MOVEDETECT – Secure Detection, Localization and Classification in Wireless Sensor Networks

Benjamin Langmann[1], Michael Niedermeier[2], Hermann de Meer[2],
Carsten Buschmann[3], Michael Koch[4], Dennis Pfisterer[5], Stefan Fischer[5],
and Klaus Hartmann[1]

[1] Center for Sensor Systems (ZESS), University of Siegen, Paul-Bonatz-Str. 9-11,
57068 Siegen, Germany
{langmann,hartmann}@zess.uni-siegen.de

[2] Department of Computer Networks and Computer Communcation,
University of Passau, 94032 Passau, Germany
{michael.niedermeier,hermann.demeer}@uni-passau.de

[3] Coalesenses GmbH, Maria-Goeppert-Str. 1, 23562 Lübeck, Germany
buschmann@coalesenses.com

[4] SINUS Messtechnik GmbH, Föpplstr. 13, 04347 Leipzig, Germany
michael.koch@sinusmess.de

[5] Institute of Telematics, University of Lübeck, 23562 Lübeck, Germany
{pfisterer,fischer}@itm.uni-luebeck.de

Abstract. In this paper a secure wireless sensor network (WSN) developed within the MOVEDETECT project is presented. The goal of the project was to design, implement and demonstrate a secure WSN for the protection of critical infrastructure. In order to provide a reliable service, the system must detect any kind of tampering with the sensor nodes, prevent eavesdropping and manipulation of the communication as well as detect, track and classify intruders in the protected region. Therefore based on previous experiences, a real-world WSN was developed, which addresses practical issues like water proofing, energy consumption, sensor deployment and visualization of the WSN state, but also provides a unique security concept, a interesting combination of sensors and sophisticated sensor data processing and analysis. The system was evaluated by examining firstly the sensors and the sensor processing algorithms and then conducting realistic field test.

Keywords: Wireless sensor network, Detection, Security, Functional safety, Networking.

1 Introduction

Wireless sensor networks (WSN) have attracted attention of many researches of different disciplines in the past driven by the increasing availability of microprocessors with wireless communication. In general, a WSN consists mainly of a

S. Balandin et al. (Eds.): NEW2AN/ruSMART 2013, LNCS 8121, pp. 284–297, 2013.

number of sensors nodes. However, management and routing nodes are possible as well and hence different network structures have been proposed, e.g. mesh or hierarchical structures. Usually, each sensor node has only very limited resources (computational power, energy supply, memory, communication bandwidth) and its purpose is the decentralized and reliable acquisition and transmission of data. Higher reasoning is either performed by dedicated processing units or outside the WSN. The applications of WSN are located mostly in the safety and security area ranging from military and police tasks to structural and health monitoring.

Within the MOVEDETECT project a demonstrator for a real-world WSN was developed to be used for the protection of critical infrastructure or small key areas and its design, implementation and evaluation is described in this paper. In addition to the practical applicability which includes water proofing, a low energy consumption and methods for the sensor deployment, the system must provide secure and reliable communication and of course accurate detection, tracking as well as classification of intruders. Therefore, a combination of techniques to ensure the systems integrity and confidentiality were applied and a sophisticated distributed approach for sensor data processing and analysis was developed. In addition, reporting and logging mechanisms allow users to constantly monitor activities inside the WSN, both in real-time and time-delayed. Moreover, the usability of the system is not impaired by the inherent complexity of the WSN, as it can be configured and operated from a central command center. The combination of these features creates a uniquely secure, flexible and usable system.

The remainder of this paper is structured as follows: Section 2 introduces related work on WSNs to protect critical infrastructure. Section 3 details the requirements of the proposed system. Section 4 covers all aspects of the system development and Section 5 demonstrates the abilities of the deployed sensors. Section 6 discusses the results of two field tests and the paper closes with a conclusion and an outlook of possible future work in Section 7.

2 Related Work

The work related to the presented project is manifold, as MOVEDETECT combines multiple research fields, e.g. communication security, functional safety but also energy efficient communication and the fusion of WSN data. Therefore, this section covers firstly the state-of-the-art in conventional (non-networked) solutions for secure infrastructures. Secondly, related work on systems that rely on wireless communication and work in critical environments is described. Finally, recent projects that partly cover the goals of MOVEDETECT are introduced and compared.

Conventional solutions to secure critical infrastructures range from very simple setups involving mechanical barriers, like doors, fences and trenches or security personnel [1] to complex – however non-networked – equipment, including e.g. passive infrared (PIR), sound and seismic sensors or video surveillance. While these devices allow detecting certain influences, they lack the possibility to cooperatively analyze a situation [2], as no data transfer between them is possible.

