Pervasive surveillance-agent system based on wireless sensor networks: design and deployment

José F Martínez, Sury Bravo, Ana B García, Iván Corredor, Miguel S Familiar, Lourdes López, Vicente Hernández and Antonio Da Silva

Abstract

Nowadays, proliferation of embedded systems is enhancing the possibilities of gathering information by using wireless sensor networks (WSNs). Flexibility and ease of installation make these kinds of pervasive networks suitable for security and surveillance environments. Moreover, the risk for humans to be exposed to these functions is minimized when using these networks. In this paper, a virtual perimeter surveillance agent, which has been designed to detect any person crossing an invisible barrier around a marked perimeter and send an alarm notification to the security staff, is presented. This agent works in a state of 'low power consumption' until there is a crossing on the perimeter. In our approach, the 'intelligence' of the agent has been distributed by using mobile nodes in order to discern the cause of the event of presence. This feature contributes to saving both processing resources and power consumption since the required code that detects presence is the only system installed. The research work described in this paper illustrates our experience in the development of a surveillance system using WNSs for a practical application as well as its evaluation in real-world deployments. This mechanism plays an important role in providing confidence in ensuring safety to our environment.

Keywords: pervasive surveillance agent, ubiquitous security system, wireless sensor network

(Some figures in this article are in colour only in the electronic version)

1. Introduction

Wireless sensor networks (WSNs) are ubiquitous networks, which are made up of tiny sensor devices, called sensor nodes. These pervasive devices are capable of monitoring and processing data with wireless communication support. They also come with independent decision-making features that respond to sensor measurements and to the information that is shared among them. A WSN is a powerful and flexible tool that allows monitoring complex environments, where data monitoring by other methods is not possible. Nowadays, the proliferation of embedded systems is enhancing the possibilities of gathering information by using WSNs. They are used in a great number of applications such as surveillance and security, environmental monitoring, health applications, smart space, industrial control and automotive [1], among others.

Regarding pervasive surveillance and security, WSNs reduce risk to humans who are exposed to these functions and reduce the work force needed in such environments. Implementation time and deployment of security systems based on WSNs are some other interesting issues to be

taken into account. Regarding this topic, García [2] claims that the sensor networks allow security system designers to quickly and easily place individual sensor/communication. On the other hand,other advantages of WSNs when applied to public buildings, such as saving cost in the wiring installation and having ubiquitous connection, are mentioned in [3]. They are unobtrusive and also require less maintenance. However, WSNs have limited power supply, computational capacities, memory and short-range radio communication features. Thereby, WSN-based surveillance systems have to be designed taking into account some trade-offs between 'system goals' and efficient use of hardware resources.

In this research paper, a virtual perimeter surveillance agent (vpSA) is proposed. It implements mobile nodes management based on a reactive agent's model. The agent's main goal is to deal with the detection of objects that cross an invisible barrier around a given perimeter of the Versmé Sanatorium in Birstonas (Lithuania). The agent deployed in the perimeter nodes analyses the data received from the environment when the virtual perimeter is crossed, discerning patients, assistant staff (authorized access), and intruders (unauthorized access). It consequently sends an alarm notification to the security staff. Thus, our agent perceives a situation occurred in the environment and makes a decision on that perception. A vpSA approach has been developed as a reactive agent that does not have any internal symbolic models of its environment. It acts as a stimulus/response type of behaviour by responding to the current security perimeter established by the fixed nodes. In order to improve network autonomy, which is one of the major challenges in WSNs, a low power consumption mode has been designed. In order to achieve low power consumption, the agent is scheduled in a sleep mode, during its normal operation. When the virtual perimeter is crossed, the agent passes to a 'wake-up state' in order to carry out required decisions.

Other parts of this paper have been organized as follows: section 2 explains the related work, focused on developing surveillance solutions using WSNs. Section 3 describes the theoretical foundations of our proposal in detail that include system specifications, and pervasive agent features and properties. Section 4 explains the experience observed in the deployment of the surveillance agent in the real environment. Section 5 shows validation results of the agent, as well as some interesting notes based on our field deployment experiences. Finally, concluding remarks and future research lines are analysed in section 6.

2. Related work

A reactive agent acts using a stimulus/response type of behaviour; hence, it does not have any internal symbolic models of the environment and acts according to the result of stimulus generated within [4]. WSNs are defined by a set of agents, connected to each other by communication interfaces [5]. These kinds of ubiquitous networks interact with their environment by means of

- actions exerted by the environment;
- external states emitted to the environment.

According to the previous study, each agent of the WSN can be defined as a *reactive decisional agent* that cooperates with other network operators in order to achieve a specific objective. In the literature [6–8], several proposals to model the WSN as heterogeneous agent systems are presented.

Byunghun *et al* [9] propose a surveillance system using a passive infrared (PIR) sensor to detect movement in a home, office or factory. First, it analyses the use of PIR sensors by security systems, proposing a region-based human tracking algorithm. This algorithm is based on PIR sensors to know the region where an object is located. They model the detection region of the PIR sensors based on location coordinate, spread angle, detection range and constant radius (maximum detection distance) of the PIR sensor. In this manner, they set the detection area accurately and show how to deploy the PIR sensors so as to detect human movement. However, detection is highly dependent on the sensor deployment. Furthermore, this mechanism has only been tested to detect one person at a time.

