D_{2Rad} can be calculated using the following formula :

$$\tan(\frac{\alpha}{2}) = \frac{(\frac{D_{2Rad}}{2})}{(d_{in} + D_{Olap-point})}; So: \quad D_{2Rad} = 2 \times (d_{in} + D_{Olap-point}) \times \tan(\frac{\alpha}{2}) \tag{3.7}$$

In this case the outside borderline area covered is d_{out}, with :

$$d_{out} = R_{rad} - d_{in} \tag{3.8}$$

The overlapping area $d_{olap-rad}$, is calculated, as follow :

$$\tan(\frac{\alpha}{2}) = \frac{(\frac{d_{olap-rad}}{2})}{(d_{out} - D_{Olap-point})}; So: \quad d_{olap-rad} = 2 \times (d_{out} - d_{Olap-point}) \times \tan(\frac{\alpha}{2}) \tag{3.9}$$

Therefore, if the scanning width is equal to 90°, the distance between two radars is, $D_{2Rad} = 18km$, this is the maximum distance between two radars we can obtain in $Part02$ as the scanning width rarely overtakes 90° in the squire radar. Hence, 3 to 4 radars are thus needed in each BGS. As a result, in $Part02$, we need to consider these distances between radars so that their positions be close to the logistic infrastructures, when taking into account the deployment constraints (4km inside the borders).

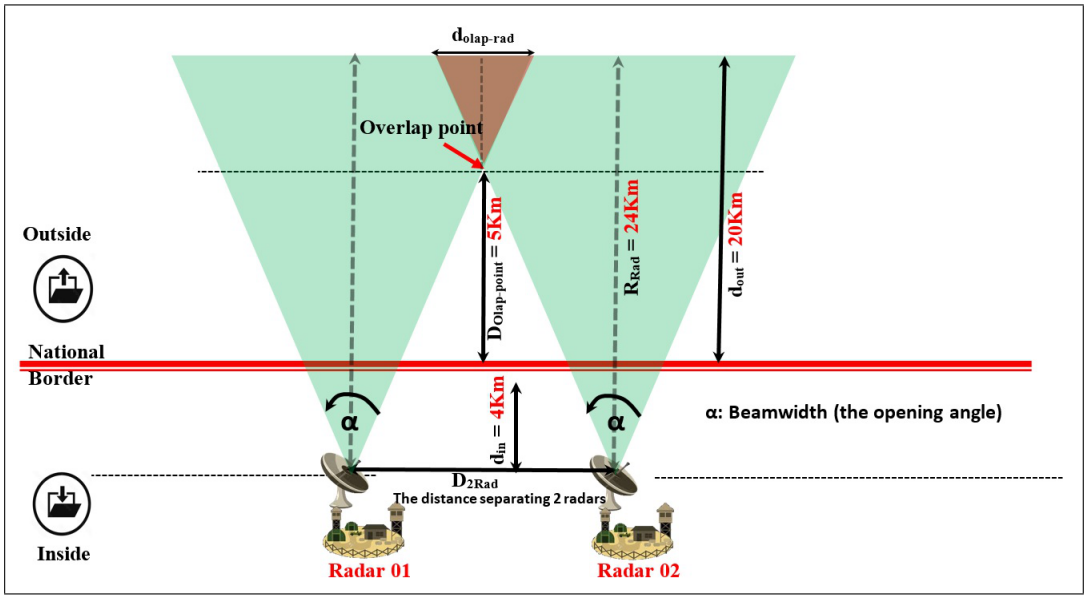


FIGURE 3.9 – Radars deployment strategy for $Part02$ of the borders.

To guarantee radars fault tolerance, the operator at the $3C$ level can deploy a mobile radars (mounted on a car, one or two mobile radars are supposed to be available in each **bgg!** level of the hierarchy of border guard forces) to replace the damaged one whenever a radar breaks down in whatever a BGS.

2. **Camera deployment :**

   The main challenge of our strategy is to find the minimum number of cameras to be deployed in order to ensure a full coverage of the area of interest with a good fault tolerance since we are dealing with a sensitive non stop application. To meet those requirements, the first goal is to determine the necessary number of cameras noted ($N_{Cam-AoI}$) to cover the entire area of interest noted L_{Cam}, this is equivalent to calculate the distance between two consecutive cameras noted D_{2Cam}. Hence, we can easily determine the required number of cameras to cover the detection range of one radar, noted $N_{Cam-Rad}$. To ensure a good fault tolerance when deploying cameras, overlapping areas between them are considered in our deployment strategy for this part of the borders. First of all, let us recall that the detection range of the cameras considered in $Part02$ can up to $10Km$. A good fault tolerance means that if for a whatever reason a camera breaks down or is unavailable, its area of responsibility must be covered by other cameras in the field. We assume that cameras at located at the **abgp!** level, 2km inside the borders. As depicted in Figure 3.10, we consider that the overlapping area between two neighboring cameras, noted $d_{olpa-cam}$ should be greater or equal than the detection range of R_{Cam}. Let us assume that $d_{olpa-cam} = 15Km$; that means that 1 camera can have 4 other cameras within its range. The length of the coverage area by $N_{Cam-AoI}$ cameras is given by the following formula :

$$L_{Cam} = N_{Cam-AoI} \times [2 \times R_{Cam} - d_{olap-cam}] + d_{olap-cam} \tag{3.10}$$

	$N_{Cam-AoI} = 1$	$N_{Cam-AoI} = 2$	$N_{Cam-AoI} = 3$	$N_{Cam-AoI} = 4$
$L_{Cam}(Km)$	20	25	30	35

TABLE 3.2 – Numerical example : the area coverage function of the number of cameras.

In this case and according to 3.10, the distance between two consecutive cameras noted D_{2Cam} can be given as follow :

$$D_{2Cam} = 2 \times R_{Cam} - d_{olap-cam} \tag{3.11}$$

Therefore, in case $d_{olap-cam} = 15km$, we obtain $D_{2Cam} = 5km$ Each **abgp!** will be in charge of 5 to 8 cameras.

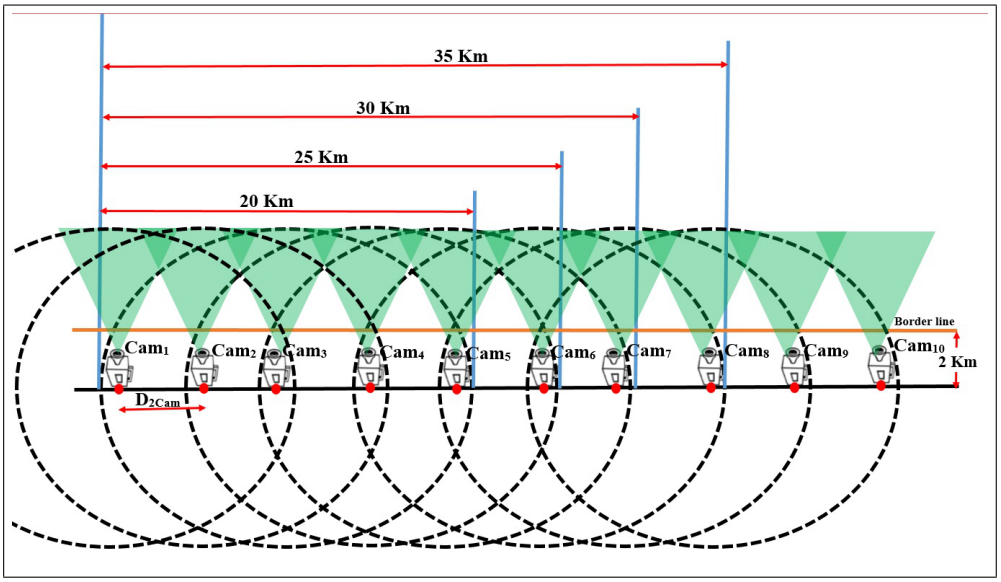


FIGURE 3.10 – Cameras deployment strategy for *Part*02 of the borders.

Remark : For exact camera positioning in the field, we assume that the geographical coordinates of these locations are already known and determined on the ground by experts, and recorded at the 3C. This positioning should avoid dead zones and all kind of bad areas.

3. **The 3C deployment :** The 3C is planted at the **bgg!** level as illustrated in Figure 3.1. The 3C must be within 30 from the borderlines. The horizontal distance between two consecutive 3Cs can reach $60km$ in the *Part*01 of the borders. The communication between the 3C and devices at the other levels is ensured by the communications network subsystem (COM).

3.4 Activation Scheduling Strategy

It is clear that the use of technology in border surveillance process further improves the quality and reliability of the service offered. However, in sensor network technology, the rationalization of certain parameters such as energy consumption, plays a decisive role in extending the network lifetime. Therefore, we further design mechanisms to reduce the attrition and the energy consumption of our surveillance network. In this section, we discuss the scheduling strategies for the activation of the cameras and the UGS, that we have proposed for the two parts of the Algerian borders, *Part*01 and *Part*02.

3.4.1 Activation scheduling strategy adopted for $Part01$

As explained before, the proposed architecture for monitoring the $Part01$ of the Algerian borders was based on four different type of devices (scalar sensors, multimedia sensors, radars and UAV). UGS and camera represent the big amount of sensors deployed in this architecture. Many sensors can be deployed to monitoring the same area, this redundancy is useful since it increases the fault tolerance of the network [69, 70]. However, this can be achieved only by enforcing a reliable activation scheduling strategy that consists in balancing the load between the network nodes. Therefore, our scheduling strategy for $Part01$ regards only UGS and cameras which are both correlated to operate in coordination.

Activation strategy for scalar sensors :

According to our deployment strategy for the $Part01$ of the borders, at least one scalar sensor should be in the field of view of one camera at a given time. When a camera rotates horizontally, 14 scalar sensors at least are within its global field of view. Add to this, each scalar sensor should be in the global field of view of at least two different cameras at a given instant. Hence, for energy saving purpose, we consider that two neighbouring scalar sensors are activated alternatively. This means that if at a given time the scalar sensor S_i is active then the sensor S_{i+1} must be in standby mode, for $i = 1..k-1$ (See Figure 3.7). In other words, among the 14 scalar sensors in the global field of view of one camera only 7 are active. Such a strategy maintains the sensing capabilities of the network as 7 active scalar sensors achieve to cover holistically the area. However, if a sensor is subject to a failure or energy depletion, its two neighbours are automatically activated as depicted in Figure 3.7. Concretely, the protocol is implemented at the 3C level which is in charge of ruling the area. The 3C sends alternatively activation and standby messages every α time units to all the scalar sensors that remain in service. The latter respond to the 3C requests by sending a *hello* message to acknowledge the request reception and notify their liveness. If the 3C does not receive the *hello* message from a sensor "i" by the end of the period, then "i" is suspected to be out of service and its neighbours "$i-1$" and "$i+1$" are then kept continuously in active mode till the sensor "i" is replaced or repaired. The value of α, which is fixed by the 3C, is dynamic and can be differently fixed through time and from a sector to another. The effect of varying the value of α on the strategy performances is discussed a little later in a dedicated section. In the extreme case of a cascading failure of scalar sensors, the 3C operator can remedy by rotating the appropriate camera to the position of the failing sensors or use mobile radars to monitor the area (meanwhile the damaged sensors are

replaced). He can also dispatch an UAV to fly over that sector in case the camera is also out of service. For sensitive areas, we suggest to double the number of sensors. This means that in each zone we can deploy two sensors rather than one. One is activated alternatively as described previously, while the second is activated only in case the first one is subject to a failure. Therefore, a camera is correlated with $28 = 14 \times 2$ sensors of which 7 are activated at a given instant. Note recalling that **active mode** means that sensing, emission and reception units are activated, **standby mode** means that only the emission and reception units are on. The algorithm in Figure 3.11 describes this strategy.

```
Begin
1  Int k, i =1 ;
2  Sensors S[];
3  While i is less than or equal to k-1
4     Si.Activate();
5     Si+1.Standby();
6     If Si.fail() = true then
7        Si-1.Activate();
8        Si+1.Activate();
9     EndIf
10    i=i+2;
End
```

FIGURE 3.11 – Algorithm of the activation scheduling strategy for scalar sensors

Activation strategy for cameras :

After the deployment phase, the 3C associates with each camera the 14 scalar sensors with which it operates and conversely, relates each scalar sensor with the cameras that can handle its alarms. Every α time units, a camera broadcasts to the 3C as well as to its correlated scalar sensors a *hello* message to notify its liveness while piggybacking some other information about its current status :

(i) ***Availability :*** This denotes whether the camera is free or busy (performing a visualization task).

(ii) ***Battery level :*** Denotes the available energy in the camera batteries.

(iii) ***Camera rotation angle :*** This is encoded by a variable A taking its value within the interval $[1, 14]$. The value of A gives the relative ID of the current scalar sensor which is in the field of view of the camera. Hence the value of A determines the 14 admissible positions of the camera when rotating, such that each position allows to cover the whole sensing range of one sensor.

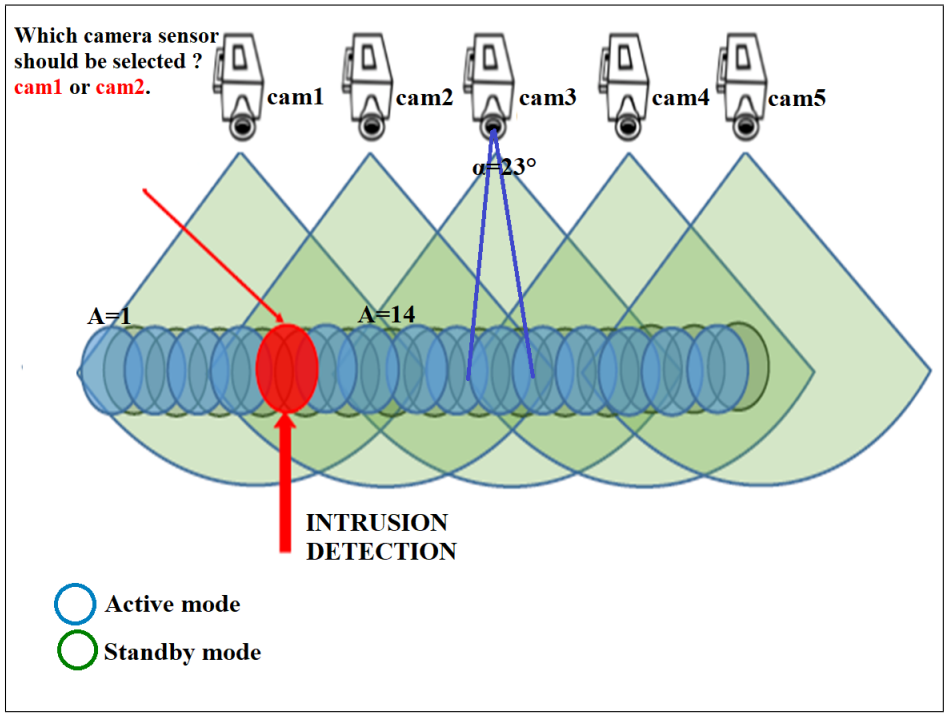


FIGURE 3.12 – Selection of the appropriate camera.

The value of α is correlated with the activation period of the scalar sensors. This means that the status of the camera should be provided to the related sensors at least once during their activation period. However, every time the camera has to change its position or its availability, it should also broadcasts its new status. As cameras are more energy consuming and more likely to fail than scalar sensors, our strategy is to activate the cameras only when receiving alarms. The scalar sensor should select the most appropriate camera to activate (see Figure 3.12). To this end, it uses the current status of the cameras in the selection process. Once the scalar sensor knows which cameras are free (available), it considers their battery level and their current position relatively to its own. As rotating the camera is energy consuming, the camera with the nearest position to the intrusion area is favoured. Considering a scalar sensor i and a free camera j at position A_j with a battery level $ECam_j$, we compute the coefficient of the camera j relatively to the scalar sensor i, as follows :

$$F_{i,j} = ECam_j - [\mid A_j - pos(i,j) \mid \times C] \tag{3.12}$$

Where $pos(i,j)$ denotes the sequential position of the scalar sensor i relatively to the global field of view of the camera j. C denotes the energy consumption of the camera when rotating with one position. Hence, the camera j with the highest coefficient $F_{i,j}$ is selected by the scalar sensor i. For the selection purpose, only the coefficient $F_{i,j}$ are calculated by using a simple formula. The sensor memory occupation is derisory as we

need to store only three parameters for each camera (the number of cameras related to each sensor is maximum 3). The $F_{i,j}$ are processed by the scalar sensor episodically whenever it detects the presence of an intruder. This does not greatly impact the energy level of the scalar sensors. Delegating this operation exclusively to cameras or to the 3C level requires more coordination, thus inducing a higher latency which cannot be afforded in such critical applications. Add to this, the global energy required for this task may be more important as the amount of exchanged data will increase. As all we know, the energy consumption due to data transmission is by far more important than that due to sensing or processing. The algorithm of this strategy is presented in Figure 3.13.

```
Begin
 1  Int i,j ;                                  // two indexes;
 2  Int m,n;                                   //camera sensors and scalar sensors number respectively;
 3  Int alpha;                                 //Time units;
 4  Camera sensor Cam[];                       //a vector of camera sensors;
 5  SelectedCam Camera sensor;  // The selected camera sensor
 6  Sensors S[];                               //a vector of scalar sensors;
 7  Int [] A;                                  //Position of a camera;
 8  Int [] ECam;                               //Energy of a camera;
 9  Const C;                                   //Camera's energy consumption when rotating with one position;
10  Int [][] Pos;                              //Sequential position of a scalar sensor relatively to the global field of view of a camera;
11  nt [][] F;                                 //Coefficient of a camera relatively to a scalar sensor;
12  Repeat for every alpha
13   For j=1 to m
14      Camj.sendHelloMessTo3C();
15      For i=1 to 14                          //The camera is correlated with 14 scalar sensors
16         Camj.sendHelloMessToSi();
17         Camj.sendAvailablToSi();
18         Camj.sendBateryLevelToSi();
19         Camj.sendRotateAngleToSi();
20         Fi,j = ECamj-(|Aj – Posi,j|*C);
21      EndFor
22   EndFor
23   If Si.intrusion() = true then
24     SelectedCam = SelectMax(Fi,j);
25     SelectedCam.Activate();
26   EndIF

End
```

FIGURE 3.13 – Algorithm of the activation scheduling strategy for camera sensors

Another solution is to let the sensor choose randomly a camera without knowing whether it is free or not, or whether it is the closest to its position or the farthest. This induces extra times due to busy cameras selection or extreme rotations. In the case we consider that the sensor broadcasts the alert to all the related cameras without a selection beforehand then we may have several cameras in charge of visualizing the same area resulting in extra latency for handling requests coming from other sensors because of the waiting time for the redundant cameras to free.

