Sensor Analysis and Selection for Open Space WSN Security Applications

Maria Charalampidou[1*], George Pavlidis[2], Spyridon G. Mouroutsos[3]
1- Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece.
Email: macharal@ee.duth.gr (Corresponding author)
2- Institute for Language and Speech Processing, Institute, 'Athena' Research Center, Xanthi, Greece.
Email: gpavlid@ceti.gr
3- Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece.
Email: sgmour@ duth.gr

Received: August 2018 Revised: October 2018 Accepted: December 2018

ABSTRACT:
The necessity to tackle the increasing common concern about safety issues, urges the scientific community to come up with the development of innovative intruder detection and early warning security systems. One of the most effective technological solutions is provided by the application of WSNs. In this endeavor, most solutions have already adopted supercomputers and other computer resource systems to process the enormous amount of data. Alternatively, to this approach, simpler and more easily implementable solutions, such as the WSNmod method, are already being put to use. In particular, WSNmod is based on three key elements, the categorization of sensor inputs, the quantization of the inputs and a time-window processing. WSNmod was introduced as an advanced intrusion detection system that focused on the minimization of the false positive alerts. Building on the idea of WSNmod, in this paper we focus, identify and quantify measurable parameters that influence the detection reliability. In addition, the very promising test results of the method and the security system are presented in a range of environmental conditions.

KEYWORDS: Wireless Sensor Networks (WSN); Sensor Selection; Ultrasonic Sensor; Motion Sensor; Vibration Sensor; Security; Intruder Detection; Decision Making; Sensors; Sensor Networks; Sensor Nodes; Policies; Security Applications; Surveillance Systems.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have become a technology tested in numerous scenarios and applications, consolidating their position as a mainstream field of research and applied sciences worldwide. In practice WSNs are a set of nodes that combine sensor technology with the computational power of microcontrollers, in a low power scheme and a wireless connection between them [20], [6] (Fig. 1). WSNs are first introduced back to the 1980s, when the United States Defence Advanced Research Projects Agency (DARPA) started the Distributed Sensor Network (DSN) program. Recent advances in WSNs are fuelling the interest in a wide variety of accurate applications such as battlefield surveillance, border control, and infrastructure protection. Nevertheless, open issues remain such as the limited energy, memory, and computational capabilities of the sensor nodes, ever since.

The inherited characteristic of WSNs from the wireless data transmission, enable ad-hoc structures in mesh topology ideal for open space monitoring. In this way, nodes act as routers and cooperate in order to transmit measurement data to a central coordinator. Subsequently, through the coordinator, a WSN can be interconnected to other networks or the Internet (Fig. 2). Thus, WSNs meet the requirements of the Internet-Of-Things (IoT) in the most suitable way [5]. In detail, WSNs operate by collecting data from heterogeneous inputs (sensors) and directing them to a monitoring center via a router. Later, the central station collects all measurements and is able to impose actions or reactions on the physical world via distributed actuators [5].

A WSN application of particular interest, both in academic terms and in terms of application, is the surveillance and security monitoring of open areas. In general, access to an area involves any potential presence, either authorized or intruding. In cases where authorized access is necessary, it is essential to be able to provide early warnings of unauthorized presence. Furthermore, if high safety and security requirements are imposed, surveillance of the area and detection of potential intrusion are of particular importance. In these cases, there is not only a need to prevent theft or vandalism or any other violation, but also a need to ensure a sense of security to the people who are the legitimate users of the facility.

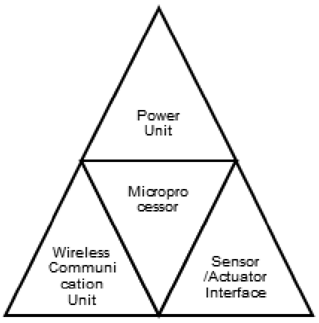


Fig. 1. Sensor node architecture.

A number of security applications can be found in the literature. These applications examine both how nodes are located and how to detect the attacker and transmit the data in the most energy efficiency way. In general, applications are based on either using a centralized management or a distributed one. Object tracking in WSN surveillance applications is one of the dominators in which the network of sensors is assigned to the task of identification and tracking an object. The network employs the decision-making, object tracking, object classifications techniques to deliver the signals to a sink node or to a central base station. Many papers have already summarized and reviewed the field [38], [39].

In terms of WSNs applications one can find examples and management schemes that developed and implemented in real-world conditions, in both small centralized [44] or extended decentralized scale [35] [36], [37]. These networks deploy magnetometers, thermal–pir sensors, optical-radar, seismic and acoustic-microphone sensors in monitored areas to detect the presence of targets in an active field. In the first centralized category, the total amount of node measurements is transmitted to a central base station where the processing is done. These implementations conclude with a communication load that puts a heavy strain on the nodes' energy consumption [44]. On the other hand the measurements from these sensors can be processed decentralized by forming a distributed decision-making scheme. In this way the measurements from each sensor node must be at the most accurate level. Therefore, in these methods a more comprehensive study is been held in the sensor and node level. The interesting thing from our point of view is that in [35], the authors spot a temperature drift that is occurred in magnetometers. Although the authors admit that there is environmental affection to their measurements, a more in-depth analysis of this affection is not given for all of the sensors used (thermal – pir sensors). Moreover in [36], even though the authors underline the effect of wind in the false alarm ratio, they overcome the problem by filtering the samples during a time window which was ultimately determined on the basis of the energy management of the nodes and not on the accuracy of the event. Another technique of target tracking in real life tested applications is given in [40] and in [41], where the WSN tracks the target by using Received Signal Strength Indicator (RSSI) which is available at WSN nodes. In particular, when WSNs are deployed in close proximity, the transmit power level enables accurate conversion of RSSI measurements to range estimates. Having this information, statistical or other fusion techniques can give accurate results. The obvious disadvantage of these methods is that the target must be a WSN node of the network thus the methods are not suitable to identify invaders along with the complete ignorance of environmental conditions that affect the transmission.

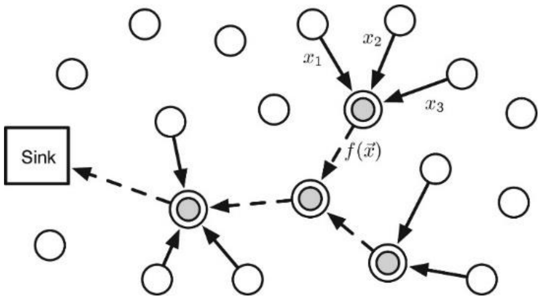


Fig. 2. Data aggregation in WSN [5].

Though WSNs may have accomplished a fine overall performance on the land, it is rather challenging to deploy a sensor network on the sea surface. Thus the protection of near-coast sea surfaces, harbor areas and oil platforms from any relative unauthorized intrusion is particularly challenging. The main challenge is that when sensors are deployed on the sea surface, they are not static and get tossed by ocean waves which makes them move around randomly. In [34] the authors present a solution for ship intrusion detection based on three-axis accelerometer sensors. In particular the researchers deploy an experimental Wireless Sensor Network (WSN) on the sea's surface to detect ships by using signal processing techniques and cooperative signal processing. Thus they can detect any passing ship and also distinguish the ship-generated waves from the ocean waves.