However, over the last years, advances in the area of networked sensor technologies have opened up new application areas for these sensor devices [3]. With new technological paradigms, like the Internet of Things (IoT) or Automated Living, the use of WSNs is rapidly growing as networked sensors are vital in these scenarios. However, as future technologies more and more depend on sensor networks, the requirements for these – now critical infrastructures – rise in a similar way, especially in the fields of security and safety. An already realized example in this area is the SmartSantander project, where more than $10,000$ IoT devices are deployed to build a so-called "Smart City". In such scenarios, strict security requirements apply, as personal and critical information is transferred. While there are research efforts in the areas of access protection, secure reprogramming over wireless connections and secure communication, a complete security solution for a wireless network does not yet exist. This example already characterizes several important aspects of WSN security: Due to the usage in unsupervised or even hostile environments while performing critical tasks, it is important to provide measures ensuring integrity and confidentiality of data (communication security) and protection of the devices against malfunctions that either occur randomly or due to tampering [4,5].

FleGSens [6] is a project for secure area monitoring using WSNs. The system is able to detect movement in critical areas and considers authenticity and data integrity of alarm signals. Other security issues, like jamming and functional safety, are not addressed. FleGSens uses a flat network hierarchy, which limits system scalability due to message collision. The used detection algorithm only considers the position of trespassers and – in contrast to MOVEDETECT – does not include a classification algorithm.

The POmSe ("Personen- und Objektdetektion mit mobilen Sensoren") project [7], evaluates the general applicability of WSNs for the protection of critical infrastructures and environments with a focus on the applicability for trespasser detection due to their inherent advantages compared to conventional security techniques (like e.g. security doors, fences, etc.). In contrast to MOVEDETECT, POmSe performs a general analysis of WSNs including the required security features in critical applications. However, the development, application and evaluation of a WSN is not included in the project, neither is a classification of trespassing objects performed.

A complementary project, named "Personen- und Objekterkennung basierend auf Trittschall (POT)" [8], evaluates the suitability of seismic sensors for the detection, classification and localization of humans and animals. It turns out that a reliable detection algorithm can be provided whereas the exact spatial localization of a person strongly depends on the environmental conditions as, e.g. the type and humidity of the surrounding soil.

In [9] a WSN for security in medical environments concentrating of high reliability and low delays is presented. A WSN to support safety in the transport domain is outlined in [10]. Here the cost is the most important design objective in order to increase the acceptance of the WSN. An approach focusing on the fusion of different sensors (underground, above ground and air) is introduced in [11] for border control. Moreover, in [11] an approach aiming at the detection of intrusions at borders is introduced. Lastly, in [12] methods to reduce the power consumption in WSNs including cameras and PIR sensors are discussed.

As shown here, the main difference between the presented related works is the implementation of a comprehensive security solution covering all necessary aspects, while still maintaining a high usability despite the high system complexity. In the following, first the requirements that originate from the usage scenario of the MOVEDETECT system are presented before the system development is described.

3 Requirements

The main functional goals of the system are defined by three tasks of the WSN: i) detection, ii) localization including tracking and iii) classification of objects in a predefined area. The system must be able to detect and locate persons or cars with certain accuracy. In our case, all values for deviations or timings are chosen in a way that the goal on the user's side – which is to be able to organize a well-directed response to a penetration of the surveillance area – is possible. For the given case, a deviation of ≤ 5 meters is therefore considered acceptable.

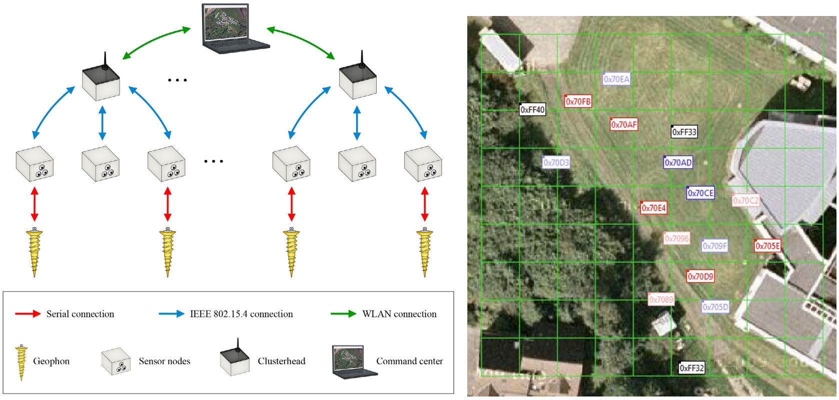
In addition, it is required to calculate the trajectory of the trespassing object to indicate its direction. In order to provide not only accurate but also timely data, the system is required to fulfill certain real-time criteria. The delay between object-entry and the signaling of the event to the user was fixed at a maximum delay of 3 seconds. Due to the special hardware used in WSNs, several additional system requirements have to be fulfilled. Among them is primarily a reliable, scalable and efficient communication architecture ensuring that all events occurring inside the monitored area are not only registered, but also that the messages of these events are transferred reliably to the base station [13].