-Example : Let's assume three free cameras Cam_1, Cam_2 and Cam_3 covering the

sensing zone of a scalar sensor S_3 which detected an intrusion. We report in Table 3.3 the relative positions of the scalar sensor relatively to each camera, together with the battery level and the current position of each camera. By using formula 3.12 and assuming $C = 20$, we obtain : $F_{1,3} = 1100 - 160 = 940$; $F_{2,3} = 1150 - 200 = 950$; $F_{3,3} = 1080 - 100 = 980$. Hence, the appropriate camera to be selected is Cam_3.

	$Pos(i,j)$	$ECam_j$	A_j
Cam_1	9	1100	1
Cam_2	4	1150	14
Cam_3	1	1080	6

TABLE 3.3 – Numerical example : camera selection.

Once a free camera receives a visualisation request from a sensor i, it handles the latter by updating its status and broadcasts a *hello* message to the 3C and all the associated sensors. Then it rotates, if needed, to the targeted area and starts sending streams to the 3C as long as a change is detected in the scenery. When the sensor i responsible of the alert receives the *hello* message, it compares the position of the camera Pos_j and its own Pos_i. If $Pos_j = Pos_i$ then the sensor confirms that the camera has dealt with its request. In this case, the sensor i stops sensing till the camera in charge of its request changes again its status (moving position or switching to free mode). Note recalling that the camera can switch off either if no changes are detected in the scenery or by decision of the operator in the 3C. If the request has not been handled by the camera($Pos_j \neq Pos_i$), and if the intrusion remains detected, the scalar sensor selects another free camera to process the visualisation request. Notice that this happens when different sensors are selecting the same camera. In this case, the camera handles the first request received and ignores the others as long as it remains in the buzzy mode. However, if no free camera is available, the sensor waits for a free camera as long as the intrusion signal is sensed.

3.4.2 Activation scheduling strategy adopted for $Part02$

In this section, we outline our proposed algorithm to schedule the activation of cameras in $Part02$ of the borders.

Let us, first, discuss the differences in terms of design constraints between $Part01$ and $Part02$. As radars are the only mean of detection used in $Part02$ and as they cover larger areas that are mainly located outside the national borders, the tolerated latency

to observe between the detection and the operational decision is much higher in $Part02$. Furthermore, the area to be monitored by each camera is huge comparing to $Part01$, as the covering range can reach $10km$ in a 3D space. Indeed, as radars can detect in addition flying objects, unlike UGS, this extends the zone subject to identification by the cameras. Therefore, cameras in $Part02$ are able to move horizontally and vertically too, to identify pedestrians, rolling as well as flying vehicles.

Comparing to $Part01$, a smaller number of cameras is required to monitor the same distance of borders in $Part02$. However, the load may be more important as the probability to observe different intrusion events soliciting the same camera is higher. Therefore, we deem useful to redesign the activation strategy presented in $Part01$ to meet the deployment and operational constraints required in $Part02$.

For this effect, we recommend to centralize the coordination and the management of the tracking and identification task at the 3C level as the latency is not a primary concern. Such a solution makes it possible to have a global view on all the network resources and to manage more efficiently the activation strategy of the cameras. Hence, all the communications need to go through the 3C (Direct communications between cameras or radars do not take place).

From a practical point of view, ensuring an uninterrupted monitoring of an intruder in a real-world environment, such as borderlines, requires the collection and the processing of data from a large surveillance area, which demands a significant increase in the number of cameras to be used. In addition to that, challenges are becoming increasingly difficult with the increasing scale and complexity of border surveillance systems, especially with the use of "networks" of cameras. It is clear that setting up a network based border surveillance system can improve the coverage, but it can also create several difficulties. On the one hand, being limited in energy and subject to damage and attrition, cameras can not remain active continuously. As for $Part1$, the idea is to activate only the appropriate cameras in terms of observing relevance. However, a fundamental question should be answered : Which criteria should be considered, and how to activate the appropriate camera in order to achieve the best compromise between an optimal tracking and the preservation of the resources ?.

To this end, we introduce **Camera Sensors Scheduling Strategy (C3S)**, a global strategy of collaboration between the various components of the network, which are : radars and the cameras. Based on the radars output(early alarms), the processing units (integrated to the server at the 3C level) generate spatio-temporal observation requests for all the intrusion events which are candidate for close-up views by the available cameras. However, this procedure may be more complex when the number of intrusions

exceeds the number of cameras, especially in the case of multiple intrusions (in convoy and / or dispersed) in harsh environments characterized by severe occlusions (obstacles) and irregular interactions.

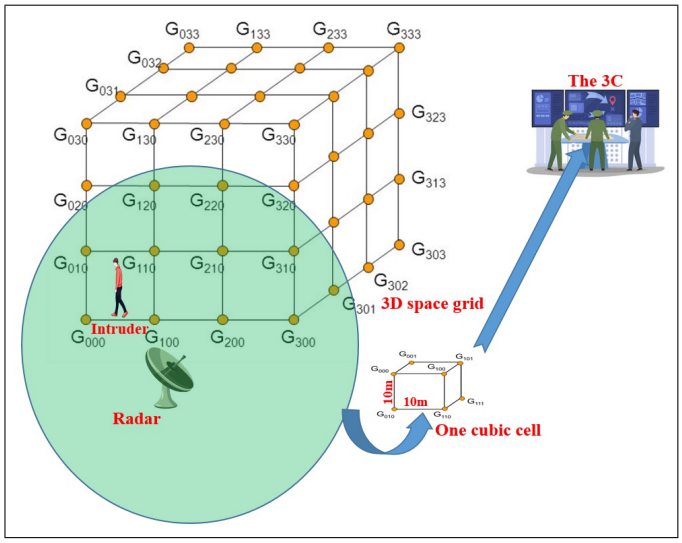


FIGURE 3.14 – Dividing the 3D space into cubic cells.

To do that, we need to divide the area of interest which is a $3D$ space into a cubic cells, forming a $3D$ regular grid as depicted in Figure 3.14. The length of the side of the cubic cell is noted D_c, The value is fixed at the 3C and corresponds to the dimensions of the area captured by a camera at a distance D_c, with the highest resolution and with a normal focus. Generally, D_c is between 10 and 50 meters. Therefore, the content of the cell should be visible within the field of view of the camera. For example if we consider a $10m$ cubic cell, it should be visible entirely at a distance of $10m$ of the camera. Each cell s is thus referenced with a number, $IdC(s)$, that allows its identification and localisation. For this effect, the 3C manages a table that associated with each cell s, its exact coordinates in the 3D space $cor(s) = (x_s, y_s, z_s)$, such that x_s y_s and z_s are respectively the 3D coordinates of the center of the cell s. We associate also the parameter $InB(s)$ that takes the value 1, if the cell s is inside the borders, 0 otherwise.

Moreover, we assume the following hypotheses :

— Let m be the number of cameras associated with each 3C (each **bgg!**).
— Let ECC be the energy capacity of the batteries of the cameras.
— For each cell s and a camera C_j, the server at the 3C maintains a table $Infield(s, j)$ which takes the value 1 if the cell s is within the covering range of the camera C_j ; 0 otherwise.
— Each radar and each camera communicates with the server at the 3C level (send

all the required information via the COM subsystem). Periodically, every ζ time units, each device exchange with the 3C a hello message, to notify its liveness. If no message is received after a number of periods, the device is suspected to be in fault, and will not be longer considered in the border surveillance task until it will be repaired or replaced ;

— The server at the 3C maintains a table that manages the status of all the cameras within the range of the **bgg!**. Therefore, for each camera C_j, it associates the record $(IdM(j), PosM(j), Or(j), En(j), Focus(j), Stat(j))$, such that :
  — $IdM(j)$ is the identifier of the camera C_j ;
  — $PosM(j) = (xm_j, ym_j, zm_j)$ is the coordinates of the position of the camera C_j ;
  — $Or(j) = (\beta_j, \gamma_j)$ denotes the orientation vector of the camera C_j when rotating with $\beta_j \in [0, 180°]$ and $\gamma_j \in [0, 180°]$ which are respectively the horizontal and the vertical rotating angles ;
  — $En(j)$ represents the available energy, given in joules, in the battery of the camera C_j ;
  — $Focus(j)$ is the current focus of the camera C_j ;
  — and finally $stat(j)$ denotes the current status of the camera C_j which can take one of the following values (OFF, standby, active, faulty).

— the 2D and 3D distances between two positions (x_i, y_i, z_i) and (x_j, y_j, z_j) are computed as follows :
$Dist2D(i, j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$
$Dist3D(i, j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}$

— Each camera C_j notifies in the hello message, the available energy in its battery $En(j)$, its current orientation vector $Or(j)$, its current focus $Focus(j)$, and its current status $stat(j)$. If the camera is faulty or OFF, it can not communicate with the 3C.

— Let I_i be an intrusion event, the state of I_i at the instant t is noted SI_i and defined by the following vector :
$SI_i(t) = (I_i, Pos_i(t), V_i(t), Typ_i(t)), St_i(t))$, such that :
  — I_i is the identifier of the intrusion.
  — $Pos_i(t) = (x_i(t), y_i(t), z_i(t))$ are the 3D coordinates of the intrusion I_i at the instant t ;
  — $V_i(t) = [xv_i(t), yv_i(t)]$ is the 2D velocity vector of the intrusion I_i measured at instant t ;
  — $Typ_i(t)$ is the intrusion classification by the Squire radar that takes its value as follows :

$$Typ_i(t) = \begin{cases} 1 & \text{If intrusion class = Tank,} \\ 2 & \text{If intrusion class = Heavy vehicle,} \\ 3 & \text{If intrusion class = Aircraft,} \\ 4 & \text{If intrusion class = drone,} \\ 5 & \text{If intrusion class = Helicopter,} \\ 6 & \text{If intrusion class = Light vehicle,} \\ 7 & \text{If intrusion class = Pedestrian.} \end{cases} \tag{3.13}$$

— $St_i(t)$ determines the status of the intrusion that can take two vales : $Closed$, if the intrusion is closed, or $Active$ is the intrusion is on.

Methodology

The network architecture of $Part02$ of the borders includes radars, and cameras. A processing unit (integrated to a server at the 3C) receives the environmental information provided by the radars, such as the positioning and the nature of the intruders to be used to monitor and schedule the observation tasks of the cameras. The reliability of the scheduling relies mainly on the predictions precision of the states of the intrusion events to be managed.

When a whatever radar detects at an instant t the presence of an intruder I_i inside its detection range, every period ζ, it communicates to the 3C, the last state $SI_i(t)$. If the intrusion I_i is new, the server at the 3C level creates a new record in the database that stores its received state. Otherwise, it connects the last received state $SI_i(t)$ to the intrusion I_i already identified in its database. As long as the intrusion I_i remains continuously in the monitored area it will keep the same identifier by the radar and the 3C server. However if it leaves the area of interest the intrusion is closed. If the same object reenter the surveillance area it will be considered as a new intrusion. Note that an intrusion can be closed by the operator, if it has been handled or if he deems that it does not worth to maintain the tracking any longer. Therefore, a closed intrusion is no more considered in the scheduling process.

In order to perform the scheduling of camera allocation, the server proceeds every ζ time units to compute some parameters associated with the recorded intrusions. Let t_ζ be the instant associated with the last scheduling period ζ, we have :

— When an intrusion state $SI_i(t_\zeta)$ is notified to the server, the latter determines the

id of the cell $Cell_i(t_\zeta)$ within which it is located at instant t_ζ by corresponding the coordinates of the cell with those of the intrusion event.

— The server maintains for each intrusion I_i, the parameter NbQ_i which computes the number of quantum allocated by the scheduler to observe the intrusion I_i.

— Then it calculates the weight $W_i(t_\zeta)$ that denotes the priority of the intrusion event I_i computed at the instant t_ζ, using the following formula :

$$W_i(t_\zeta) = \frac{1}{Tprog_i(t_\zeta) \times Typ_i(t_\zeta) \times (1 + NbQ_i)} \tag{3.14}$$

Such that, $Tprog_i(t_\zeta)$ denotes the progression time of the intrusion I_i measured at instant t_ζ :

$$Tprog_i(t_\zeta) = \begin{cases} \infty & if\ yv_i(t_\zeta) \leq 0 \\ \frac{Dist2D_{i,S_i}(t_\zeta)}{\sqrt{xv_i(t_\zeta)^2 + yv_i(t_\zeta)^2}} & otherwise \end{cases} \tag{3.15}$$

Such that s_i is the closest borderline cell to the intrusion I_i relatively to its velocity vector (See Figure 3.15).
$Dist2D_{i,s_i}(t_\zeta) = \sqrt{(x_i(t_\zeta)) - x_{s_i})^2 + (y_i(t_\zeta) - y_{s_i})^2)}$
Remark : when $yv_i(t_\zeta) \leq 0$ this means that the intruder is moving away from the borders.

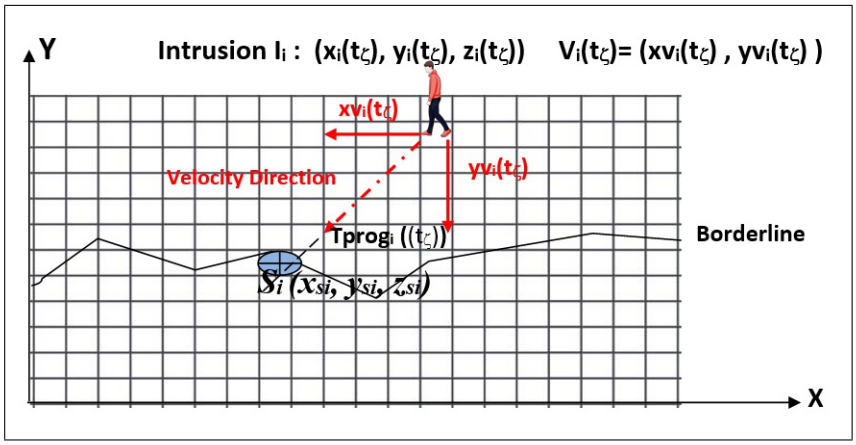


FIGURE 3.15 – Illustration of the calculation principle of the intruder progression parameter in the area of interest.

— Then for each camera C_j for each intrusion I_i, the server computes the following parameters :

— $Rotating_{i,j}(t_\zeta) = (LR_{ij}(t_\zeta), VR_{ij}(t_\zeta)$ denotes the rotating vector of the camera C_j so that to have the intrusion I_i visible within its field at instant t_ζ when using a normal focus (See Figure 3.16).

$$LR_{ij}(t_\zeta) = \begin{cases} \alpha' - \beta_j & if\ x_i(t_\zeta) < xm_j \\ 180° - \beta_j - \alpha' & otherwise \end{cases} \qquad VR_{ij}(t_\zeta) = \theta - \gamma_j \quad (3.16)$$

such that,
$Tang(\alpha') = \frac{|y_i(t_\zeta) - ym_j|}{|x_i(t_\zeta) - xm_j|}$ $\quad Tang(\theta) = \frac{|z_i(t_\zeta) - zm_j|}{Dist2D_{ij}(t_\zeta)}$

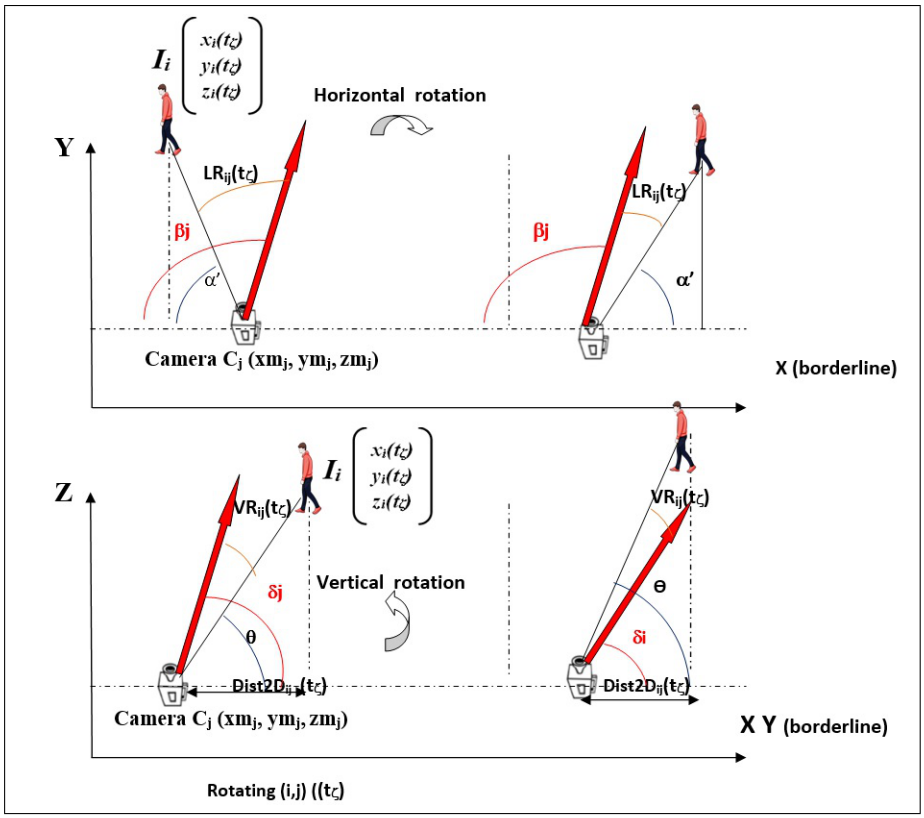


FIGURE 3.16 – Camera rotations to have the intrusion in the FoV.