In the market, the ShotSpotter system has recently gained attention. The system is a gunfire detection and location technology based on acoustic sensor signals. Recently, a memorandum of understanding has been signed between the ShotSpotter and General Electric (GE) Lighting and ShotSpotter to bring gunshot detection to light fixtures as an option in GE's suite of intelligent LED technology for cities[1]. Furthermore, acoustic signal is also used in Shooter Localization with Mobile Phones (SOLOMON), a mobile app that collects sound waves through microphones mounted on soldiers' headsets. The data processing of the signals determine the enemy shooter location data that are displayed on the soldiers' phones via Google Maps.

Currently DARPA has introduced a new vision for using IoT in the military to tackle the energy efficiency and expand the WSNs' lifespan. Started in 2015, the agency admits that their high-end sensors used by the military to detect vibration, light, sound or other signals on a battlefield are energy-intensive. Thus a new project for sustainable sensor energy has burst out. As DARPA notes, Near Zero Power RF and Sensor Operations (N-ZERO), "seeks to overcome the power limitations of persistent sensing by developing wireless, event-driven sensing capabilities that would allow physical, electromagnetic and other sensors to remain dormant — effectively asleep yet aware — until an event of interest awakens them.".

Regarding decision-making methods at the simulation level, an interesting scenario is presented in [11]. In the paper, the researchers present a method of deploying and processing of a WSN. At first the division of the monitoring area into subareas is done. Afterwards the subnetwork's central node is put in awake mode to detect random invasions, and when the energy level of that node falls below a threshold, its redundant node is triggered simultaneously. In this way, it is not necessary to replace the nodes, that lack of energy increases the overall lifespan of the network. Nevertheless the intrusion detection accuracy of the WSN is not given.

Another simulation work is given in [43]. Specifically, the authors in [43] present a model of node management and distributed decision making which is also based on the division of the network into subareas (cells) this time evenly. In this case, however, cells only communicate with 1-hop nodes. The supervisor (each node operates as a supervisor) can change the status of a cell to alive, hazardous or dead depending on the state of the node itself (if it detects something, so it is set to dead state) or if its neighbours have detected something (set as a hazard). In this case, it is clear that the organization of the network is completely distributed and that the thresholds are crucial so that panic does not spread along the network in case of a false alarm.

Apart from the applications that use classic intrusion detection sensors (magnetometers, radar, pir, ultrasonic, etc), there is also a parallel survey that attempts to adopt high precision sensors rather than their energy requirements. For example, in [32], the WSN is based on cameras and motion detection sensors are creating a wireless multimedia sensor network; when intruders cross the border, a motion detector triggers the attached camera. The camera grabs the image and sends it to the sink via the WSN. Since the image to be transmitted requires a large bandwidth, only important parts of the image are sent via reliable paths. The data transmission of an image is far greater than the normal data of the WSNs. Therefore, the study, deploys an encoding scheme that is applicable to image partitions rather than the full image along with a priority factor. In order to evaluate the images from the cameras, the threshold was set by testing a sample of reference images. The outcomes of the method are based on simulation results.

In future WSNs, more types of sensors could be deployed. For instance, the semiconductor chiplets, or "dielets" (Fig. 3) could be attached to the basic nodes supplementary. By affixing this dielet into chipsets, objects, cars or even systems, the tagging would enable the connectivity of the artefact with only a footprint of the size of a dust speck. As envisioned in DARPA's Supply Chain Hardware Integrity of Electronics Defense (SHIELD) program, by the end of the program, each of these dielets will host up to 100,000 transistors. The dielet would also host a two-way radio communication, an on-board security encryption algorithm, an energy harvesting process that casts away the constant need for a battery-due to the use of a cable during scanning of the object, and a set of passive sensors for tamper-detection—all the while consuming less than 50 microwatts and costing at about a fraction of a cent [2]. Although dielets are designed for tagging a new era of sensor applications which may arise.

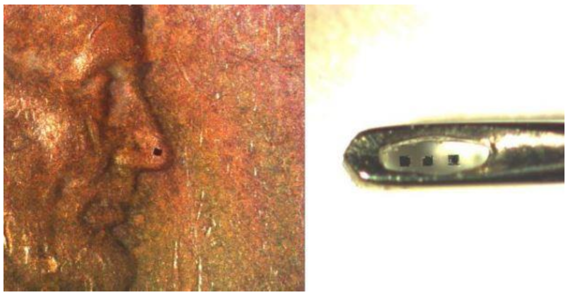


Fig. 3. DARPA's dielets**.**

Recently, a novel approach towards the development of a sophisticated decision-making system for accurate intrusion detection was proposed (the *WSNmod*) [19]. WSNmod is based on three key elements: the assessment of the certainty of the inputs, the quantization of the inputs using three-valued logic and the time-based filtering of the sequence of alarms. The algorithm was applied to a Wireless Sensor Network (WSN) that was used for intrusion detection of an open area. The basic

[1] http://www.shotspotter.com/

[2] https://www.darpa.mil/news-events/2015-09-04

characteristic of WSNmod is that the sensors in the WSN nodes can be divided into two categories: the first category is the sensors that provide direct information about an intrusion, which are called *primary sensors*; the second category is the sensors that can be used to characterize the level of trust to the measurements taken by the sensors in the first category; the second category sensors are called *secondary sensors*. The secondary sensors do not provide information about an intrusion but they provide additional information about the environmental conditions that may directly influence the “quality” of the measurements taken by the primary sensors. Thus, the secondary sensors can measure any quantity that can be used to determine the reliability of measurements from the primary sensors. Although the system presented a novel idea on how to include environmental parameters in open area intrusion detection, there was no in-depth analysis of how these parameters affect the measurements and the overall decision-making process.

Apparently, although the definition and role of primary parameters are clear, as the parameters that relate with the main intrusion measurements, the definition and role of the secondary parameters cannot be simply limited to that the measurements of environmental conditions. As in any WSN an ecosystem of nodes is being formed, and it can be easily visualized how decisions on a node basis can be a secondary parameter for the network also. In this view, a broad set of parameters can play the role of the secondary parameters, which might either significantly or not influence the overall system outcome. As an indicative example an alarm at a node is naturally expected to be detected almost simultaneously at a neighboring node. If there is no intrusion detected at a neighboring node then it is very likely that the event is a false positive.

In this study, we summarize the most appropriate sensors for intrusion detection, identify the parameters which have the greatest impact on the measurements, test the effect of those parameters and present results demonstrating the significant effect of those parameters on the intrusion detection systems.

2. MEASUREMENT DATA FOR SECURITY APPLICATIONS

Practically, given the selection of an appropriate group of sensors and a network structure, the stage of WSN data aggregation includes the collection of sensor measurements. The selection of an appropriate group of sensors is based on the specifics of each application. The network structure mainly consists of the individual sensor nodes, the arrangement of the sensor nodes, the communication and routing infrastructure and the detection logic along with the distribution of decision making and inaction. On the other hand, the data aggregation consists of all measurements and accompanying metadata (provenance, timestamps, geolocation data, environmental data, etc.).

