An efficient WSN based solution for border surveillance

Mohamed Lamine Laouira, Abdelkrim Abdelli, Jalel Ben othman and Hyunbum Kim.

Abstract—Since a long time, the integrity of physical borders is seen as a challenging concern. Indeed, governments have to facilitate travelling and trade so that economies continue to grow while preventing the entry of dangerous entities. To this aim, several conventional techniques were enforced to secure borders in the recent past. However, due to the immensity of the area to be monitored, such solutions require an intensive human involvement and high maintenance costs. This advocated to use new technologies, such as Wireless Sensor Networks (WSN), to reduce the costs and improve the efficiency of the border surveillance system. Although using and combining these technologies has been already addressed in different existing solutions, it still some key points to be considered like energy efficiency, load balancing and redundancy elimination. In this paper, we first propose a multilayer hybrid architecture based on cameras, scalar sensors, radars and UAVs to design a border surveillance system. Then, a detailed deployment strategy is discussed. Finally, an activation scheduling strategy based on load balancing and energy saving is addressed. The simulation results show that our solution could not only detect the intrusion in border areas, but also outperforms the other solutions by managing efficiently the network and extending its lifetime.

Index Terms—Border Surveillance, WSN, Energy efficiency, Deployment Strategy, Scheduling Strategy, UAV.

1 Introduction

TODAY, wireless sensor network (WSN) are omnipresent and we can find them either in many sectors of activity such as banking, transport and industry or in places of living such as cities, offices and public facilities. However, one of the most sensitive application of WSN is securing borders or what we call today **Border Surveillance**, especially when border intrusion activity becomes a crucial concern of any country or organization over the world. The design of a WSN based architecture for border surveillance should enjoy many challenging features, such as full area coverage, low cost deployment (low power consumption, low memory storage, low bandwidth use) and high rate of reliability.

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. Border surveillance techniques have shifted from classical methods such as human patrols, installation of barriers, construction of insulation walls and trenching, to the use of new surveillance techniques such as implementing Wireless Sensor Networks (WSN), Radars, Cameras towers as well as Unmanned Areal Vehicles (UAVs). These new technologies allow the integration of hundreds of cameras, seismic and infrared sensors, UAVs, satellites and radar coverage. The goal of these networks is to monitor borders and create a *virtual fence* [1], which generates a huge amount of video information that far exceeds the monitoring capabilities of security officers.

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, some questions are raised: *(i)* How to design the appropriate border surveillance system ? *(ii)* Which technology should be used to achieve border surveillance requirements (such as, low cost deployment, high coverage rate and low power consumption) ?

In this paper, we first propose a new hybrid wireless sensor network architecture for border surveillance. The goal behind this multilayer framework is to detect and track any border intrusion with minimum human involvements by combining multimedia sensors, scalar sensors (UGSs), radars and UAVs. These kinds of sensor nodes collaborate together to provide detection and tracking capabilities that are hardly achieved by using one system. Scalar sensors are deployed on the first layer (called detection level) of the proposed architecture, and are responsible for intrusion detection. Once the penetration is detected an alert is sent from the scalar sensors to the associated multimedia sensor which is deployed on the intermediate layer (called visualization level). Radars are also considered to extend the coverage area beyond the border lines. The information captured at this level are sent to the Command and Control Center (3C), located at the upper layer (decisional level). By fusing the information received from the multimedia sensors and radars, the tracking of intruders is achieved by calling UAVs

- *M.L. Laouira is Research Scholar at the University of Science and Technology Houari Boumediene, Algiers 16111, Algeria. E-mail: mlaouira@usthb.dz*
- *A.Abdelli is a Professor at LSI Laboratory, Dept. of Computer Science, USTHB University, Algiers, Algeria. E-mail: Abdelli@lsi-usthb.dz*
- *J.Ben othman is a Professor at L2S Lab CNRS, Centralesuplec, University of Paris Sud, France. E-mail: jalel.ben-othman@univ-paris13.fr*
- *H.Kim is an Assistant Professor at Dept of Computer Science, University of North Carolina at Wilmington, NC, USA. E-mail: kimh@uncw.eduz*

Manuscript received Month dd, yyyy; revised Month dd, yyyy.

to patrol the area to track the intruders instead of having recourse to human patrols. Indeed, this can be useful in the case we deal with inaccessible areas or that require the involvement of a huge number of humans.

In addition to that, a detailed deployment strategy of the equipments of each layer of the architecture is proposed. Finally, for energy saving, load balancing and redundancy elimination, an activation scheduling strategy is proposed. The latter implements the way scalar sensors and cameras are activated. Such a challenging issue is very important to deal with as the majority of existing border surveillance solutions suffers from the lack of a long term strategy that can contributes to extend the network lifetime. To highlight the efficiency of our solution, we compare our scheme to other existing methods. The simulation results show that our solution could not only detect the intrusion in border areas, but also outperforms the other schemes by extending the network lifetime while maintaining its efficiency.

The remainder of this paper is organized as follows. Section 2 reviews essential works related to border surveillance. A detailed description of our border surveillance architecture is given in Section 3. In Section 4, the deployment strategy of each level of the architecture is proposed. In Section 5, the activation scheduling strategy, used to exchange information between the two first layers of the proposed architecture, is discussed. The experimental results evaluating and comparing our solution with other techniques are reported in Section 6. Finally, we conclude our paper and give some orientations for future works.

