A novel modular Wireless Sensor Networks approach for security applications

Maria Charalampidou

Department of Electrical and Computer Engineering
Democritus University of Thrace
Xanthi, 67-100, Greece
Email: macharal@ee.duth.gr

George Pavlidis

Institute for Language and Speech Processing
Institute / 'Athena' Research Center,
Xanthi, 67-100, Greece
Email: gpavlid@ceti.gr

Spyridon Mouroutsos

Department of Electrical and Computer Engineering
Democritus University of Thrace
Xanthi, 67-100, Greece
Email: sgmour@ duth.gr

Abstract: Nowadays surveillance systems are becoming increasingly complex by combining a variety of sensors and systems in order to deliver more accurate decisions. This is due to the fact that the development of a simple and yet efficient algorithm for intruder detection is of a high interest both to academia and the market. This paper presents a novel approach towards the development of a sophisticated decision making system for accurate intrusion detection. The method is based on three key elements: the assessment of the certainty of the inputs, the quantization of the inputs using the three-valued logic and the time-based filtering of the sequence of alarms. The algorithm was applied to a Wireless Sensor Network (WSN) that is used for intruder detection of an open area. The overall setup, the theoretical analysis and preliminary evaluation results of the proposed method show that this is an interesting and rather promising approach.

Keywords: Wireless Sensor Networks (WSN); three valued logic; security; intruder detection; decision making; sensors; sensor networks; sensor nodes; policies; security applications; modular approach; modular; surveillance systems; novel approach; intrusion detection.

Biographical notes: Maria Charalampidou is a PhD candidate at the Electrical and Computer Engineering of the Democritus University of Thrace (DUTh). She received her diploma (2010) and master degree (2012) from the same university in power electronics and mechatronics, respectively. Her current field of research is in the field of wireless sensor networks and decision making algorithms. She is also interested in sensor measurements, robotics and mathematics.

Dr. Pavlidis received his PhD in Electrical Engineering, earning the distinction of the Ericsson Awards of Excellence in Telecommunications. He has been working for numerous R&D projects with emphasis on multimedia systems in culture and education. In 2002 he joined the ‘Athena’ Research Center, where he is now a research director, head of the Multimedia Research Group and head of research at ‘Clepsydra’ Cultural Heritage Digitization Center. His research interests involve 2D/3D imaging, CBIR, multimedia technologies, human-computer interaction, intelligent user interfaces, multi-sensory environments and ambient intelligence, 3D digitization and reconstruction, 3D-GIS and mixed/augmented/virtual reality. Dr. Pavlidis is a member of the Technical Chamber of Greece, of the Hellenic Researchers' Association, a senior member of the IEEE, and a founding member of the ‘Athena’ Research Center’s Researchers’ Association.

Prof. Spyridon Mouroutsos is Associate Professor and Director of the Lab of Special Engineering at the Electrical and Computer Engineering Department of Democritus University of Thrace (DUTh). He has been a visiting Prof. at the Dept. of Manufacturing Engineering of Salford University, UK and an adjunct Profes-sor at the Depts. of Environmental Engineering, Production and Management Engineering, Architectural Engineering of DUTh, having taught Automation of Energy Systems, Measurement Systems Technology, CAD Systems, Standards and Standardization, Technical Drawing and Systems Design. He has been an expert at FP7-NMP. Prof. Mouroutsos holds a Diploma in Electrical Engineering from DUTh (1981) and a Ph.D. from the same University (1986). His research has been funded by EU and National sources. He has been involved for more than 20 years in numerous R&D projects in areas such as Mechatronics and Systems Automation, Wireless Sensing, Educational Technology and Applied Mobile

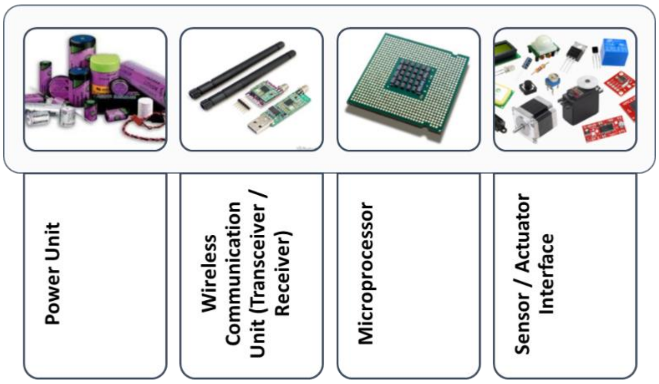
Computing. He has been a Referee, Committee Member or Member of the Editorial Board for numerous International Scientific and Technical Journals and Conferences, and has acted as evaluator for National and EU research grant applications. He has 87 publications in refereed journals, technical proceedings and edited books. He is a member of the Technical Chamber of Greece.

1 Introduction

Over the past decades, Wireless Sensor Networks (WSNs) have been tested in numerous scenarios and applications consolidating their position as an active field of research and development worldwide. Nowadays, WSN applications can be found in industrial control (Xiao et al., 2016), environmental monitoring, wild life monitoring (Mainwaring et al., 2002), (Dessart and Hunel, 2014), even in healthcare (Dimaet et al.,2014) and military applications (Qian at al., 2012). The process of observing a real phenomenon and evaluating its behavior is known as event detection in WSNs (Wittenburg et al., 2010).

The WSNs consist of sensor nodes. The nodes combine sensor technology with the computational power of microcontrollers and a wireless communication interface in a low power scheme (Akyildiz et al., 2002). These nodes actually offer an integrated system of distributed computing power (and, in some cases, storage space). Moreover they enable networking and monitoring of various measured entities (Figure 1).

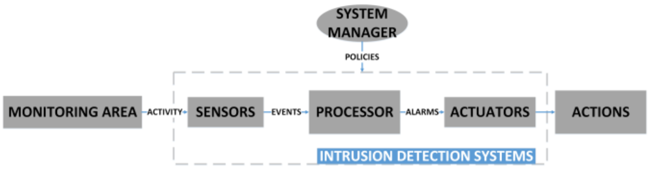
Figure 1 Sensor node architecture (Gupta, 2013)


Power Unit
Wireless Communication Unit (Transceiver / Receiver)
Microprocessor
Sensor / Actuator Interface

A WSN application scenario of particular interest is in the surveillance and security monitoring of an open area. Generally, accessibility to an area involves any possible presence, either authorized or of an intruding nature. It is, therefore, necessary to be able to provide early warnings in the event of unauthorized presence. In cases where high safety requirements are necessitated, surveillance of the area and detection of potential intruders are of particular importance. In these cases, not only is there a provision of preventing theft, vandalism or any other violation, but also a sense of security to people who are the legitimate users. On the other hand, false alarms (either false positive or false negative) reduce the performance of the security system and to some extent the sense of reliability; therefore, modern security systems should take seriously into account the false-alarm factor. However, control algorithms especially for WSNs and other combined systems are usually complex and require high computational power and memory when they are going through the simulation and laboratory applications to real life dimensions (Phung et al., 2007).