In general, during the process of intrusion detection one should specify the measured quantities that the decision-making algorithm would take into account. Either in the case of model-based decision-making or in the case of data-driven methods, researchers have identified a number of measured quantities and data processes [34], [35], [21], [22]. The commonplace of both approaches is that they use weighted instances of measurements to determine a final result. Recently, there is also ongoing research on decision-making where a sensor selection process is held as a preprocessing stage, in order to exclude a number of measurements that are highly correlated and considered as redundant [7], [8]. For example, a vibration sensor and a passive infrared sensor located at the same detection spot, are expected to collect closely correlated information concerning the existence of an intruder. Although it seems reasonable to discard the redundant sensors, in this study we argue that this might not be such a reasonable idea. The impact of secondary parameters that might influence the measurements taken by the selected sensors is expected to be different for each of them. As a consequence, a corrupted measurement from one specific sensor could be replaced by a non-corrupted measurement by its “complementary” sensor. In this case, an intelligent inference system should weight the measurements against their reliability and base its decision on the most reliable set of data. In any case, uncorrelated output from different sensors, can, in general, enhance the decision-making process by the fusion of their measurements.

The most common sensors for security applications as identified in the literature [9], [10], [21]-[24], and the commercial applications are:

- sensors detecting electromagnetic signals
    - *passive infrared sensor (PIR)*, to detect motion in a zonal spatial range;
    - *laser* or *LED proximity sensors*, to detect presence and proximity based on light detection;
    - *magnetic sensor*, an inductive sensor, usually to detect armored presence or vehicle;
    - *optical sensors and cameras*, to detect and identify presence (possible ethical issues apply [17]);
    - *optical fibers*, as a hybrid approach to control passage, by detecting the interruption of an optical signal;
- sensors detecting mechanical signals
    - *ultrasonic-proximity sensors*, for determining the distance of a potential intruder;
    - *fence vibration sensor*, a capacitive sensor, to detect unauthorized passage;

- *mechanical vibration sensors*, to detect any motion by the produced vibrations;
- *mechanical contact sensors*, to detect contact;
- *pressure sensor*s, to detect contact and touch;
- *glass breaker sound-pulse sensors*, to detect glass breaking-like sounds;
- *microphones*, to detect and recognize presence and identity;

The above non-exhaustive list of sensors' types in the recent bibliography is enhanced with complex sensors of any combination [10]. This strategy is chosen in order to reduce false alarms. Systems based on these sensors are sometimes enhanced with sensors and detectors which are not primarily used in security applications, such as *microwave* sensors, *geophones*[3], *fancy fence cable* sensors [16].

In this study, we focus on three of the most widely used sensors (for monitoring and security applications), namely, the ultrasound, the infrared and the vibration sensors. These sensors are supposed to be part of a distributed network forming a WSN in an open space. The sensors are organized into nodes each of which includes one sensor of each type. The nodes are placed at points considered as passages or potential passages for intruders in the area of interest and transmit their data wirelessly to a command center for processing. In the following paragraphs a basic description of the sensors is provided, including the parameters that mostly affect their measurements. Summarizing this analysis, a table with the identified complementary (secondary) measurements is given for each of the sensors. It is worth mentioning that all of the selected sensors are already known to be affected by both temperature and wind speed [26] - [30]. The complementary (secondary) parameters that are identified as relevant in this study are:

- Wind speed
- Temperature
- Humidity
- Barometric pressure
- Acoustic noise
- Material
- Color – visual characteristics

2.1. Ultrasonic Sensor

Ultrasound is a mechanical wave. The bandwidth ranges from approximately 20 kHz up to several GHz. Sound can propagate through compressible media such as air, water and solids as longitudinal waves and also as transverse waves in solids. Thus, the medium is very crucial for the propagation speed of sound. In the air, the sound propagation deviates from being perfect spherical due to a number of factors, including absorption of sound, non-uniformity of the propagation medium due to meteorological conditions (refraction and turbulence), and interaction with the ground and solid obstacles (such as barriers). The operational principle of ultrasonic sensors is based on the emission and reception of an ultrasound within the same material. The pulse can be generated with a high pulse voltage (Ultrasound Pulse Voltage) on a piezoelectric disk. Then the returning sound is detected by another (or the same) piezo disc producing a relative amount of voltage. The echo of the pulse is generated by the reflection on any surface between the first tangential surface of the transmitting disc and the final surface of the opposing object.

In order to measure ultrasound there are three main ways:

a. By measuring the travel time (Time of Flight) from transmitting to receiving; in this case one or more emitters and one or more receivers are usually used, and the positioning of the elements allows simultaneous target detection and mapping of the monitored space. The principal equation is:

$$ToF = 2 * L / (c \pm V) \tag{1}$$

Where L is the distance between ultrasonic transducers travelled, c is the speed of sound in the medium, V is the average velocity of the medium.

b. By measuring the frequency shift – Doppler effect. The principal equation is:

$$f_D = \frac{f_e\, v\, r}{c} cos(\alpha) \tag{2}$$

Where f_e is the emission frequency, f_D is the receiver frequency (Doppler frequency), v_r is the relative speed between the transmitter and the receiver, c is the speed of light ($3 * 10^8\ m/s$), $\alpha €[0, \pi]$ is the angle of the velocity vector. The maximum f_D happens when α=0. $max(f_D) = (v_r * f_e)/c$

c. By measuring the pulse width. The amplitude of the reflected wave is given as:

$$A_r = \frac{R_1 - R_2}{R_1 + R_2} \tag{3}$$

Where

$$R1 = q_1 c_1,$$
$$R2 = q_2 c_2,$$

Where q is the density of each material, c is the speed of the source, and A_r is the ratio between reflected and incident amplitudes.

[3] http://argosfp7project.blogspot.gr/

In addition, the speed of sound in air is proportional to the square root of the absolute temperature by the relation:

$$c = 20.05\sqrt{T + \frac{e}{p}} \tag{4}$$

Where T is the absolute temperature (K), e is the partial pressure of water vapor (psi) and p is the barometric pressure (psia).

One of the important factors in using ultrasound sensors is that of the influence of the ultrasonic reflection, especially as the reflection that can vary from object to object. The amount of reflected ultrasound depends on the *material* of the object upon which it is reflected. In the case of an intruder the reflection depends mostly on the person's clothing. Another important factor that affects ultrasonic measurements is the presence of *ambient acoustic noise* [31]. Industrial operations for example such as impact, bending, grinding, drilling, fluid or air sprays produce an amount of ultrasound noise. Especially fluid or air sprays produce significant amount of noise therefore the ultrasonic requires operation at higher frequencies. The most influencing factor that affects measurements is the *transmitting medium*, the air in our case. Specifically, the parameters that affect the measurements are the *wind speed and direction*, the *air pressure*, the *air humidity* and the *air temperature*. The wind speed and direction may shift the reflected signal in such a way as to affect both the intruders' detection and their exact position. In addition, it is worth mentioning that over open ground, substantial vertical wind velocity gradients commonly exist due to friction between the moving air and the ground. Thus, the wind speed profiles are strongly dependent on the time of day, weather conditions and the nature of the surface and affect the acoustic waves [3]. This can lead to chain reactions and incorrect detection, or to false negative results (no intrusion detection). It should be emphasized that the measurement of the wind speed is affected considerably by the temperature and humidity of the air. Therefore, by including a sensing element of temperature and humidity, the ultrasonic measurements should be readjusted. As far as the air pressure is concerned in practice, the sound speed is reduced to about 1% at the altitude of 3km above the sea, rendering air fluctuations negligible [3]. On the other hand, ultrasonic sensors are not affected by the color or other visual characteristics of the detected object. The overall influencing parameters of ultrasonic sensors are shown in Table 1.

