The use of Secure Wireless Sensor Networks to Control and Protect Critical Infrastructure

Milan Stanojević[1], Petar Spalević[2], Ivan Milovanović[3], Saša Stanojčić[4]

Abstract — **Critical infrastructures are attractive targets for attack by unauthorized persons with hostile intentions. Wireless sensor networks with modern communications and sensor technology can give the ability to detect unwanted effects. Proper design and structure of this network can provide a high level of protection of critical infrastructure, with a focus on early detection within the monitored zone. This paper will be presented elements of a wireless sensor network and how it can be optimally used in the control, monitoring and protection.**

Keywords — **Critical infrastructure, Wireless sensor networks, Detection, Security, Scalability.**

I. Introduction

The level of threat to critical infrastructure from attacks of various terrorist, criminal or activist groups in recent years has increased significantly, and therefore they must be adequately secured. The term "critical infrastructure" has not yet received its official definition in Serbia. However positive global consulting practice in this field, we can come to the fact that the term "critical infrastructure" refers to assets and property, which is essential for the everyday functioning of social, economic, political and cultural system of a country [1]. To achieve success in such a demanding enterprise it is necessary that use modern information technology. This technology must be based on modern sensors and sensor systems, with advanced analysis of data obtained from the sensors and their fusion [2]. As a logical choice to solve the problem of this kind of imposed wireless sensor networks (*Wireless sensor network* - WSN). These networks due to its characteristics: agility, self-organization, scalability, mobility, bidirectional communication, autonomy and large number of various types of sensors stand for an intelligent control system [3]. The objective of this paper is to present the conceptual design of the design of such a control system whose role is to protect critical infrastructure. The work is structured in the following sections: Section 2 briefly explains the elements of WSN and a goal that must be achieved on the basis of user requirements; Chapter 3 presents a method for the realization of solutions, its functions, network elements, problems and solutions related to safety and the flow of data, along with a brief overview of the problem of energy supply; Chapter 4 briefly points to the essential requirements in the implementation of the proposed solution and conclusion of work.

[1]Milan Stanojević – University Singidunum, 32 Danijelova str., 11000 Belgrade, Serbia, E-mail: milan.stanojevic.16@singimail.rs

[2]Prof. PhD Petar Spalević – Faculty of engeneering, 7 Kneza Milosa str., 38220 Kosovska Mitrovica, Serbia, E-mail: petar.spalevic@pr.ac.rs

[3]Ivan Milovanović, University Singidunum, 32 Danijelova str., 11000 Belgrade, Serbia, E-mail: imilovanovic@singidunum.ac.rs

[4]Ms. Prof Saša Stanojčić, High Technical School of Telecommunication, 16 Zdravka Čelara str., 11000 Belgrade, Serbia, E-mail: stanojcic.sasa@gmail.com

II. Analysis Required Characteristics of the System

A wireless sensor network consists of a large number of small and inexpensive sensor nodes, with minimal computing power and energy consumption. The main objective of the network is to listen, feel, act and send information from their environment to the unit for data collection (Data Sink), which processes them [4]. The system must be autonomous and without the need for excessive maintenance and the presence of technical staff. In order to exercise its primary security feature inevitably imposes a requirement that the system must be secure. Autonomy in the absence of technical personnel opens a lot of opportunities to attack the system, such as tamper breach, physical manipulation and compromising of sensor nodes. To achieve basic functions of the system it is necessary for it to incorporate a single security concept, which consists of a secure communication within the network, mechanism that will give the functional safety during operation and self-protective function. The idea is that the system its basic function defined by three main tasks: (1) to achieve a detection, (2) to achieve the localization and (3) to provide a classification of the object in a monitored area [3][6]. Due to the limited access to the energy supply, energy efficiency of the system must be carefully planned, both in hardware and in software design. This is especially important if one considers that node devices in the network should have the ability to communicate with each other. All mentioned characteristics of the system should be integrated so that they represent a security concept that should guarantee the confidentiality, integrity and availability of wireless sensor networks at any time [5]. Besides the possibility of creating reports and recording events (incidents), the system should allow the user to supervise the activities of the network, configuration and management from a single command center. Only in this way, the network will be secure, flexible and usable to a given situation, to respond at the required conditions.

III. Proposal Design and Network Architecture

The topology of wireless sensor networks is hierarchically arranged and dynamically self-organized network of equal

nodes. They are connected to different types of sensors, which thus form a single sensor node (*SN-Sensor Node*). These nodes are hierarchically organized into sets or groups of higher levels, called clusters (*Cluster)* where in within the cluster a single node is selected that will have the role of leader and gateway, so-called cluster head (*CH-Cluster Head*). It regional connects multiple sensor nodes and acts as a base station, as shown in Fig. 1. Within the cluster, the nodes are not allowed to communicate with each other (peer-to-peer). The aim of such restrictions is the energy efficiency of the network. To improve it is necessary to use the energy-efficient modulation for communication with the sensor nodes and that the nodes can support mode with reduced power consumption [5]. More than one cluster head (CH) is connect to the command center (C), whose function is to collect data from the sensor nodes (SN). Cluster heads have a role to manage and merged the information into the process of data transfer from sensor nodes to the command center [2]-[4].