Li and Parken [10] propose an anomaly detection system by using WSNs and mobile robots. The architecture proposes a cluster topology. Each cluster has a cluster head and multiple cluster members. Each cluster covers a geometric region and is responsible for detecting the environmental changes in that region. The sensor network uses a fuzzy adaptive resonance theory (ART) neural network to detect intruders. The system detects time-related changes by using the Markov model. First, the sensor network learns what conditions of an environment are 'normal', and then compares the current environment conditions with the reference model in order to detect environmental changes.

When a change is detected, the WSN determines that conditions of the environment do not match the reference model. It informs the mobile robot about such a situation; the robot then displaces to the area to verify whether the reported event is related to an intruder. Intrusion detection in WSNs provides higher flexibility due to the collaboration of robots in reaching places and performing tasks that cannot be performed by fixed nodes.

Zappi *et al* [11] propose a technique that detects humans who cross through a door or gate. In this approach, four sensor nodes are used: three of them are equipped with infrared sensors that sample the output of the PIR detector and identify the number of peak pairs and the direction of the first peak. The fourth node sensor receives all information and infers the number of people and direction of movement. The number of persons is extracted by means of the number of peaks detected by each node and duration of the second peak which is measured by the central node. The direction of movement is detected by looking at the indication of the three sensors. The most important limitations of this system are its high dependence on network topology and set-up of PIR sensors.

According to the literature described in this section, it is concluded that WSNs are widely used in tracking events or objects (e.g. building monitoring and control, industrial process control and energy monitoring) by means of their wireless communication capabilities, their easy interaction with other external networks and their tiny sizes that allow

Table 1. Characteristics of the Luminite TX500/40 PIR detector.

Items	Datasheet
Detection distance	40 m
Field of view	1°
Supply voltage	9 V from PP3
Consumption in stand-by mode	9 μA
Temperature range	−10 + 50 °C

them to integrate with the environment easily. However, no previous works using an intruder detection system through cooperation with mobile sensor nodes have ever been applied. As far as is known, there are no companies providing this type of application. Otherwise, specialized companies (Crossbow Technologies[1], Sentilla[2], Libelium[3]), offering hardware for designing and deploying similar kinds of applications, would be offering such systems.

3. Specification of the surveillance agent

This section describes the mechanism used by the vpSA for the detection of intruders, as well as its architectonic and functional description. Moreover, the selected middleware that allows deployment of the agent and provides basic services, such as communication support, is outlined.

Presence detection mechanisms are used in cases where a perimeter has not been physically defined, or when a perimeter is not visible to people for security reasons.. Thus, presence detection systems generate an invisible barrier around the perimeter and perform actions when the perimeter is altered in order to prevent intrusions. In the following section, the features of the sensors used for detecting intrusions at the perimeter are described.

3.1. Characterization of passive infrared sensors

PIR sensors are pyroelectric devices. They can be used for detecting movements by means of changes in temperature emitted by objects inside the marked area. Treatment of PIR sensor data is simpler than those implemented by a microphone, ultrasound or other visual means and contrast. They do not require any device or object detection signal. PIR sensors have proven performance, and are inexpensive and easy to integrate with other systems [12]. Thus, they are widely applied in alarm systems, lighting controlled by motion and robotics applications such as intrusion detection [13].

For this study, a Luminite TX500/40 passive infrared sensor has been used[4] . This provides a detection range of up to 40 × 1° (see table 1). The TX500/40 PIR sensor is for long-range narrow applications, being suitable for perimeter protection. A 9 V lithium PP3 battery powers this PIR.

[1] Crossbow Corporation Inc. (available at http://www.xbow.com).
[2] Sentilla Corporation (available at http://www.sentilla.com).
[3] Libelium Comunicaciones Distribuidas SL (available at http://www.libelium.com).
[4] Luminite Electronics Ltd (available at http://www.luminite.co.uk/productpage.php?WEBYEP_DI=301).

3.2. Middleware

As was presented in previous sections, the vpSA approach is based on agent paradigm. This technology requires space for interpretation, storage and control, commonly known as 'agent platform'. Agent platforms are standardized by the Foundation for Intelligent Physical Agents (FIPA)[5] . This platform provides different services such as communication among agents, reactivity and behaviour. In order to provide support for deployment of the agent in the sensor nodes, lightweight software has been used in order to provide abstraction from the underlying sensor platform heterogeneity and communication at a network level by means of an application programming interface (API). In this manner, a μSMS (micro subscription management system) middleware approach has been developed in the framework of the μSWN Research Project[6].

The main reason for using μSMS middleware abstraction is its ease for providing deployment of agent-based services over resource-constraint devices. Among these features we can emphasize the development of lightweight component-based services as well as the event-driven publish/subscribe communication paradigm. On the one hand, the publish/subscribe interaction model is widely applied in WSNs because it offers an asynchronous interaction model between components. The components are notified when an event of interest is generated, without having to continuously poll the data source. This enhances the decoupling between information producers and consumers, while minimizing energy consumption [14]. Moreover, this architecture uses the middleware components paradigm for service creation. The use of these components offers several advantages to software engineering. These advantages include independence (low coupling between architecture pieces), interoperability (by means of well-specified service interface contract) and reusability (business logic of the components is properly encapsulated). Considering μSMS proposal, the interface of each component is very compact. That means the minimum required methods for controlling the lifecycle of each component (see section 3.3) and the minimum to interact with the rest of the architecture by using an underlying event-based model have been defined. This allows the framework subsystem to schedule the components in a low-consumption mode in order to increase the autonomy of the sensor nodes.