The security of the system is of major importance, especially when the unattended operation of the system is taken into account. The system's overall security concept therefore comprises not only IT security measures but also functional safety aspects. It is required to protect the system from coincidental or targeted physical damage and hardware failures. Additionally, energy efficiency has to be carefully considered in both the hardware and software design, because the sensor nodes are powered with batteries and the intended operating time is two weeks.

4 WSN System Design

This section presents the general structure of the system to give an overview of how MOVEDETECT works. As depicted in Fig. 1a, the system is based on a hierarchical structure that consists of a single command center, several clusterheads on the intermediate level and for each clusterhead multiple sensor nodes on the bottom level. In the prototype system, which is described later on, a total number of 100 sensor nodes is used (10 clusterheads with 10 sensor nodes each). Due to the system's scalability, the system can however also be employed using a much larger number of nodes.

The sensor nodes are equipped with different sensor combinations and are described in the following section. An evaluation of the individual sensors can be found in Section 5.



(a) MOVEDETECT system structure (b) Visualization

Fig. 1. Structure of the MOVEDETECT WSN and the visualization software Spyglass

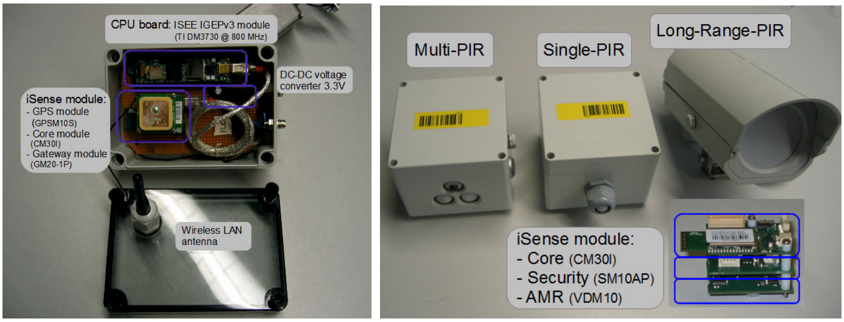
4.1 Hardware Design

In this section, the hardware concept is described in the order of the previously shown three levels: command center, clusterheads, and sensornodes.

The command center aggregates data from the clusterheads and displays the information to the user (cf. Fig. 1b). This information is presented using the detection algorithms described in Section 4.3 and delivered to a network visualization software called *Spyglass* [14]. The existing open-source Spyglass was extended to have a control window that allows to send commands to the network, e.g. restarting of nodes, sending messages to a number of nodes, or reprogramming nodes.

Each clusterhead consist of two components: an embedded-PC board (ARM-based CPU with 800 MHz, 512 MB RAM, 512 MB flash memory, power requirement of about 1.5 W) and an iSense sensor node. The embedded PC maintains the WiFi connection to the command center, pre-processes sensor data and performs network management tasks. In order to communicate with the sensor nodes, an iSense sensor network device was attached to the CPU board as depicted in Fig. 2a.

Several different configurations of sensor nodes have been designed, which differ in the type of attached sensors and housing (Fig. 2b) but all include several iSense modules. The Core Module includes a Jennic JN5148 32-bit RISC controller and an IEEE 802.15.4 compliant radio interface. The radio chip operates



(a) Clusterhead

(b) Sensor nodes

Fig. 2. Hardware components of the WSN

at a frequency of 2.4 GHz, offers 16 different radio channels, provides a data transfer rate of 250 kB/s and includes a hardware AES engine as well as an ultra-stable real-time clock (RTC) (typical 6 ppm). The second type of housing contains a long-range Siemens IS392 PIR sensor and an accelerometer.

In the sensor network, the previously described four types of sensors are utilized for various purposes. The general detection of activity in the observed area is performed by PIR sensors, which can be differentiated into three types: Single-PIRs (Panasonic AMN34111) with a range up to 10 m, Multi-PIRs (AMN31111 + 2 × AMN33111) with a range of approximately 5 m and Long-Range-PIRs (Siemens IS392) with a range up to 50 m. With the Multi-PIRs, the directions of moving objects can be estimated and Long-Range-PIRs play a significant role in the detection of new objects entering the surveillance area. Fig. 3 shows detection results for these different PIR sensors.