Table 1. Ultrasonic Measurement influencing parameters.

Parameter	Degree of influence
Wind speed	Significant
Temperature	Significant
Humidity	Significant
Barometric pressure	Minor
Acoustic noise	Significant
Material	Significant
Color – visual characteristics	None

2.2. Passive Infrared Detector

Passive infrared detectors are "designed to initiate an alarm condition in response to the change in radiation at wavelengths within the specified band of the infrared spectrum, which results from the presence of an intruder."[4] The range of these detectors is limited and offer a last-minute warning to the overall setup. Passive infrared sensors use pyroelectric elements. The elements emit and absorb the IR energy focused onto them. When the amount of IR energy the elements receive differs, the output of the detector swing high or low.

As derived from the operation principle the device is unsuitable for applications in areas with any king of heat source and radiators. Specifically, the sensor does not work well when the difference in temperature of the object and the background is less than 7°C. Also, PIRs are more sensitive and effective to a horizontal movement across the detector rather than away from or towards it, and hence the mounting and positioning of the sensor is of great importance. Moreover, the sensor is not reliable in detecting targets moving particularly fast or slow. That is because radiation from such objects is similar to background thermal noise. Moreover, to detect slowly moving or crawling people, the lower limit frequency of a transfer band of PIR detector should be near zero. Furthermore, detectors should never be subject to direct sunlight, and even reflected light can cause a problem if deflected onto the PIR. Sunlight falling directly onto a PIR will certainly cause unwanted activations, and care must be taken in case the device is in an area with mirrors or highly polished metal, as they will reflect IR energy. The PIR must be sealed against the entry of insects or draughts by filling entry holes with silicone. Rodents, birds or pets can trigger the sensor and cause false alarms. In some cases, even the connecting wires to the controller can become 'antenna influenced' and transmit radiofrequency interference [4]. Apart from accidental false alarms due to animal detection further triggers can be caused because of loose materials, such as polyethylene sheeting, plastic bags and accidental flapping in the wind, swaying foliage and moving

[4] Australian Standard AS2201.3

animals.

In Table 1 the major parameters that affect the detector are presented.

Table 2. PIR measurement influencing parameters.

Parameter	Degree of influence
Wind speed	Moderate
Temperature	Significant
Humidity	Minor
Barometric pressure	None
Acoustic noise	None
Material	None
Color – visual characteristics	Moderate

2.3. Vibration

Vibration stands for the phenomenon in which mechanical oscillations (periodical or random) occur around an equilibrium point. Vibration is the generic term for a time dependent rectilinear or rotational displacement. The type of vibration sensor applicable to our case is the accelerometer. An accelerometer is a device that measures relative acceleration. Accelerometers have multiple applications in industry and science. Highly sensitive accelerometers are components of inertial navigation systems for aircraft and missiles. Accelerometers are used to detect and monitor vibrations in rotating machinery. Accelerometers are used in smart mobile devices and digital cameras so that images on screens are always displayed upright. The principle of operation is based on the displacement of a small mass within the silicon integrated circuit. Consistent with Newton's second law of motion ($\vec{F} = m \cdot \vec{a}$), as an acceleration is applied to the device, a force develops which displaces the mass. Therefore, many events could trigger a false alarm including; a fence cabling that loose foliage, wind, and other random and irrelevant vibrations. Moreover, climate parameters such as temperature or humidity (though corrosion) can affect the sensor's output by altering sensors impedance. The major parameters that affect the detector are presented in Table 3.

Table 3. The major parameters that affect the detector

Parameter	Degree of influence
Wind speed	Significant
Temperature	Minor
Humidity	Minor
Barometric pressure	None
Acoustic noise	Minor
Material	None
Color – visual characteristics	None

3. EXPERIMENTAL SETUP AND EVALUATION

In order to be able to quantitatively assess the impact of the secondary parameters on the primary sensor measurements, an evaluation was designed and carried out. The evaluation of the hypothesis of the effect of the secondary parameters-sensors on the primary ones was held by placing a hypothetical intrusion detection wireless node in a closed controlled environment. Thus the setup included a single node installation in order to detect intrusion-related actions and secondary/environmental quantities that relate to the qualification of the primary sensors' measurements reliability. The primary sensors that were placed are: an ultrasonic sensor of a maximum 6 meters, an infrared PIR motion detector of a maximum 5 meter range and a vibration sensor. The vibration sensor was placed in a nearby point attached to a wire fence or other elastic material of the passage. The secondary sensors selected are those of temperature and wind speed. Moreover the secondary sensors were installed close to the primary ones in order to acquire environmental measurements on the spot. Fig. 4 and Fig. 5 give a graphical representation of the topology installed and the possible passage scenarios that were selected and executed while the vibration sensor is not included in the graphical representation because it was attached to the nearby fence simulating the last physical barrier of protection.

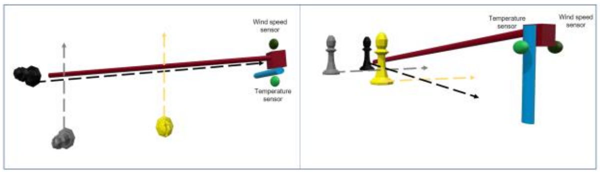


Fig. 4. Graphical representation of the sensor topology and the test scenario for the ultrasonic sensor.

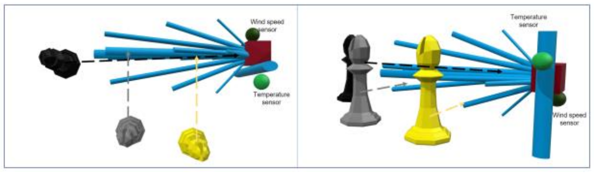
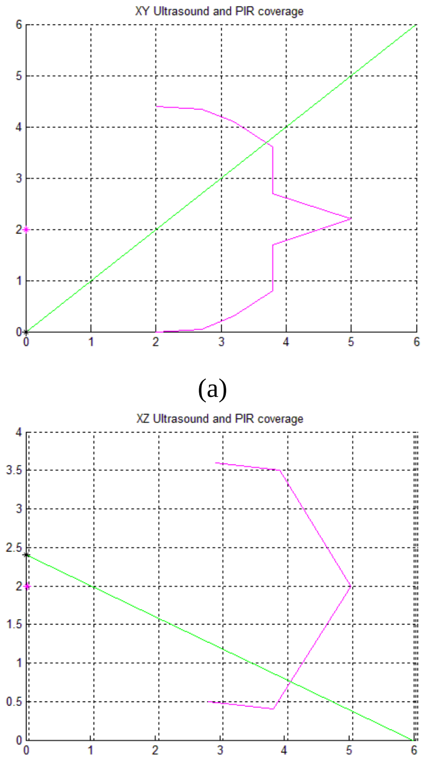


Fig. 5. Graphical representation of the sensor topology and the test scenario for the PIR sensor.