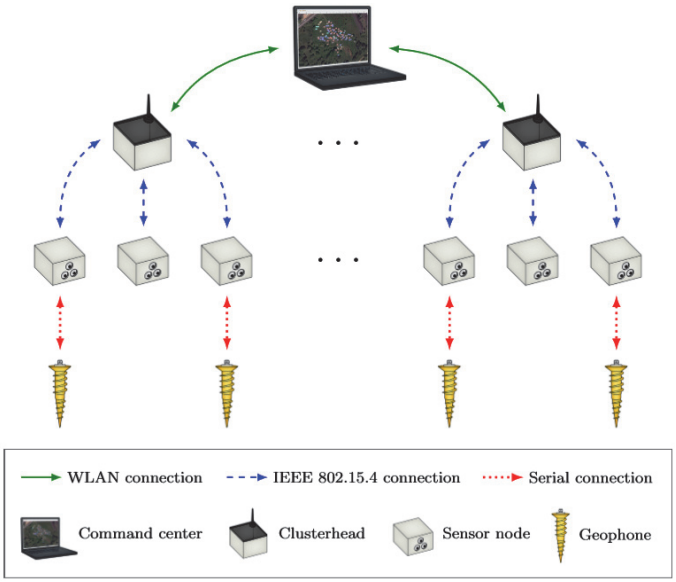

Fig. 1. The structure of generally system of wireless sensor networks [3]

Sensor nodes can be equipped with a different combination of sensors displayed in table 1. The purpose of these sensors is detection of people, vehicles and goods, and this is exactly what the system should detect.

TABLE 1
SENSOR TYPES [3]

Sensor type	Application
AMR	Ferromagnetic sensor
Accelerometer	Sensor speed and acceleration
Singl-PIR	Motion sensor
Multi-PIR	Multiple motion sensor
Longrange-PIR	Long range motion sensor
Geophone	Vibration sensor
GPS	Location

A. WSN Hardware

As shown in Fig. 1 wireless sensor networks would be organized in three hierarchical levels: command center, cluster heads and sensor nodes.

Command center (C) collects information from the cluster heads (CH) and displays information to the user using software for the network visualization. The software has the ability to control the sensor network on a basic level. So, using the software we can restart the node, send a message to a certain number of nodes, or perform reprogramming nodes. Each cluster head hardware consists of two parts: (1) built-in mini-PC motherboard (the processor needs to be energy efficient, with a particular RAM and flash memory) and (2) hardware sensor node. The role of Mini-PC board is that maintains a WiFi communications with the command center (C), carried out a preliminary processing of data from sensors and to performs certain tasks on network. The role of the hardware sensor node to communicate with the rest of the sensor nodes in a lower hierarchy

Depending on the shape and properties of the monitored zones in use are several different configurations of sensor nodes. In the housing are located the central module that owns the controller with enough capacity ROM, RAM and flash memory for instructions and data, as well as the radio interface who is compatible with the IEEE 802.15.4 standard in the 2.4 GHz frequency, with 16 different radio channels, with a transfer rate of 250 KB/s and AES encryption. In addition, the central module has the ultra-stable real-time clock (RTC) with maximum 6ppm, voltage regulator and a large range of connectors for connection to sensors [3]. The use of accelerometers inside each enclosure to the sensor node is assumed, and whose role is to register any attempt to open the casing or movement

In the sensor network are implemented four types of sensors. The first type of sensor would be a PIR sensor, who had their three different versions depending on the required characteristics. Sensor versions are: single-PIR with the detection possibility of up to 10 meters, multi-PIR (with more individual PIR sensors with different characteristics) with the possibility of detection of up to 5 meters and long-range-PIR with the detection possibility of up to 50 meters. Usage of the multi-PIR sensor is intended to give information based on which is made assessments of a direction of the object movement, while the use of long-range-PIR sensor is intended to detect an object moving close to the monitored area and every entrance to the zone.

The second type of sensor for detecting is the geophone. Concrete model consists of three sensor capsules that are placed in a waterproof housing, with the aim of detecting vibration in all three axes. The casing is connected to the sensor node over communication and power cable.

The ferromagnetic or AMR (anisotropic magneto-resistive) sensors are used for the detection of metal objects. These sensors are used for classification of type of object. Namely because of their energy inefficiency these sensors are used in combination with PIR sensors, where they are included as needed, as shown in Fig. 2 [3].