2 Related work

Border surveillance techniques can be distinguished into two classes: conventional methods based techniques on a hand, and those based on new technologies, on the other hand. New technologies are either used separately or combined to achieve border surveillance requirements. In this section, we discuss the most significant and recent works that addressed the border surveillance problematic.

- In the recent past, conventional methods were used for borders surveillance. These methods call the use of: *manned aircraft*, *physical obstacles* such as trenches, fences and walls; *human patrols* (pedestrian or in vehicles); *permanent or temporary immigration checkpoints* to detect illegal aliens or activities. Such techniques can be used separately or combined to provide a high level of border security, depending on the type of threat and the sensitivity and the geographical nature of the area. However, using them require the deployment of an extensive human resources especially when the borders are very large and subject to intrusion and contraband. For some years now, these solutions are progressively abandoned and being replaced by cyber-technologies, where and when needed, to reduce the cost of the surveillance task while increasing its reliability.

One of these technologies is using Fiber Optic Sensors (FOSs). In [2] a based FOSs technology for border surveillance is proposed where FOSs are seismic sensors that can measure pressure waves in the earth caused by intruders. However, the implementation of such a system requires the deployment of a single wire along the border that ensures sensors interconnection with the command center. As a consequence, the occurrence of any single point-of-failure can affect the communication. Moreover, deploying wired sensors along borders is very expensive and difficult due to the harsh environmental conditions. The last but not the least, the use of fiber optic seismic sensors alone without additional technologies can generate a very high amount of false alarms due to the absence of a mechanism for confirming the intrusion.

To address some of FOS limitations, a new kind of sensors was introduced, especially after several years of researches in military applications domain. Recently, the use of passive sensors for remote battlefield applications is becoming more popular [3]. For instance, *Unattended Ground Sensors* (UGSs) have been used as a technology to monitor US borders with Mexico. According to a BBC news report, titled *US-Mexico border: Efforts to build a virtual wall*, elaborated in *29 August 2012* by *Anahi Aradas*, the US government announces that some $7,500$ sensors were acquired between 2003 and 2007 to create a movement detection perimeter. UGSs can detect vibration/seismic activities or magnetic anomalies and differentiate between human and vehicles intrusion with a high accuracy. Moreover, UGSs can pick up moving heavy vehicles (such as tanks) from a distance of 500 meters and walking humans from 50 meters [3]. For example, 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 are proposed in [4]. 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. To classify the targets and estimate their numbers, ultrasonic sensors are utilized. Detection and classification are achieved by *Dempster-Shafer* fusion of data coming from the sensors. Data is collected in real-world environments at three different locations, where a total of 26 scenarios with various combinations of people, animals, and payload are enacted. 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). In [5], acoustic sensors are used to evaluate the noise produced by the foot-steps of a stranger. Once collected, sensed signals are then converted into power spectral density and compared with reference value to identify the intruder. In [6], a four layer nodes architecture and a deployment strategy are proposed. The first layer of nodes, called *Basic Sensing Nodes* (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 *Data Relay Node* (DRN), that forms the second hierarchical layer of the network. The main role of a DRN is to collect the data received from different BSNs 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, then to provide an appropriate quality of service (QoS) to the generated flows before forwarding them to the *Network Control Center* (NCC) for analysis and decision making. Although this deployment strategy provides mathematical

control models to evaluate the performances of the network regardless to connectivity and coverage, the proposed architecture is based only on using scalar sensors, thus yielding many false alarms. Indeed, even though the deployment of UGSs is not costly, the efficiency of UGSs based systems is often limited due to the high rate of false alerts and classification errors. Additional works related to using UGSs for border surveillance are available in [7].

Due to the limited information provided by scalar sensors, multimedia sensors have been used to provide high accuracy in the detection of humans and keep false alarms to a minimum [8]. This includes inter alia night vision scopes, wireless and/or thermal cameras that are placed on surveillance towers. However, 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. The last but not the least, the implementation of mechanisms that guarantee energy saving and load balancing is more than desirable to extend the network lifetime.

Unmanned Aerial Vehicles (UAVs) have been deployed to ensure an automatic detection and to track illegal border crossing. According to [9], [10], the use of this technology (UAVs) was adopted by the U.S. Customs and Border Protection (CBP) after being tested in 2004 to patrol the United States international land borders. In addition to the large coverage provided by this technology, electro-Optical cameras are capable to identify an object of milk pack size from an altitude of 60.000 feet. UAVs also can provide precise and real-time imageries towards a ground control operator, who would then disseminate the information so that border patrol agents can be deployed quickly. Finally, UAVs can fly for more than 30 hours without having to refuel, comparatively to the helicopters, average flight time of which is just over 2 hours. In a recent work presented in [11], an architecture for border patrol was addressed. This heterogeneous architecture which combines UAVs with UGSs, operates as follows. Upon any UGS detects an intrusion of any type, it sets off an alert. UAVs are then directed to the site subject of intrusion to investigate the area. Similar architectures for border surveillance techniques using UAVs and UGSs are presented and discussed in [12], [13]. The use of UAVs and UGSs in border patrolling makes the control process independent of human decision. Consequently, the decision making process becomes less prone to human error and hence less consuming in terms of human resources. However, this kind of techniques suffers from some issues such as low rate of reliability and availability of the system especially when UGSs are subject to failures. Therefore, the need of a strict deployment strategy in this case is more than necessary. In addition to that, as the decision-making process can be too long, especially in certain circumstances when the area is not open to view, it can yield to the escape or the vanishing of intruders before the arrival of the human patrols. Despite the potential benefits of using UAVs for border surveillance, UAVs have some limitations such as the high risk of damages which is multiple times higher than that of manned aircraft. The risk is increased in inclement weather conditions which further impact negatively UAV's surveillance capabilities. Additionally and according to a CBP (Customs and Border Protection) general inspector, the costs of operating an UAV are more than the double of those operating a manned aircraft. This is because UAVs require a significant amount of logistical support and specialized operator and maintenance trainings. Finally, UAVs suffer from a major issue, which is the lack of an unified world legislation governing the use of this technology exceptionally in border areas, especially as the civilian use of UAVs increases exponentially. Based on the above, UAVS and UGSs should be combined with other technologies to enforce a more resilient 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 UAVs,UGSs ...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 European External Border Surveillance System (EUROSUR) is an example of using satellite technology [14]. The purpose of EUROSUR is to reduce the movement of illegal immigrants across borders by using the common technical framework based on Satellite, UAVs and sensors. This system is operational since $December$ 2013. However, its global cost amounts to 244 $million$ for $2014 - 2020$ which is covered by the multi-annual financial framework of the EU. In addition to this higher cost, the major limitation of EUROSUR emerges from the complexity of technical operations and maintaining coordination.