Two 2D sections of the coverage area of the sensors are shown in Fig. 6, The ultrasonic sensor was positioned inclined from top to bottom for best possible detection performance. The motion sensor was positioned at a level suitable for typical intrusion detection. According to this configuration three safety zones for intruder detection can be considered. The first zone, based on the ultrasound sensor, detects the existence of a potential intruder recognizing events from a point possibly outside of the protected area. The second zone, based on the PIR sensor, detects intruders the moment they enter the zone, while in most cases the signal goes hand in hand with the alarm from the ultrasonic sensor. The third zone, based on the vibration sensor, identifies intruders entering the area and producing vibrations. Obviously, the sensor zones and overall sensor placing can be rearranged; however the aforementioned setup is strongly proposed for open space systems considering the pros and cons of each sensor type.



(a)

(b)

Fig. 6. Ultrasound and PIR sensor coverage: (a) XY or top view; (b) XZ or side view.

Eleven different scenarios with and without the wind affection were executed in various temperature conditions covering a hypothetic time span of about three minutes each. It is worth noting that the first scenario that was executed each time was the zero-trigger scenario where no trigger was performed. Thus an evaluation of a *non-intrusion scenario* –normal state scenario– with stable, yet varying environmental conditions for all the primary sensors, was executed. Table 4 shows the experimental scenarios from which the data derived. In particular the table shows the sensors of the node that are activated each time and in relation to the environmental conditions (temperature and wind speed at the node location). The sensors of the node were initially triggered individually (Ultrasonic, Motion, Vibration) and then triggered in a combination of two, at least two and eventually three out of three sensors were triggered. More specifically, 11 different scenarios were performed in a varying temperature of 0° Celsius to 27° Celsius, with as well as without the presence of a constant wind speed of 3.4 m/s, always measured at the spot. Thus, in total, 22 scenarios were applied, and they were executed at 10 different temperature levels initially without the influence of wind speed and repeated at the same temperature levels as the wind effect. The summary of the data sets evaluation results of the scenarios is shown Table 5. In order to make the results more tangible to the reader, and to acquire useful outcomes, a series of graphs is shown in Fig. 8.

Overall, all combinations of primary and secondary sensors were tested, and the primary sensors were calibrated using a wide range of environmental measurements. The environmental conditions were recorded during every test cycle along with all the primary detection measurements. The sampling period was 200 msec (a frequency of 5 Hz). Thus, an experimental set of 3 minutes is expected to give a result of approximately 900 measurements. More specifically each scenario had the same 3 minutes overall duration and the same activations (one per 30 seconds) considering the number and the duration of each trigger. So, from the execution of each scenario, 6 alarm signals should arise from the correct sensor, and their duration should be at about 10sec; thus in total the alarm signal is expected to be at about 300 measurements. Considering the aforementioned, the output of the alarms from each scenario is expected to be of the form, or roughly the shape of Fig. 7. Additionally all possible noise sources of interference were removed from the environment and the humidity was maintained at steady levels.

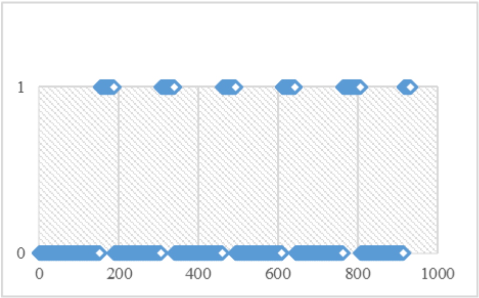


Fig. 7. A reference ideal alarm output of each scenario.

Table 3. The experiment scenarios.

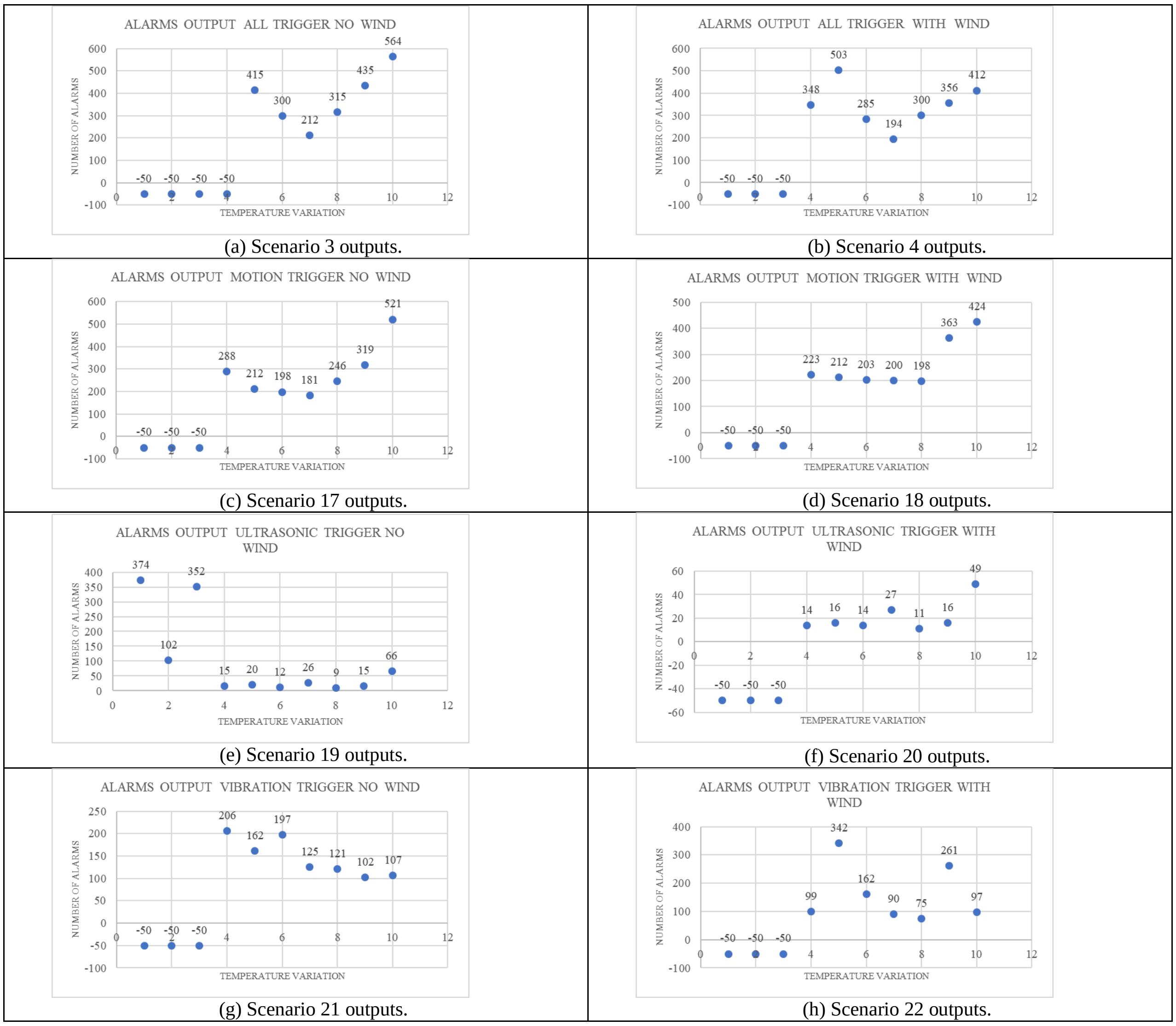
Scenario	Description	Primary sensor triggered			Secondary sensor triggered	
		Ultrasonic	PIR	Vibration	Temperature	Wind speed
1.	No Trigger	--	--	--	X	
2.	No Trigger	--	--	--	X	X
3.	Motion Ultrasonic & Vibration Trigger (MUV)	X	X	X	X	
4.	Motion Ultrasonic & Vibration Trigger (MUV)	X	X	X	X	X
5.	At Least Motion & Ultrasonic Trigger (LMU)	X	X		X	
6.	At Least Motion & Ultrasonic Trigger (LMU)	X	X		X	X
7.	At Least Motion & Vibration Trigger (LMV)		X	X	X	
8.	At Least Motion & Vibration Trigger (LMV)		X	X	X	X
9.	At Least Ultrasonic & Vibration Trigger (LUV)	X		X	X	
10.	At Least Ultrasonic & Vibration Trigger (LUV)	X		X	X	X
11.	Motion & Ultrasonic Trigger (MU)	X	X		X	
12.	Motion & Ultrasonic Trigger (MU)	X	X		X	X
13.	Motion & Vibration Trigger (MV)		X	X	X	
14.	Motion & Vibration Trigger (MV)		X	X	X	X
15.	Ultrasonic & Vibration Trigger (UV)	X		X	X	
16.	Ultrasonic & Vibration Trigger (UV)	X		X	X	X
17.	Motion Trigger (M)		X		X	
18.	Motion Trigger (M)		X		X	X
19.	Ultrasonic Trigger (U)	X			X	
20.	Ultrasonic Trigger (U)	X			X	X
21.	Vibration Trigger (V)			X	X	
22.	Vibration Trigger (V)			X	X	X