At this point, μSMS architecture can be seen as a multi-agent platform for enriched service composition on WSNs. This middleware approach provides support for the exchange of information between sensor nodes in a lightweight manner, which is a cornerstone in embedded computing devices, such as WSN[6]. Figure 1 illustrates the core components diagram of the architecture, where the vpSA is deployed.

The description of the main elements of the μSMS architecture is as follows.

Resources. This middleware component is responsible for controlling hardware resources of the nodes. Its main

[5] Foundation for Intelligent Physical Agents (available at http://www.fipa.org/specs/fipa00023/index.html.).
[6] μSWN: Solving Major Problems in Micro Sensorial Networks (IST-034642) European FP6 Project Site www.uswn.eu/j/index.php.

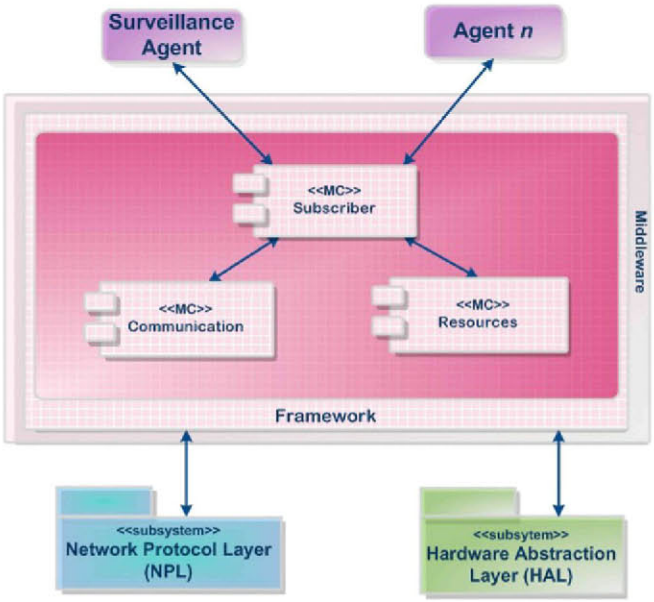

Figure 1. Overview of the μSMS middleware architecture.

functions include management of timers, LEDs, DAC (digital to analogue converter), ADC (analogue to digital converter), GPIO (general purpose I/O) and batteries, among others.

Subscriber. This middleware component represents the kernel of the publish/subscribe system. It provides publication and subscription capabilities to the rest of the components in the architecture. In this manner, the subscriber allows the application agents to exchange data with the agents deployed in the rest of the network nodes, through eventing service.

Communication. This middleware component is responsible for sending and receiving data events in the sensor network. It uses the services offered by the NPL (network protocol layer) subsystem, offering the rest of the architecture a well-defined interface to support the inter-node communication.

Framework. This middleware subsystem is responsible for managing the lifecycle of the component and agents in the nodes. The main task of the framework subsystem is the execution scheduling of the components that are instantiated in the nodes.

Hardware abstraction layer (HAL). This subsystem allows taking advantage of the resources of the sensor nodes by isolating the application agents from the underlying hardware heterogeneity. Thus, using the services offered by HAL, the resources component provides a uniform interface to access the physical node capabilities.

Network protocol layer (NPL). This subsystem encapsulates the low-level radio communication protocols. Its objective is to decouple the middleware of the specific used routing scheme features, using a stratified approach. Communication component wraps in order to provide a common interface, with independence from the specific implementation applied in the NPL. The following subsections explain the technical details of the physical, MAC and routing protocol layers that have been used.

3.2.1. Physical and MAC layers. This approach is based on IEEE Std 802.15.4-2006, which specifies a standard protocol stack widely used in a low-rate wireless personal area network (LR-WPAN). IEEE 802.15.4 protocol stack defines a physical (PHY) layer and a medium access control (MAC) layer. The PHY layer operates at 868 MHz (11 radio channels, 20 kbps), 915 MHz (11 radio channels, 40 kbps) and 2.4 GHz (16 radio channels, 250 kbps) frequency bands, with a wireless transmission range up to 100 m. The IEEE 802.15.4 MAC layer uses a CSMA-CA (carrier sense multiple access-collision avoidance) algorithm to detect and avoid collisions in a shared transmission medium, offering a guaranteed time slot (GTS) as the optional mechanism. This feature is focused on allocating a specific duration within a superframe structure, in order to offer low latency for user applications with real-time requirements.

3.2.2. Routing protocol. ZigBee specification 2006 networking technology has been considered in this approach. It is an IEEE 802.15.4-based protocol stack aiming to achieve low cost and low power consumption in resource constraint and embedded devices. This standard defines, over an IEEE 802.15.4 MAC layer, a network (NWK) layer and an application support (APS) layer. The NWK layer implements the routing protocol, which offers multi-hop communication support for several networking topologies, including star, cluster tree and mesh; the latest has been used in our WSN deployment. Moreover, confidentiality service is provided by this routing scheme, using 128 bits symmetric cryptography for the advanced encryption service (AES) protocol. The APS layer is over NWK in order to offer a set of general functionalities, such as services of binding and discovery.

3.3. Agent properties

The most important properties of the proposed vpSA are as follows.

Agent status. It describes the necessary information to distinguish between two agents of the same type. The state is mainly affected by the agent inputs, which are data acquired by the sensors and information from other agents.