Blighter Border Surveillance Radar is one of the border surveillance systems based on modern electronic scanning radars, called Blighter. They are designed and built to provide continuous and 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 are now operational in more than 10 other countries, including the USA, France, Poland, Australia, South Korea, Qatar, Saudi Arabia, the Czech Republic and Oman. This kind of radars employs electronic rather than mechanical scanning which provides highest possible levels of system availability and reliability. Moreover, 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 [15]. However, using this kind of radars depends on the global satellite communications network, called BGAN (an Inmarsats service,) which obliges the users of this technology to pay an extra cost for being subscribed to this network. As the demand for flexible protection against penetration of intruders during day and night time is increased, the Czech Company ***EVPU Defence*** presented in May 2015 the ***BMS-MIRA 42*** system, as a response. EVPU Defence is a low cost solution for the monitoring and the surveillance of small areas of interest such as boundary lines, airports, coastal areas, that can be easily and quickly integrated on standard vehicles. The basic configuration of this system consists of Pan/Tilts, sensor container with uncooled IR cameras, daylight CCD TV camera. By combining its power detection with cameras, its increases its operational efficiency. Optionally, it can include laser range finder,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSUSC.2019.2904855, IEEE Transactions on Sustainable Computing

operators console and power supply pack [16]. This mobile monitoring system communicates by radio with a command center, patrols and intervention elements. However, since it is embarked on a vehicle, it requires human involvement for car driving. Moreover, it becomes difficult to deploy when roads are inaccessible to cars.

The last border surveillance solution that we discuss in this section is called **BorderSense** and represents a hybrid wireless sensor network architecture. According to [17], this technique can detect and track an intruder with minimum human involvements through using three types of sensor nodes: Multimedia sensor nodes that are equipped with video cameras or night vision scopes (deployed on the surveillance towers); scalar sensor nodes that are equipped with vibration/seismic sensor (deployed on the ground or buried underground); and finally mobile sensor nodes that roam throughout the border on the surface or in the air. The authors reported that this technique achieves to reduce significantly the rate of false alarms. However, we report several limitations to this technique. First of all, 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. Secondly, to deal with the unidirectional sensing of the cameras, the authors have suggested the use of a rotating mechanism to direct them. However, the feasibility of this solution has not been discussed. Finally, we report a lack of a coordination between the cameras and the ground/underground sensors. Indeed, the latter 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 available energy of the cameras while ensuring a load balancing. We investigate and discuss some of these issues in the next sections wherein a new architecture for border surveillance is proposed and discussed by taking into account the problematic raised above.

3 PROPOSED NETWORK ARCHITECTURE FOR BORDER SURVEILLANCE

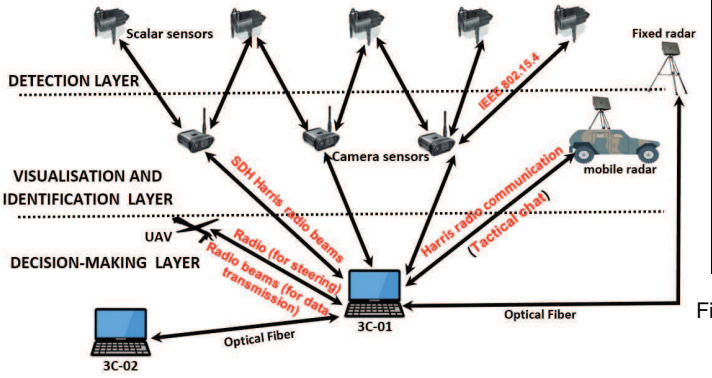


Fig. 1. Global hierarchy among the three layers of the proposed architecture.