— $EnerC_{i,j}(t_\zeta)$ denotes the energy required to rotate the camera C_j towards the position of the intrusion I_i and to adjust the focus to obtain a close up observation.

$$EnerC_{ij}(t_\zeta) = (LR_{ij}(t_\zeta) + VR_{ij}(t_\zeta))EUR + Focus_{ij}(t_\zeta)EUF \quad (3.17)$$

$$Focus_{ij}(t_\zeta) = \begin{cases} \frac{\frac{Dist3D(i,j)}{DisF}}{Focus_j} & if Focus_j \leq \frac{\frac{Dist3D(i,j)}{DisF}}{Focus_j} \\ \frac{Focus_j}{\frac{Dis3D(ij)}{DisF}} & otherwise \end{cases} \quad (3.18)$$

Such chat : EUR is the number of energy units consumed by rotating the camera with 1°. EUF is the number of energy units consumed when updating the focus with one scale. $DisF$ is the distance observed when upgrading the focus of the camera with one scale unit to obtain a close up observation.

— $Trot_{i,j}(t_\zeta)$ denotes the time needed for the camera C_j to rotate toward the position of the intrusion I_i.

$$Trot_{ij}(t_\zeta) = (LR_{ij}(t_\zeta) + VR_{ij}(t_\zeta))TUR \tag{3.19}$$

such that, TUR is the time needed to rotate the camera with one degree.

— Then, the scheduler has to elaborate the different observation requests to associate with the m cameras. Let $Req_k(t_\zeta), k = 1..P$ be the set of requests to elaborate at instant t_ζ. To do so, the scheduler workouts whether it can first regroup different intrusion events into one group request, this is possible if all the intrusion events of the group are visible within the field of view of one camera providing that the used focus offers an acceptable image quality to identify all the intrusions of the group. The latter is determined by considering any couple of intrusion events within a maximal predefined distance $Dist_{Max}$.

$$\forall, I_{i1}, I_{i2} \in Req_k, Dist3D(i_1, i_2) \leq Dist_{Max} \tag{3.20}$$

— Therefore, the request Req_k of a group of intrusions, defined at t_ζ is characterized by the tuple $(List_k, PR_k, WR_k, Tprog_k)$ such that :
  — $List_k$: determines the list of intrusion events within the group request Req_k.
  — PR_k : is the id of the cell that determines the gravity center of all the positions of the intrusions events within the group request Req_k.
  — WR_k : denotes the weight of the request computed as the sum of the weight of all the intrusion events within the group Req_k. Formally, we have :

$$WR_k = \sum_{i \in req_k} W_i(t_\zeta) \tag{3.21}$$

  — $Tprog_k$ is the minimum progression time when considering all the intrusion events within the group request : $Tprog_k = MIN_{i \in Req_k} Tprog_i(t_\zeta)$

  We are particularly interested in the acquisition of a high quality close-up videos of intruders to better identify them and ensure their uninterrupted tracking, until their interception. Every ζ, new group requests for spatio-temporal observation are created by applying the same rules.

According to the literature, [67, 71], cameras planning is a preemptive and an "online" scheduling problem, because it is done whenever tasks arrive in the system (from the temporal parameters of all tasks during the application execution).

At any time and by using tasks parameters of the specific instant, the scheduling algorithm is able to handle requests that have not been previously enabled. This makes it flexible to adapt to environment changes. Hence, we have to plan a set of n group

requests on a the architecture composed of m cameras. This type of problem was formulated for the first time by [72]. It is a question to apply on all the cameras a global scheduling strategy and to make sure that at every period t_ζ, the highest priority tasks are attributed to the m cameras, otherwise processors are left idle (or inactive). In this approach, in addition to the preemption of the tasks, the migration of these tasks is also allowed. A task can therefore begin its execution on a camera C_j, then be preempted by a higher priority task, to resume its execution on another camera $C_{j'}$, with $j \neq j'$. This phenomenon is called task migration and is a feature of global approaches. To highlight this approach, the literature proposes the use of the Round Robin (RR) algorithm.

Round Robin algorithm is specially adapted to systems called ***in shared time***. It is a question of a preemptive scheduling by turnstile that defines a time slice called *quantum*. Each camera C_j owns a queue wherein requests assigned by the scheduler each period ζ are sorted according to their weights WR_k The higher priority request in the queue acquires the camera for a maximum time equal to the quantum Q. We assume that Q is fixed by the 3C and its value is the same for all the cameras. If the request is closed before the end of the quantum, it releases the camera and the next request in the queue is considered. If the request remains active at the end of the quantum, it may lose the camera or migrate to another camera, depending on the result of the last scheduling period (performed every ζ).

In our solution, we try to avoid the identical allocation of resources to all the tasks. To achieve this, we propose the use of a weighted version of the RR algorithm that allows assigning requests to multiple cameras while considering their different load capacities and their relevance to observe an intrusion group request. This is scheduling adjusted dynamically every period ζ to ensure fairness, by recomputing the group requests and their weights.

The overall performance of the cameras is strongly related to the ability of each one to perform the observation tasks assigned to it. The capacity level of a given camera can be quantified by the precision of the calculation of its relevance for the task to be accomplished. We determine the relevance of a camera C_j to the group request Req_k by measuring the following factor :

$$R_{k,j}(t_\zeta) = Infield(s,j) \times \frac{ECC}{En(j) - EnerC_{s,j}(t_\zeta)} \times \frac{1}{1 + NbR_j} \times \frac{1}{Trot_{s,j}(t_\zeta)} \quad (3.22)$$

Let $s = PR_k$ be the position of the center of the group. Such that, NbR_j is the number of observation requests already scheduled in the queue of the camera C_j. NbR_j is incremented every time a new request Req_k is assigned to the camera C_j

The value of $R_{k,j}(t_\zeta)$ is a dynamic weight which represents the relevance of the

camera C_j to observe the group request Req_k at the instant t_ζ. This parameter plays a decisive role in the allocation and the balancing of the observation requests on the different cameras.

According to the formula 3.22, assuming a request Req_k, the highest value of $R_{k,j}(t_\zeta)$ when varying j, allows to determine the camera j to assign to the Req_k. The first part of the formula allows to promote only the cameras that have the intrusion request within their observation range, and exclude the others. The second factor favours the cameras that are close to the intrusions so that to manage efficiently their available energy when rotating and updating their focus. The third part of the formula promotes the cameras that are free $NbR_j = 0$ or that have the lesser requests in their queues ; this allows to balance the load over all the cameras equitably. Finally, the last part of the formula gives priority to the fastest camera to get in position to observe the intrusion scene. This factor makes it possible to reduce the time elapsed before servicing the observation requests.

If different requests are assigned to the same camera, they are sorted in the related queue according to their weights. According to formulas 3.14, and 3.21, an intrusion group request has more chances to be considered than a single intrusion request. Moreover, an intrusion with a higher risk of harmfulness and a faster progression time towards the borderline has more interest. Finally, an intrusion that has been already observed has lesser chances to be promoted again by the scheduler.

When a request is handled by a camera, the latter rotates to the position, if needed. Then it starts to track the travelling of the intrusions automatically, by rotating and adjusting its focus. Indeed, the PTZ cameras considered in $Part02$ are endowed with a tracking module allowing them to follow the moving targets in the captured videos. The 3C is informed about the updates in the state of each camera when receiving periodically their hello messages.

This activation scheduling strategy is mainly depending on two parameters which are : the period ζ and the value of the quantum Q. These two parameters are set at the 3C and their values impact greatly the performances and the lifetime of the network.

If the period ζ is reduced, the accuracy of the tracking as well as the latency will be improved. On the other hand, the load will increase sensibly, as sensors are sending more frequently hello messages to notify updates, resulting in more scheduling periods to perform at the 3C. Besides, the energy of cameras may be depleted more rapidly due to communication overhead. On the contrary, if we augment the period ζ, the load will be decreased as sensors will have lesser messages to notify to the 3C, and hence lesser

scheduling periods to perform by the latter. However, updates will not be notified to the 3C in time resulting in a loss of the accuracy of the detection and the tracking as well as an increase of the request latency.

As regards Q, it is useful to point out that the consideration of the preemption concept in our strategy allows it to avoid the situation where a camera could potentially track an intruder for a very long period of time. Choosing an appropriate value for Q is essential especially, when there are multiple intrusions in the borderline. A small value will increase the time of camera-request switching and hence the reduce of the request latency, while a big value will have the opposite effect. Whatever the values of Q and ζ we consider, we should have $\zeta < Q$ by far, this is because the updates should be notified to the server before performing the next quantum allocation. As for $Part01$, we deem that the values of Q and ζ should be dynamic and greatly correlated with the number of intrusions P. Concretely, if the latter is up, the value of ζ and Q should be reduced to allow the network to cope with the high number of observation requests, with an acceptable latency. On the other hand, if P is down, Q and ζ should be increased to reduce the processing and the communication overhead.

```
Pseudo-code (executed at each 3C level)
Begin
Q: quantum;
Repeat every ζ time units
  Foreach Camera Cj in BGG
    {
       IdM(j)=camera's ID;
       PosM(j)=Camera's position;
       Get En(j);
       Get Or(j);
       Get Focus(j);
       Get Stat(j);
    }
  Foreach Intrusion Ii in BGG
    {
      Ii=Intrusion's ID;
      Get Posi(t);
      Get Vi(t);                          //The state of the intrusion Ii: SIi(t)
      Get Typi(t);
      Get Sti(t);
      If Ii.new()=true than
         Requests.Add(Ii);
      Else
         SIi(t):=last SIi(t);
      Get Celli(t);
      Set Ii.NbQi;                        // Number of quantum allocated to Ii
      Calculates Wi(t)                    //Priority of the intrusion Ii
    }
  Foreach Camera Cj and Intrusion Ii
    {
      Calculates Rotatingi,j (t);
      Calculates EnerCi,j(t) ;
      Calculates Troti,j(t);
      Calculates Rk,j(t);                 //Relevance of the camera Cj to observe the requests Reqk
      Affect during Q time Cj to Reqk  Where Rk,j(t) is the Max
    }
    End
```

FIGURE 3.17 – Pseudo-algorithm for the entire procedure.

3.5 Performance evaluation

3.5.1 Evaluation of the ASS adopted for the *Part*01

To evaluate the performances of our solution dedicated for the *Part*01 of the Algerian borders, we mainly tested the activation scheduling strategy and compared it to other techniques. To this aim, we conducted a series of simulations under Xubuntos-2.1 virtual machine, running the version 2.1.0 of TinyOS. In our tests, three key factors were targeted. The first one is the *energy consumption of the network* to assess its lifetime. As in [73] and [1], we mainly considered the energy consumption related to data

transmission and sensing. This is because the energy consumption due to data transmission its too much bigger comparing with that of processing and to a lesser degree with that of sensing.
The second factor is the *camera response time* that denotes the time elapsed between the detection instant of the intrusion by the scalar sensor and the moment when the camera starts handling the alarm. This includes all the delays such as processing times, data transmission delay, and waiting times.
The last factor is the *load balancing* to assess the selection fairness of our activation strategy and hence the lifetime of the network. These parameters have been all tested while varying the number of intrusions.

Simulation parameters :

In our simulations, we considered the following : area size of $(630m \times 200m)$; the number of scalar sensors is 30 (from S_0 to S_{29}) ; the number of camera sensors is 5 (from Cam_0 to Cam_4). Moreover, we assumed in all the simulations $\alpha = 1sec$. Practically, this is a very low value that is more likely to increase the amount of exchanged messages. In fact, we wanted to test our solution in the worst case.
The deployment technique used in the simulation is the same as the one explained before. A **TelosB** mote was used as a scalar sensor since it is compatible with TinyOS platform, an OmniVision **OV9655** is promoted as a camera since it is compatible with the TelosB Mote. The initial energy of each scalar sensor and each camera sensor are assumed to be 29160 and 58320 joules respectively. The value of C is assumed constant and equal to 5 joules. The coordinates and the status of the scalar sensors are reported in Table 3.4 whereas those of the camera sensors are shown in Table 3.5.

Id	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}
X	50	70	90	110	130	150	170	190	210	230	250	270	290	310	330
Y	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
State	W	S	W	S	W	S	W	S	W	S	W	S	W	S	W

Id	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
X	250	370	390	410	430	450	470	490	510	530	550	570	590	610	**630**
Y	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
State	S	W	S	W	S	W	S	W	S	W	S	W	S	W	S

TABLE 3.4 – Scalar sensors coordinates (W : woken-up(Activated), S :slept (Standby)).

Id	Cam_0	Cam_1	Cam_2	Cam_3	Cam_4
X	180	280	380	480	580
Y	205	205	205	205	205

TABLE 3.5 – Camera sensors coordinates.

- Obtained Results :

For the sake of comparison, we considered three well known activation strategies that we have also implemented. The first is based on a random choice (Random selection) while the second is based on a circular scheduling (Tourniquet). Finally, the third is that defined in the **BorderSense** approach [45], already discussed in the third chapter of this thesis. This last technique considers that the sensor to activate is fixed beforehand. It should be noted that the simulation environment was identical for all the compared techniques.

1. **Network energy consumption :** For network energy consumption, the obtained results are shown in Table 3.6 and figure 3.18, respectively.

Intrusion number	2	4	6	8	10	12	14	16
Random selection	23,20	23,20	23,20	23,20	23,20	23,20	23,20	27,16
Tourniquet	5,48	10,95	15,35	17,63	19,64	19,75	24,14	31,40
BorderSense	4,42	9,14	12,02	17,96	23,05	27,87	32,25	39,52
Proposed technique	**3,14**	**6,27**	**9,35**	**12,29**	**15,93**	**17,57**	**23,09**	**23,46**

TABLE 3.6 – Network energy consumption (in joule) vs the number of intrusions.

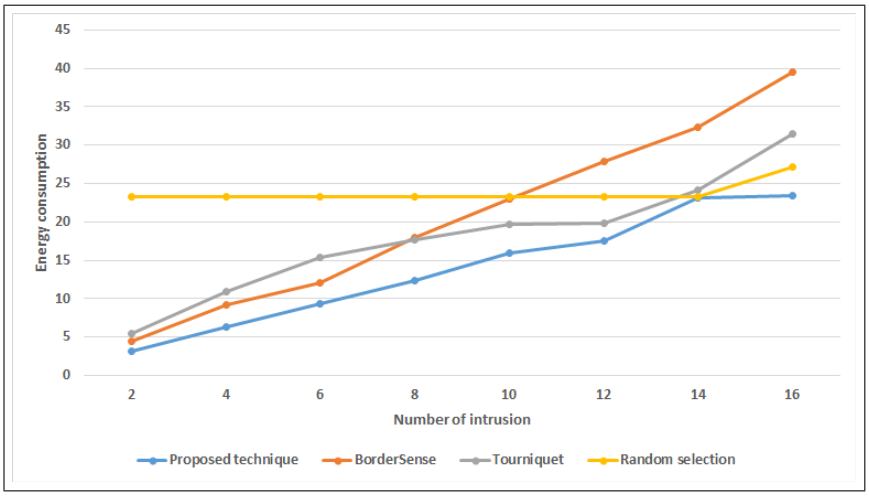


FIGURE 3.18 – Network energy consumption (in joule) vs the number of intrusions.

2. **Cameras response time :** For cameras response time, the experiment results are reported in Table 3.7 and Figure 3.19.

Intrusion number	1	3	5	7	9	11	13	15
Random selection	2.88	4.42	7.77	11.49	14.88	19.98	27.05	27.5
Tourniquet	2.88	4.41	6.6	22.65	24.9	27.39	30.27	31.81
BorderSense	2.88	4.42	6.64	22.67	32.11	33.87	36.61	42.09
Proposed technique	**2.89**	**4.44**	**7.83**	**10.16**	**14.17**	**17.85**	**18.01**	**21.7**

TABLE 3.7 – Cameras response time(in Seconds).

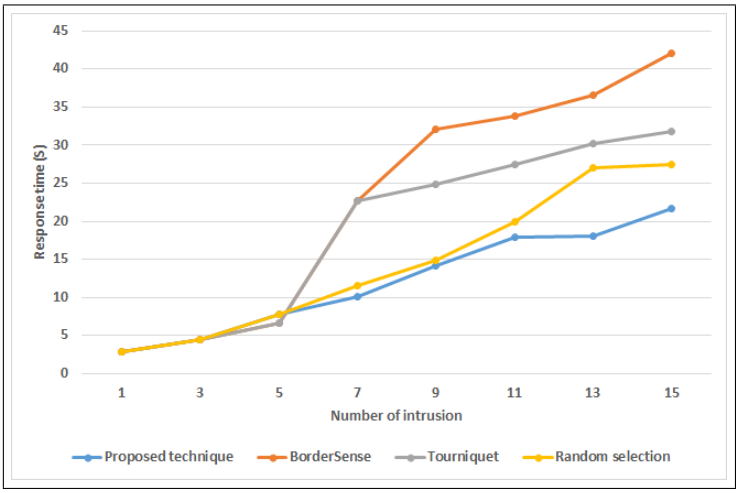


FIGURE 3.19 – Cameras response time (in Seconds).

3. **Load balancing :** To assess this parameter, we calculate the variance of the consumed energy which represents the dispersion of the energy consumption of a node around the average energy consumption in the network. The smallest the deviation is, the less the node consumption is dispersed. The obtained results are shown in Table 3.8 and Figure 3.20.