The general schematic model of an intrusion detection system is shown in Figure 2. The scheme is based on the one designed from the Intrusion Detection Working Group (IDWG) of the Internet Engineering Task Force (IETF). The model contains all the important components of an intrusion detection system (Gopi and Sivaprakash, 2014). The square boxes represent software or hardware components, while the ellipses represent human roles and policies.

Figure 2 Schematic model of an intrusion detection system.



An intrusion detection system observes the activity of the MONITORED AREA. The data are captured and synthesized as alarm events by the SENSORS component of the intrusion detection system, or the sensor node in case of a WSN. In most of the cases (commercial or scientific) the system reads several sensors simultaneously and feeds events to the PROCESSOR, avoiding a simplistic single data-source acquisition and analysis. These events are processed by a PROCESSOR, which decides whether an event is malicious and should trigger an alarm or not. The decision depends both on an automated analysis technique and on the configuration imposed by the SYSTEM MANAGER.

This MANAGER prescribes what could be in a word described as the policy of the system that includes heuristics and rules about the conditions to trigger alerts, the information to be sent to the MANAGER and the appropriate responses under various conditions.The PROCESSOR uses the policy imposed by the MANAGER and produces the appropriate responses (alarms) to one or several ACTUATORS to proceed with the appropriate ACTIONS.

Traditionally, solutions to the problem of security and intrusion detection have centered on the use of human security, which is labor-intensive and expensive, and on the use of video cameras and image processing (see (Ahmedali and Clark, 2006) for example). In general, there are many techniques used for the surveillance of an open area. Mainly, they are using:

1. Surveillance cameras, as shown in (Pasqualetti et al., 2013), where a network of identical pan-tilt-zoom (PTZ) cameras used for video surveillance and researchers focus on development of distributed and autonomous surveillance strategies for the detection of moving intruders.

2. Biometrics, like in (Hanirex et al., 2013) (Bai et al., 2013), where iris data are being used to improve the security in an intrusion detection system and detect the system's security state.

3. Surveillance sensors for deployment of embedded surveillance systems by using time-variation ultrasonic coding signals with multiple pyroelectric infrared sensors (PIR) to detect an intruder in a home or a storehouse (Bai et al., 2013). Other sensor examples include vibration sensors (Bokareva et al., 2006) where researchers developed a dual leaky coaxial cable (DLCX) for an intruder detection sensor based on microwave technologies. The sensor consists of a sensor unit and two leaky coaxial cables (LCXs) working as transmitting (Tx) and receiving (Rx) antennas respectively. It can detect an intruder that penetrates a surveillance area formed around the LCXs.

4. Microphones, as cited in (Intani and Orachon, 2013), where the overall system takes advantage of sound along with image processing to detect an intruder, then notify and sent a signal to the system administrator when an event occurs.

Beyond these traditional techniques, recent work has explored the idea of using a team of autonomous (or semi-autonomous) agents to patrol the area, potentially reducing costs and increasing reliability (Agmon et al., 2008). However this planning task is difficult: organizing the team of agents to best patrol the area is computationally expensive, even for relatively small problem instances (While et al., 2013).

Meanwhile WSN's main objective has come to be the reliable interpretation of real world monitoring for event identification and easy to use user services and applications. It is therefore the most effective embodiment of ambient intelligence and ubiquitous computing. While many WSN efforts have already been in the market and tested in real applications successfully the WSN market is expected to grow up to $1.8 billion by 2024 (Harrop and Das, 2015). At the same time the need to strengthen the feeling of security against any intruder who may threaten people or equipment regardless of the installation location is becoming first priority. Thus, WSNs is a promising solution to surveillance and security applications. For example in (Bellazreg et al., 2013a) and in (Bellazreg et al., 2013b) the researchers engaged WSNs for border surveillance.

Amongst the latest security WSN applications that have been developed, there are the collaborative WSN and Robot security systems, which are equipped with appropriate sensors and deployed in a variety of environments and topologies. For example, in (Li et al., 2008), the authors present an indoor intruder detection system that uses a WSN and a ground mobile robot. Upon the detection of an intruder, the mobile robot travels to the position where the intruder is detected for further investigation. Another example is given in (Lin et al., 2008), where an intruder detection system which consists of zigbee sensor modules that detect intruders and 'abnormal' conditions. The sensor nodes transmit intrusion alarms to the monitoring center. If an intruder is detected, the robot moves to that location autonomously and transmits images to remote mobile devices of security guards, in order to determine and respond to the situation in real time. In addition in (Cho et al., 2006) researchers introduce a WSN and ground mobile robots collaboration for indoors navigation at a construction site (warehouses, office buildings, manufacturing facilities) providing both security and safety. Another home security application is cited in (Tian and Geng, 2009) where a WSN and a ground robot household security system is proposed. The system is composed of the robot node and the sensor nodes of the WSN for monitoring temperature, humidity, gas leaks, fire and housebreaking. The robot node undertakes the task of collecting and processing sensor data from the WSN, but also acts as the interface of the system with users.

In any case, false-positive and false-negative intrusion identifications can be regarded as estimators about the surveillance systems' reliability and robustness. False positives are mainly produced by an incorrect characterization of the vulnerability. This erroneous characterization often occurs when the system cannot sufficient distinguish between the normal conditions and an actual malicious attempt. It is thus important to analyze alarms with prior knowledge about the monitored area, to ensure proper evaluation of the severity of the events. At the same time, false negatives mostly occur on new attacks. In this case no pattern or signature is associated to this newly encountered attack, and as a result, an attack happens without the system's reaction at any level. Usually, the systems are trained to recognize sample event streams containing modeled or real scenario attacks, in order to ensure that they can detect the intrusions of similar event streams. Obviously, this approach cannot guarantee the effective operation of the system in any case. Note that misuse-detection techniques are usually less-well suited for the detection of internal malicious activity. And that's because, most commonly, registered users have access and privileges on the system that are able to carry out the most malicious activities bypassing known intrusion detection scenarios.