Agent behaviour. It defines the agent's ability to react to a specific execution condition, based on the perception and action taken previously. Thus, the agent makes decisions according to the event detected by the sensors.

Communication capabilities. vpSA has interaction capabilities among nodes through the agent middleware platform provided by the μSMS abstraction. As previously mentioned, it offers agents support to interact with other actors through publish/subscribe paradigm, using an event-driven communication model.

Autonomy. vpSA performs its task without intervention from humans or other agents, through orders and/or queries. The agent is interested in a specific event,

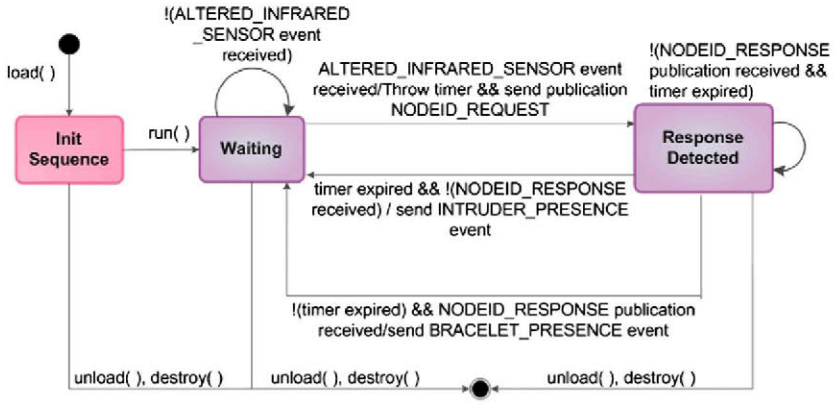

Figure 2. State diagram of the fixed nodes.

so when this event occurs, the agent executes the corresponding action. This procedure implies that agents running on the mobile node wake up from a low power consumption mode and consequently perform corresponding functions automatically.
Common objectives. Both in the fixed and mobile nodes, agents perform a set of specific tasks. They interact to achieve common 'detecting presence' goal.
Lifecycle. The agent has capacity of being 'born' when it is developed and activated; to 'live' while it is operational; to 'clone' itself by distributing its knowledge over mobile nodes in order to fulfil its main objective; and to 'die' when it is unloaded from the node.

3.4. Surveillance agent roles

Agents have been installed in two types of sensor nodes: 'fixed nodes' and 'mobile nodes'. Fixed nodes are used for making the virtual perimeter, and 'mobile nodes' are used for detecting clients and assistant staff. The main agent functionalities in these nodes are as follows.

3.4.1. Fixed nodes. The virtual perimeter is made up of fixed nodes. These nodes are equipped with PIR sensors, which can detect any motion from people crossing the perimeter. The fixed nodes distinguish clients, assistant staff and intruders. This information is then sent to the sink node and, from there, to the security staff of the sanatorium via WiFi. All the collected information is stored in a database.

3.4.2. Mobile nodes. The clients and assistant staff are equipped with this kind of node. The nodes send a signal identifying themselves when a fixed node of the virtual perimeter makes a request. They have a business logic that allows collaborating with the fixed nodes to discern the type of intrusion (i.e. authorized or unauthorized).

3.5. Surveillance agent functions

The main design goals of the vpSA are as follows.

- Detection of access to the perimeter of clients, identifying sanatorium staff or intruders passing through the area.
- Alarm indication directed to sanatorium security personnel, reporting that an unauthorized person has crossed the perimeter.

3.5.1. Agent functions in the fixed nodes. As shown in figure 2, vpSA located in the fixed nodes remains in a low power consumption mode until the virtual perimeter is crossed. Once the agent receives an 'altered infrared sensor' event, the identification of its neighbours will be requested. If there are mobile nodes in this area, they have to respond with their identification to the fixed node so it can inform bracelet identification to the security personnel and determine the 'bracelet presence' event. Otherwise, if an intruder has altered the perimeter, the fixed node will process an alarm of 'intruder presence' and inform the security staff. The period of time between the request for identification and its corresponding response depends mainly on the time required between the sensor nodes (fixed and mobile) to communicate and exchange such events. In any case, the time is not more than 3 s for the fixed nodes and 2 s for the mobile nodes.

3.5.2. Agent functions in the mobile nodes. The vpSA located in the mobile nodes remains in a low power consumption mode until an identification request event is received from the fixed node (perimeter node). Once the agent receives a 'request identification' event, it responds to the perimeter node that has requested for it. The time that transpires is not more than 2 s. The agent then returns to the low-consumption mode.

4. Implementation details

The vpSA has been deployed at the Versmé Sanatorium in Birstonas (Lithuania). Two different types of nodes have been installed: fixed nodes that make up the virtual perimeter, and mobile nodes (bracelets) that are worn by sanatorium patients and authorized staff. Messages are interchanged when the virtual perimeter is crossed, both by a bracelet or an intruder.