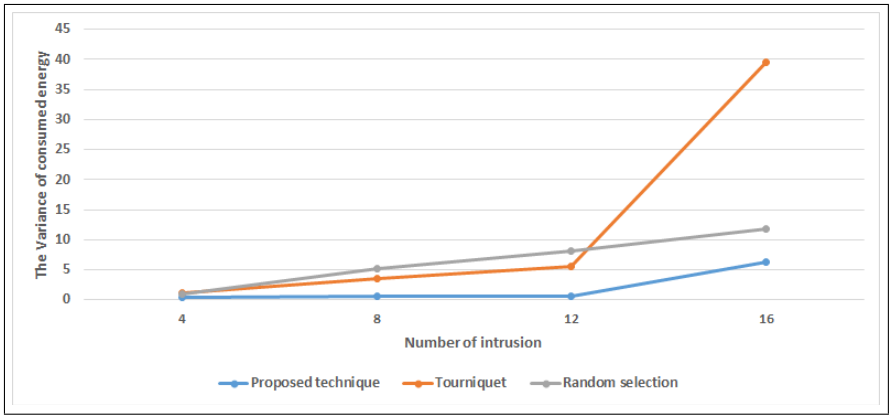


FIGURE 3.20 – Load balancing : The Variance of consumed energy by nodes.

Number of intrusion	4	8	12	16
Random selection	0,9456	5,1649	8,1542	11,8721
Tourniquet	1,2172	3,5559	5,6007	39,6210
Proposed technique	**0,4547**	**0,5599**	**0,6150**	**6,2020**

TABLE 3.8 – Sensors load balancing.

- Interpretation :

From Table 3.6, we remark that the energy consumption varies proportionally with the number of intrusions. The obtained results show in overall that the proposed approach consumes less energy compared to the other techniques. Table 3.7 shows that the cameras response time is also proportional to the number of intrusions. However, our activation strategy reports smaller latencies than the others, especially when the number of intrusions increases. With regard the to load balancing, we notice that the variance of the consumed energy is also proportional to the number of intrusions. Table 3.8 shows that our strategies provide a better load balancing mechanism, which can lengthen the lifetime of the network by maintaining the set of nodes or at least the majority of them functional.

3.5.2 Evaluation of the ASS adopted for part 02

To evaluate the ASS adopted for $Part02$ of the borders, we conducted simulations to assess the network lifetime and the performances of the solution in terms of energy consumption and response times.To this aim, a case study describing intrusion scenarios has been considered.

- Simulation environment, parameters and methodology

All the simulations were performed on a Lenovo server running on Windows 8 $64-bit$ with an IntelXeon CPU $E5-2680V22.8Ghz$ processor and $12GB$ of RAM. As regards the programming language, we opted for $C\#.Net$ 2012 since it is so similar to C++. Besides, it supports DMA (Dynamic Memory Allocation), that helps to free and allocate memory, and is one of the fastest and most powerful programming language. Table 3.9 recalls the parameter values considered in our simulations.

Parameter	Value
D_c	100m
$Dist_{max}$	100m
$DistF$	100m
ECC	233280j
EUR	1.5j
EUF	0.75j
TUR	0.05s
M	5
ζ	1s
Q	10s
Simulation Time	30s

TABLE 3.9 – General parameters values considered in our simulations.

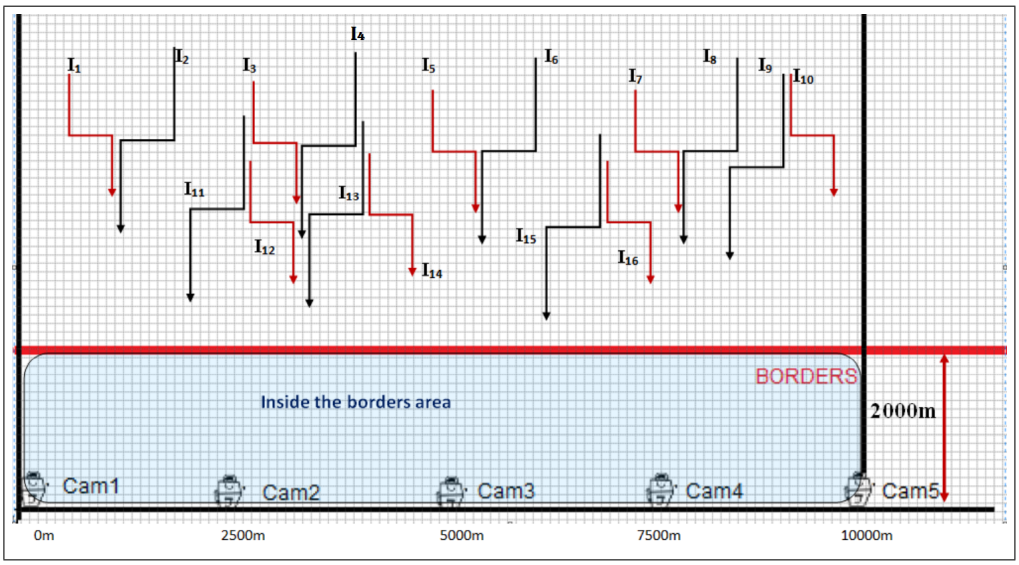


FIGURE 3.21 – Simulation environment and scenario.

In our simulations, we considered a 3D area of 10km dimensions in overall. According to our deploying strategy, if we assume the overlapping zone of two cameras $d_{olap-cam} = 17.5km$ then the distance between two cameras is $L_{Cam} = 2 \times 10 - 17.5 = 2.5km$. Therefore, 5 cameras are needed to monitor this area (see Figure 3.21). The cameras parameter values observed at instant $t = 0$ of our simulation are given in Table 3.10. The five cameras are positioned at distance of 2km inside the borders and at 5m of height from the soil. We assume that all the cameras remain ON during the entire time of the simulations.

	C_1	C_2	C_3	C_4	C_5
$En(j)$	198288	209952	186624	167962	123480
$Pos(j)$	(0,0,0)	(2500,0,5)	(5000,0,5)	(7500,0,5)	(10000,0,5)
$Or(j)$	(90,0)	(90,0)	(90,0)	(90,0)	(90,0)
$Focus(j)$	1	1	1	1	1

TABLE 3.10 – Camera's parameters at instant $t = 0$.

16 intrusions are considered in our simulation scenario. The progression of each during the 30s is depicted in Figure 3.21.

I_i	Type	0s	10s	20s	30s
I_1	Tank	(500,7000,0)	(500,6500,0)	(1000,6500,0)	(1000,6000,0)
I_2	Drone	(1700,7300,100)	(1700,6500,100)	(1050,6500,100)	(1050,5600,100)
I_3	Pedestrian	(2500,7000,0)	(2500,6500,0)	(3000,6500,0)	(3000,6000,0)
I_4	L vehicle	(3700,7300,0)	(3700,6500,0)	(3050,6500,0)	(3050,5600,0)
I_5	H vehicle	(4500,7000,0)	(4500,6500,0)	(5000,6500,0)	(5000,6000,0)
I_6	Helicopter	(5700,7300,100)	(5700,6500,100)	(5050,6500,100)	(5050,5600,100)
I_7	Pedestrian	(6500,7000,0)	(6500,6500,0)	(7000,6500,0)	(7000,6000,0)
I_8	Aircraft	(7700,7300,100)	(7700,6500,100)	(7050,6500,100)	(7050,5600,100)
I_9	Drone	(8300,7100,100)	(8300,6300,100)	(7650,6200,100)	(7650,5300,100)
I_{10}	Pedestrian	(8350,7100,0)	(8350,6600,0)	(8850,6600,0)	(8850,6100,0)
I_{11}	L vehicle	(2400,6700,0)	(2400,5900,0)	(1750,5900,0)	(1750,5000,0)
I_{12}	Tank	(2500,6300,0)	(2500,5800,0)	(3000,5800,0)	(3000,5300,0)
I_{13}	Drone	(3700,6650,100)	(3700,5850,100)	(3050,5850,100)	(3050,4950,100)
I_{14}	Tank	(3750,6350,0)	(3750,5850,0)	(4250,5850,0)	(4250,5350,0)
I_{15}	Helicopter	(6200,6650,100)	(6200,5850,100)	(5550,5850,100)	(5550,4950,100)
I_{16}	Pedestrians	(6250,6350,0)	(6250,5850,0)	(6750,5850,0)	(6750,5350,0)

TABLE 3.11 – Intrusion profile and progression during simulation time.

We assume that all the intrusions are within the field of view of the 5 cameras during the simulation time. The profile and the progression of the intrusions are described in Table 3.11. We assume that every 10s each intrusion changes either its speed or its direction. By considering two consecutive positions of a given intrusion in Table 3.11, we can determine its velocity vector during the period of 10 seconds. For example, I_1 moves from the position $(500, 7000, 0)$ at instant $t = 0$ to $(500, 6500, 0)$ at instant $t = 10s$. The coordinates of the velocity vector at instant $t = 10s$ are $V_1(10) = (\frac{500-500}{10}, \frac{7000-6500}{10}) = (0, 50)$. Hence, we conclude that the tank has progressed with a constant speed of 50m/s during the first $10s$ with a velocity vector $(0, 50)$. We thus can determine the

intermediate positions of the tank, when assuming its altitude constant. For example, at instant $t = t_0 + l$ such that, $l \in [0, 10s]$, we have :
$Pos_i(t) = (x_i(t_0) - (xv_i \times l), \quad y_i(t_0) - (yv_i \times l), \quad z_i(t_0))$. Accordingly, the position of I_1 at instant $t = 7$ is : $Pos_i(t) = (500, 6650, 0)$.

Furthermore, for any instant of the simulation time, we can estimate thereof the 2D and the 3D distances between intrusions and between each intrusion I_i and each camera C_j . For example, the 2D and 3D distances between the camera C_1 and the intrusion I_1 at instant $t = 0$ are :

$$Dist2D_{I1,C1}(0) = \sqrt{(500-0)^2 + (7000-0)^2} = 7017\text{m}\,;$$

$$Dist3D_{I1,C1}(0) = \sqrt{(500-0)^2 + (7000-0)^2 + (0-5)^2} = 7017\text{m}.$$

Therefore, the time needed to access the borders for the intrusion I_i estimated at instant t is : $Tprog_i(t) = \frac{y_i(t)-2000}{yv_i(t)}$. For instance, we have $Tprog_1(0) = \frac{7000-2000}{50} = 100s$.

Hence, according to formula 14, we can determine the weight of the intrusion I_1 at instant $t = 0$, we obtain : $W_i(0) = \frac{1}{100\times1\times(1+0)} = 0.01$.

According to the Formula 16, we can determine the rotation angles at instant t. For example, at $t = 0$ the rotation angles of the camera C_1 towards the intrusion I_1 are obtained as follows : $LR_{1,1}(0) = 180° - 90° - Itang(\frac{7000-0}{500-0}) = 4°$.

$VR_{1,1}(0) = 0° - Itang(\frac{0-5}{7017}) = -0.04°$.

According to formula 18, the needed focus variation for the camera C_1 to observe the intrusion I_1 at $t = 0$ is : $Focus_{1,1}(0) = \frac{7017}{100} = 70$.

According to formula 17, the energy required to rotate the camera C_1 towards I_1 at instant $t = 0$ is : $EnerC_{1,1}(0) = (4° + 0°) \times EUR + 70 \times EUF = 58.5j$.

Besides, the time needed for the camera C_1 to rotate to the intrusion I_1 at $t = 0$ is : $Trot_{1,1}(0) = (4° + 0°)TUR = 2s$.

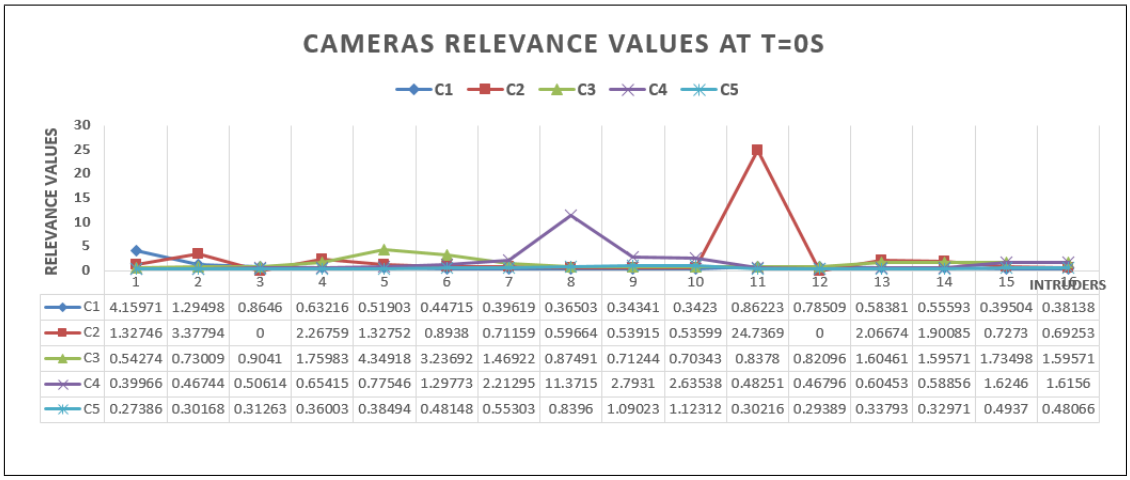
Moreover, at $t = 0$ the intrusion I_1 cannot be grouped with any other intrusion event as the 3D distances with the 15 other intrusions are greater than $100m$. So a singleton request is generated for I_1. The relevance factor of the camera C_1 relatively to I_1 measured at $t = 0$ is :
$R_{1,1}(0) = 1 \times \frac{198288-58.5}{233280} \times \frac{1}{1+0} \times \frac{1}{2} = 0.59$.

N.B : The scheduler can group intrusion events when it is possible. Grouping intrusions in one request can be done by calculating the distance $3D$ using formula 3.20. In our simulations, we found that there was only one group request that involves the intrusions I_3 and I_4 that starts at $t = 20s$ ($Dist3D(i_3, i_4)(20s)$=50m ¡ $Dist_{Max}$=100m).

Simulation results

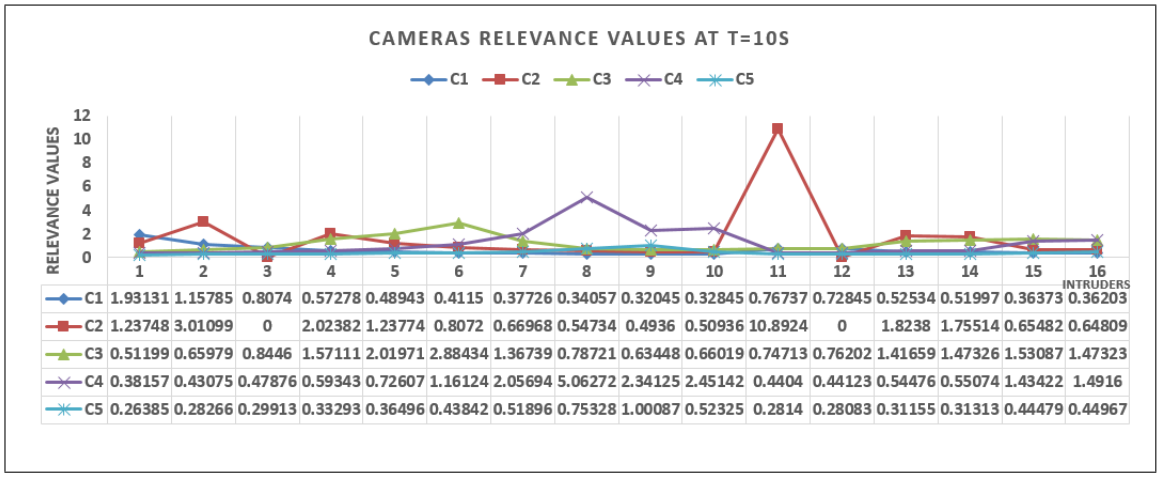
After giving the simulation environment and parameters, we study now the behavior of our algorithm throughout the calculation of some performance indicators.

— **Cameras relevance values at key moments :**
In order to affect the intrusion to the most relevant camera, the scheduler must compute the relevance of each camera C_j to observe each intrusion I_i each period ζ. We calculated the values $R_{i,j}$ at key moments (quantum allocation), we give the most relevant camera for each intrusion event. Obtained results are shown in Figures 3.22, 3.23, 3.24, 3.25.