The second type of sensors used for detection purposes are geophones. They are comprised of three seismic capsules (SM-24, Sensor Nederland) in an orthogonal arrangement, an analog signal conditioning part and a microcontroller-based (ARM-Cortex M3 MCU) signal processing unit. The complete geophone is housed in a protection enclosure and is connected to the sensor node via a communication cable that also provides the required power. For a sufficient coupling to the ground, a soil drilling tool in combination with a screw-shaped housing is used.

The iSense Vehicle Detection Modules are used for object classification, since only moving metallic objects influence their measurements. They are based on a 2-axis Phillips KMZ52 anisotropic magneto-resistive sensor bridge that is combined with two amplifier stages as well as circuitry for de-gaussing and earth-magnetic field compensation. It exploits the fact that large ferro-magnetic objects distort the earth-magnetic field to detect such objects by observing field changes. To achieve a detection range of more than 5 m, it amplifies the bridge output by a factor of approximately $40,000$ and features a sensitivity of 786.2 mV/(kA/m) at a bandwidth of 1 kHz. Because the module typically has a current consumption of $20 - 25$ mA during operation, it is activated after observing PIR sensor events within less than 180 ms.

The last sensor is an accelerometer, which is part of every sensor node. Its sole purpose is the detection of physical tampering with the sensor nodes, since even small movements of the device trigger the accelerometer.

4.2 Communication and Security

The communication and security architecture of the WSN is only outlined due to its complexity. The sensor nodes communicate based on the energy-efficient IEEE 802.15.4 standard with their associated clusterhead while applying adaptive frequency hopping. In order to prevent messages from being forged or manipulated, the message payload is encrypted using the AES-CBC-128 cipher, which is supported by a crypto co-processor available in all sensor nodes, which makes it very fast and energy-efficient. In addition, a timestamp, a CBC-MAC AES, and a sequence number is added to the payload. These are used to achieve resistance against replay attacks, delayed massage sending, or manipulation of the message order. The system also uses an advanced key management approach. The clusterheads pre-process and compact the data coming from the sensor nodes and communicate with the command center via TCP/IP-based connections over WiFi.

The integrity of the WSN is ensured on all levels. The sensor nodes and the clusterheads analyze the sensor data as well as test their CPU, RAM and firmware at start-up for manipulations, send heard beat messages regularly and observe their accelerometer.

4.3 Detection, Classification and Tracking of Objects

In order to achieve a robustness and reliability suitable for long term surveillance, the detection, tracking and classification methods are implemented in a simple yet effective way. After the WSN is started, the detection algorithm first remains in a waiting state, until a significant amount of sensor events are registered, which indicates an object entering the area. If the amount of events remains low, it is assumed that these are caused by random noise or other sources like wind. Additionally, it is required that there is a local accumulation of events. The amount of random noise depends on the sensor type as well as on other factors like the position of the sensor, the time of the day and the weather conditions. If the sensor data satisfies these conditions, it is inferred that an object is inside the surveillance area and an initial position is determined. Afterwards, only sensor events in a vicinity of the current position of the detected object are handled, until the object leaves the surveillance area. Each sensor event suggests possible locations of the object. For PIR sensors this is a cone of a specific length whereas for all other sensors, this is a radial symmetric area around the sensor node with a certain radius. The current position of the object is then determined by averaging the suggested positions of the sensor events while factoring in the previous position of the object.

The tracking simply consists of a concatenation of the determined object positions. The classification of the object (person, person carrying metal object, car or unknown) is performed by an analysis of the AMR and geophone events. Magnetic sensor events in the vicinity of the object suggest a car or a motorbike and geophone events indicate footsteps, but there need to be an accumulation of these events, which exceeds the noise level. Experiments show that the AMR sensors are surprisingly affected by wind (possibly due to movement of cables or the sensor node itself). An object in the surveillance area is considered to have left this area if the last known position is near the border of the area and further sensor events are below the detection level for some time.