In a security system there are a number of available inputs. The inputs derived from sensors, which are divided into three main categories depending on the stimuli they receive. The first category includes acoustic/sound/vibration sensors such as geophones (Katsarakis et al., 2015), (Katsarakis et al., 2014) (Honey, 2003). The second category includes presence/proximity sensors or radars such as passive infrared, ultrasonic, microwave or even fence (i.e. tense, spring and other mass stimuli) sensor (Honey, 2003), (Ramon et al., 2015), (Saipulla et al., 2010), (Tsujita et al., 2013), (Jisha et al., 2010) The third category is based on the intruder movement and including speed and direction of the subject (Suthaharan and Bandari, 2012). Another type of sensor, in particular a multi sensor can be considered a combination of cameras and microphones (Bouchard, 2014). Worth noting here that cameras are indeed the type of sensors that offers the greatest information expressivity and can enable to extract many spatial features. However, cameras and microphones are considered highly invasive and video processing data is of a high complex. Furthermore, people tend to reject the idea of using them in home or work environments (Demeris et al., 2008). In addition some researchers have drawn attention toward the exploitation of the Microsoft Kinect to replace cameras (Stone and Skubic, 2011), but it is still not easy to process the output data. An analytical and introspective literature review for each of the aforementioned sensors (Carulloand and Parvis, 2001), (Moffat, 1988), (Honey, 2003), (Everest and Pohlmann, 2009) (Northrop, 2005) reveals a need for the study of other sensors (such as the ones that measure environmental quantities) that determine how the quality of measurements of the sensors is affected by indirect effects. Of paramount importance especially in outdoors applications are the environmental quantities, since "bad" weather conditions have a negative impact on outdoors measurements. However environmental conditions are not the only quantities to consider. For example, an ultrasonic sensor may be affected by reflecting surfaces of the environment or even the type of the surface of the detected object (felt, wool, or foam rubber) (Honey, 2003), (Everest and Pohlmann, 2009). Of a particular interest one may note the case of an intruder being covered by a material with very low reflectance (such as a vantablack material (Gent, 2014). It is apparent that the overall uncertainties assigned to each measurement must include the measuring system uncertainties plus all those associated with system disturbances, system-sensor interactions, and the idealizations invoked in the data interpretation equations (Moffat, 1988).

While all types of elegant mathematics (neural networks, genetic algorithms, fuzzy logic, chaos) have already been applied in various WSN data mining algorithms and applications, this paper proposes an alternative approach based on the three-valued logic and a two-step processing. Specifically, the three-valued logic is an extension of the classical two-valued Aristotle's syllogistic (or what is called today the Boolean logic), and allows the output of a statement to deal with three situations, usually including a representation of the uncertainty. In general, there are a number of well-known three-valued logics, like Łukasiewicz’s (Borowski, 1970) or Kleene’s (Kleene, 1952), and Sobociński’s (Sobociński , 1952). According to Łukasiewicz the third value has the meaning of possible. In addition Kleene (and afterwards Nelson (Nelson, 1940)) via a logical formula interpret the third value either as undefined (i.e. value out of the definition domain) or unknown (i.e. value that cannot be computed). Moreover, Sobociński proposed the third value to adopt the idea of irrelevant. In this way, a clear distinction between fuzzy logic and three-valued logic has been accomplished. Thus, fuzzy logic can be described as the method of classification that is based to a set of both truth and relevant values and a weight factor of truth. Another aspect of what the third value represents is given by the meaning of inconsistent. According to this definition, the value is both true and false and this is why some approaches, such as Priest’s (Priest, 1979) and Belnap’s (Belnap, 1977) imply average truth values by using the square of opposition (Parry and Haker, 1990).

Using this logic along with data and decision processing, we propose the use of a WSN that consists of fixed and mobile nodes in a modular and parametric form, the WSNmod (WSN-modular), in order to surveillance an open area of interest. The system setup, the decision-making algorithm, and evaluation results are presented in detail in the following paragraphs.

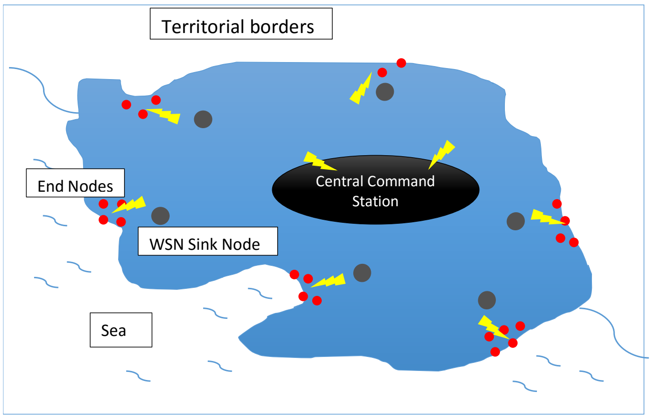
2 Description of the WSNmod

The proposed security system is a *decentralized modular system*, which consists of scattered fixed and mobile nodes forming a hierarchical modular WSN that is placed in an open area that can hypothetically include territorial and sea borders (Figure 3). The WSN consists of several *end nodes* (red-colored), which are placed in possible intruder passages, and they are equipped with sensors. Their main role is to monitor the passage. The network also consists of *sink nodes* (grey-colored) as routers, in order to transmit the signals to a *central command station* (black-colored), which acts as a coordinator. Every node can transmit an alarm to the central station to declare a possible intruder event. In addition, preliminary decisions are being made in the nodes and then forwarded to the central station to enable actuators. The overall supervision is accomplished by the central station, where all the alarms can be visualized and processed.

The proposed system, *WSNmod*, is shown in Figure 4. In overall the system estimates a risk factor (the *Target*). The risk factor indicates the probability of an intruder to be in the coverage area of the security system. Specifically, the *Target* can take any of the three values: *False (0), True (1), and Stand-by (-1).* A False (0) value indicates that it is unlikely that there is an intruder in the area and defines the *"Normal”* state. A True (1) value indicates that it is likely there is an intruder in the area, and defines the *"Alarm"* state. A Stand-by (-1) value declares that the system cannot conclude about a state with sufficient confidence, and defines the *"Unspecified”*. Thus, an alarm state, indicates that there is an intruder within the area is high likelihood. Additionally, the system activates the alarm indicators and react in order to restrain the intruder according to a pre-defined set of rules that form a *policy*. The risk factor is estimated by taking into account the measurements of the WSN that are classified into risk levels too. The assessment of the overall level of risk detected by the system depends on two basic key dynamics: the risk level that is assessed by the fusion of the sensor data and the frequency of the detected alarms.

Regarding the sensor fusion, it must be noted that the sensors in the WSN nodes can be divided into two categories. The first category are the sensors that provide direct information about an intrusion, and which are called *primary sensors*. The second category are 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 from the primary sensors. The measurements taken by the primary sensors are quantized into three levels: False (0), True (1), and Stand-by (-1). A False (0) value indicates that the measurements of the primary sensor does not indicate the presence of an intruder and defines the *"Sensor Normal"* state. A True (1) value indicates that the measurements of the primary sensor indicate the presence of an intruder and define the *"Sensor Alarm"* state. A Stand-by (-1) value indicates that the measurements of the primary sensor indicate that the presence of an intruder within the area is inconclusive and defines the *"Sensor Unspecified"* state.

Figure 3 WSNmod system setup



On the other hand, the measurements taken by the secondary sensors are also ranked into the same three levels: False (0), True (1), and Stand-by (-1). A False (0) indicates that the measurements of the corresponding primary sensor can be characterized as reliable; this defines the *"Normal state of measurement conditions"* of the primary sensor. A True (1) indicates that the measurements of the primary sensor cannot be considered as trustworthy; this defines the *"Alarm state of measurement conditions"* of the primary sensor. A Stand-by (-1) indicates that the measurements of the primary sensor are taken in borderline abnormal conditions thus they cannot be regarded as entirely trustworthy; this defines the *"Unspecified state of measurement conditions"* of the primary sensor.