Figure 3 shows the vpSA deployed in fixed nodes as previously subscribed to 'ALTERED_INFRARED_SENSOR' events. This kind of event will be thrown by the Resources

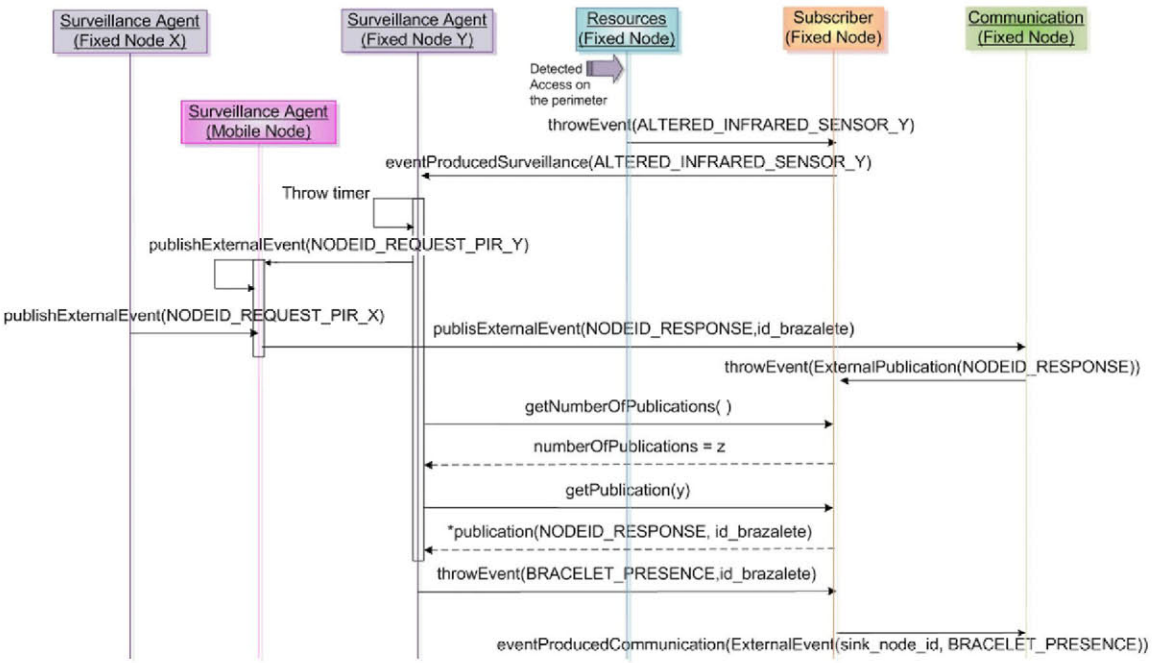

Figure 3. Surveillance scenario: 'bracelet detection' use case.

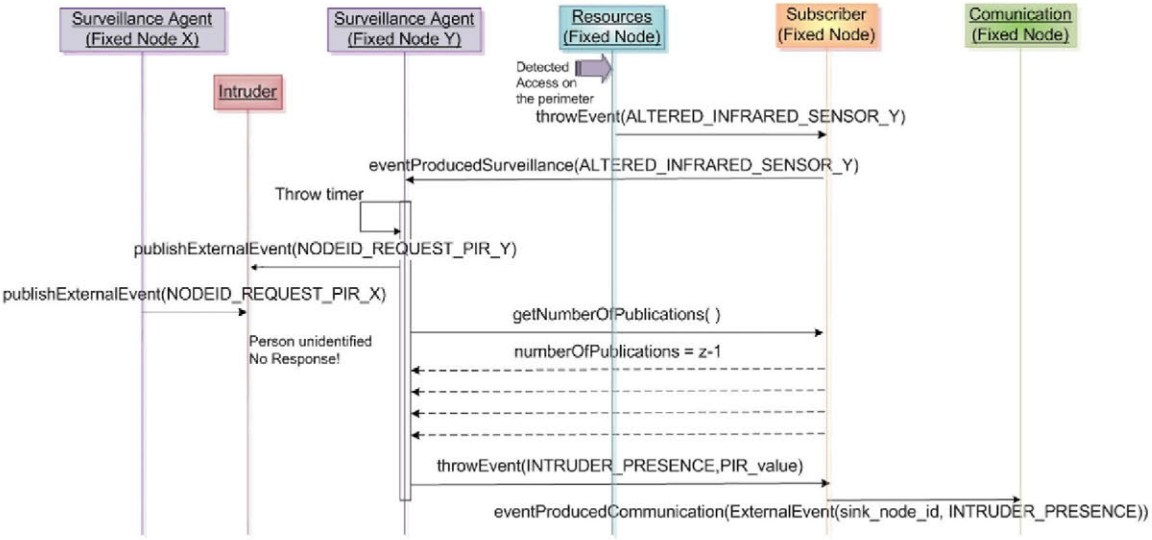

Figure 4. Surveillance scenario: 'intruder detection' use case.

component of the μSMS middleware when the PIR sensor is excited. When a presence is detected, the fixed node connected to the PIR sensor generates a 'NODEID_REQUEST' external publication, which will be delivered to the neighbouring nodes via broadcast communication. The bracelet node that crosses the perimeter has to reply with a 'NODEID_RESPONSE' external publication; the fixed node will wait for the answer from the bracelet node for a short period of time (3 s). If the 'NODEID_RESPONSE' event is received from the bracelet node, the fixed mote will throw a 'BRACELET_PRESENCE' event containing the identification of the bracelet node that has generated the presence in the perimeter. Otherwise, in the case of intruder detection, an 'INTRUDER_PRESENCE' event will be generated (see figure 4).

5. Validation scenario

In order to validate our approach in the real-world environment, a surveillance perimeter has been deployed at the Versmé Sanatorium in Birstonas (Lithuania), as shown in figure 5. This sanatorium is an establishment for specialized treatment and recreation, providing rehabilitation, support rehabilitation, ambulatory rehabilitation and sanatorium treatment services.