5 Sensor Evaluation

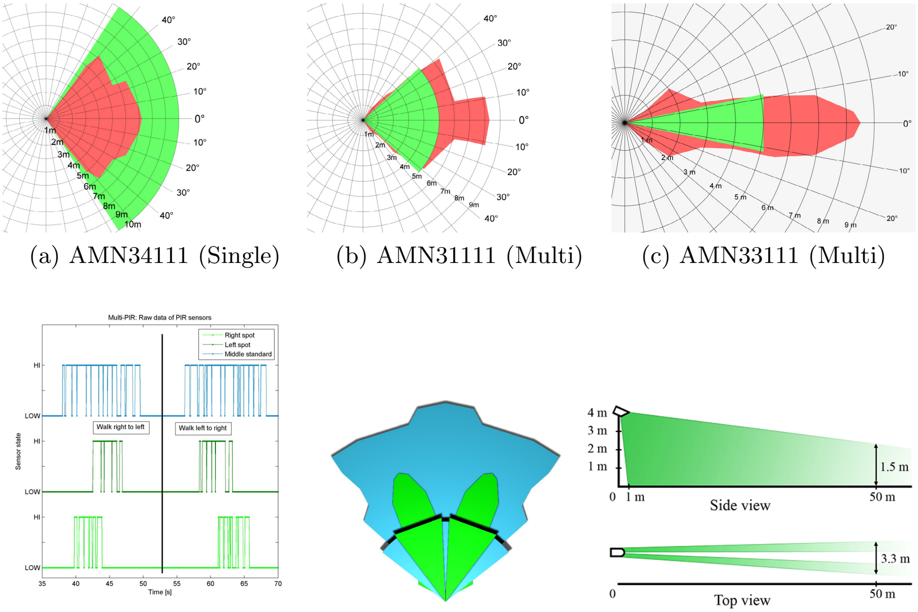
The sensors employed by the sensor nodes need to be analyzed in order to achieve a desired quality of the surveillance, since datasheets often do not provide information in the way or detail required. Additionally, the preprocessing algorithms of the geophones and PIR sensors need to be evaluated and characterized. In the following an excerpt of the sensor related experiments is given.

For the PIR sensors, the region in which objects produce sensor events must be known in order to perform a localization of intruding objects. It is common to conduct simple walking and driving tests for this purpose, for which a path is defined and repeatedly driven or walked, respectively. In Fig. 3 the results for normal walking are given. Green marks the detection area specified in the datasheet, while red marks the region in which sensor events actually occur in practice. In Fig. 3e the joint detection region of a Multi-PIR sensor node is visualized. Here green marks the region where the two spot type PIR sensors (AMN33111) are sensitive and blue the region of the standard PIR type (AMN31111).

In Fig. 3d, the exemplary behavior of a Multi-PIR sensor node is shown for a walk-by test, in which a person crosses the detection area from right to left with normal walking speed and vice versa. It was found that the direction of the object can be determined reliably simply using the 3-PIR sensors included in a Multi-PIR sensor node. To do so, the time at which each PIR sensor activates is measured and compared. This is not possible using Single-PIR sensors, but promises more accurate localization and tracking of objects.

In order to be able to detect intruders and therefore to provide a basis for tracking, a robust algorithm is required, which filters the incoming signal at the geophone to isolate those representing human footsteps. To overcome the problem of varying environmental conditions (mostly soil quality and humidity as well as ground coverage with plants) and of disturbing seismic noise, a procedure with an adaptive threshold was developed and implemented. It is based on the so-called “sta/lta - picking”, which is used in earthquake location scenarios [15]. The decision whether there is an event is made by comparing the ratio of a short and a long time average of the seismic signal with an empiric constant. By introducing an adaptive constant an accommodation to varying conditions is achieved. An example is shown in Fig. 4a.

The output event of a geophone reliably signals a person within the detection range. By calculating the geometric center of gravity of one or more geophones



(a) AMN34111 (Single)

(b) AMN31111 (Multi)

(c) AMN33111 (Multi)