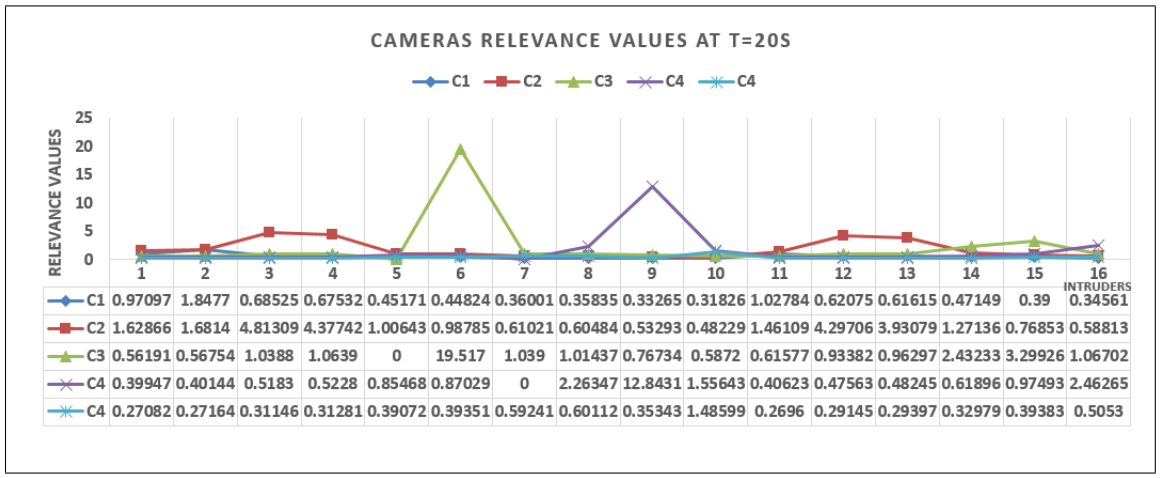
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C1	4.15971	1.29498	0.8646	0.63216	0.51903	0.44715	0.39619	0.36503	0.34341	0.3423	0.86223	0.78509	0.58381	0.55593	0.39504	0.38138
C2	1.32746	3.37794	0	2.26759	1.32752	0.8938	0.71159	0.59664	0.53915	0.53599	24.7369	0	2.06674	1.90085	0.7273	0.69253
C3	0.54274	0.73009	0.9041	1.75983	4.34918	3.23692	1.46922	0.87491	0.71244	0.70343	0.8378	0.82096	1.60461	1.59571	1.73498	1.59571
C4	0.39966	0.46744	0.50614	0.65415	0.77546	1.29773	2.21295	11.3715	2.7931	2.63538	0.48251	0.46796	0.60453	0.58856	1.6246	1.6156
C5	0.27386	0.30168	0.31263	0.36003	0.38494	0.48148	0.55303	0.8396	1.09023	1.12312	0.30216	0.29389	0.33793	0.32971	0.4937	0.48066

FIGURE 3.22 – Camera relevance at t=0s.



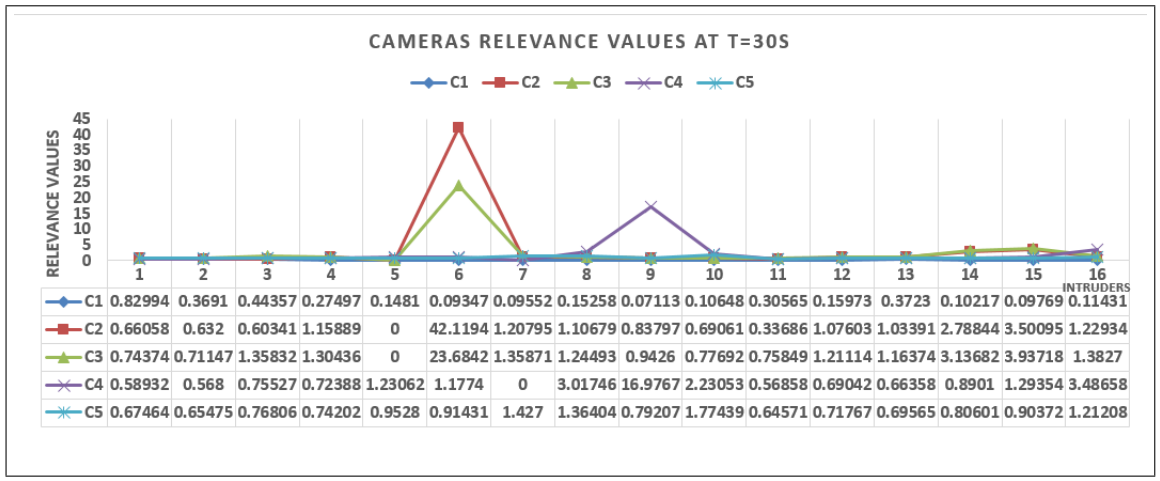
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C1	1.93131	1.15785	0.8074	0.57278	0.48943	0.4115	0.37726	0.34057	0.32045	0.32845	0.76737	0.72845	0.52534	0.51997	0.36373	0.36203
C2	1.23748	3.01099	0	2.02382	1.23774	0.8072	0.66968	0.54734	0.4936	0.50936	10.8924	0	1.8238	1.75514	0.65482	0.64809
C3	0.51199	0.65979	0.8446	1.57111	2.01971	2.88434	1.36739	0.78721	0.63448	0.66019	0.74713	0.76202	1.41659	1.47326	1.53087	1.47323
C4	0.38157	0.43075	0.47876	0.59343	0.72607	1.16124	2.05694	5.06272	2.34125	2.45142	0.4404	0.44123	0.54476	0.55074	1.43422	1.4916
C5	0.26385	0.28266	0.29913	0.33293	0.36496	0.43842	0.51896	0.75328	1.00087	0.52325	0.2814	0.28083	0.31155	0.31313	0.44479	0.44967

FIGURE 3.23 – Camera relevance at t=10s.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C1	0.97097	1.8477	0.68525	0.67532	0.45171	0.44824	0.36001	0.35835	0.33265	0.31826	1.02784	0.62075	0.61615	0.47149	0.39	0.34561
C2	1.62866	1.6814	4.81309	4.37742	1.00643	0.98785	0.61021	0.60484	0.53293	0.48229	1.46109	4.29706	3.93079	1.27136	0.76853	0.58813
C3	0.56191	0.56754	1.0388	1.0639	0	19.517	1.039	1.01437	0.76734	0.5872	0.61577	0.93382	0.96297	2.43233	3.29926	1.06702
C4	0.39947	0.40144	0.5183	0.5228	0.85468	0.87029	0	2.26347	12.8431	1.55643	0.40623	0.47563	0.48245	0.61896	0.97493	2.46265
C4	0.27082	0.27164	0.31146	0.31281	0.39072	0.39351	0.59241	0.60112	0.35343	1.48599	0.2696	0.29145	0.29397	0.32979	0.39383	0.5053

FIGURE 3.24 – Camera relevance at t=20s.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C1	0.82994	0.3691	0.44357	0.27497	0.1481	0.09347	0.09552	0.15258	0.07113	0.10648	0.30565	0.15973	0.3723	0.10217	0.09769	0.11431
C2	0.66058	0.632	0.60341	1.15889	0	42.1194	1.20795	1.10679	0.83797	0.69061	0.33686	1.07603	1.03391	2.78844	3.50095	1.22934
C3	0.74374	0.71147	1.35832	1.30436	0	23.6842	1.35871	1.24493	0.9426	0.77692	0.75849	1.21114	1.16374	3.13682	3.93718	1.3827
C4	0.58932	0.568	0.75527	0.72388	1.23062	1.1774	0	3.01746	16.9767	2.23053	0.56858	0.69042	0.66358	0.8901	1.29354	3.48658
C5	0.67464	0.65475	0.76806	0.74202	0.9528	0.91431	1.427	1.36404	0.79207	1.77439	0.64571	0.71767	0.69565	0.80601	0.90372	1.21208

FIGURE 3.25 – Camera relevance at t=30s.

— **Energy consumption and load balancing between cameras :**
To evaluate the efficiency of our algorithm in terms of energy consumption and load balancing (balancing energy consumption) between the five (5) cameras, we compared the performances of our solutions to three other solutions, which are : Round-Robin Selection (RRS), Random Selection (RS) and Static Selection (SS). **RRS** is based on Round-robin scheduling, one of the algorithms employed in process and network schedulers. **RS** is based on a random number between 1 and m (where m is the number of cameras, 5 in our scenario). **SS** is based on the cutting of the area of interest into several portions, each portion is correlated to a well determined camera. If an intruder enters the borderline from such a portion, it will be assigned to the camera responsible for that portion.
The parameters considered for these simulations are those given in Table 3.10.
To estimate the energy consumption for the four techniques, we calculate the residual energy of each camera. Then, to evaluate the energy load balancing, we calculate the standard deviation (SD) between them. When the standard deviation is small, it means that the values of energy are not widely dispersed around the mean (homogeneous series), hence the energy consumption is well balanced between all the cameras. Inversely, if the values of energy are widely dispersed around the mean (heterogeneous series), this means that the energy consumption is not balanced between the cameras. Obtained results are given in Table 3.12 and presented in Figure 3.26.

	RRS	RS	SS	Proposed
C_1	152174.512	89229.678	39737.0741	191266.092
C_2	134969.143	157464.323	58645.8101	204986.963
C_3	43067.0769	149299.825	56724.6201	181670.84
C_4	91615.6364	83981.129	131220.313	162438.341
C_5	12436.8345	61740.876	113284.404	115610.301
Mean	86852.64056	108343.1662	79922.44426	**171194.5074**
St.Dev	59286.84214	42488.06799	39844.03932	**34716.08618**

TABLE 3.12 – Remaining energy(Joules) and load balancing after 30 seconds of simulation.

To demonstrate further the efficiency of our strategy in terms of load balancing, we calculated for each camera the consumed energy in each period of the simulation time. Obtained results are shown in Figure 3.27.
Note that the energy consumption measured in the simulations includes only the effort needed for each camera to rotate and adjust the focus to visualize the intrusion.

— **Effect of intrusion grouping on the energy consumption :**
Another aspect of conserving energy in our solution is to consider the possibility

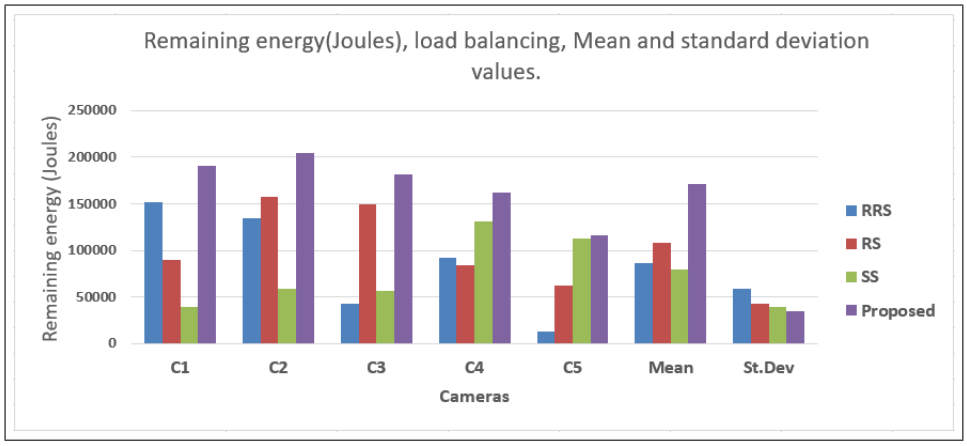


FIGURE 3.26 – Remaining energy (Joules) and load balancing between cameras.

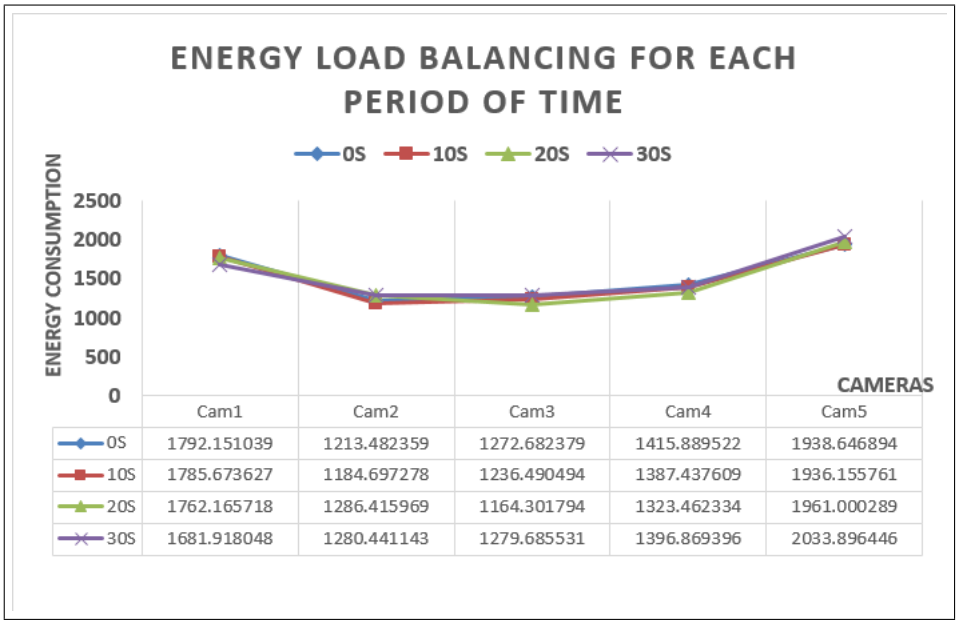
of intrusions grouping. To study the effect of the parameter $Dist_{Max}$ on intrusion grouping and indirectly on energy saving, we performed further simulations when increasing the value of $Dist_{Max}$ to follow the behavior of our algorithm in terms of energy saving and response time. We considered three values for $Dist_{Max}$: $100m$, $150m$ and $200m$. After calculating the distances between all the intrusions, we obtained the grouping results depicted in Table 3.13, when assuming $Q = 10s$.

	t=0s	**t=10s**	**t=20s**
$Dist_{Max}$=100m	/	/	(I_3-I_4)
$Dist_{Max}$=150m	(I_9-I_{10})	(I_{11}-I_{12})(I_{13}-I_{14})(I_{15}-I_{16})	(I_1-I_2)(I_3-I_4)(I_5-I_6)(I_7-I_8)(I_{12}-I_{13})
$Dist_{Max}$=200m	(I_9-I_{10})	(I_{11}-I_{12})(I_{13}-I_{14})(I_{15}-I_{16})	(I_1-I_2)(I_3-I_4)(I_5-I_6)(I_7-I_8)(I_{12}-I_{13})

TABLE 3.13 – Intrusion grouping when varying $Dist_{Max}$ with $Q = 10s$.

We calculate the consumed energy for each camera without considering intrusion grouping and then with grouping according to Table 3.13 when varying ($Dist_{Max}$=$100m$, $150m$ and $200m$). We determined also the saved energy for $Dist_{Max}$=$200m$ comparatively to $Dist_{Max}$=$100m$. Obtained results are shown in Figure 3.28.

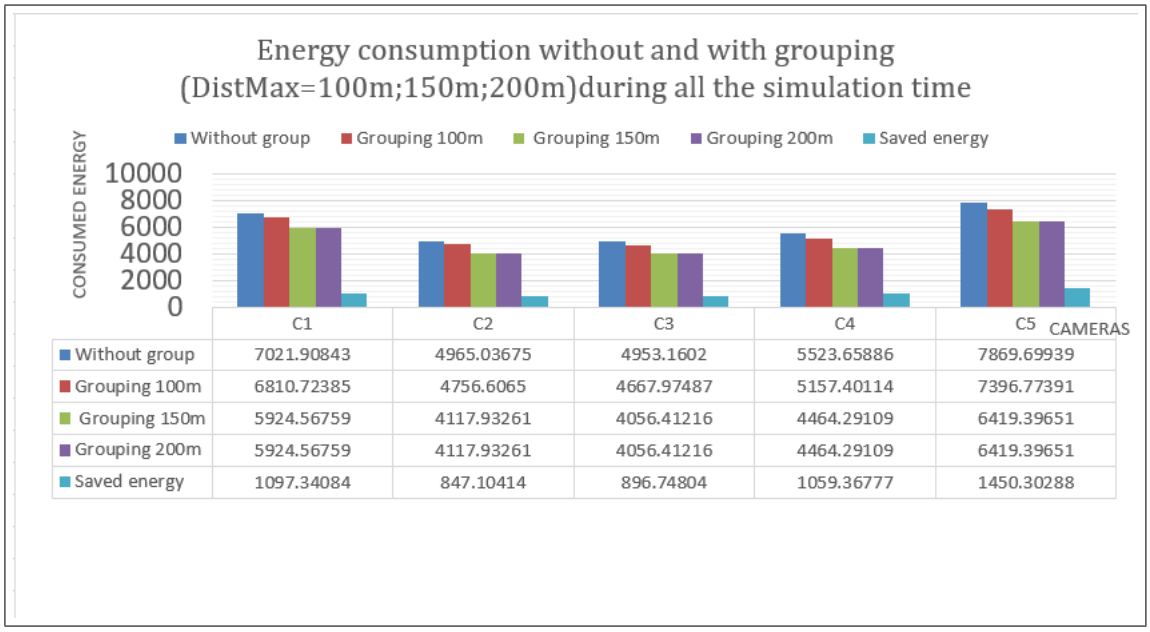
— **Assessing the response time of intrusion requests :**
Measuring the response times in borders surveillance is very important especially in some critical situation or when the number of intrusions exceed the number of cameras which is the case of our simulation scenario. The response time determines the time elapsed from the moment when an intrusion event is detected and recorded in the system (in our case all the events are starting and detected at $t = 0$), to the instant when a camera is allocated to its observation for the first time. The intrusions requests that are never processed during the simulation time will get a maximum latency equal to $30s$. On the other hand, the requests



	Cam1	Cam2	Cam3	Cam4	Cam5
0S	1792.151039	1213.482359	1272.682379	1415.889522	1938.646894
10S	1785.673627	1184.697278	1236.490494	1387.437609	1936.155761
20S	1762.165718	1286.415969	1164.301794	1323.462334	1961.000289
30S	1681.918048	1280.441143	1279.685531	1396.869396	2033.896446

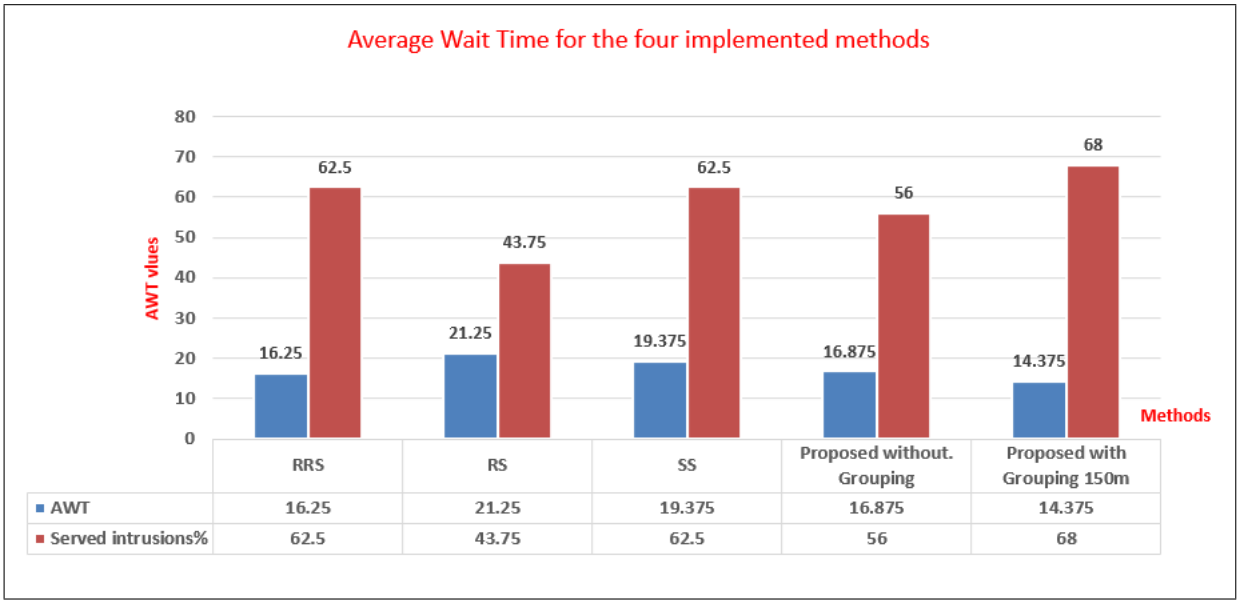
FIGURE 3.27 – Energy load balancing between the 5 cameras in each period of time.

that have been served at least one time, should have their response time either equal to 0s, 10s or 20s, as we assume in our simulation $Q = 10s$. In other words, either they have been served a camera for the first time at the first, the second, or the third quantum service. Our algorithm in both versions (with and without grouping intrusions) was compared to the four methods already discussed before. Grouping intrusion schema is available in Table 3.13. Obtained results are shown in Table 3.14, the Average Waiting Time for each methods is depicted in Figure 3.29.