Table 4. Summarized table of the results of the experiments.

Triger type	Temperature level (°c)	Wind level (with or without wind)	Number of alarms	Number of dataset samples	Temperature level (°c)	Wind level (with or without wind)	Number of alarms	Number of dataset samples
NO TRIGGER	0-1	NO	0	1008	21-22	NO	212	922
U	0-1	NO	374	982	21-22	NO	463	930
NO TRIGGER	6-7	NO	0	981	21-22	NO	448	926
U	6-7	NO	102	761	21-22	NO	305	917
NO TRIGGER	11-12	NO	0	978	21-22	NO	234	919
MUV	11-12	NO	352	1021	21-22	NO	236	922
LMU	14-15	NO	342	940	21-22	NO	181	918
LMV	14-15	NO	326	936	21-22	NO	28	920
LVU	14-15	NO	348	940	21-22	NO	26	918
MU	14-15	NO	312	932	21-22	NO	128	921
MV	14-15	NO	391	935	21-22	NO	125	919
M	14-15	NO	288	938	21-22	YES	194	914
NO TRIGGER	14-15	NO	37	932	21-22	YES	147	916
U	14-15	NO	15	935	21-22	YES	204	888
VU	14-15	NO	193	940	21-22	YES	214	916
V	14-15	NO	206	943	21-22	YES	249	918
MUV	14-15	YES	348	937	21-22	YES	220	906
LMU	14-15	YES	352	935	21-22	YES	200	918
LMV	14-15	YES	307	938	21-22	YES	23	918
LVU	14-15	YES	361	938	21-22	YES	27	920
MU	14-15	YES	325	937	21-22	YES	124	924
MV	14-15	YES	357	938	21-22	YES	90	920
M	14-15	YES	223	930	22-23	NO	315	940
NO TRIGGER	14-15	YES	10	933	22-23	NO	263	894

U	14-15	YES	14	940	22-23	NO	265	919
VU	14-15	YES	96	939	22-23	NO	383	948
V	14-15	YES	99	938	22-23	NO	348	946
MUV	16-17	NO	415	944	22-23	NO	275	939
LMU	16-17	NO	263	939	22-23	NO	246	945
LMV	16-17	NO	382	938	22-23	NO	0	931
LVU	16-17	NO	434	945	22-23	NO	9	943
MU	16-17	NO	307	939	22-23	NO	146	940
MV	16-17	NO	271	938	22-23	NO	121	932
M	16-17	NO	212	897	22-23	YES	300	950
NO TRIGGER	16-17	NO	17	922	22-23	YES	252	940
U	16-17	NO	20	941	22-23	YES	247	946
VU	16-17	NO	138	987	22-23	YES	279	948
V	16-17	NO	162	931	22-23	YES	241	933
MUV	16-17	YES	503	950	22-23	YES	253	945
LMU	16-17	YES	507	951	22-23	YES	198	930
LMV	16-17	YES	481	931	22-23	YES	15	928
LVU	16-17	YES	514	938	22-23	YES	11	940
MU	16-17	YES	266	931	22-23	YES	89	947
MV	16-17	YES	483	935	22-23	YES	75	927
M	16-17	YES	212	931	23-24	NO	435	944
NO TRIGGER	16-17	YES	346	918	23-24	NO	460	922
U	16-17	YES	16	941	23-24	NO	488	950
VU	16-17	YES	368	936	23-24	NO	357	939
V	16-17	YES	342	930	23-24	NO	329	938
MUV	19-20	NO	300	935	23-24	NO	342	938
LMU	19-20	NO	251	936	23-24	NO	319	938
LMV	19-20	NO	286	933	23-24	NO	54	920
LVU	19-20	NO	310	934	23-24	NO	59	941
MU	19-20	NO	238	930	23-24	NO	15	933
MV	19-20	NO	278	934	23-24	NO	102	939
M	19-20	NO	198	933	23-24	YES	356	939
NO TRIGGER	19-20	NO	0	919	23-24	YES	369	936
U	19-20	NO	12	928	23-24	YES	389	938
VU	19-20	NO	188	934	23-24	YES	451	951
V	19-20	NO	197	932	23-24	YES	387	931
MUV	19-20	YES	285	936	23-24	YES	370	941
LMU	19-20	YES	243	929	23-24	YES	363	939
LMV	19-20	YES	287	932	23-24	YES	392	345
LVU	19-20	YES	280	940	23-24	YES	16	944
MU	19-20	YES	236	933	23-24	YES	104	951
MV	19-20	YES	266	917	23-24	YES	261	932
M	19-20	YES	203	928	26-27	NO	564	959
NO TRIGGER	19-20	YES	7	929	26-27	NO	455	940
U	19-20	YES	14	933	26-27	NO	406	961
VU	19-20	YES	167	932	26-27	NO	317	934
V	19-20	YES	162	927	26-27	NO	440	926
MUV					26-27	NO		
LMU					26-27	NO	521	941
LMV					26-27	NO	253	922
LVU					26-27	NO	66	888
MU					26-27	NO	121	934
MV					26-27	NO	107	951
NO TRIGGER					26-27	YES	412	937
U					26-27	YES	643	939
VU					26-27	YES	426	935
V					26-27	YES	519	945
MUV					26-27	YES	519	939
LMU					26-27	YES	277	942
LMV					26-27	YES	424	936

LVU					26-27	YES	160	925
MU					26-27	YES	49	936
MV					26-27	YES	156	936
M					26-27	YES	97	941



(a) Scenario 3 outputs. (b) Scenario 4 outputs.