(d) Multi-PIR response

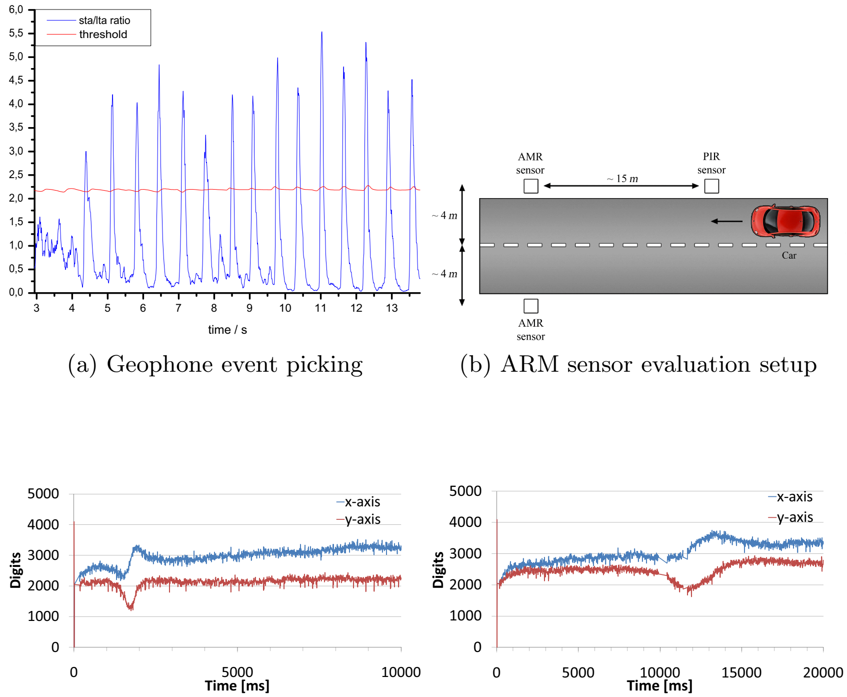
(e) Multi-PIR range

(f) Long-Range-PIR: IS392

Fig. 3. Experimental evaluation of the detection ranges of the different PIR sensor types. Green marks the detection area specified in the datasheet and red the actual detection area for walks with normal speed.

reporting events with similar timestamps, it is possible to locate (and track) an intruder within the sensor network.

For the vehicle detection based on the AMR sensors, the activation procedure, the sensor range and detection algorithms were tested prior to the implementation of the final system. The according test setup is shown in Fig. 4b. Two sensor nodes with a vehicle detection module are positioned at opposite sides of a road in a distance of 8 m from each other. A sensor node with a PIR sensor is placed next to the road 15 m before the AMR nodes. A vehicle then passes the installation at speeds of 50 km/h or 5 km/h, respectively. Once a sensor event of the PIR sensor is triggered, the sensor node sends a wireless message to the two AMR sensor nodes. This simulates a delay as it would occur in the final installation, where the communication would work via the clusterhead, instead of directly between the sensor nodes. Upon reception of that message, the AMR nodes activate their vehicle detection modules, de-gauss and calibrate the sensors to compensate for the static earth magnetic field, start sampling the two sensor module channels, and forward the live data to a forth sensor node that is connected to a PC to record timestamps and sensor data for all three nodes.



(a) Geophone event picking

(b) ARM sensor evaluation setup

(c) AMR sensor data for a fast car

(d) AMR sensor data for a slow car

Fig. 4. Results of the geophone event picking algorithm for footstep detection, test setup for the AMR sensor evaluation and AMR sensor data for fast and a slow car passing by

Fig. 4c shows the sensor readings of one of the AMR nodes for a vehicle speed of 50 km/h. The time axis of the diagram is set to start at 0 at the time when the PIR sensor event occurred. The y-axis shows the sensor signal as ADC digits, where 1 digit represents 0.59 mV or a field change of 786.2 mV/(kA/m). It is visible that the sensor signal starts around $t = 0.2$ s, as the calibration process commences before that.

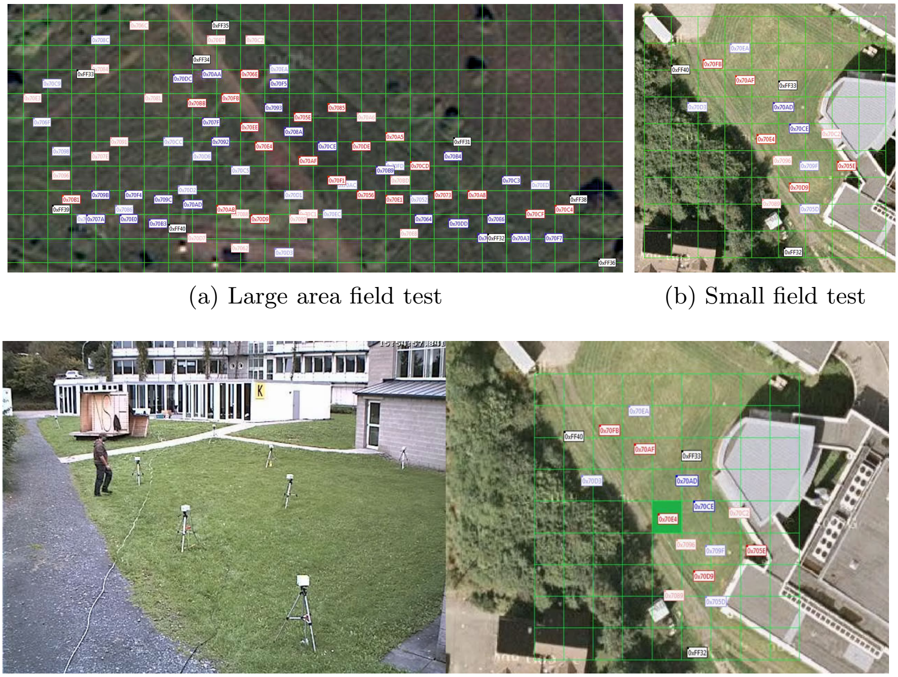
The AMR sensor starts up and calibrates fast enough to be in normal operation by the time the vehicle passes by the sensor (characteristic signal shape between $t = 1$ s and $t = 2.3$ s). Consequently, the system would still work properly if the PIR sensor is placed at a distance of only 3 m to the AMR sensors.