	C1	C2	C3	C4	C5
Without group	7021.90843	4965.03675	4953.1602	5523.65886	7869.69939
Grouping 100m	6810.72385	4756.6065	4667.97487	5157.40114	7396.77391
Grouping 150m	5924.56759	4117.93261	4056.41216	4464.29109	6419.39651
Grouping 200m	5924.56759	4117.93261	4056.41216	4464.29109	6419.39651
Saved energy	1097.34084	847.10414	896.74804	1059.36777	1450.30288

FIGURE 3.28 – Energy consumption without and with grouping.



	RRS	RS	SS	Proposed without. Grouping	Proposed with Grouping 150m
AWT	16.25	21.25	19.375	16.875	14.375
Served intrusions%	62.5	43.75	62.5	56	68

FIGURE 3.29 – Average Waiting Time for the four implemented methods.

— **Effect of intrusion grouping on request response times :**
The goal here is to observe the effect of grouping or not grouping intrusions on this parameter. In this simulation, we define the request response time for the 16 intrusions when varying the distance $Dist_{Max}$ during the simulation time (Without grouping, with grouping $Dist_{Max}$= 100, 150 and 200m). We calculate also the saved time amount when $Dist_{Max}$=200m. Obtained results are depicted

I_i	RRS	RS	SS	Proposed(without grouping)	Proposed(grouping at 150m)
I_1	30	0	30	0 (by C_1)	0
I_2	10	0	20	20 (by C_1)	20
I_3	30	10	0	20 (by C_2)	20
I_4	10	30	30	30 (Not served)	**20** ($I_3 - I4$) at t=20s
I_5	0	30	20	0 (by C_3)	0
I_6	10	10	0	10 (by C_3)	10
I_7	0	30	20	30 (Not served)	30
I_8	30	20	30	0 (by C_4)	0
I_9	30	10	20	10 (by C_5)	**0** ($I_9 - I10$) at t=0s
I_{10}	0	30	10	0 (by C_5)	0
I_{11}	0	30	30	0 (by C_2)	0
I_{12}	30	30	20	30 (Not served)	**10** ($I_{11} - I12$) at t=10s
I_{13}	20	20	0	30 (Not served)	30
I_{14}	20	30	30	30 (Not served)	30
I_{15}	30	30	30	30 (Not served)	30
I_{16}	10	30	20	30 (Not served)	30
AWT	16.25	21.25	19.375	16.875	**14.375**
Served intrusion (%)	62.5%	43.75%	62.5%	56.25%	**68.75%**

TABLE 3.14 – Intrusions response time(seconds) and the average waiting time (**awt!**).

in table 3.15 and Figure 3.30.

	AWT	Grouped intrusions	Grouping instant	Time saving
Without grouping	16.875	/	/	/
Grouping at 100m	16.250	$(I_3 - I_4)$	20s	10s
Grouping at 150m	14.375	$(I_9 - I_{10}); (I_{10} - I_{11})$	0s	40s
Grouping at 200m	14.375	$(I_9 - I_{10})$	0s	40s

TABLE 3.15 – Effect of intrusion grouping on average wait time for intrusions.

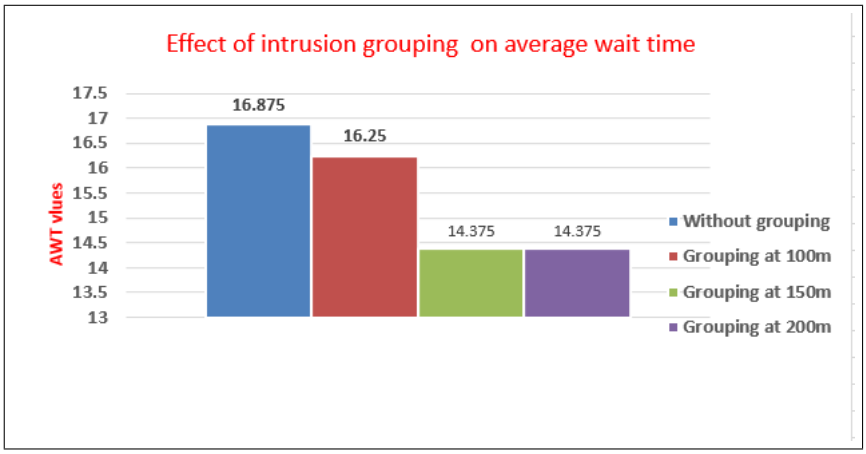


FIGURE 3.30 – Effect of intrusion grouping on average wait time

- Results interpretation

— For cameras relevance values at key moments, we made the necessary calculations to obtain the relevance of each camera in relation to each intrusion at key moments (when the quantum is allocated). If we take a look on the obtained results at $t = 10s$, we find out that the intrusion I_{11} which is a **light vehicle** is relevant to $C2$ because this intrusion is the closest ($Dist2D_{I_{11},C_2} = 5900.84m$) to the camera $C2$ and the fastest to progress towards the borders.

— Through the simulation related to energy consumption and load balancing, we notice that between the four implemented approaches, our algorithm ensures the best load balancing between the five cameras. This appears by computing the standard deviation which was the smallest for our solution, such a performance makes it possible to better manage the resources of the network and hence extending the lifetime of our network. For energy consumption, the average residual energy for each camera was the highest for our algorithm. On the other hand, the SS algorithm was the poorest in terms of energy saving because it doesn't have any mechanism selection which forces the cameras to make a lot of extra effort to turn towards intrusion and consequently consume more energy.

— Additional simulations were conducted to observe the effect of intrusion grouping on energy consumption. Through the obtained results we observed that grouping intrusions has a positive effect on reducing the energy consumed by each camera. As events are grouped, they are less requests to handle, and hence the load on cameras is reduced.

— Regarding the evaluation of the request response time, even though our algorithm is not the best, it favours the requests that have the the highest priority in terms of the type and the time needed to progress to the borders (by computing the weights). Therefore, events that are not urgent may be discarded or delayed against recent ones of higher priority. However, when considering intrusion grouping, events are grouped in same requests, thus improving the global response time and hence the average waiting time **awt!** is reduced. In this case our solution is outperforming the other algorithms.

3.6 Conclusion

In this chapter, approaches relating to the surveillance of the two parts of the Algerian borders $Part01$ and $Part02$ were proposed. Within this context, network architectures for both parts, the fault tolerant deployment schemes of components for both architectures as well as the activation scheduling strategies for both areas were addres-

sed and discussed. Obtained simulations results show the effectiveness of the proposed approaches in terms of reducing the energy consumption and improving the lifetime of the network.

Chapitre 4

Additional mechanisms for strengthening our approach

4.1 Introduction

After presenting in the previous chapter our architectures for securing Algerian borders, in this chapter we design some additional mechanisms for strengthening the proposed solutions. Therefore, we introduce two mechanisms, the first one is for studying the effectiveness of adapting the scalar sensors activation period (called α previously) on energy consumption and the network lifetime. This mechanism is considered for the activation scheduling strategy designed for $Part01$ of the borders. The second mechanism considered also for $Part01$ of the borders aims to overcome a serious issue which is deploying and energy supplying system for UAV during their flight.

4.2 Motives

In the previous chapter, we introduced our contribution related to the proposal of a new architecture for securing Algerian borders. To properly strengthen this proposed architecture, other mechanisms are necessary to meet purely operational needs. For instance, adjusting the activation period of scalar sensors and cameras plays a very important role in the decision-making process, ditto , the use of UAV in the process of border surveillance requires the establishment of strict mechanisms for power management and access to this critical resource. In what follows we will detail all of these

notions.

4.3 The effectiveness of adapting the sensors activation period on the network lifetime

It is noteworthy to point out that the solutions discussed in the sequel represent a continuation of the other contributions already presented in the previous chapter which deals with the border surveillance architecture dedicated to secure the $Part01$ of the Algerian borders.

Just to remind, when we discussed the scheduling strategy for $Part01$ of the Algerian borders, we designed the activation scheduling strategy for scalar sensors. In this solution, a segment contains 14 scalar sensors within the global field of view of one camera. Each scalar sensor should be in the global field of view of at least two different cameras at a given instant, as depicted in figure 3.12. Also, we considered that two neighbouring scalar sensors are activated alternatively which means that if at a given time the scalar sensor S_i is active then the sensor S_{i+1} must be in the standby mode, for $i = 1..k-1$ (see figure 3.7). In other words, among the 14 sensors in the global field of view of one camera only 7 are active. For that, the 3C sends alternatively activation and standby messages every α time units to all the scalar sensors that remain in service. The latter respond to the 3C requests by sending a *hello* message to acknowledge the request reception and notify their liveness.

If the 3C does not receive the *hello* message from a sensor "i" by the end of the period, then "i" is suspected to be out of service and its neighbours "$i-1$" and "$i+1$" are then kept continuously in active mode till the sensor "i" is replaced or repaired. Hereafter, we discuss the effect of varying the value of the parameter α on energy consumption and the network lifetime. In the previous chapter, the solution is assessed by fixing the same value of α to $1sec$(by the operator at the 3C level) for all the segments of $Part01$ of the borders.

In this part, we investigate additional policies that makes the value of α dynamic according to the risk of the intrusion. We demonstrate through simulations that this dynamic strategy reduces significantly the energy consumption while it increases the lifetime of the network. Therefore, the activation period my be tuned according to the intrusion risk. When the number of intrusion alerts increases it can be reduced to enhance the reactivity of the network. Conversely, it should be augmented in peacetime

when the number of intrusions decreases. In this case, the network is divided into different sectors, each sector can be governed by a different value of α following the risk of intrusion. To do that, we introduce a new parameter to assess the intrusion level, given by the number of alerts recorded in one sector during a given time (a multiple of α).

$$IntruI = \frac{Numalert}{p \times \alpha} \tag{4.1}$$

After $p \times \alpha$ time units, we re-evaluate the parameter $IntruI$ and we determine the integer value of the ratio between the new and the old value of the intrusion indicator.

$$RatioIn = \frac{IntruI_{old}}{IntruI_{new}} \tag{4.2}$$

Let α_{min}, α_{max} denote respectively the minimal and the maximal value of the activation period within a sector. Initially, each sector associates with α the value α_{min}. After computing the $RatioIn$ the new value α_{new} is determined as follows :

$$\alpha_{new} = MAX(\alpha_{min}, \alpha_{old} \times RatioIn) \quad if \quad RatioIn \leq 1 \tag{4.3}$$

$$\alpha_{new} = MIN(\alpha_{max}, \alpha_{old} \times RatioIn) \quad if \quad RatioIn > 1 \tag{4.4}$$

That means that if the number of intrusions increases then the value of α is reduced proportionally, and conversely, such that the new value of α be within the range [α_{min}, α_{max}].

4.3.1 Simulation parameters and scenario

Our simulation have been conducted using the programming language $C\#$ of Microsoft visual studio 2010.net, installed on Condor Intel Core i7, $3.0GHz$, RAM :$4.0Go$ OS : Windows 7. In our experiments, we assessed some performance parameters during the simulation time T_{sim}. We considered three cases, the activation strategy with a fixed value of $\alpha = \alpha_{min}$, then $\alpha = \alpha_{max}$, and finally by enforcing the rules (2), (3), (4) and (5) to compute the value of dynamic α. We are interested in evaluating the following performance parameters.

— The number of messages exchanged in the network.

— The average energy consumption of a scalar sensor : We assume $E_{InitOneSS}$ the initial energy level of each sensor. A scalar sensor looses a particular amount of energy every transmission and reception. E_{trans}, E_{recep} are respectively, the values of consumed energy by one scalar sensor when transmitting, respectively receiving one message.

— The average energy consumption of a camera : We assume $E_{InitOneC}$ the initial energy level of each camera. The same values are considered to transmit and receive messages as for scalar sensor nodes. Notice that if the energy level of a device depletes, it cannot receive or transmit any more data.

— The last parameter to assess is the latency of the camera (reactivity) : this denotes the time elapsed from the moment the intrusion is detected by a scalar sensor to the time when the selected camera starts to visualize the zone subject of the intrusion. The following table reports the considered values during our simulations.

Parameters	value range
Number of sensors k	28 to 140$nodes$
T_{sim}	300sec
$[\alpha_{min}, \alpha_{max}]$	$[1sec, 5sec]$
p	5
$E_{InitOneSS}$	29160$Joules$
$E_{InitOneC}$	100000$Joules$
E_{trans}	08$joules$
E_{recep}	05$joules$
C	12 $joules$

28 scalar sensors are covered by 3 cameras according to the deployment strategy discussed previously in the third chapter of this thesis. Initially, each camera is directed to the first sensor $ID = 1$. We assume that moving the camera by one position takes $1sec$. During the time simulation, we assumed first a progressive increase of the number of alerts recoded in the network starting from $\frac{k}{10}$ alerts in all the network during the first period α then to increase, linearly $\frac{k}{9}$, $\frac{k}{8}$, to reach a maximum of k alerts (each sensor sends an alert during α), then we observe a reverse scenario by decreasing the number of alerts, and so on. Notice that the intrusions are distributed randomly over the network.

4.3.2 Obtained results :

In the first simulations, we assessed the global number of exchanged messages in the network while increasing the number of scalar sensors by a multiple of 28 (28, 56, 84, 112, 140). The results are shown in Figure 4.1.

The Figure 4.2 depicts the average energy consumption per sensor when varying the

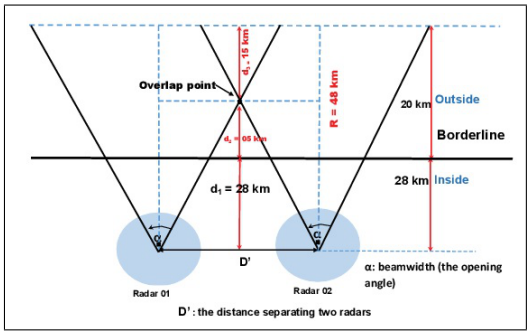


FIGURE 4.1 – Number of exchanged messages function of k.

number of nodes.

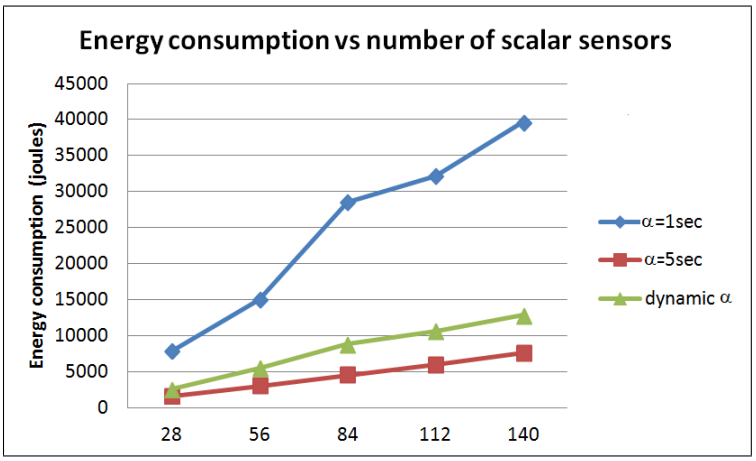


FIGURE 4.2 – Average Energy consumption of a scalar sensor (in joules) function of k.

The Figure 4.3 illustrates the average energy consumption of a camera when varying the number of sensors.

The Figure 4.4 assesses the reactivity of the solution by assessing the average latency of a camera when varying the number of sensors.