The current work is to put in the context of a large project that aims at defining an operational framework for securing the Algerian borders. Algeria which is the largest country in Africa enjoys huge segments of borders ($6511km$) that are shared with 6 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 (1739 with Morocco; $1376km$ with Mali; 982 with Lybia; 461 with Mauritania; and $956km$ with Niger). Algeria is facing different threats along its frontiers, drugs and goods smuggling, arm trafficking, illegal immigrations and more seriously intrusions of AQMI and ISIS groups from Lybia, Mali and Niger sides. Therefore, securing the borders by using traditional means stands not efficient while proved to be very costly in terms of human deployment. With the collaboration of the military department, the goal of the current research project is to design a global solution to secure the borders by introducing new technologies so that to be able to achieve a full coverage of it with affordable costs. Particularly, the big challenge is to deal with the hostility of the sahara areas where it stands very difficult to deploy any human or material solution being giving the resources scarcity and the non availability of domestic supply networks in terms of energy and communication. To deal with this issue, using heterogeneous WSNs might be the solution as the latter consider various kinds of sensors that possess different capabilities in terms of sensing, processing, storage and communication. According to a report published in 2016 by FLIR company [18], 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 $360°$ coverage every second out of a distance up to $40km$. 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.

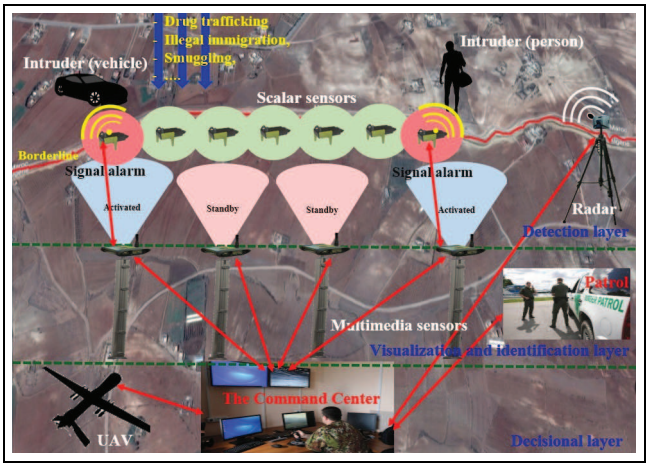


Fig. 2. Proposed Network Architecture for Border Surveillance.

For this purpose and as illustrated in figure 1, we consider in our solution a hybrid three layers architecture based on UGSs, Radars, Cameras and UAVs. UGSs and Radars are used for intrusion detection, while cameras are used for visualizing and identifying the nature of intrusions. UAVs 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 in the Algeria's saharan borders. As pictured in figure 2, the three layers of the proposed architecture are: The **detection layer**; the **visualization and the identification layer**; and finally the **decisional layer** (the 3C). Technically, the three layers could communicate via several technologies, as the 802.15.4 standard, $4G$ mobile networks, WIFI or satellites. However, although $4G$ 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 those 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 UGSs 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 the 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.

3.1 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** (UGSs) which are the elementary nodes, represent the big amount of sensors used in our architecture. The main task of UGSs is to perform seismic or vibration measurements. The use of UGSs is to substitute to radars, and to assist the cameras in targeting the intrusion. As UGSs are cheaper they can be deployed in full extent to cover the area unlike radars and cameras. In addition, their need in terms of energy is very low comparatively to other equipments, 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 a selected camera for 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* [19]. 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. UGSs 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 UGSs. 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, UGSs 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, UGSs are still used because they can be deployed everywhere and are more precise to detect pedestrians at near distances of the borders. 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 borders, 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 cameras can be activated by the 3C operator. In our architecture, we recommend the use of a specific radar, called SQUIRE [20], 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 our solution, radars are not correlated directly with cameras, unlike UGSs, because the detection range of radars is far bigger than the visualisation field of the cameras. In addition, the latter become inaccessible when radars are mobile. Therefore, the decision to activate the appropriate camera for identification is left to the 3C operator once the intrusion signal is geo-positioned on the map.

3.2 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 borderlines to identify the intrusion threat, its nature, and estimate the level of its dangerousness. In our architecture, cameras provide the 3C operator with a real time snapshots and video streams of the covered area. To extend their lifetime, cameras are in standby mode for most of the time, they can be activated by the 3C operator or when an alert is sent by the correlated scalar sensors. To avoid the transfer of a huge amount of unnecessary data, we consider the use of the *digital change detection* technique. That means that cameras 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 cameras, called ***RS-TV wireless camera or RS-TP thermal imaging camera***, commercialized by the company *RADIOBARRIER* [19] 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 cameras are permanently mounted on towers. RS-TP thermal imaging camera has a detection range that can up to 200 meters. 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.

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.

3.3 Decision-making layer

This level refers to the different command and control centers (3C) 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 the cameras 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 UAVs to perform a virtual investigation into the desired place.

Compared to conventional border surveillance techniques presented in section II, our architecture reduces considerably the deployment of an extensive human resources while providing a real time decision making architecture for border surveillance. Furthermore, the combination of several technologies such as scalar sensors, camera sensors, radars and UAV can considerably reduce the maintenance cost of the architecture while improving its reliability which makes it operate either in peacetime or wartime. In the next sections, we discuss the deployment and the activation scheduling strategies considered in our architecture to improve its energy efficiency and extend its lifetime.

4 Deployment strategy description

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 [21]. According to [22], sensor nodes can be either dropped from the air using a helicopter (random deployment), in this case the number of sensors required will be much higher, or deployed manually by placing the nodes in appropriate geographic coordinates. In our case, the manual deployment is used in accessible areas, while random deployment will be performed in inaccessible areas.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSUSC.2019.2904855, IEEE Transactions on Sustainable Computing

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. We assume in our solution that the 3C units are the first to be deployed then come the cameras on towers before deploying UGSs. Finally, radars are deployed when and where needed according to the zone coverage to obtain.