A WSN has been deployed using fixed nodes to mark the virtual perimeter on the external part of the sanatorium, which is 810 m long. In order to enable the mechanism of identification in the fixed nodes, a bracelet (mobile node) is assigned to every patient and assistant staff at the sanatorium.

Figure 5. Virtual perimeter in sanatorium.

During the evaluation, 14 patients, each wearing a bracelet, were supervized by 5 assistant staff. The bracelets are made of Crossbow TelosB nodes (so-called motes) that integrate additional biomedical sensors in order to spread their capacity of sensing data such as heart rate, body temperature and humidity. In some particular cases, the sanatorium staff will use a PDA to receive presence events from the perimeter. When an intruder is detected inside the perimeter, the fixed node alerts the security staff by reporting the type of intrusion, which could have been generated by a client or by an intruder. The personnel will then have to confirm the event and make decision accordingly. The data about the event are saved in a database for further analysis and consultation.

Figure 5 shows the fixed nodes deployed around the sanatorium perimeter, represented by dots. They contain PIR sensors, which are used to detect the presence of people crossing the perimeter.

The virtual perimeter is made up of 50 TelosB mote sensor platforms and used as implementation target. Because of project cost constraints, a sub-perimeter has been selected in order to deploy the validation scenario. Only 16 nodes from 50 needed to cover the complete perimeter were used. In the next stage of the project, the perimeter will be completely covered by deploying 34 more nodes. In the TelosB platform, a sensor board can be plugged into each sensor node (mote) in order to carry out several environment readings including light, temperature, humidity, infrared, etc. The deployed TelosB runs on two AA batteries, with a lifespan that depends on communication use and computation resources. Communications within a 75–100 m outdoor range vary greatly under environmental conditions, as can be observed in the datasheet. The motes run the TinyOS operating systems and are equipped with 48 kB of flash memory and 10 kB of RAM memory, IEEE 802.15.4-compliant radio. Moreover, these nodes are equipped with infrared sensors (LUMINITE TX500/40).

5.1. Deployment requirements

In the preliminary tests, it was identified that the same physical event was detected by two or more nodes, generating alarms in places where incursions were not carried out. This was due to the overlapping of motes coverage ratio inside the detection area. In other words, two motes shared part of their detection area.

Hence, it was also determined that the deployment of fixed nodes considers the intersection range of the infrared sensors. This intersection area just involves two consecutive fixed nodes that take part of the surveillance perimeter. Thus, it has been guaranteed that the bracelet will only respond to those fixed nodes involved in the sector where it has crossed. It thereby reduces false alarms. Two major requirements are necessary in order to enable a proper detection of people wearing bracelets: the two nodes involved in a perimeter sector have to be deployed within the maximum PIR detection distance between them (40 m), and their PIRs must be accurately brought face to face. This ideal scenario is illustrated in figure 6.

As a validation requirement, multi-hop radio configuration has been validated. Network deployment was designed so as not to exceed five hops between sensor nodes and sink node. In order to set this scenario up, both physical location of sensor nodes and strength of their radio signal were taken into account.

5.2. Validation results

It took a period of 8 days to carry out the tests. During this time, both intrusion and authorized (identified by bracelets) incursions through the perimeter were generated. Figure 7 illustrates the alarm generated on the application of the security staff once the perimeter has been violated. The WSN-CAD surveillance application graphically shows two kinds of perimeter crossings: performed by a bracelet (authorized access) and intruder.

In this period, the energy consumption of the hardware components making up the virtual perimeter surveillance has been determined.

This study was focused on calculating the autonomy of our surveillance system, paying special attention to the perimeter nodes since replacing their batteries is a bit difficult: they are usually hung from lampposts or similar places that are not easily accessible. Such a problem for mobile nodes does not occur since they are completely accessible to users.

As previously mentioned, TelosB motes and Luminite TX500/40 PIRs are the two main hardware components of the perimeter nodes. Luminite TX500/40 PIRs are connected to TelosB motes through their GPIO pins. Each of those hardware elements has its own energetic characteristics (see tables 2 and 3), so consumption calculations have to be performed independently.

In order to calculate the autonomy of both TelosB mote and Luminite TX500 PIR according to the generated events

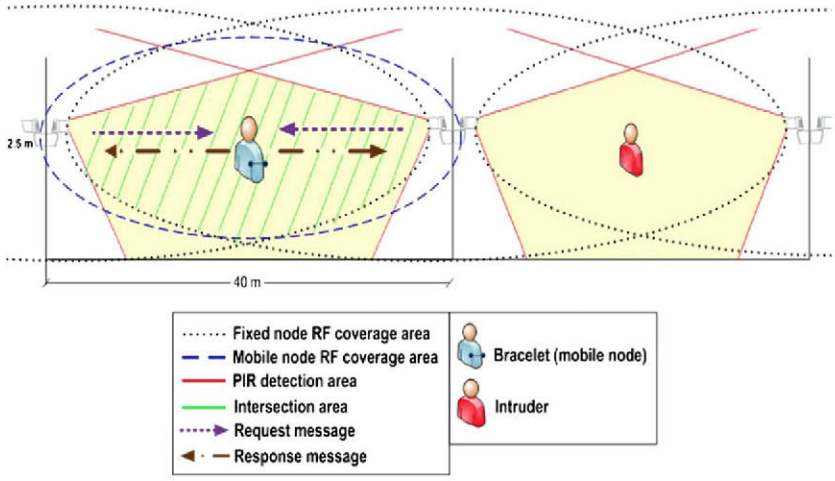

Figure 6. PIR sensor deployment conditions.