(c) Scenario 17 outputs. (d) Scenario 18 outputs.

(e) Scenario 19 outputs. (f) Scenario 20 outputs.

(g) Scenario 21 outputs. (h) Scenario 22 outputs.

Fig. 8. Indicative graphs of scenario measurements.

As shown by the set of measurements and the graphs, the influence of the secondary parameters is evident. Noting here that the value of -50 in graphs indicates that the measurements of the data set were not accepted due to execution errors. Despite of these random and other errors that we accept may affect the results of our experiments, some conclusions can be safely extracted from the whole project.

First of all the secondary variables affect the measurements of the primary sensors in a way that we did not take into consideration at the beginning of the project. In particular, after a thorough review of the measurements and spikes one by one, the sensing range of the sensors- in particular the ultrasound sensor- varies in terms of temperature. More precisely the range reduces for about 30% when the environmental temperature drops at 0 degrees while a 10% decrease of the range appears in all of the measurements taken below 10 degrees. This deviation gradually increases as the temperature approaches zero. The result of this is the unsuccessful coverage of the field by the sensor and urges the need to use denser nodes of ultrasonic or use alternative sensors as well. Apparently if this parameter (temperature) is not taken into account in the decision-making process, false alarms will definitely occur. In terms of the wind parameter the measurements showed a deviation up to 5%. This means that there is a probable drift of the measurements according to the direction of the air as expected. In addition, after a closer look at the number of events in the case of the ultrasound sensor we will find out that in most of the scenarios, the number of alarm measurements are much lower than expected. At this point, it is worth noting that the sensor eventually detects the potential attacker (thus detecting six possible invasions over a three-minute scenario) without giving the expected number of measurements at about 300 but much less, about 20-60. Thus, a great dependence of the sensor response on the invader's clothes appeared. Apparently in some cases a number of experiments were repeated due to the non-detection of the intruder in normal environmental conditions due to their clothing.

In the case of infrared detector we observed that the sensor in general presents a constant yield with very small deviations of less than 1%. However as the temperature rose above 20 degrees, more and more false alarms were recorded with the deviation in the expected number of alarms to eventually exceed 70%. This in practice means that more than 2 out of 3 sensor measurements as the temperature rises above 25 degrees do not represent actual intruder detection. As far as the wind affection on the infrared sensor is concerned, it is negligible and the whole operation of the sensor is robust. What is interesting though is the affection of the wind in an open space environment. In this case the false alarms increased in the presence of wind. This fact, however, is due to external parameters such as the movement of light objects and their detection by the sensor, and not due to a faulty sensor operation.

In the case of the vibration sensor, it is unaffected when the temperature varies. In contrast, in the case of wind, the sensor experienced a slower dampening of its oscillation after an alarm than under normal environmental conditions. This could lead to an erroneous estimation of the number of invaders. In more detail in the case of wind, the sensor occurred slightly more alarm events than in the cases of no wind, especially when the scenario was about a combination of alarms of two or more sensors. This fact and the behaviour of the vibration sensor is because of the natural activation of the sensor due to the wind.

4. CONCLUSIONS

As the security systems are becoming more and more complex to detect the intruder and to set early warnings to the users, in the current work, an investigation of the reasons that affect primary sensor's accuracy is held. Under this scope, if we can accurately determine the confidence level of the measurements, then we can define the outcome of the decision-making process in an easier way. A decision-making algorithm of this theory -the WSNmod was implemented in a previous work and showed encouraging results. In this study the parameters that affect the primary variables were put under the microscope. For this purpose we developed a series of scenarios in which we alternate each time a secondary variable with respect to the primary one and we study their dependence. The results showed a strong correlation of the environmental parameters in the measurement, and the argument that each system is in direct relation to the change of the secondary variables was strengthened. Currently we are working on various setups and simulations, including other sets of secondary sensors, different environmental and target configurations of the system and other intrusion scenarios, to identify the extent to which the secondary parameters can affect the primary ones along with the WSNmod method and its benefits to the security applications.

REFERENCES

[1] JCGM 200:2012 (JCGM 200:2008 with minor corrections), *International Vocabulary of Metrology – Basic and General Concepts and Associated Terms* (VIM 3rd edition).

[2] JCGM 100:2008, (GUM 1995 with minor corrections), *Evaluation of measurement data – Guide to the expression of uncertainty in measurement*.

[3] Course: ME 458 "**Engineering Noise Control**," *Fall 2000, Instructor: J. S. Lamancusa, Lecture*: 1:25 - 2:15 M W 217 Hammond, Chapter 10: Outdoor sound propagation, pp. 4-7.

[4] Gerard Honey, "**Intruder Alarm Detection Devices**," *Intruder Alarms (Second Edition), edited by Gerard Honey, Newnes*, Oxford, pp. 48-94, 2003.

[5] J. Lopez, R. Rios, F. Bao, G. Wang, "**Evolving privacy: From Sensors to the Internet of Things**," *In Future Generation Computer Systems*, Vol. 75, pp. 46-57, 2017.

[6] Gupta, D. K., "**A Review on Wireless Sensor Networks, Network and Complex Systems**." *Network and Complex Systems*, 3(1), pp. 18-23, 2013.

[7] C. C. Aggarwal, A. Bar-Noy, S. Shamoun, "**On Sensor Selection in Linked Information Networks**," *In Computer Networks*, Vol. 126, pp 100-113, 2017.

[8] S.-L. Chua, L. K. Foo, "**Sensor Selection in Smart Homes**," *In Procedia Computer Science*, Vol. 69, pp 116-124, 2015.

[9] Va. Bapat, P. Kale, V. Shinde, N. Deshpande, A. Shaligram, "**WSN Application for Crop Protection to Divert Animal Intrusions in the Agricultural Land**," *In Computers and Electronics in Agriculture*, Vol. 133, pp 88-96, 2017.

[10] Honey, G., "**Intruder Alarm Detection Devices**," *In: Intruder Alarms. Newnes: Oxford*, pp. 48-94, 2003.

[11] Gopi K. and Sivaprakash S., "**Cluster Based Intrusion Detection System for Wireless Sensor**

Networks," *International Journal of Innovative Research in Computer and Communication Engineering*, 2(1), pp. 993-999, 2014.

[12] Li, Y.Y. and Parker, L.E., "**Intruder Detection using A Wireless Sensor Network with an Intelligent Mobile Robot Response**," *Huntsville, AL, Southeastcon*, 2008. IEEE, pp. 37-42, 2008.

[13] Bokareva, T., Hu, W., Kanhere, S., Ristic, B., Gordon, N., Bessell, T., Rutten, M., and Jha, S., "**Wireless Sensor Networks for Battlefield Surveillance**," *s.l., Land Warfare Conference*, 2006.