At the second stage the sequence of alarms is been processed. The sequence is being processed as a sequence of events and indicators, and the process is based on the frequency and density of the alarm indicators.

2.1 Stage 1: Quantization of measurements

As it can be seen in Figure 4, the first step of the algorithm in the WSNmod is the quantization of the sensor measurements at three levels, regardless the type of sensor (primary or secondary). Since the quantization supports three distinct levels it is apparent that a special case of the typical three-valued logic (Ciucci, 2013) (Ciucci and Dubois, 2012) is at hand. In WSNmod a three-valued set on the set X can be defined as a mapping

$$f: X \rightarrow L_3$$

where $L_3 = \{F, SB, T\}$ is a chain of truth values, with T meaning true, F meaning false and SB (Standby) is the value standing in between. In our case L_3 is equipped with the ordering relation

$$T > SB > F$$

The quantization of the measurements at the first step of the WSNmod acts like a simple risk estimator, producing either a ***risk level A*** *(Normal State) "No intruder is within the area of interest"*, or a ***risk level B*** *(Stand-by State) "An intruder existence is probable within the area of interest but a safe conclusion cannot be exported"*, or a ***risk level C*** *(Alarm State) "An intruder has violated the area of interest"*. This way every input assumes one of the three states that indicate the level of risk that each sensor detects. Risk level A indicates that an intrusion is highly improbable (Normal state), risk level B indicates that an intrusion is probable but inconclusive (Stand-by state) and finally, risk level C, indicates that an intrusion is very likely that has happened (Alarm state). The risk levels, the states, the values and the state descriptions are given in Table 1.

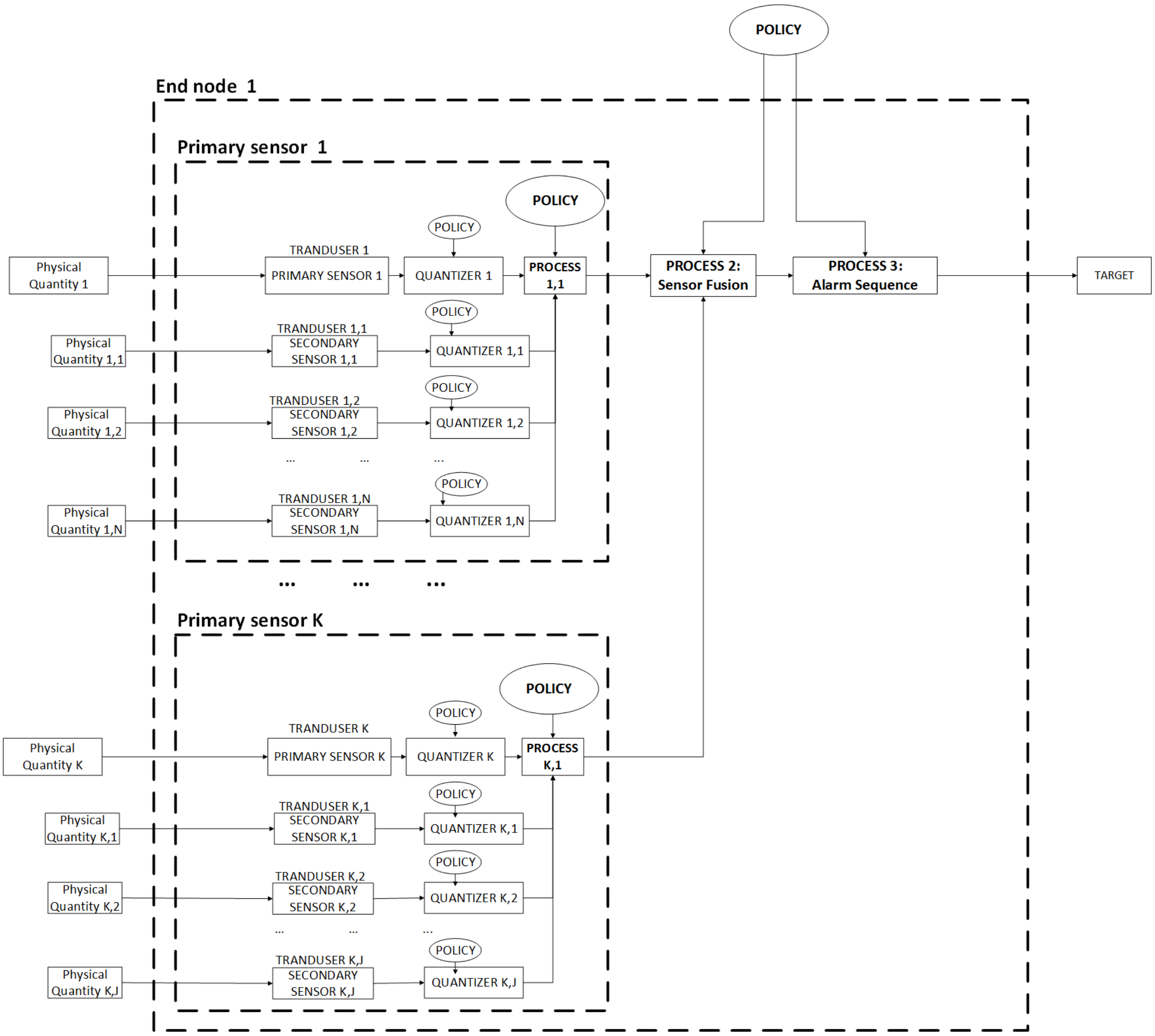
2.2 Stage 2: Filtering of primary sensor values

After the quantization of the sensors' measurements, the quantized values of the primary sensors are being processed according to their "quality", which is pointed out by the secondary sensors. Specifically, for every primary sensor, a set of the secondary sensors are being considered, in order to assess the quality of the measurement of the primary sensors, based on the environmental condition limits imposed by the sensor manufacturers. Before processing the primary sensors' values, the corresponding secondary sensors *{SK$_1$, SK$_2$, … , SK$_J$}* for each primary sensor are being fused according to the *three-valued OR operator* as shown in Table 2.

Table 1 Risk levels and corresponding values, state and descriptions.

Risk level	Value	State	State Description
A	False (0)	Normal	Intrusion Improbable
B	SB (-1)	Standby	Inconclusive
C	True (1)	Alarm	Intrusion Highly Probable

Figure 4 WSNmod abstract algorithm flowchart



The primary sensors' output is subsequently being processed according to the policy given in Table 3 that represents a newly-defined logical operation on the three-values between primary and secondary sensor values. In essence, a primary sensor's output (*PSO*) remains unchanged when the measurements are taken under "normal" measuring conditions (as defined by the manufacturers), or are being changed in questionable conditions. This way false alarms produced under questionable environmental conditions are being significantly reduced. Any *selected policy* can then be used to cope with the case when measurements from the secondary sensors are in the SB level (-1), in order to form the final output of the corresponding primary sensor. A "conservative" (non-risky) policy would, for example, turn the output to "alarm", or a policy that would favor less false positives would turn the output back to "normal" (non-intrusion). Essentially *this step is a false-positive rejection mechanism* that relies on assessing the quality of the primary measurements according to the secondary measurements that make use of the corresponding manufacturer guidelines.