4.1 3C deployment

This level is the only one of our architecture that requires human involvement. The number of 3C required to cover the entire borderline depends mainly on the extent of the border bung and the organization of armed forces responsible for securing the borders. Often and in relation to operational requirements, the 3C must be within 50 km from the borderlines. The horizontal distance between two consecutive 3C can reach 50 km. Each device in the architecture is affiliated and controlled by one 3C at a given time. The communication between UGSs 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 will 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 (radars, UAVs) as in cellular networks.

4.2 Cameras deployment

To provide a bigger view field and a better coverage, multidirectional Pan-Tilt-Zoom cameras are considered in our architecture. The viewing angle of such a camera is $\alpha = 23°$, 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 cameras and its correlated scalar sensors is d= 125 meters, which is less than the radio range of the scalar sensor. Hence, the covered area by this camera at a given time, noted W, is (see figure 3.A):

$$W = 2 \times d \times \tan(\frac{\alpha}{2}) \quad (1)$$

For $\alpha = 23°$ and d=125 meters, we have $W = 50$ meters, namely two times the sensing range of an UGS. 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.B).

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

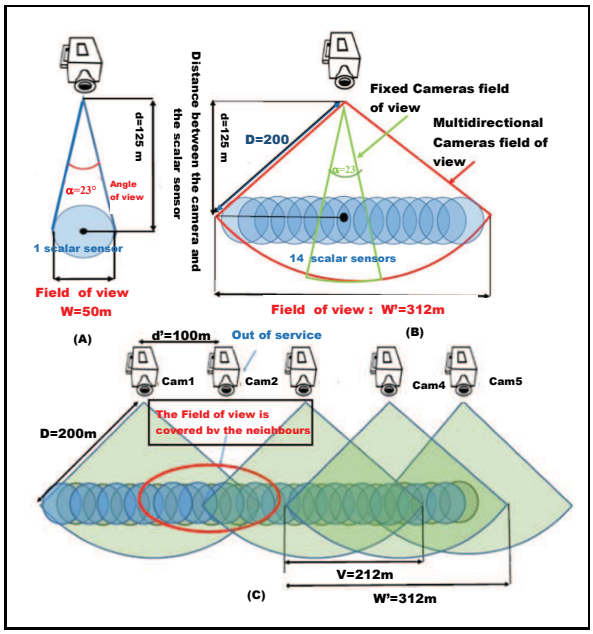


Fig. 3. (A): Field of view of a fixed camera (B): Field of view of a multi-directional camera (C): Overlapping area between two consecutive cameras

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-C). In this case, the overlapping zone between two cameras is:

$$D_{olapcam} = (W^{'} - d^{'}) = 212 meters. \quad (3)$$

4.3 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 with a good fault tolerance. 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 the borderline so that to be within the view field of the cameras and their radio range. To enhance the availability and increase the lifetime of the network, we assume that two neighbouring sensors overlap each other with a distance $D_{olap} = 30 meters \geq R_s = 25$ (see figure 4). 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:

$$L = k \times (2R_s - D_{olap}) + D_{olap} \quad (4)$$

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

$$k = \frac{(L - D_{olap})}{(2R_s - D_{olap})} \quad (5)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSUSC.2019.2904855, IEEE Transactions on Sustainable Computing

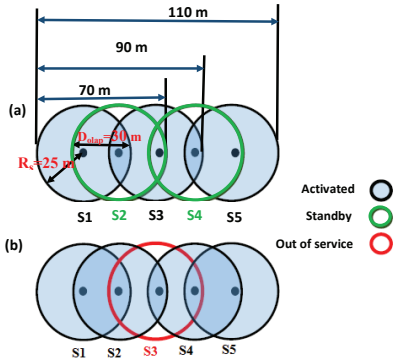


Fig. 4. (A): Scalar sensors deployment (03 activated sensors and 02 in standby mode) (B): If S3 fails, its area is monitored by S2 and S4.

According to equation 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. 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.

4.4 Radars deployment

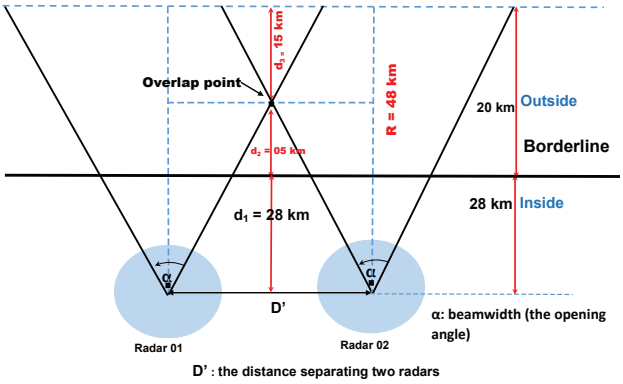


Fig. 5. Radars deployment : The overlapping area between two consecutive radars.

The goal of our deployment strategy is to use a minimum number of radars while ensuring a full area coverage. The detection range of the **SQUIRE** radars 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 5). We assume that the radars are placed at a distance of $d_1 = 28\ km$ to the inside of the borderline. 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 5, D' can be calculated using the following formulae:

$$\tan(\frac{\alpha}{2}) = \frac{(\frac{D'}{2})}{(d_1 + d_2)}; \quad D' = 2 \times (d_1 + d_2) \times \tan(\frac{\alpha}{2}) \quad (6)$$

The overlap zone between two neighbouring radars prevents, at best, high attenuation, extinction phenomena and cover the masks induced by mountain slopes.