[14] Khan, B.A., Sharif, M., Raza, M., Umer, T., Hussain, K. and Khan, A.U., "**An Approach for Surveillance Using Wireless Sensor Networks (WSN)**," *Journal of Information & Communication Technology*, 1(2), pp. 35-42, 2007.

[15] Quaritsch, M., Kruggl, K., Wischounig-Strucl, D., Bhattacharya, S., Shah, M. and Rinner, B., "**Networked UAVs as Aerial Sensor Network for Disaster Management Applications**," *Elektrotechnik & Informationstechnik*, 127(3), pp. 56-63, 2010.

[16] B. Dong, J. Hao, V. Paulose, "**Armored-cable-based FBG Security Fence for Perimeter Intrusion Detection with Higher Performance**," *In Sensors and Actuators A: Physical*, Vol 180, pp. 15-18, 2012.

[17] T. Coelho Moreira, "**The Electronic Control of the Employer in Portugal**," *LLI*, Vol. 2, No. 1, 2016.

[18] T. Coelho Moreira, "**Every Breath You Take, Every Move You Make: Cybersurveillance in the Workplace and the Worker's Privacy**," *in Masaryk University Journal of Law and Technology*, Vol. 7, No. 1, 2013.

[19] Charalampidou, Maria, George Pavlidis, and Spyridon G. Mouroutsos, "**A Novel Modular Wireless Sensor Networks Approach for Security Applications**," *International Journal of Security and Networks 12.1*: pp. 40-50, 2017.

[20] Akyildiz, I., Su, W., Sankarasubraniam, Y. and Cayirci, E., "**A Survey on Sensor Networks**," *IEEE Communications Magazine*, Vol. 40, No. 8, pp.102–114, 2002.

[21] Gopi K, Sivaprakash S, **Cluster Based Intrusion Detection System for Wireless Sensor Networks**, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, Special Issue 1, 2014.

[22] Li, Y.Y. and Parker, L.E. "**Intruder Detection using a Wireless Sensor Network with an Intelligent Mobile Robot Response,**" *Southeastcon, IEEE, Huntsville, AL*, pp. 37–42, 2008.

[23] Bokareva, T., Hu, W., Kanhere, S., Ristic, B., Gordon, N., Bessell, T., Rutten, M. and Jha, S. **"Wireless Sensor Networks for Battlefield Surveillance,"** *Land Warfare Conference*, 2006.

[24] Khan, B.A., Sharif, M., Raza, M., Umer, T., Hussain, K. and Khan, A.U. **"An Approach for Surveillance Using Wireless Sensor Networks (WSN),"** *Journal of Information and Communication Technology*, Vol. 1, No. 2, pp.35–42., 2007.

[25] Quaritsch, M., Kruggl, K., Wischounig-Strucl, D., Bhattacharya, S., Shah, M. and Rinner, B. **"Networked UAVs as Aerial Sensor Network for Disaster Management Applications,"** *Elektrotechnik and Informationstechnik*, Vol. 127, No. 3, pp.56–63, 2010.

[26] Honey, G. **"Intruder Alarm Detection Devices,"** *Intruder Alarms. Newnes, Oxford*, pp.48–94, 2003.

[27] Carullo, A. and Parvis, M. **"An Ultrasonic Sensor for Distance Measurement in Automotive Applications,"** *Sensors Journal*, Vol. 1, No. 2, p.143, 2001.

[28] Moffat, R.J. **"Describing the Uncertainties in Experimental Results,"** *Experimental Thermal and Fluid Science*, Vol. 1, No. 1, pp.3–17, 1998

[29] Everest, F.A and Pohlmann, K. **"Absorption,"** *Master Handbook of Acoustics, McGraw Hill*, pp.180, 181, 2009.

[30] Northrop, R. **"Applications of Sensors to Physical Measurements,"** *Introduction to Instrumentation and Measurements, Taylor and Francis*, pp.343–500, 2005.

[31] H. E. a. L. N. B. Bass, **"Ultrasonic Background Noise in Industrial Environments,"** *The Journal of the Acoustical Society of America*, Vol. 78, No. 6: 2013-2016, 1985.

[32] K. Irgan, C. Ünsalan, S. Baydere, "**Low-cost Prioritization of Image Blocks in Wireless Sensor Networks for Border Surveillance,"** *In Journal of Network and Computer Applications*, Vol. 38, pp. 54-64, 2014.

[33] M. Thiel, G. Flachenecker, W. Schade, C. Gorecki, A. Thoma, R. Rathje, **"Planar Ultra-Thin Glass Seals with Optical Fiber Interface for Monitoring Tamper Attacks on Security Eminent Components,"** *In Optics and Lasers in Engineering*, Vol. 98, pp. 89-98, 2017.

[34] L. Gu, Kaishun W., Zhongwen G., H. Luo, L. M. Ni, **"Ship Detection with Wireless Sensor Networks",** *IEEE Transactions on Parallel & Distributed Systems*, Vol. 23, pp. 1336-1343, July 2012.

[35] L. Gu et al., **"Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments,"** *Proc. Third Int'l Conf. Embedded Networked Sensor Systems (SenSys '05)*, pp. 205-217, 2005.

[36] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, M. Miyashita, "**A Line in the sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking**," *In Computer Networks*, Vol. 46, Issue 5, pp. 605-634, 2004.

[37] M. F Duarte, Y. H. Hu, **"Vehicle Classification in Distributed Sensor Networks,"** *In Journal of Parallel and Distributed Computing*, Vol. 64, Issue 7, pp. 826-838, 2004.

[38] M. Fayyaz, **“Classification of Object Tracking Techniques in Wireless Sensor Networks Wireless Sensor Network,**” pp. 121-124, 2011.

[39] E. F. Nakamura, A. A. F. Loureiro, and A. C. Frery, **“Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications,”** *ACM Computing Surveys*, Vol. 39, No. 3, Article 9, Publication date: August 2007

[40] F. Viani, L. Lizzi, P. Rocca, M. Benedetti, M. Donelli and A. Massa, **“Object Tracking Through RSSI Measurements in Wireless Sensor Networks,”** *in Electronics Letters*, Vol. 44, No. 10, pp. 653-654, May 8 2008.

[41] G. Blumrosen, B. Hod, T. Anker, D. Dolev, and B.s Rubinsky. 2013. “**Enhancing RSSI-based Tracking Accuracy in Wireless Sensor Networks,”** *ACM Trans. Sen. Netw. 9, 3, Article 29*, 28 pages, 2013.

[42] I. Arfaoui, N. Boudriga and K. Trimche, **“Resilience of Thick-line WSN based Surveillance Systems under Irregular Crossings,”** *22nd Asia-Pacific Conference on Communications (APCC),* Yogyakarta, pp. 307-314, 2016.

[43] S. Allali, H. Menouar and M. Benchaiba, **“Grid Architecture for Lightweight WSN-based Area Monitoring and Alerts Dissemination,”** *International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet*, pp. 1-7, 2016.

[44] P. Rothenpieler, D. Kruger, D. Pfisterer, S. FischerInternational, FleGSens, **“Secure Area Monitoring using Wireless Sensor Networks,”** *Science Index, Electronics and Communication Engineering*, Vol:3, No:8, 2009.