Table 2 Fusion of secondary sensors with a three-valued OR operator

		S2		
		0	**-1**	**1**
S1	**0**	0	-1	**1**
	-1	-1	-1	**1**
	1	**1**	**1**	**1**
***** S_i: *Secondary sensor i*				

Table 3 Mapping of primary sensors output by the fused secondary sensors

PSO = f (S)		**P**		
		0	**-1**	**1**
S	**0**	**0**	**-1**	**1**
	-1	**0**	**-1**	**-1**
	1	**0**	**0**	**0**
**** PSO: Primary Sensor Output***				

2.3 Stage 3: Fusion of filtered primary sensor values

The fusion of the filtered primary sensor values (as produced by step 2) can follow any policy imposed by the operators of WSNmod. An example policy is shown in Table 4 for a case that includes three (3) primary sensors $\{P_1, P_2, P_3\}$. According to this policy, the output is set to "alarm" if at least one of the primary sensors' value is at the alarm level. This policy tries *to eliminate false-negative alarms ("conservative", non-risky approach)*. Moreover, in this policy, the fusion outputs the "normal" level only in case all primary sensors are in this state. All the other cases output the "SB" level.

2.4 Stage 4: Processing of the alarm sequence

After the final sensor fusion of Step 3, in order to estimate the overall risk factor, the sequence of consecutive fusion outputs is being processed in three more steps. A crucial parameter for this

Table 4 Example policy for primary sensors' values fusion

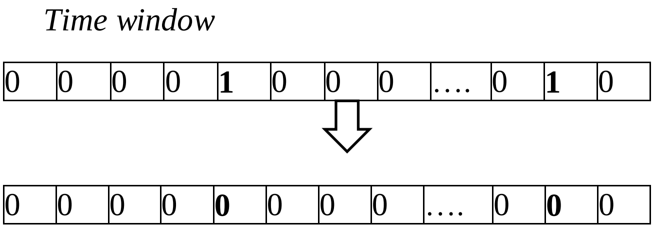
SF	**P1**	**0**	**-1**	**1**	**0**	**-1**	**1**	**0**	**-1**	**1**
	P2	**0**	**0**	**0**	**-1**	**-1**	**-1**	**1**	**1**	**1**
P3	**0**	0	-1	**1**	-1	-1	**1**	**1**	**1**	**1**
	-1	-1	-1	**1**	-1	-1	**1**	**1**	**1**	**1**
	1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
** SF: Sensor Fusion,* P_i*: Primary sensor i*										

processing is the time window for the sequence. The final output depends on the frequencies of the states and especially the frequency of the “alarm” events. This is also another point to impose a user-defined policy but at least one rule should be considered: the time frame should be wide enough to include fusion outputs that capture real-world events. Or, rephrasing, the frequency of detection should be more than twice the frequency of the most frequent event, according to the well known Nyquist sampling theorem. Practically, the time window must cover a time period at least twice the required time for the phenomenon to change its status from normal to alarm.

2.5 Step 4-1: Elimination of isolated alarms

During the first step an elimination of isolated alarms within the total duration of the time window is being carried out. These incidents are considered as singular alarm incidents (false-positives), most probably due to noisy measurements, and thus are being discarded (Figure 5).

Figure 5: False-positive alarm elimination



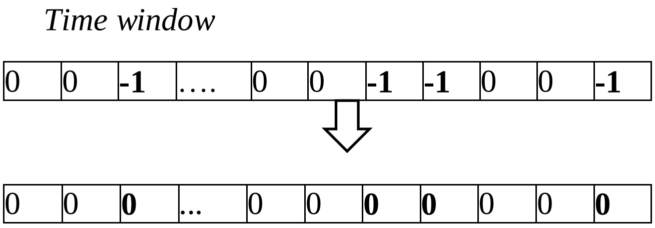
Time window

0	0	0	0	**1**	0	0	0	….	0	**1**	0
0	0	0	0	**0**	0	0	0	….	0	**0**	0

2.6 Step 4-2: Elimination of scattered SBs

During transients such as the occurrence of an intruder or other unexpected disturbances, it is likely that the sequence of results does not present stability and uniformity within the time window. Therefore, the system could send confusing information to the user. An approach to reduce these phenomena is to *use the time window as inertia* of the system, in order to monitor the signal sequence and replace the vague information with a clear and precise, as possible, message to the user. An example policy here would be to assume that if the values change frequently during the time window between Normal state and SB state, then the SB states are eliminated (changed back to Normal) (Figure 6). In such a policy it could also be the case to assume that if the values change frequently between Alarm and SB, then the output is changed to Alarm (Figure 7).

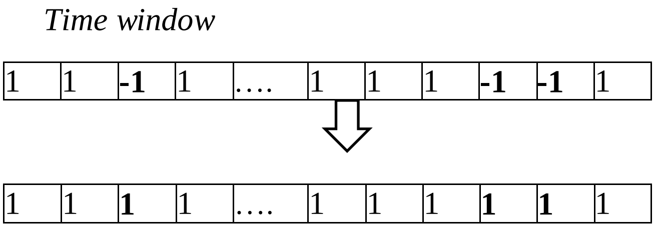
Figure 6: SB status elimination between normal states



Time window

0	0	**-1**	….	0	0	**-1**	**-1**	0	0	**-1**
0	0	**0**	...	0	0	**0**	**0**	0	0	**0**

Figure 7: SB status elimination between alarm states



Time window

1	1	**-1**	1	….	1	1	1	**-1**	**-1**	1
1	1	**1**	1	….	1	1	1	**1**	**1**	1

2.7 Step 4-3: False-positive elimination

In the last stage, the method is checking once more the target sequence for alarm singularities and repeats step 4-1. In such cases these single alarm events are not taken into consideration and they are erased as false alarms.

Finally the overall output of WSNmod is been produced according to the three-value logic operation defined in Table 5.According to this operation, a rate of alarm indication is being calculated and the final decision depends not only on a fusion of sensor measurements but also on a combination of sensor measurements and frequencies of events.

Table 5 The overall intrusion risk factor estimation

Target		**Frequency**		
		Low	**Medium**	**High**
SF	**0**	0	-1	**1**
	-1	0	-1	-1
	1	0	0	0

3 Experimental setup and evaluation

In order to evaluate WSNmod, a number of experiments have been performed. The experiments included a single node that consisted of sensors selected to detect intrusion-related quantities and secondary environmental sensors that relate to the qualification of the primary sensors. As far as the security applications and the decision making of intruder detection within the area of interest, it is apparent from the literature (Honey, 2003), (Gopi and Sivaprakash, 2014), (Li and Parker, 2008) (Bokareva et al., 2006), (Khan et al., 2007), (Quaritsch et al., 2010) and market applications that the three most common primary sensors for security applications are: the *ultrasonic-proximity sensor* for determining the distance of the potential intruder, the *Passive Infrared Sensor (PIR)* to detect motion, and a *magnetic* or *vibration sensor*. In outdoor installations the vibration sensors require neither a fixed infrastructure nor any special wiring. Thus, for the experimental evaluation of WSNmod *Ultrasonic, PIR and Vibration sensors* have been selected.