Figure 4d shows the sensor readings of one of the AMR sensors for a vehicle speed of 5 km/h. As expected, the signal occurs much later, between $t = 9$ s and $t = 16$ s. The challenge is to develop a detection algorithm that detects vehicles from both the signal patterns, while still being robust against the signal drift that occurs when no vehicles passes.

6 Field Tests of the WSN

In the course of the project MOVEDETECT two main field tests of the whole WSN were conducted. Fig. 5a shows an illustration of the first testing terrain painted by the Spyglass application and it consisted of 100 sensor nodes and 10 clusterheads organized in 10 clusters, where one cluster was reserved for energy consumption monitoring. The surveillance area was a field with a path through and had a maximum width of 125 m and a length of 50 m at the largest extend. The nodes were distributed arbitrarily in distances of 5 m to 10 m from each other. After this initial setup, those 10 sensor nodes nearest to a clusterhead form one sensor cluster.

After the WSN was fully configured, several aspects of the whole system and their interactions had to be verified: First, the general system functions, like network connectivity, message sending, relaying and receiving as well as displaying of system events at the command center. Second, the detection, localization and classification had to be assessed and third a security evaluation to test the WSN's security and safety features was performed.



(a) Large area field test

(b) Small field test

(c) Example of a walking test

Fig. 5. Spyglass renderings of the maps for the field tests performed within the scope of the MOVEDETECT project (grid size is 5 m × 5 m)

Table 1. Event symbols and classification colors in the visualization using Spyglass

Symbol	Meaning	Symbol	Meaning
Geo	Geophon event	Mag	AMR event
LPIR	Longrange-PIR event	MPIR	Multi-PIR event
⚠	Accelerometer event	SPIR	Single-PIR event
⚠	Node communication issue	✖	Node failure
🔋	Energy drain alert		
Color	**Classification**	**Color**	**Classification**
🟩	Human	🟦	Vehicle
🟪	Human with metal object	🟨	Unknown

In the second field test of the WSN a total number of 17 sensor nodes partitioned in 2 clusters were utilized. The surveillance area was a small field surrounded by bushes and buildings with a path going through it. Again, a set of walking and driving detection test were performed.

In order to verify the functions assessed in the field trials, multiple verification techniques were used. For the detection, localization and classification, a Mobotix IP-camera was used in combination with the Spyglass user interface. By doing so, it is possible to document if objects were on the one hand detected and localized and on the other hand if the classification works correctly and the real-time requirement of the system is fulfilled. As an example, Fig. 5c shows one of the walking tests done during the second field trial. As the figure depicts, the person walking on the grass was detected and classified correctly, which is indicated by the green field in the middle of the grid. Similar results were also achieved for other walking styles, like crawling or running, as well as tests with other trespassing objects, e.g. cars (the classification changed in those tests respectively). Furthermore, it was evaluated if a classification of a person carrying metal objects is possible, which would be especially useful to detect weapons like firearms. While the detection works with large ferromagnetic objects, like e.g. fire extinguishers or crowbars, as long as the distance between the object and the sensor node is ≤ 2 m, it is not possible for firearms. This is due to the low mass of ferromagnetic parts in modern firearms, resulting in a very low amplitude of the AMR sensor's readings, which does not trigger an event. All classification grid colors and symbols used in Spyglass are shown in Table 1.

Moreover, the varying weather conditions during the field trials, ranging from sunshine to thunderstorms, proved the system's adaptability and its resistance against hazardous environments.