Figure 7. WSN-CAD surveillance application.

Table 2. Consumption of hardware execution modes.

Hardware component	Execution mode	Current consumption
TelosB mote	Tx mode (0 dBm)	25.3 mA
	Rx mode	23 mA
	Idle mode	21 μA
Luminite TX500/40 PIR	Stand-by mode	9 μA
	Alarm mode	20 mA

of presence during validation (see table 4), let us consider a balanced distribution of those events of presence between nodes that make up the virtual perimeter. In this manner, 42 events of presence are counted in total (per day and node), of which 13 events are of INTRUDER_PRESENCE and 29 events are of BRACELET_PRESENCE.

Table 3. Battery supply for hardware components.

Hardware component	Battery	Battery features
TelosB mote	4xAA (redesigned motes)	Lithium rechargeable 1.5 V; 2900 mAh
Luminite TX500/40 PIR	1xPP3	Lithium 9 V; 230 mAh

Table 4. System validation results.

	Use case	
Classification	Bracelet	Intruder
True positive (*tp*)	4277	1125
False positive (*fp*)	17	8
False negative (*fn*)	0	0

5.2.1. Luminite TX500/40 PIR autonomy analysis. When a Luminite TX500/40 PIR is excited because of a perimeter crossing, the PIR hardware turns from 'stand by' mode to 'alarm' mode. The 'alarm mode' of Luminite TX500/40 PIR activates for 3 s every time it is excited. The PIR thereby works in that mode almost 1 min per day, consuming 0.92 mAh according to energy data shown in tables 2 and 3. Therefore, the Luminite TX500/40 PIR can autonomously work for 251 days; it is equivalent to detecting approximately 10 542 events of presence.

5.2.2. TelosB mote autonomy analysis. Every time fixed nodes process an event of presence, TelosB motes need to send two messages via radio (see figure 2): first, a NODEID_REQUEST publication, and second, a PRESENCE event to identify the kind of detected presence. Eventually, if a NODEID_RESPONSE event is received from a bracelet, then a BRACELET_PRESENCE event is thrown to the gateway; otherwise, an INTRUDER_PRESENCE event is thrown. The node has to switch the RF transceiver on for 8 ms in order to transmit the two necessary messages (NODEID_REQUEST and PRESENCE event), and 4.3 ms

to receive a NODEID_RESPONSE event, if needed. Taking into account the TelosB mote energy characteristics as shown in tables 2 and 3, the mote consumption is 43.71 mAh per day. Originally, TelosB mote was equipped with 2 AA batteries but fixed TelosB motes were redesigned in order to increase their autonomy by enabling two more AA batteries. From the consumption per day previously obtained, fixed TelosB motes making up the virtual perimeter can thereby autonomously work for 265 days; this is equivalent to transmitting approximately 11 130 events of presence.

5.3. Performance evaluation

In this section, experimental results that evaluate the performance of the surveillance-agent system based on WSNs described in the previous section are presented.

Table 4 shows the results obtained during system validation. The results are classified into three categories. The first set of results, *true positive* (*tp*), refers to those events properly discerned by the node indicating who crossed the perimeter. During the validation test, 4277 bracelets and 1125 intruders were detected as true positive (i.e. bracelet nodes and intruders, respectively).

The second set of results, *false positive* (*fp*), indicates that (1) 17 bracelet accesses were detected as intruder, and (2) 8 intruder accesses were detected as bracelet. In the case of (1), it has been concluded that the false positive was caused by a deficient radio signal of either fixed node or of the bracelet (e.g. reflections, attenuations and interferences), which did not allow proper communication among bracelets and fixed nodes. It is then not possible to exchange messages that allow identification of the mobile node. In order to avoid this situation, the characteristics of deployment in order to optimize the performance of the PIRs have been modified. In the case of (2), false positive was due to an intruder crossing the perimeter when there was a bracelet in the radio coverage area of the fixed node.

Finally, *false negative* (*fn*) represents those events of presence that occurred inside the perimeter and that were not detected by the node. False negative was 0%; as in all cases an alarm was generated when the perimeter was crossed by either an intruder or a bracelet.

According to the data shown in table 4, the performance metrics defined in [15] have been adapted in order to determine both precision and recall of the system.

In the context of this work, precision indicates the percentage of detections properly classified from the total detections. Specifically, precision is the number of true positives divided by the total number of elements labelled as belonging to the positive class. Thus, precision is obtained by applying (1) that corresponds to 99%, which indicates that the system has a high degree of precision. This rate has been achieved through collaborating fixed nodes with mobile nodes:

$$\text{precision} = \frac{tp}{tp + fp}. \quad (1)$$

Regarding recall, it indicates the number of events correctly detected from those that should have been detected. Hence, the number of detected events of presence from the total occurred presence has been obtained by applying expression (2), which corresponds to 1. That has been so due to deployment, as explained in section 5.1, that allowed not only the detection of every unauthorized crossing, which is the major goal of our surveillance-agent system, but also the detection of every perimeter intrusion from authorized staff and patient crossings:

$$\text{recall} = \frac{tp}{tp + fn}. \quad (2)$$

5.4. Lessons learned

The work described in this paper is our experience with a pervasive surveillance agent based on WSNs in a practical application, and its evaluation through an actual deployment of motes. Several lessons have been learnt from the work performed in this research, which can be applied to making decisions during the development of a system related to pervasive surveillance. The following points are some remarks that could be useful to future researchers involved in the development and management of pervasive surveillance systems based on WSNs.