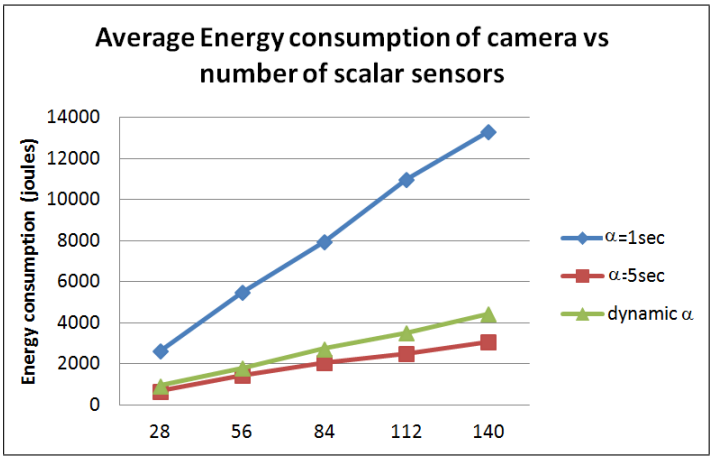


FIGURE 4.3 – Average energy consumption of a camera function of k.

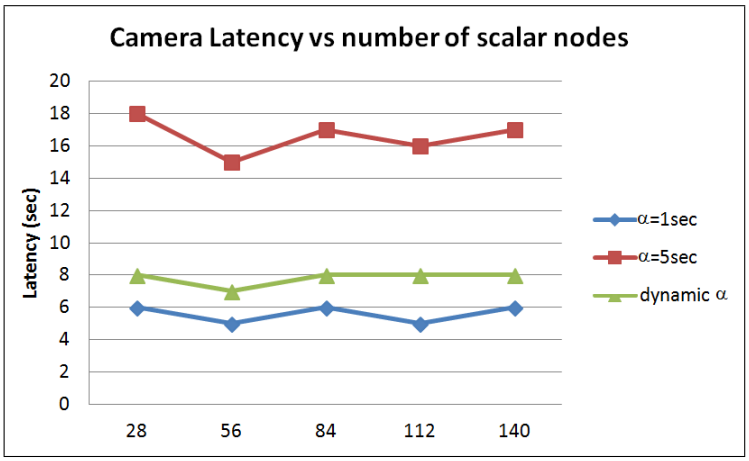


FIGURE 4.4 – Average latency of a camera function of k.

4.3.3 Results interpretation

The first general impression is that the increase of the value of α incomes in reducing significantly the number of exchanged messages and hence the energy consumption of scalar sensors and cameras. However, the latency of the network in visualizing the intrusion becomes slower which is not practicable in some situations. As we can see through the different performed simulations, making α computed dynamically results in reducing the number of messages and the energy consumption comparatively to when assuming a minimal value $\alpha_{min} = 1sec$. On the other hand, it provides an acceptable latency comparatively to when assuming $\alpha_{min} = 5sec$. This makes our solution a compromise between these two extreme alternatives and also the most operationally appropriate one.

4.4 A Wireless energy supply solution for UAV

We design in this section a solution for energy supply for UAV. As we know, UAV suffer from a major issue which is the short flight time due to their energy supplying limitations. To overcome this issue, a Wireless Power Transfer (WPT) system based on rectennas is designed to supply their batteries during their flight. A rectenna is a specific antenna embedded on the UAV that transforms guided radio frequencies sent from an on-ground transmitter antenna into **dc!** (**dc!**) current. Finally, to manage the access of UAV to the WPT system, we develop a scheduling strategy based on an improved WRR algorithm.

To supply UAV with energy without the need of stopping, we consider the deployment of a WPT system based on using rectenna technology. A rectenna is a special type of receiving antenna used for converting radio waves into direct current. The WPT system needs the deployment of transmitting antennas on the ground to send guided high radio frequencies to the rectenna embedded on the UAV. However, only a maximum of 84 % of the transmitted energy can be collected at distance less than $10meters$, by using guided microwaves within the range of $2.45GHz$. Better performances can be obtained at longer distances by transmitting millimeter waves [74], making it possible to miniaturize the rectenna and increase the **dc!** output power. Furthermore, by increasing the frequency, the beam directivity can be improved, and the power loss is reduced at high distances[74]. Moreover, the efficiency of this technique in open space relies on the media through which the radios waves are travelling. Thus, the ability to efficiently transfer waves through open space depends on whether or not a clear line of sight exists between source and target. This is not an issue, as UAV operate in a no crowded area where obstacles are rare and the weather is always sunny and hot. As described in Figure 4.5, we assume in our solution the deployment of a transmitting antenna at each **abgp!**. This antenna can be mounted on a mobile truck parked near the ABGP camp and the UAV depot. The latter is generally located in the center of the transversal border. Therefore, as the camera can capture image at distance of 1.6 km, the UAV can stand not far from the ground antenna to charge its battery, while being tracking the intruders within the camera field. The truck can move when possible to be the closest to the operating UAV. However, during charging both should be in stationary mode.

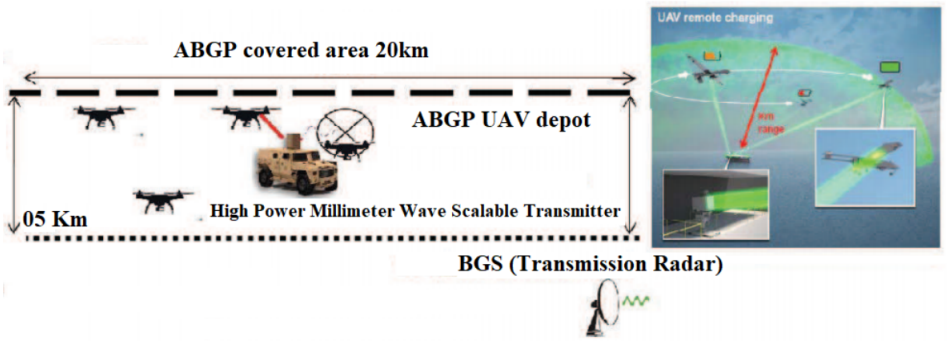


FIGURE 4.5 – The proposed WPT system based on rectenna.

4.4.1 Scheduling strategy for WPT access

To charge its battery, an UAV should receive an amount of radio waves in its direction by the ground antenna. More it is close to the latter more the energy loss is reduced and hence the charging time is shortened. When different UAV need to be charged, the simple way to manage the system is to implement a **rr!** (**rr!**) policy. To improve the access to the WPT system, we design a scheduling strategy based on an improved WRR algorithm. The structure for the WRR is similar to **rr!**, in that it is simply a **fcfs!** (**fcfs!**) queue with priority. Therefore, processes (UAV in our case) are dispatched in a first-in-first-out sequence but each process is allowed to run for only a limited amount of time called time-slice or quantum q. However, the power transmission stops if an UAV has finished charging its battery before the quantum ends.

The radio beam is then directed to next UAV in the queue. If the quantum ends before the UAV has finished charging its battery, the power transmission is stopped and the UAV is inserted in the queue according to its priority. The queue is rearranged after a complete cycle with the highest priority UAV requesting the WPT system first. This enables high priority UAV to get the access first and always be at the beginning of the UAV queue. Once an UAV has completed charging its battery, a new UAV is accepted in the queue. At this point, the UAV are reorganized in descending weight and the algorithm continues. Priority (weight) of the UAV is determined, as follows :

— UAV without mission in progress (Low priority=1) ;
— UAV with mission in progress and intruder type detected is a person (Medium priority=2) ;
— UAV with mission in progress and intruder type detected is a vehicle or truck (High priority=3).

UAV with the same level of priority can be distinguished by considering the highest

value of the following parameter :

$$Pdis = \frac{E_C}{Dist_G} \tag{4.5}$$

where, E_C is the amount of the energy consumed in the battery, and Dis_G is the distance that separates the UAV from the transmitter. Therefore, the closest UAV to the antenna with less energy remaining in its battery is promoted in the queue.

4.4.2 Simulation parameters

All the simulations are performed on a *lenovo* server running Windows 8 $64-bit$ with an IntelXeon **cpu!** (**cpu!**) $E5-2680V22.8Ghz$ processor and $12GB$ of **ram!** (**ram!**), codes were writing in $C\#$ and C^{++} languages. In the conducted simulations, we assumed that all the UAV are at the same distance from the transmitter. We compare our strategy with RR algorithm. The needed energy power for each UAV is quantified by time units, for example if an UAV needs 10 kilojoules of energy, it requires 10 units of access time to the WPT. In this simulation, we mainly evaluate the effect of varying q on the WPT performances. We considered four UAV ($UAV_i, i = 1..4$) that need to access the WPT. Lot of scenarios were performed, we give only some of them : UAV with the same burst time (needed time units to complete battery charging), BT and with different burst times. Assuming the UAV arrival times AT, we vary the value of q (q = 2 or 5 or 10 time units). Then we calculate for each UAV : the completion charging time CT ; the turn-around time TaT (CT- AT) ; and the **wt!** (**wt!**) (TaT- BT) and the average values.

4.4.3 Obtained results

For the effect of varying q, obtained results are reported in Table 4.1. We noted that the values of **ct!** (**ct!**), **tat!**(**tat!**) and **wt!** of each UAV decrease when increasing q as well as their average values. For instance, in Table 4.1 (same burst times), WT values of the UAV_1 and UAV_2 were 15 and 19 respectively and they passed to 0 and 9, after increasing q from 5 to 10. This stands in both situations, UAV with the same burst times or with different burst times. Through this simulation, we have demonstrated that the best value of q should be slightly greater than the average burst time (batteries charging time) of the UAV (See the fourth part of table 4.1, the average burst time =9.5s and the q value chosen is $10s$), as it is greatly recommended in the literature.

(Same burst time, q=05)					
	BT	AT	CT	TaT	WT
UAV_1	10	0	25	25	15
UAV_2	10	1	30	29	19
UAV_3	10	2	35	33	23
UAV_4	10	3	40	37	27
AVGs	10	/	**32.5**	**31**	**21**
(Same burst time, q=10)					
	BT	AT	CT	TaT	WT
UAV_1	10	0	10	10	0
UAV_2	10	1	20	19	9
UAV_3	10	2	30	28	18
UAV_4	10	3	40	37	27
AVGs	10	/	**25**	**23.5**	**13.5**
(Different burst time, q=02)					
	BT	AT	CT	TaT	WT
UAV_1	8	0	26	26	18
UAV_2	10	1	32	31	21
UAV_3	6	2	22	20	14
UAV_4	14	3	38	35	21
AVGs	9.5	/	**29.5**	**31**	**18.5**
(Different burst time, q=10)					
	BT	AT	CT	TaT	WT
UAV_1	8	0	8	8	0
UAV_2	10	1	18	17	7
UAV_3	6	2	24	22	16
UAV_4	14	3	38	35	21
AVGs	9.5	/	**25**	**20.5**	**11**

TABLE 4.1 – Effect of varying the time quantum(with Same and different burst times)

Hereafter, we compare our scheduling strategy with RR, the obtained results are reported in Table 4.2. Compared to RR algorithm, our algorithm promotes UAV with higher priority to access the WPT system. For instance, in Table 4.2, it is assumed that UAV_4 has a crucial mission. If we use the RR algorithm, UAV_4 has to wait 12 time units to be charged, whereas it accesses directly to the WPT system (waiting time =0) by using our strategy. On the other hand, the average values of WT for both algorithms are close (6 and 6.75). This was expected since RR manages UAV access according to **fcfs!** policy and the burst time is the same in both algorithms.

(RR with same priorities and same burst time, q=05)					
	AT	BT	**Priority**	TaT	WT
UAV_1	0	5	2	5	0
UAV_2	1	5	2	9	4
UAV_3	2	5	2	13	8
UAV_4	3	5	2	17	**12**
AVGs	/	5	/	11	6
(WRR with different priorities and same burst time, q=05)					
	AT	BT	**Priority**	TaT	WT
UAV_1	0	5	2	10	5
UAV_2	1	5	1	14	9
UAV_3	2	5	1	18	13
UAV_4	3	5	3	5	**0**
AVGs	/	5	/	**11.75**	**6.75**
(WRR with different priorities and different burst time, q=05)					
	AT	BT	**Priority**	TaT	WT
UAV_1	0	8	2	20	12
UAV_2	1	12	3	12	0
UAV_3	2	6	2	24	18
UAV_4	3	4	1	27	23
AVGs	/	7.5	/	20.75	**13.25**

TABLE 4.2 – Simple RR algorithm vs WRR algorithm(proposed)

4.5 Conclusion

In this chapter, we presented two solutions to improve the architecture of *Part*1 of the borders. In the first solution we studied the effectiveness of adapting the scalar sensors activation period (α) on both energy consumption and the network lifetime. In the second solution, we designed an energy supplying system for UAV. To this end, we proposed the use of a WPT system based on rectennas to charge UAV during their flight. To manage the access of UAV to the WPT system, we suggested a scheduling strategy based on an improved Weighted Round-Robin algorithm. Reported simulations results show that both proposed algorithms improve the performances of the system.

General conclusion

- Context

The work carried out in this thesis mainly revolves around a transversal study which aims to design solutions for securing land borders in general, and Algerian frontiers in particular. Therefore, our design has been adapted to the specificities of Algerian land borders, as it is a part of a big project of the Algerian Ministry of National Defense which aims to define an operational framework for securing the Algerian land borders.

Such a problematic is an old raised challenge, and till today, securing physical borders is still bringing a real headache to all governments over the world. Indeed, the last decade has shown the proliferation of cross-border crimes such as terrorism, drug and arms trafficking and illegal immigration. Therefore, securing borders becomes a primary concern and a critical task to guarantee for all the countries facing such scourges.

Algeria is the largest country of the Mediterranean area and the largest one in Africa after the partition of Sudan. Its land borders are spread over more than **5238** km of which 25% constitutes the north border strip and 75% is the south border strip. This border strip presents physical, economic and social characteristics : a mountainous and rugged terrain in the North and an extensive desert of sand or rockery of $Hamada$ and Erg and rocky mountain ranges such than $Tassili$ and $Hoggar$, in the South. The eastern and western borders of the northern part are distinguished by contrasting relief where the plains are extended as one progresses to the south via the highlands of $Tell$ and the $SaharanAtlas$. These are therefore borders made up of coastal plains, plains of the highlands or semi-arid zones and, finally, of the regions located at the foot of the Saharan Atlas. These borders present a variety of physical characteristics making their surveillance difficult and requiring modern equipment and increased regional cooperation.

In a recent past, several conventional techniques such as human patrols, installa-

tion of barriers, construction of insulation walls and trenching were used for securing Algerian borders. However, those methods suffer from intensive human involvement and high deployment cost. In addition, these solutions appear to be not appropriate to achieve the new security challenges. As a result, the Algerian government has launched recently a big project that consists in modernizing the border surveillance system by integrating new communication technologies to deal with the new threats and security concerns. This is the subject of this thesis, which aims to design a reliable, fault tolerant and efficient framework for securing Algerian border surveillance, valid in both peace and wartime.

- Balance sheet

The studies carried out during this thesis allowed us to answer certain topical questions linked to border surveillance and to contribute to solve this problematic by providing solutions than can be summarized through the following points :

- To identify clearly the key problematic of the subject of this thesis, we carried out a deep reading of the literature related to this field of research. As a result, an up-to-date state of the art on border surveillance technologies was elaborated ;
- Once a clear statement on the real issue of border surveillance has been identified, we proposed a new hybrid wireless sensor network architecture for border surveillance. For this effect, two essential segments of the Algerian borders are considered, the first part called $part01$, concerned the north-west and south-west border strip ; the second part includes the extreme-south border strip, called $part02$. $Part2$ considers the use of radars and cameras, while $part01$ is reenforced with additional surveillance equipments such as (UGS) and (UAV).
- A detailed deployment scheme for each layer of the proposed architecture (for both $part01$ and $part02$) is also addressed in this thesis, this scheme allow to calculate the required number of each equipment to deploy to achieve an optimal coverage.
- For energy saving, load balancing, fault tolerance and redundancy elimination, an activation scheduling strategy was proposed for both $part01$ and $part02$ of the borders. One of these strategies implements the way scalar sensors and multimedia sensors are activated in $part01$ of the borders, while the other strategy implements the way radars and multimedia sensors are activated in $part02$ of the borders ;
- To highlight the efficiency of the proposed scheduling strategy for both parts of our borders, we compared our solutions to other existing methods and we reported simulation results that confirm that our solution outperforms the other

schemes by extending the network lifetime while maintaining its efficiency.
— We studied in this thesis the effectiveness of adapting the activation period of scalar sensors and cameras on the lifetime of the network. Obtained results show that this period should be reduced in crisis time to enhance the fault tolerance of the network while it should be augmented in peacetime.
— For energy supply in border surveillance architecture based on the combination of radars with mobile camera sensors that are embedded in UAV, we proposed a WPT system based on rectennas to supply wirelessly UAV batteries with power during their flight. To manage the access of UAV to the WPT system, we implemented an active UAV scheduling strategy based on an improved WRR algorithm. Reported simulations results show that the proposed algorithm improve the performances of the system comparing to using round robin technique.

- Prospects

Let us recall that the work presented in this these is a part of a big project that aims to secure Algerian borders. Therefore, the work that we carried out within the framework of this thesis offers many interesting perspectives that we can summarize through the following points :

— First of all, testing the feasibility of the proposed solutions on the system already deployed in the field seems to be an obvious step. Indeed, the studies carried out have so far only been validated by simulations. The behaviour of algorithms on real platforms would therefore be a decisive factor for the evolution of the latter ;
— A second perspective would consist in dealing with a very important aspect, which is the rationalization of the data transfer process (texts or multimedia) to the Command and Control Center. This requires the implementation of a reliable data transfer mechanisms that are able to save the energy of equipments as well as extend the lifetime of the monitoring network. Fusing data before sending will be one of those mechanisms ;
— The activation mechanisms proposed in this thesis are all based on the collaboration between the different types of sensors. Packet loss therefore becomes critical for a convenient running of the monitoring process, especially for large-scale networks (one of the important characteristics of border monitoring applications) where collisions and packet loss are more frequent. In an effort of improving and expanding our work, a study should therefore be considered on the routing and transport aspect of data when scaling up ;
— Finally, other parameters must be taken into consideration when calculating the

relevance of the cameras. These parameters mainly depend on the nature of the terrain and the type of threat surrounding the area of interest.