4.5 Unmanned Aerial Vehicle deployment

UAV is used in our solution to perform virtual patrol 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 **theguardian** in 13 November 2014, the US government has operated about $10,000$ drones to cover about 900 miles, much of it in Texas. The HE300 which is considered in our architecture can fly during 02 hours to cover a range of 50Km with a cruising speed of 90Km/h. For operational reasons, we suggest the deployment at least two HE300 for every 3C, as it may be necessary to patrol two different places simultaneously.

5 Activation Scheduling Strategy

Many recent researches consider that the activation scheduling of sensors in a WSN is one of the key techniques to consider for extending the network lifetime. As a dense deployment is required, many sensors are in charge of monitoring the same area. This redundancy is useful since it increases the fault tolerance of the network. However, this can be achieved only by enforcing a reliable activation scheduling strategy that consists in balancing the load between the network nodes

5.1 Activation strategy for scalar sensors

According to our deployment strategy, at least one scalar sensor should be in the field of view of one camera at a given time. When rotating, 14 scalar sensors at least are within the global field of view of one camera. 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 4). In other words, among the 14 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 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 4. Concretely, the protocol is implemented at the 3C unit 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSUSC.2019.2904855, IEEE Transactions on Sustainable Computing

3C, is dynamic and can be differently fixed through time and from a sector to another. Increasing α results in reducing the amount of exchanged messages between the 3C and the sensors, in counterpart, the time to detect a potential sensor failure is increased. Hence, during a crisis time, α should be reduced to enhance the fault tolerance of the network, while it should be augmented in peacetime to extend its lifetime. In the extreme case of a cascading failure of 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 reception units are on.

5.2 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 on or off (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 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.

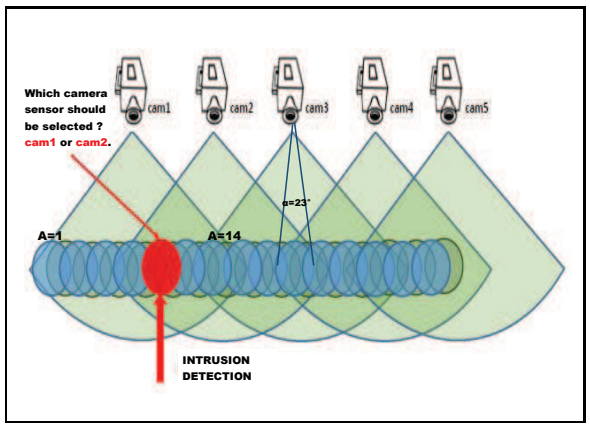


Fig. 6. Selection of the camera.

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 6). To this end, it uses the current status of the cameras in the selection process. Once the scalar sensor knows which cameras are free, 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:

$$F_{i,j} = ECam_j - [\mid A_j - pos(i,j) \mid \times C] \qquad (7)$$

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.
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 farest. 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 1 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 7 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 1
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 will confirm 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.

6 Simulation and Analysis of the Proposed Solution

To evaluate the performances of our solution compared to other border surveillance techniques, we tested the proposed deployment and activation strategies. 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 [23] and [24], we mainly considered the energy consumption related to data transmission and sensing. This is because the energy consumption of a sensor node is by far due to data transmission, 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.

6.1 Simulation parameters

In all 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 out solution in the worst case. For lack of space, we could not report all the simulations as those assessing the behaviour of the network in terms of latency and energy consumption when varying the value of α.
The deployment technique used in the simulation is the same as the one explained in section 4. 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 the scalar and the cameras 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 2 whereas those of the cameras are shown in Table 3.

Id	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
X	50	70	90	110	130	150	170	190
Y	80	80	80	80	80	80	80	80
State	W	S	W	S	W	S	W	S

Id	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}
X	210	230	250	270	290	310	330
Y	80	80	80	80	80	80	80
State	W	S	W	S	W	S	W

Id	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}
X	250	370	390	410	430	450	470	490
Y	80	80	80	80	80	80	80	80
State	S	W	S	W	S	W	S	W

Id	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
X	510	530	550	570	590	610	**630**
Y	80	80	80	80	80	80	80
State	S	W	S	W	S	W	S

TABLE 2
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
Cameras coordinates.

6.2 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 already discussed in the *related works* section [17]. 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.

6.2.1 Network energy consumption

For network energy consumption, the obtained results are shown in table 4 and figure 7, 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 4
Network energy consumption (in joule) vs the number of intrusions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSUSC.2019.2904855, IEEE Transactions on Sustainable Computing

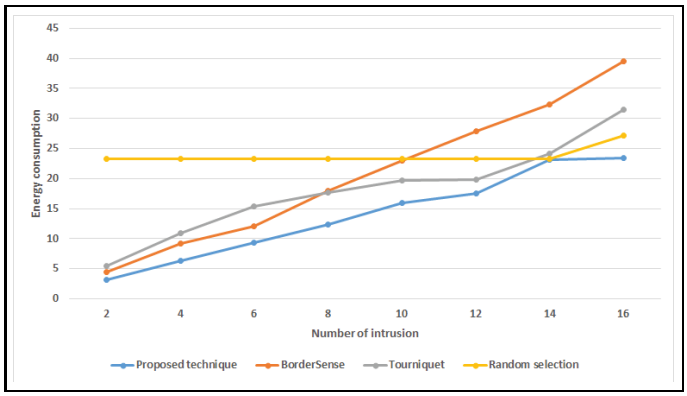


Fig. 7. Network energy consumption (in joule) vs the number of intrusions.