7 Conclusion and Future Work

The MOVEDETECT system is a WSN solution capable of monitoring and securing critical infrastructures as was demonstrated in this paper. It provides security by using different sensors to detect, locate, track and classify various types of trespassers while operating in a secure and safe way. This is achieved by employing several functional safety and security features to guarantee high levels of confidentiality, integrity and availability. The system operates in real-time using efficient detection algorithms and a network hierarchy. MOVEDETECT enables its user to keep track of the events inside the sensor network by logging all events in a database for later analysis and, at the same time, reporting it in real-time to the command center. Moreover, the system uses a scalable, hierarchic network structure making it easily extendable for a wider area, if necessary. To adapt the system to changing usage conditions, it is possible to dynamically reconfigure the whole system in the field by using an over-the-air-programming (OTAP) function. This unique combination of features makes the system ideal for unattended operations in hazardous environments.

While the described features already enable a secure detection of trespassing objects, additional hardware, e.g. video cameras, could be included in the concept in order to document trespassers in future work. These devices could be integrated as a type of additional sensor into the existing sensor nodes and be activated if an object is detected by the other sensors. Of course, these new nodes would need to be carefully analyzed, especially their energy consumption and network traffic generation would need to be carefully balanced with the achievable visual quality. Another possible method is to treat the sensor nodes with visual capabilities separately and not to integrate them into the existing network hierarchy. The visual data would then be sent directly to the command center using WiFi.

Acknowledgments. The work was funded by and organized in cooperation with the German Federal Office for Information Security (BSI - "Bundesamt für Sicherheit in der Informationstechnik") within the project MOVEDETECT. We also thank the Federal Police of Germany, in particular Mr. Vehrkamp, for their support and numerous constructive discussions.

References

1. Critical Infrastructure Assurance Office: Practices for securing critical information assets (January 2000)
2. Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: a scalable and robust communication paradigm for sensor networks. In: Proceedings of the ACM Mobi-Com 2000, Boston, MA, pp. 56–67 (2000)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38, 393–422 (2002)

4. Roman, R., Zhou, J., López, J.: On the security of wireless sensor networks. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3482, pp. 681–690. Springer, Heidelberg (2005)
5. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Communications of the ACM 47(6), 53–57 (2004)
6. Rothenpieler, P., Krüger, D., Pfisterer, D., Fischer, S., Dudek, D., Haas, C., Zitterbart, M.: Flegsens – secure area monitoring using wireless sensor networks. In: Proceedings of the 4th Safety and Security Systems in Europe (2009)
7. Bonitz, F., Ghobadi, S.E., Hartmann, K., Hauff, H., Herrmann, R., Kargel, C., Löpprich, O.E., Heckmann, D., Maisch, M.M., Seidl, A., de Meer, H., Ruser, H., Sachs, J., Wenzl, K.: Personen- und objektdetektion mit mobilen sensoren - abschlussbericht zum archbeitspacket 3 (teil b) - bericht zum meilenstein 5. End report (September 2010)
8. Koch, M., Hubert, C.: Personen- und objekterkennung basierend auf trittschall (pot). Technical report (2011)
9. Kaseva, V., Hämäläinen, T.D., Hännikäinen, M.: A wireless sensor network for hospital security: from user requirements to pilot deployment. EURASIP J. Wirel. Commun. Netw. 2011, 17:1–17:15 (2011)
10. Bohli, J.M., Hessler, A., Ugus, O., Westhoff, D.: A secure and resilient wsn roadside architecture for intelligent transport systems. In: Proceedings of the First ACM Conference on Wireless Network Security, WiSec 2008, pp. 161–171. ACM, New York (2008)
11. Sun, Z., Wang, P., Vuran, M.C., Al-Rodhaan, M.A., Al-Dhelaan, A.M., Akyildiz, I.F.: Bordersense: Border patrol through advanced wireless sensor networks. Ad Hoc Netw. 9(3), 468–477 (2011)
12. Magno, M., Marinkovic, S., Brunelli, D., Benini, L., Popovici, E.: Combined methods to extend the lifetime of power hungry wsn with multimodal sensors and nanopower wakeups. In: 2012 8th International on Wireless Communications and Mobile Computing Conference (IWCMC), pp. 112–117 (2012)
13. Estrin, D., Govindan, R., Heidemann, J., Kumar, S.: Next century challenges: Scalable coordination in sensor networks. In: Proceedings of International Conference on Mobile Computing and Networks (MobiCom 1999), Seattle, WA, USA (August 1999)
14. Institute of Telematics, University of Lübeck, G.: Spyglass, a modular and extensible visualization framework for wirelesssensor networks (2006), `https://github.com/itm/spyglass`
15. Havskov, J.: Instrumentation in Earthquake Seismology. Modern Approaches in Geophysics. Springer (2004)