- The sensors for deployment have to be chosen considering the characteristics of coverage to be modelled.
- The geographical factors of the place that will be monitored for the detection of intrusions have to be taken into account.
- The number of required sensors has to be calculated in order to guarantee the expected security level from the sensed spatial density and the critical level of the monitored area.
- The set of information, which is extracted from data that is generated by the agent, allows determining the weaknesses of the coverage area and discovering vulnerabilities for hypothetical intrusion paths.

6. Conclusions and future research

The work described in this paper has presented our experience about developing a surveillance system using WSNs for practical applications and evaluating their deployment in the real world. A mechanism for controlling virtual perimeters using WSN that manage mobile nodes in a specific environment has been proposed. A deployment mechanism has been used in order to guarantee effective detection and an efficient use of motes, which operate in a low power consumption mode in periods when events are not received. In addition, the 'intelligence' of the agent has been distributed by using mobile nodes to discern who has caused the event of presence: the client, the sanatorium staff or the intruder. Moreover, our system has the capacity to detect more than one authorized person crossing the perimeter since the system is based on intelligent distribution supported by mobile nodes. This characteristic contributes in saving both processing resources and power consumption.

The deployment of this solution results in cost savings because cables are not required during installation. Therefore,

this kind of deployment could become more spatially dense than traditional approaches. Currently, those mechanisms play an important role in building confidence in our environment to ensure safety, becoming key elements for preventing multiple types of threats and allowing better quality of life for humans.

As future research, the manner how to integrate the agent in the formation of dynamic surveillance of virtual perimeters in runtime will be studied. Advanced context-aware applications could be developed from this improvement (e.g. from livestock control to baggage logistics). It is a research challenge, which could be solved by designing multi-sensorial surveillance systems that combine different data sources from diverse positional sensors (e.g. ultrasonic transducer, stereo vision, laser triangulation).

Acknowledgments

The work presented in this research paper has been partially funded by the VI Framework Programme of the European Union within the μSWN 'Solving Major Problems in Micro sensorial Wireless Networks' project (code: TSI-034642). The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] García-Hernández C F, Ibargüengoytia-González P H, García-Hernández J and Pérez-Díaz J A 2007 Wireless sensor networks and applications: a survey *Int. J. Comput. Sci. Netw. Secur.* **7** 270

[2] Garcia M L 2008 *Design and Evaluation of Physical Protection Systems* (Portsmouth, NH: Butterworth-Heinemann) pp 86–8

[3] García A B, Martínez J F, López J M, Prayati A and Redondo L 2008 *Problem Solving for Wireless Sensor Networks (Computer Communications and Network Series)* (London: Springer) pp 177–207

[4] Bounabat B, Romadi R and Labhalla S 1999 Designing multi-agent reactive systems: a specification method based on reactive decisional agents *Approaches to Intelligence Agents* (Berlin: Springer) p 775

[5] Romadi R and Berbia H 2008 Wireless sensor network a specification method based on reactive decisional agents *3rd Int. Conf. on Information and Communication Technologies: From Theory to Applications (ICTTA 2008)* pp 1–5

[6] Frantisek Z Jr and Frantisek Z 2008 Simulation for wireless sensor networks with intelligent nodes *10th Int. Conf. on Computer Modeling and Simulation (UKSIM 2008)* pp 746–51

[7] Wang X, Bi D-W, Ding L and Wang S 2007 Agent collaborative target localization and classification *Wirel. Sensor Netw. Sensors* **7** 1359–86

[8] Rogers A, Corkill D D and Jennings N R 2009 Agent technologies for sensor networks *Intell. Syst. IEEE* **24** 13–7

[9] Byunghun S, Haksoo Ch and Hyung S L 2008 Surveillance tracking system using passive infrared motion sensors in wireless sensor network *Int. Conf. on Information Networking (ICOIN 2008)* pp 1–5

[10] Li Y Y and Parker L 2008 Intruder detection using a wireless sensor network with an intelligent mobile robot response *Proc. IEEE SoutheastCon (Huntsville, AL, USA)* pp 37–42

[11] Zappi P, Farella E and Benini L 2007 Enhancing the spatial resolution of presence detection in a PIR based wireless surveillance network *IEEE Conf. on Advanced Video and Signal Based Surveillance (AVSS 2007)* pp 295–300

[12] Singh J, Madhow U, Kumar R, Suri S and Cagley R 2007 Tracking multiple targets using binary proximity sensors *Proc. 6th Int. Conf. on Information Processing in Sensor Networks (IPSN '07) (Cambridge, MA, USA)* (New York: ACM) pp 529–38

[13] Moghavvemi M and Lu Ch S 2004 Pyroelectric infrared sensor for intruder detection *TENCON 2004 IEEE Region 10 Conf.* vol 4 pp 656–9

[14] Boonma P and Suzuki J 2009 Toward interoperable publish/subscribe communication between sensor networks and access networks *IEEE Consumer Communications and Networking Conf.* pp 1–6

[15] Yuan Y L and Parker L E 2008 Detecting and monitoring time-related abnormal events using a wireless sensor network and mobile robot *IEEE /RSJ Int. Conf. on Intelligent Robots and Systems (IROS 2008)* pp 3292–8