6.2.2 *Camera sensors response time*

For cameras response time, the experiment results are reported in Table 5 and Figure 8.

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 5
Cameras response time(in Seconds).

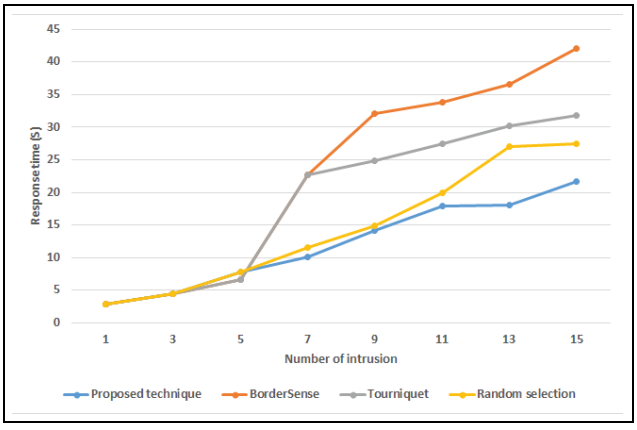


Fig. 8. Cameras response time (in Seconds).

6.2.3 *Load balancing*

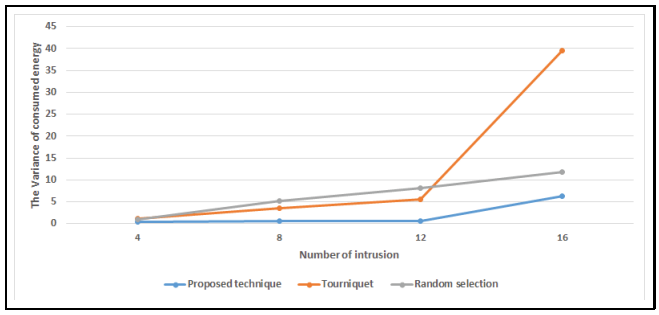


Fig. 9. Load balancing: The Variance of consumed energy by nodes.

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. It should be noted that this parameter has not been evaluated for the BorderSense due to the specificity of the technique. The obtained results are shown in Table 6 and Figure 9.

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 6
Sensors load balancing.

6.3 Interpretation

From table 4, 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 5 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 to load balancing, we notice that the variance of the consumed energy is also proportional to the number of intrusions. Table 6 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.

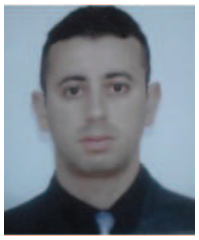
7 Conclusion

In this paper, a WSN based solution for detecting and monitoring borders against intrusions was introduced. In this context, an efficient multilayer hybrid architecture is put forward and discussed. The proposed framework combines multidirectional cameras, scalar sensors (UGSs), Radars and UAVs to reduce the deployment and maintenance costs of the surveillance task. These equipments collaborate together to provide an efficient solution. Thanks to the use of smart deployment and activation scheduling strategies we achieve to extend the lifetime of the network and reduce the impact of false alarms. Simulation results comparing our solution with existing techniques have been reported and show the efficiency of the proposed approach. Future researches will lead us to extend the deployment and activation strategies to new features so that to cope with different requests simultaneously and deal with node failures.

References

[1] D. Papademetriou and E. Collett, A new architecture for border management, Management Policy Institute, Washington, DC-USA, MAR 2011.
[2] G. Loney, Border intrusion detection: thinking outside the perimeter, 41st Annual IEEE International Carnahan Conference on Security Technology, pp. 0106, Oct 2007.
[3] E. Systems, Unattended ground sensors network (USGN), http: /defense-update.com/newscast/0608/news/news1506 ugs.htm, Copyright 2016 Defense-Update.
[4] 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, vol. 09, no. 03, pp. 468 477, Jul 5-8 2011.