All three aforementioned sensors are organized into nodes, each of which includes one sensor of each type. The nodes are placed at points considered as potential passages for intruders in the area of interest and transmit their data wirelessly. In addition, a number of secondary sensors are considered for each node. All of the selected sensors are affected by both temperature and wind speed (Honey, 2003), (Carullo, and Parvis, 2001), (Moffat, 1988), (Everest and Pohlmann, 2009), (Northrop, 2005). Thus, a *Temperature* and a *Wind speed* sensor have been considered as secondary sensors for every node.

In order to evaluate the proposed method a series of intrusion scenarios have been simulated. The intrusion scenarios included *single node activations from vertical, horizontal and random intrusion movement (in relation to the field of detection) and under various environmental conditions*. In these scenarios, certain assumptions have been made regarding the conditions and the policy of the system. Specifically, the temperature varied between *3^oC* to *24^oC* and the wind speed between *1 m/s* to *4 m/s*. The sampling period was *200 msec* (corresponding to a frequency of *5 Hz*). Assuming that any possible intruder would activate any sensor for at least 1 second while passing the node, the detection time window was set to 2 seconds. The policy for the sensor fusions is given in Table 6 and Table 7 while in Figure 8 and in Table 8 an example of a WSNmod node setup is presented. The node is placed within the area of interest facing a possible intruder passage.

As shown in Figure 8, the node can be an infrastructure of about 6m tall where all the sensors could be placed. Specifically, the ultrasonic sensor can be placed facing directly the passage and inclined in a way that it detects from a height of about 1.5 meters and above. The motion sensor can be placed so that motion could be detected for objects higher than *10 cm* to reduce the risk of detection reptiles and rodents.

Both the infrared and ultrasonic sensor can be placed facing the passage, whereas the vibration sensor can be placed on an elastic fence or other elastic border on the passage in order to be activated when an intruder goes through the passage. Ten different scenarios were simulated in various environmental conditions covering a hypothetic time span of about one hour and a half each. Table 8 shows the simulated scenarios.

Table 9 and Figure 9 show the evaluation results for the proposed method in the simulated scenarios. Specifically, Table 9 shows the results of simulations in absolute numbers and percentages, and the diagram of Figure 9 shows the deviations from the ground truth for both ‘1’s - alarms and ‘0’s - normal states.

The first column denotes the scenario, the following three columns show the ground truth values, which can only be alarm activations (‘1’s) or normal conditions (‘0’s). In the next four columns the results of WSNmod are given (as described in §2.3 and §2.4).

Table 6 Primary sensors vs secondary sensors policy

PUO = f (W)		**U**				**PMO = f (T)**		**PIR**				**PVO = f (W)**		**V**		
		0	**-1**	**1**				**0**	**-1**	**1**				**0**	**-1**	**1**
W	**0**	0	-1	**1**		**T**	**0**	0	-1	**1**		**W**	**0**	0	-1	**1**
	-1	0	-1	-1			**-1**	0	-1	-1			**-1**	0	-1	-1
	1	0	0	0			**1**	0	0	0			**1**	0	0	0

Table 7 Overall sensors fusion policy

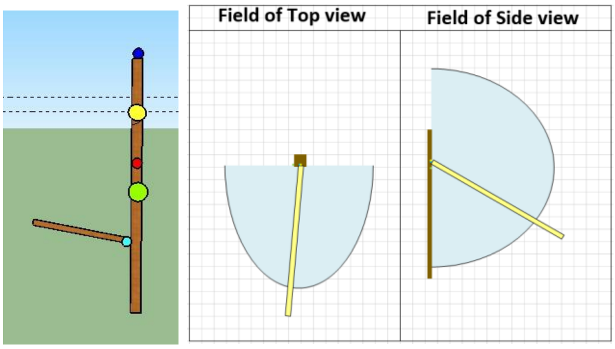
SF	**U**	**0**	**-1**	**1**	**0**	**-1**	**1**	**0**	**-1**	**1**
	V	**0**	**0**	**0**	**-1**	**-1**	**-1**	**1**	**1**	**1**
M	**0**	0	-1	**1**	-1	-1	**1**	**1**	**1**	**1**
	-1	-1	-1	**1**	-1	-1	**1**	**1**	**1**	**1**
	1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Table 8 The experiment scenarios

Scenario	***Description***	***Sensors triggered***		
		U	*M*	*V*
1.	*No trigger enabled*	-	-	-
2.	*At least one trigger enabled for every record*			
3.	*Only motion sensor is triggered*	-	*Y*	-
4.	*At least motion and ultrasonic sensors triggered*	*Y*	*Y*	-
5.	*At least motion and vibration sensors are triggered*	-	*Y*	*Y*
6.	*Both motion and ultrasonic sensors are triggered*	*Y*	*Y*	-
7.	*Both motion and vibration sensors are triggered*	-	*Y*	*Y*
8.	*At least one of motion, ultrasonic and vibration sensors are triggered*	*Y*	*Y*	*Y*
9.	*At least ultrasonic and vibration sensors are triggered*	*Y*	-	*Y*
10.	*At least two of motion, ultrasonic and vibration sensors are triggered*	*Y*	*Y*	*Y*

The values of these results can be either 1, 0, or -1, since these are the possible outcomes of the proposed algorithm. In the following five (2+3) columns all previous values are given in percentages. The last two columns present the deviations of WSNmod results to the ground truth, as a signed percentage difference between ground truth data and WSNmod results.

Figure 8: The node setup of the experiments.



A positive deviation indicates that the calculated results are less than the corresponding ground truth data while a negative deviation indicates that the estimated results are more than they originally were considered. As it is evident from these two columns, the method manages to keep deviations low. This deviation diminishes to zero in the two extreme scenarios of ‘all-alarms’ and ‘no-alarms’ (1 and 10), which is a first indication that WSNmod performs as expected for the trivial cases. In the other scenarios where there is a combination of both normal and alarm states the method approaches the ground truth with a very high precision, as denoted by the overall deviation range that is limited within *[0.60%, 1.47%]*. It is also worth noting that after a detailed study of both the ground truth and the WSNmod results the deviations seem to occur mostly due to the duration of alarms. In particular, since WSNmod, under the adopted case study policy, considers isolated alarms as noise, the method tends to discard alarms of a very short duration. By adopting another policy, these deviations can be erased, through, for example, a careful tuning of the time window duration or by increasing the sampling frequency. Another important aspect of the system's performance worth mentioning is its ability to cancel uncertainties in decisions, as evident from the low counts of '-1' (uncertain) results. It is clear that in the simulated scenarios the range of the uncertain results is limited to the interval *[0.00%, 1.03%]*, which is a rather small interval and supports the overall robustness and efficiency of WSNmod.