Bibliography

[1] Chin-Ling Chen and I-Hsien Lin. Location-aware dynamic session-key management for grid-based wireless sensor networks. *Sensors (Basel, Switzerland)*, 10 :7347–70, 08 2010.

[2] P. Kumar, S. Lee, and H. Lee. E-sap : Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors (Basel)*, 12(02) :1625 to 1647, Feb 2012.

[3] Microcontrollerslab. WIRELESS SENSOR NETWORKS (WSN) AND APPLICATIONS. `https://microcontrollerslab.com/wireless-sensor-networks-wsn-applications/`, Dec, 2020.

[4] J. Zhang, G. Song, G. Qiao, Z. Li, and A. Wang. A wireless sensor network system with a jumping node for unfriendly environments. *International Journal of Distributed Sensor Networks*, doi :10.1155/2012/568240, Jul 2012.

[5] libelium. Cahpter 1 : Introduction to Wireless Sensor Networks. Quick Start ! `https://www.libelium.com/`, Jan, 2014.

[6] D. Papademetriou and E. Collett. A new architecture for border management. *Report of the Migration Policy Institute, Washington, DC, USA*, Mar 2011.

[7] FLIR Forward-Looking InfraRed. Discover the Best Technology for Border Surveillance. `http://www.flirmedia.com/MMC/CVS/Surveillance/SV_0006_US.pdf`, Accessed date : December 07, 2020.

[8] ML. LAOUIRA, A. Abdelli, J. Ben othman, and K. Hyunbum. An adaptive activation scheduling strategy for a border surveillance network. *IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA*, pages 9–13, Dec. 2019.

[9] ML. LAOUIRA, A. Abdelli, and J. Ben othman. Wireless energy supply scheduling strategy in a combined border surveillance architecture. *IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan*, pages 9–13, 7-11 Dec. 2020.

[10] ML. LAOUIRA, A. Abdelli, J. Ben othman, and K. Hyunbum. An efficient wsn based solution for border surveillance. *IEEE Transactions on Sustainable Computing journal*, page 12p, March. 2019.

[11] I. Boulanouar. *Algorithmes de suivi de cible mobile pour les réseaux de capteurs sans fil*. PhD thesis, Université Paris-EST, 2014.

[12] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras. Applications of wireless sensor networks : An up-to-date survey. *Applied System Innovation journal*, 3(14) :doi :10.3390/asi3010014, Feb 2020.

[13] M.R Bouakouk, A. Abdelli, and L. Mokdad. Survey on the cloud-iot paradigms : Taxonomy and architectures. *IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6, Sep. 2020.

[14] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : a survey. *Computer Networks*, 38 :393 to 422, 2002.

[15] R. Bellazreg. *Security, Deployment and Scheduling in WSN-based Applications : Models and Applications*. PhD thesis, Engineering School of Communications, SUPCOM-Tunisia, 2014.

[16] F. AlFayez. *A WIRELESS SENSOR NETWORK SYSTEM FOR BORDER SECURITY AND CROSSING DETECTION*. PhD thesis, Faculty of Science and Engineering Manchester Metropolitan University, 2015.

[17] ML. LAOUIRA. Fusion des données dans les réseaux de capteurs multimédias. *Faculty of Electronics and Computer Science, University of sciences and technology Houari Boumediene, Algeria*, Apr 2014.

[18] K. Bajaj, B. Sharma, and R. Singh. Integration of wsn with iot applications :a vision, architecture, and future challenges. *EAI-Springer Innovations in Communication and Computing. Springer, Cham.*, Marr 2020.

[19] N. ASSAD. *Optimisation du déploiement des réseaux de capteurs sans fil : Couverture de la zone de surveillance et connectivité du réseau dans une application de détection d'intrusion.* PhD thesis, UNIVERSITÉ MOHAMMED V FACULTÉ DES SCIENCES -Rabat-Morocco, 2015.

[20] Unattended Ground Sensors Defense Update. International Online Defense Magazine. `https://defense-update.com/`, 2006 Issue 01.

[21] Digital Barriers. Unattended Ground Sensors RDC C-IDS Covert remote detection and classification system. `https://www.digitalbarriers.com/`, Accessed date : December 09, 2020.

[22] Polus-St. RADIOBARRIER, Wireless Perimeter Security System. `https://polus-st.com/products/radiobarrier-perimeter-security-system/`, Accessed date : December 09, 2020.

[23] Applied Research Associates Inc (ARA). Security Solutions : The Continuing Evolution of Perimeter Security. `https://www.ara.com/pathfinder/security-solutions-the-continuing-evolution-of-perimeter-security/`, Accessed date : December 09, 2020.

[24] National Research and Safety Institute (INRS). CHAMPS ELECTROMAGNETIQUES. `https://www.inrs.fr/`, November, 2020.

[25] D. Vivet. *Perception de l'environnement par radar hyperfréquence. Application á la localisation et la cartographie simultanées, á la détection et au suivi d'objets mobiles en milieu extérieur*. PhD thesis, UNIVERSITÉ BLAISE PASCAL - CLERMONT II-FRANCE, 2012.

[26] Islam T. Almalkawi, M.Guerrero. Zapata, J.N. Al-Karaki, and J. Morillo-Pozo. Wireless Multimedia Sensor Networks : Current Trends and Future Directions. *Sensors journal ISSN 1424-8220*, 10 :6662 to 6717, Jul 2010.

[27] Lynred by Sofradir and Ulis. COMMENT FONCTIONNENT L'INFRAROUGE ET LES CAMÉRAS THERMIQUES. `https://www.lynred.com/fr/blog/comment-fonctionnent-linfrarouge-et-les-cameras-thermiques`, May, 2020.

[28] Specialist in Immigration Policy and Specialist in Military Aviation. Homeland security : Unmanned aerial vehicles and border surveillance. *Congressional Research Service, Report for Congress*, RS21698 :01–06, Jul 2010.

[29] Météo Algérie. Climat en algéie. `http://www.algerie-meteo.com/Climat.html/`, Last access : January 2018.

[30] E. ZEINO MAHMALA and H. REIFELD. *La crise securitaire au Sahel, Quelles repercussions sur les pays du Maghreb arabe ?* Konrad-Adenauer-Stiftung, Aug 2015.

[31] H. LABDELAOUI. *La gestion des frontiéres en Algérie, Rapports de recherche CARIM*. Robert Schuman Centre for Advanced Studies, Institut universitaire europÃ©en, San Domenico di Fiesole (FI), Italie, 2008/02- accessed date : November 25, 2016.

[32] A. Benantar. Sécurité aux frontiéres, portée et limites de la stratégie algérienne. *Année du Maghreb*, 14 :147 to 163, 2016.

[33] A-WIHRSA. Algeria-Watch : Information on the Human Rights Situation in Algeria. `http://www.algeria-watch.org/fr/article/mil/menaces_frontieres.htm`, Last access : January 2018.

[34] CGN-MDN. Unités des Gardes-frontiéres. `hhttp://www.mdn.dz/site_cgn/`, Last access : January 2018.

[35] G. Loney. Border intrusion detection : thinking outside the perimeter. *41st Annual IEEE International Carnahan Conference on Security Technology, Ottawa, Ont., Canada*, pages 01–06, Oct 2007.

[36] A. Arch Owen, G. Duckworth, and J. Worsley. Optasense : Fibre optic distributed acoustic sensing for border monitoring. *European Intelligence and Security Informatics Conference, 22-24 Aug 2012, Odense, Denmark*, page 362 to 364, 2012.

[37] T. He, S. Krishnamurthy, Jhon A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh. Energy-efficient surveillance system using wireless sensor networks. *Proceedings of the 2Nd International Conference on Mobile Systems, Applications, and Services, MobiSys 04, Boston, MA, USA*, pages 270–283, June 2004.

[38] T. Damarla, A. Mehmood, and J. Sabatier. Detection of people and animals using non-imaging sensors. *14th International Conference on Information Fusion, Chicago-Illinois, USA*, 09(03) :468–477, 5-8 Jul 2011.

[39] R. Bellazreg, N. Boudriga, K. TrimÃ¨che, and S. An. Border surveillance : A dynamic deployment scheme for wsn-based solutions. *Wireless and Mobile Networking Conference (WMNC), 6th Joint IFIP*, 01 :23–25, Apr 2013.

[40] J. Robert and P. Gervasio. An unattended ground sensor architecture for persistent border surveillance. *Proc. SPIE 6980, Wireless Sensing and Processing III*, 6980 :69800A–69800A–8, Apr 2008.

[41] T. Yang, D. Mu, W. Hu, and H. Zhang. Energy-efficient border intrusion detection using wireless sensors network. *EURASIP Journal onWireless Communications and Networking*, 2014(1) :01–12, MAR 2014.

[42] S. VAISHNAVI, K. BALA KRISHNA, N. RACHANA, TR NIKITHA, and M. DARSHINI. Border surveillance and intrusion detection using wireless sensor networks. *Journal of Information Storage and Processing Systems*, 19(1) :208–217, Apr 2020.

[43] S. Babu Nr, A.G. Swaminathan, and D. C. Joy Winnie Wise. Boarder analysis with ensora and doa using wireless sensor networks. *Sixth International Conference on Emerging trends in Engineering and Technology*, pages 76–83, 16-18 Dec 2013.

[44] X. Gong, J. Zhang, D. Cochran, and K. Xing. Optimal placement for barrier coverage in bistatic radar sensor networks. *IEEE/ACM Transactions on Networking*, 24(1) :259–271, Feb 2016.

[45] Z. Sun, P. Wanga, CM. Vuran, MA. Al-Rodhaan, Al-Dhelaan AM., and IF. Akyildiz. Bordersense : Border patrol through advanced wireless sensor networks. *Ad-Hoc Networks*, 09(03) :468–477, May 2011.

[46] D. Bein, W. Bein, A. Karki, and B.B. Madan. Optimizing border patrol operations using unmanned aerial vehicles. *12th International Conference on Information Technology - New Generations*, pages 479–484, 13-15 Apr. 2015.

[47] K. Kalyanam, P. Chandler, M. Pachter, and S. Darbha. Optimization of perimeter patrol operations using unmanned aerial vehicles. *Journal of Guidance, Control, and Dynamics*, 35(02) :434–441, Apr. 2012.

[48] A R. Girard, A S. Howell, and J K. Hedrick. Border patrol and surveillance missions using multiple unmanned air vehicles. *43rd IEEE Conference on Decision and Control,CDC.*, 01(10.1109/ITNG.2015.83) :620–625, 14-17 Dec. 2004.

[49] N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla, and A. Kakran. "smart border surveillance system using wireless sensor network and computer vision". *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, London(United Kingdom) :183–190, Apr. 2019.

[50] A. Aradas. Us-mexico border : Efforts to build a virtual wall. *BBC news report*, Aug 2012.

[51] Elta Systems. Unattended ground sensors network (USGN). `http://defense-update.com/newscast/0608/news/news1506_ugs.htm`, Copyright 2016 Defense-Update.

[52] B. Hayes and M. Vermeule. Borderline the eu's new border surveillance initiatives, assessing the costs and fundamental rights implications of eurosur and the "smart borders" proposals. *Proposals : a Study by the Heinrich BÃ¶ll Foundation*, Jun 2012.

[53] Telephonics Trusted Technology for a Tactical Advantage. A new approach to protecting vulnerable sites. https ://www.digitalbarriers.com/solutions/digital-walls/, Last access Dec 2020.

[54] Official Online Show Daily News, International Defence Official Web TV, and Security Technologies Fair. EVPU DEFENCE at IDET 2015. `http://www.evpudefence.com/en/`, 19-21 May 2015, Brno-Czech Republic.

[55] Indra. SECURITY SOLUTIONS and SERVICES : INTEGRATED BORDER SURVEILLANCE SYSTEMS. `https://www.indracompany.com/en/surveillance-border-protection`, Last access Dec 2020.

[56] Fotech solutions. Discover new insights and optimise your operations with fibre enabled monitoring and asset management. `https://www.fotech.com/products/helios-das/`, Last access Dec 2020.

[57] Photonics media. Invisible Border Patrol Employs Lasers, Optics. `https://www.photonics.com/Articles/Invisible_Border_Patrol_Employs_Lasers_Optics_/a45320`, Dec 2010.

[58] Rheinmetall-defence. Rheinmetall Vingtaqs II Long Range. `https://www.rheinmetall-defence.com/media/editor_media/rm_defence/publicrelations/pressemitteilungen/2015/idex_press_kit/2015-02-22_Rheinmetall_IDEX_Vingtaqs.pdf`, Feb 2015.

[59] International Exhibition of National Security and Resilience. Radiobarrier at ISNR 2016. `http://www.radiobarrier.com/how-it-works/`, 15 to 17 March 2016 Abu Dhabi, United Arab Emirates.

[60] J. Blazakis. Border security and unmanned aerial vehicles. *Congressional Research Service, Report for Congress*, RS21698 :01–06, Jan 2004.

[61] C.C. Haddal and J. Gertler. Homeland security : unmanned aerial vehicles and border surveillance. *Congressional Research Service, Report for Congress*, RS21698 :01–10, JUL 2010.

[62] the mobile satellite company Inmarsat. Border Surveillance Systems, Blighter scanning radar and sensor solutions. `http://www.inmarsat.com/wp-content/uploads/2015/12/Blighter_e.pdf`, Jul 2015.

[63] G. Thales. SQUIRE Ground Surveillance Radar. `https://www.thalesgroup.com/en/squire-ground-surveillance-radar`, Thales groupe, 2018.

[64] Telephonics Trusted Technology for a Tactical Advantage. ARSS radar, Advanced Radar Surveillance System. `https://www.telephonics.com/soft-gate/gated-assets/uploads/39870-TC-ARSS-Brochure.pdf`, 2016.

[65] A. Salim, W. Osamy, and A. Khedr. Effective scheduling strategy in wireless multimediasensor networks for critical surveillance applications,. *Journal of Applied Mathematics and Information Sciences*, 12(01) :101–111, Jan. 2018.

[66] N. Boudriga. A wsn-based system for country border surveillance and target tracking. *Advances in Remote Sensing*, 05(01) :51–72, Mar. 2016.

[67] A. El-maadi and M.S. Djouadi. Large-scale surveillance system : detection and tracking of suspicious motion patterns in crowded traffic scenes. *Automatika :Journal for Control, Measurement, Electronics, Computing and Communications*, 57(01) :173–187, Jan. 2017.

[68] drone elite. The best top 10 drones-2020. http ://drone-elite.fr/, 2020.

[69] H. Ben Kaouha, A. Abdelli, K. Bouyahia, and Y. Kaloune. Fdan : Failure detection protocol for mobile ad hoc networks. *IEEE FGIT-FGCN (1)*, pages 85–94, Dec. 2010.

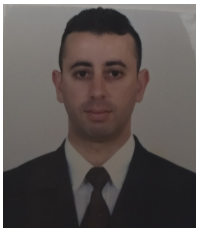
[70] H. Ben Kaouha, A. Abdelli, N. Badache, J. Ben othman, and L. Mokdad. Towards improving failure detection in mobile ad hoc networks. *GLOBECOM, San Diego, USA*, pages 1–6, Dec. 2015.

[71] F.Z. Qureshi and D. Terzopoulos. Surveillance camera scheduling : a virtual vision approach. *Journal of Multimedia Systems*, 12(03) :269–283, Dec. 2006.

[72] F. Xia, Z. Xu, L. Yao, W. Sun, and M. Li. Prediction-based data transmission for energy conservation in wireless body sensors,. *The 5th Annual ICST Wireless Internet Conference (WICON),*, Mar. 2010.

[73] oleumtech Brent McAdams. Wireless Sensor Networks : Applications in Oil & Gas. `https://oleumtech.com/solutions/oleumtech-wireless-sensor-networks-applications-in-oil-and-gas`, Dec, 2020.

[74] N. Shinohara. Recent wireless power transfer technologies via radio waves ;. *River Publishers : Gistrup, Denmark,*, 2018.



Mohamed Lamine LAOUIRA Is a doctoral student in the third year of his doctoral degree. He obtained his Engineer degree in computer science in Jun 2002 from the Military Ploy-technique School(EMP), he obtained his first diploma of Post graduate studies in Apr 2014 from USTHB university. His current research interests include wireless sensor networks, border surveillance applications, security and forensics solutions. Actually, he is a researcher at the Computer Science Department of the USTHB university and also the responsible for the Department of Criminal Sciences of the Algerian National Gendarmerie and permanent researcher at the Research and Development Center of the Algerian National Gendarmerie.

Abstract

Today, new security challenges, such as terrorism, transnational crimes, drug and arms trafficking, necessarily require a new strategies to address cross-border security. For a long time, conventional techniques such as human patrols, installation of barriers, construction of insulation walls and trenching, were used for securing borders over the world. However, those conventional techniques suffer from some issues such as intensive human involvement and high deployment cost, especially when the border line is very large. To overcome these issues, the use of technology for border surveillance was pushed fastly. The research work carried out in this thesis contributes to a large project which aims to define an operational framework for securing the Algerian land borders. To do that, a multilayer framework to detect and track any border intrusion with minimum human involvements was proposed based on the combination of several technologies such as multimedia sensors, radars, UAV. For energy saving, load balancing and redundancy elimination, an activation scheduling strategy was proposed also. Finally, for energy supply in border surveillance architecture based on the combination of radars with mobile camera sensors that are embedded in UAVs, we proposed a Wireless Power Transfer (WPT) system based on rectennas to supply wirelessly UAVs batteries with power during their flight.

Keywords : Wireless Sensor networks (WSN), Energy consumption, Network lifetime, Border surveillance, Camera sensors relevance, Scheduling strategy, Radars, Unmanned Areal Vehicles, network architecture, nodes deployment.