[5] K. K.B.Madhavi and G. RishikeshM, Border security using wins, International Journal of Advanced Trends in Computer Science and Engineering, vol. 03, no. 01, pp. 112116, Feb 2014.
[6] R. Ramzi Bellazreg, N. Boudriga, K. Trimche, and S. An, Border surveillance : A dynamic deployment scheme for wsn-based solutions, Wireless and Mobile Networking Conference (WMNC), 6th Joint IFIP, vol. 01, pp. 2325, Apr 2013.
[7] J. Robert and P. Gervasio, An unattended ground sensor architecture for persistent border surveillance, Proc. SPIE 6980, Wireless Sensing and Processing III, vol. 6980, pp. 69 800A69 800A8, Apr 2008.
[8] S. Babu Nr, A. Swaminathan, and D. C. JoyWinnieWise, Boarder analysis with ensora and doa using wireless sensor networks, Sixth International Conference on Emerging trends in Engineering and Technology, pp. 7683, 16-18 Dec 2013.
[9] J. Blazakis, Border security and unmanned aerial vehicles, Congressional Research Service, Report for Congress, vol. RS21698, pp. 0106, Jan 2004.
[10] C. Haddal and J. Gertler, Homeland security: unmanned aerial vehicles and border surveillance, Congressional Research Service, Report for Congress, vol. RS21698, pp. 0110, JUL 2010.
[11] D. Bein, W. Bein, A. Karki, and B. Madan, Optimizing border patrol operations using unmanned aerial vehicles, 12th International Conference on Information Technology - New Generations, pp. 479484, 13-15 Apr 2015.
[12] K. Kalyanam, P. Chandler, M. Pachter, and S. Darbha, Optimization of perimeter patrol operations using unmanned aerial vehicles, Journal of Guidance, Control, and Dynamics, vol. 35, no. 02, pp. 434441, Apr 2012.
[13] A. R. Girard, A. S. Howell, and J. K. Hedrick, Border patrol and surveillance missions using multiple unmanned air vehicles, in Decision and Control, 2004. CDC. 43rd IEEE Conference on, vol. 01, no. 10.1109/ITNG.2015.83, pp. 620625, 14-17 Dec 2004.
[14] B. Hayes and M. Vermeule, Borderline the eus new border surveillance initiatives, assessing the costs and fundamental rights implications of eurosur and the smart borders proposals, Proposals: a Study by the Heinrich Bll Foundation, Jun 2012.
[15] t. m. s. c. Inmarsat, Border Surveillance Systems, Blighter scanning radar and sensor solutions, http://www.inmarsat.com/ wp-content/uploads/2015/12/Blighter e.pdf, Jul 2015.
[16] O. O. S. D. News, I. D. Official Web TV, and S. T. Fair, EVPU DEFENCE at IDET 2015, http://www.evpudefence.com/en/, 19-21 May 2015, Brno-Czech Republic.
[17] Z. Sun, P. Wanga, C. Vuran, M. Al-Rodhaan, A.-D. A.M., and I. Akyildiz, Bordersense: Border patrol through advanced wireless sensor networks, Ad-Hoc Networks, vol. 09, no. 03, pp. 468 477, May 2011.
[18] FLIR, Discover the Best Technology for Border Surveillance 2016, http://www.flirmedia.com/MMC/CVS/Surveillance/ SV 0006 US.pdf, Accessed date: December 07, 2016.
[19] Radiobarrier, How it works? http://www.isnrabudhabi.com/, Accessed date: November 25, 2016.
[20]] T. group, SQUIRE Ground Surveillance Radar, https://www.thalesgroup.com/en/squire-ground-surveillance-radar, last access, Juin 2017.
[21] Seema and R. Goyal, A survey on deployment methods in wireless sensor networks, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 03, no. 07, pp. 540 543, Jul 2013.
[22] T. Yang, D. Mu, W. Hu, and H. Zhang, Energy-efficient border intrusion detection using wireless sensors network, EURASIP Journal onWireless Communications and Networking, pp. 0112, MAR 2014.
[23] F.Xia, Z.Xu, L.Yao, W.Sun, M.Li, Prediction-based data transmission for energy conservation in wireless body sensors, The 5th Annual ICST Wireless Internet Conference (WICON), 1-3 March 2010.
[24] M.Elshrkawey, S.M. Elsherif, M.E.Wahed, Journal of King Saud University Computer and Information Sciences, vol. 30, no. 02. Pages 259-267, Apr2018.



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.

Abdelkrim Abdelli Is a Professor at the Computer Science Department of the USTHB university. He obtained his Engineer degree in computer science from USTHB university in 1993, he got his first diploma of Post graduate studies from USTHB university in 1994, after that he obtained his Master degree in computer science from the same university in 1998. In 2007 he obtained a PHD in computer science from USTHB under the supervision of Pr. N. Badache. He is a professor since 2014 after obtaining the degree of Habilitation to conduct research projects in computer science in 2009. Professor Abdelli was involved in several research projects such as CNEPRU (2014-2017), Project national PNR (2011-2013), cooperation Project CMEP (2012-2015), Project MOVES (2006-2008) and others.

Jalel Ben othman Dr. Ben-Othman received his B.Sc. and M.Sc. degrees both in Computer Science from the University of Pierre et Marie Curie, (Paris 6) France in 1992, and 1994 respectively. He received his PhD degree from the University of Versailles, France, in 1998. He was an Assistant Professor at the University of Orsay (Paris 11) and University of Pierre et Marie Curie (Paris 6), in 1998 and 1999 respectively. He was an Associate Professor at the University of Versailles from 2000 to 2011. He is now full professor at University of Paris 13. Dr. Ben-Othmans research interests are in the area of wireless ad hoc and sensor networks, Broadband Wireless Networks, multi-services bandwidth management in WLAN (IEEE 802.11), WMAN (IEEE 802.16), WWAN (LTE), security in wireless networks in general and wireless sensor and ad hoc networks in particular. His work appears in highly respected international journals and conferences, including, IEEE ICC, Globecom, LCN, VTC, PIMRC, etc.

Hyunbum Kim Dr. Hyunbum Kim joined to the Department of Computer Science at University of North Carolina at Wilmington, NC, USA in August 2014. He received Ph.D. degree in computer science from the University of Texas at Dallas, Richardson, TX, USA under the supervision Dr. Jorge A. Cobb. He received M.S. degree in computer science and engineering from Hanyang University, South Korea under the supervision of Dr. Heekuck Oh. Also, he received B.S. degree in computer science from Pyeongtaek University, South Korea. His research interests include system and algorithm design/analysis/optimizations in various areas including Internet of Things (IoT), unmanned aerial vehicles (UAVs), smart cities, cyber physical systems, edge computing, vehicular ad-hoc networks (VANET), mobile computing, distributed computing, wireless sensor networks and cyber security.