Lastly, it should be stressed that all results presented here reflect a specific setup, a preset policy and predefined simulated scenarios and can only capture a glimpse of the variety results that can be attained by WSNmod under various conditions, sets of sensors, alarm rules and decision policies supported by this method.

4 Conclusions

In this paper a new method and approach to decision making for security applications is presented. The method has been designed to be used in WSNs for open area intruder detection and was named WSNmod, since it represents a modular WSN. The method is based on a three-valued quantization of measurements, their fusion according to logics based on three-valued-logic and the processing of sequences of decisions within a time window. The system is hierarchical, highly modular and supports user-defined policies in various stages. WSNmod has been tested with simulated data under various environmental conditions by using a preselected set of sensors, a predefined policy and under various intrusion scenarios and has shown that it can reach a very high detection accuracy.

Figure 9: Bar graph of WSNmod deviations.

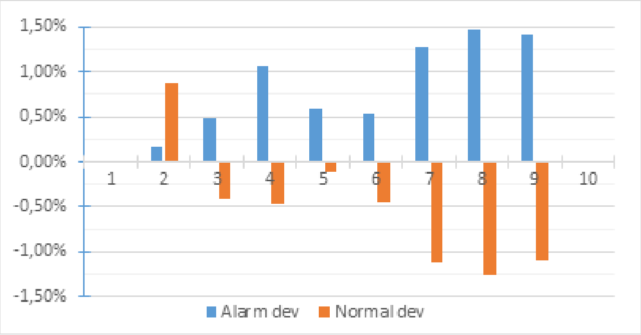


Table 9 Evaluation of WSNmod using simulated data and scenarios

Scenario	Ground Truth			WSNmod				Ground truth (%)		WSNmod (%)			Alarm dev	Normal dev
	1	0	all	-1	1	0	all	1	0	-1	1	0		
1	0	7969	7969	0	0	7969	7969	0.00%	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%
2	244	5275	5519	57	235	5227	5519	4.42%	95.58%	1.03%	4.26%	94.71%	0.16%	0.87%
3	301	3365	3666	3	283	3380	3666	8.21%	91.79%	0.08%	7.72%	92.20%	0.49%	-0.41%
4	359	4739	5098	30	305	4763	5098	7.04%	92.96%	0.59%	5.98%	93.43%	1.06%	-0.47%
5	2226	3274	5500	26	2194	3280	5500	40.47%	59.53%	0.47%	39.89%	59.64%	0.58%	-0.11%
6	717	7147	7864	7	675	7182	7864	9.12%	90.88%	0.09%	8.58%	91.33%	0.53%	-0.45%
7	964	4735	5699	9	891	4799	5699	16.92%	83.08%	0.16%	15.63%	84.21%	1.28%	-1.12%
8	534	5129	5663	12	451	5200	5663	9.43%	90.57%	0.21%	7.96%	91.82%	1.47%	-1.25%
9	1672	7973	9645	31	1535	8079	9645	17.34%	82.66%	0.32%	15.91%	83.76%	1.42%	-1.10%
10	6978	0	6978	0	6978	0	6978	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%

Currently we are working on various setups and simulations, including other sets of sensors, different policies in various stages of the system and other intrusion scenarios, to identify the extent to which WSNmod can be of benefit to security applications.

5 References

Agmon, N., Kraus, S. and Kaminka, G., 2008. Multi-robot perimeter patrol in adversarial settings. s.l., ICRA 2008. *IEEE International Conference on Robotics and Automation*, pp. 2339-2345.

Ahmedali, T. and Clark, J., 2006. Collaborative multi-camera surveillance with automated person detection. s.l., *Third Canadian Conference on Computer and Robot Vision*, p. 39.

Akyildiz, I., Su, W., Sankarasubraniam, Y., and Cayirci, E., 2002. A survey on sensor networks. *IEEE Communications Magazine*, 40(8), pp. 102-114.

Bai, Y.W., Cheng, C.C. and Xie, Z.L., 2013. Use of a time-variation ultrasonic signal and PIR sensors to enhance the sensing reliability of an embedded surveillance system. Regina, SK., 2013 *26th Annual IEEE Canadian Conference on Electrical and Computer Engineering (CCECE*), pp. 1-6.

Bellazreg, R., Boudriga, N. and Sunshin A., (2013). Border Surveillance using sensor based thick-lines. Bangkok, 2013 *International Conference on Information Networking (ICOIN*), pp. 221-226.

Bellazreg, R.,Boudriga, N., Trimèche, K. and An, S., (2013). Border surveillance: A dynamic deployment scheme for WSN-based solutions. Dubai, *Wireless and Mobile Networking Conference (WMNC*), 2013 6th Joint IFIP, pp. 1-8.

Belnap, N. J., (1977). A Useful Four-Valued Logic. In: J. Dunn, ed. Modern Uses of Multiple-Valued Logic. s.l.:*Springer Netherlands*, pp. 5-37.

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

Borowski, L., (1970). Selected Works of J. Łukasiewicz. North-Holland, Amsterdam: s.n.

Bouchard, K., (2014). Unsupervised spatial data mining for human activity recognition based on objects' movement and emergent behaviors. pp 104-105 ed. Chicoutimi, Canada: *Ph.D Thesis, Université du Québec en Outaouais (UQO)/Université du Québec à Chicoutimi (UQAC)*.

Carullo, A. and Parvis, M., (2001). An ultrasonic sensor for distance measurement in automotive applications. *Sensors Journal*, 1(2), pp. 143-.

Cho, Y. K., Charles, W. and Youn, J.-H. (2006). Wireless Sensor-driven Intelligent Navigation Robots for Indoor Construction Site Security and Safety. s.l., 23rd *Int. Symp. on Automation and Robotics in Construction 2006. ISARC 2006,*, pp. 493-498.

Ciucci, D. and Dubois, D.,(2012). Relationships between Connectives in Three-Valued Logics, Advances on Computational Intelligence. *Communications in Computer and Information Science*, Volume 297, pp. 633-642.

Ciucci, D. and Dubois. D., (2013). A map of dependencies among three-valued logics. *Information Sciences*, Volume 250, pp. 162-177.

Demeris, G., Hensel, B.K., Skubic, M. and Rantz, M., (2008). Senior residents' perceived need of and preferences for "smart home" sensor technologies. *International Journal of Technology Assessment in Health Care*, 24(1), pp. 120-124.

Dessart, N. and Hunel, P., (2014). Data collection using WSN for counting individuals and habitat characterization. *Journal of Computational Science*, 5(4), pp. 624-632.

Dima, S.-M., Panagiotou, C., Tsitsipis, D., Antonopoulos, C., Gialelis, J. and Koubias, S., (2014). Performance evaluation of a WSN system for distributed event detection using fuzzy logic. *Ad Hoc Networks*, Volume 23, pp. 87-108.

Everest, F.A and Pohlmann, K., (2009). Absorption. In: Master Handbook of Acoustics.

s.l.:*Mc Graw Hill*, pp. 180-181.

Felemban, E., (2013). Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology. *Int. J. Communications, Network and System Sciences*, Volume 6, pp. 251-259.

Gent, E., (2014). Engineering and Technology. [Online] Available at: http://eandt.theiet.org/news/2014/jul/vantablack-dark.cfm?origin=EtOtherNews [Accessed 19 January 2015].

Gopi K. and Sivaprakash S., (2014). Cluster Based Intrusion Detection System for Wireless Sensor Networks. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(1), pp. 993-999.

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

Hanirex, D.H. and Kaliyamurthie, K.P., (2014). Authentication and Authorization for High Security Manets. *Middle-East Journal of Scientific Research*, 19(7), pp. 9041-907.

Harrop, P. and Das, R., (2015). Wireless Sensor Networks (WSN) 2014-2024: Forecasts, Technologies, Players The new market for Ubiquitous Sensor Networks (USN). s.l.:IDTechEx.

Honey, G., (2003). Intruder alarm detection devices. In: Intruder Alarms. Newnes: *Oxford*, pp. 48-94.

Intani, P. and Orachon, T., (2013). Crime Warning System using Image and Sound Processing. Gwangju, 2013 13th *International Conference on Control, Automation and Systems (ICCAS*),, pp. 1751-1753.

Jisha, R.C., Ramesh, M.V., Lekshmi, G.S., (2010). Intruder tracking using wireless sensor network. s.l., 2010 *IEEE International Conference in Computational Intelligence and Computing Research (ICCIC*),, pp. 1-5.

Katsarakis, N., Pnevmatikakis, A., Tan, Z.-H. and Prasad, R., (2014). Combination of Multiple Measurement Cues for Visual Face Tracking. Wireless Personal Communications, *Special issue on "Intelligent Infrastructures & Beyond*", 78(3), pp. 1789-1810.

Katsarakis, N., Pnevmatikakis, A., Tan, Z.-H. and Prasad, R., 2015. Improved Gaussian Mixture Models for Adaptive Foreground Segmentation. Wireless Personal Communications, *special issue on "Current trends in information and communication technology"*, pp. 1-15.

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

Kleene, S., 1952. Introduction to Metamathematics. Amsterdam: North–Holland Pub. Co.

Li, Y.Y. and Parker, L.E., (2008). Intruder detection using a wireless sensor network with an intelligent mobile robot response. *Huntsville, AL, Southeastcon, 2008. IEEE.*

Li, Y.Y. and Parker, L.E., (2008). Intruder detection using a wireless sensor network with an intelligent mobile robot response. *Huntsville, AL, Southeastcon, 2008. IEEE*, pp. 37-42.

Lin, C.-H., Yang, S.-H., Chen, H.-T. and Song, K.-T., (2008). Mobile robot intruder detection based on a Zigbee sensor network. s.l., *IEEE International Conference on Systems, Man and Cybernetics*, pp. 2786-2791.

Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., Anderson, J., (2002). Wireless Sensor Networks for Habitat Monitoring. s.l., Proceeding WSNA '02 *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 88-97.

Moffat, R. J., (1988). Describing the uncertainties in experimental results. *Experimental Thermal and Fluid Scienc*e, 1(1), pp. 3-17.

Nelson, D., 1949. *Constructible Falsity. Journal of Symbolic Logi*c, 14(1949), pp. 16-26.

Northrop, R., (2005). Applications of Sensors to Physical Measurements. In: Introduction to instrumentation and measurements. s.l.:*Taylor and*

Francis, pp. 343-500.

Parry, W.T. and Haker, E.A., (1990). Aristotelian logic. *SUNY Press* ed. s.l.:s.n.

Pasqualetti, F., Zanella, F., Peters, J.-R., Spindler, M., Carli, R. and Bullo, F., (2013). Camera Network Coordination for Intruder Detection. s.l., *IEEE Transactions on Control Systems Technolog*y, pp. 1669-1683.

Phung, N.D., Gaber, M.M., Rhm, U., (2007). Resource-aware online data mining in wireless sensor networks. s.l., *IEEE Symposium on Computational Intelligence and Data Mining*, pp. 139-146.

Priest, G., (1979). The logic of paradox. *The Journal of Philosophical Log*ic, Volume 8, pp. 219-241.

Qian, H., Sun, P. and Rong, Y., (2012). Design Proposal of Self-Powered WSN Node for Battle Field Surveillance. *Energy Procedia*, 16(B), pp. 753-757.

Quaritsch, M., Kruggl, K., Wischounig-Strucl, D., Bhattacharya, S., Shah, M. and Rinner, B., (2010). Networked UAVs as aerial sensor network for disaster management applications. *Elektrotechnik & Informationstechnik*, 127(3), pp. 56-63.

Ramon, C.F. Araújo, Rodrigo M.S. de Oliveira, Josivaldo de S. Araújo,, (2015). A method for locating multiple intruders with multistatic radars. *Applied Mathematical Modelling*, 39(17), pp. 5241-5252.

Saipulla, A., Liu, B., Xing, G., Fu, X., and Wang, J., 2010. Barrier coverage with sensors of limited mobility. s.l., In Proceedings of the eleventh *ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '10*)., pp. 201-210.

Sobocinski, B., (1952). Axiomatization of a partial system of three-valued calculus of propositions. *Journal of Computing System*s, Volume 1, pp. 23-55.

Stone, E.E. and Skubic, M., (2011). Evaluation of an inexpensive depth camera for passive in-home fall risk assessment. s.l., *5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth*), pp. 71-77.

Suthaharan, S., and Bandari, S., (2012). Intruder detection in public space using suspicious behavior phenomena and wireless sensor networks. s.l., Proceedings of the *1st ACM international workshop on Sensor-Enhanced Safety and Security in Public Spaces*, pp. 3-8.

Tian, W. J. and Geng, Y.,, (2009). A New Household Security Robot System Based on Wireless Sensor Network. s.l., *2nd Int. Conf. on Future Information Technology and Management Engineering*, pp. 187 - 190.

Tsujita, W.,Inomata, K., Hirai, T., (2013). Development of dual leaky coaxial cable for intruder detection sensor. s.l., *2013 IEEE International Conference in Technologies for Homeland Security (HST),*, pp. 126-129.

While, L., Sun, Y.F. and Barone, L., (2013). A Market-based Approach to Planning in Area Surveillance. Cancun, 2013 *IEEE Congress on Evolutionary Computation (CEC*), pp. 2687 - 2694.

Wittenburg, G., Dziengel, N., Wartenburger, C., Schiller, J., (2010). A system for distributed event detection in wireless sensor networks. pp 94-104, Proceedings of the *9th ACM/IEEE International Conference on Information Processing in Sensor Networks*,, pp. 94-104 .

Xiao, X., He, Q., Fu, Z., Xu, M. and Zhang, X., (2016). Applying CS and WSN methods for improving efficiency of frozen and chilled aquatic products monitoring system in cold chain logistics. *Food Control,* Volume 60, pp. 656-666.