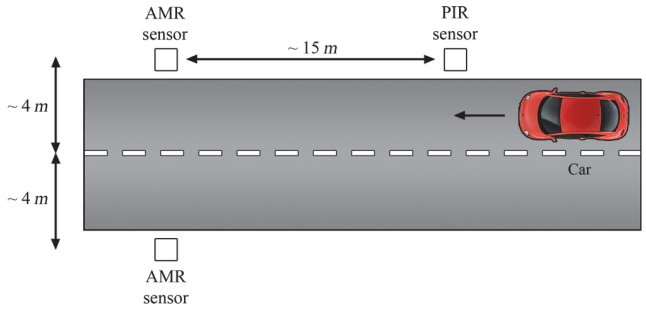

Fig. 2. Using AMR sensors in combination with PIR sensor [3]

The last sensor is an accelerometer, which is an integral part of each sensor node. Its primary purpose is to detect the smallest movements of SN casing. It is used in the physical protection of sensor node from possible unauthorized access.

B. WSN Software

A software architecture of a wireless sensor network consists of: (1) a hierarchical communication structures, (2) security structures, and (3) the algorithm for the detection, localization and classification.

Hierarchical communication structures provide scalability in networks. As shown in Figure 1, the communication between the command center and the cluster heads takes place via a standard TCP/IP protocol through a WiFi network, while the communication in the sensor network based on energy-efficient IEEE 802.15.4 standard. Sensor nodes determined sensor values passed to the cluster head, where is made the previous corrections given values, and then are passed to the command center where they fuse, process, visualize and present to an operator.

There is also a flow of data from the command center to the lower hierarchy device as a configuration instructions, requests for reprogramming of sensor nodes or commands to reset node. All established communications within sensor networks are protected.

Security architecture should provide: (1) security of the communication, and (2) the functional safety of the system. With a communication security is guaranteed a required level of protection for the system operation, while the functional safety guarantee detection of hardware system failure. Although the standard IEEE 802.15.4 offers the possibility of several security options, we do not use them for two main reasons. The first reason is that as additional protection security protocols need to be kept separate from the underlying communication protocol. Therefore, the system is tougher and more resistant to attacks. The second reason is that the security protection provided in the IEEE 802.15.4 standard are not considered safe enough for use in the framework of the proposed scenarios [3].

Conceptual design for communication security system is to integrate all the security features that will be able to detect any violation of the integrity of the system. Communication security is designed in two levels of protection: the level of adaptive frequency hopping (AFS) and the level of security protection. AFS level includes adaptive frequency hopping, time synchronization, manage the available communication channels and procedures for initiating a joint session between the sensor node and cluster head. The goal of the security protection is to achieve confidentiality, integrity and availability. To protect messages against counterfeiting and manipulation, we keep information with the AES encryption, which is available within the crypto coprocessors existing in all sensor nodes. The encryption process is very fast and energy efficient. The aim is to achieve a system resistance to attacks. As for the communication between the cluster head and the command center, it is realized through standard IEEE 802.11g WiFi, which in the context of its security functions offers WPA2 encryption. It is considered more than enough to protect data in a wireless sensor network.

Crucial to a functioning security of wireless sensor networks is the physical integrity and the integrity of nodes, as well as their sensors. During the constant surveillance of network, we achieve real time detection of current and constant errors, as well as discovering the failure of components. When an error is detected, then they can be managed and therefore achieve more secure state of sensor networks. The reliability of the network is very important in the process of detection of threats. Undetected threat due to the cancellation of a sensor or part of a system, can create holes in a monitored zone. Hence, in system is embedded functional security measures to detect errors in the operation and had taken measures to ensure the proper functioning of the system. Some of the measures which the system periodically performs are: (1) check the integrity of the memory (RAM, ROM, Flash memory), (2) check code entered into the memory with the original code, (3) check the CPU (perform is necessary, due to high energy consumption), (4) check the sensor at the partial or total cancellation and (5) the log read errors in the command center. After the completed check user at the command center could see the validity of the network and to respond if necessary. In cases of cancellation, the first step is the reconfigure network so that adjacent elements in the network take over part of the functions, and if defective device significantly affects the safety, immediately replace the defective device with the correct.

The required characteristics of wireless sensor networks in long-lasting conditions of monitoring are robustness and reliability. Therefore, methods of detection, localization and classification must be easily and effectively implemented in a hierarchical network. In Figure 3. shows the flow of information in the proposed algorithm for the detection, localization and classification [1]. Sensor node is located at the lowest hierarchical level and as such is responsible for data acquisition from sensors. In a wireless sensor network after the first start detection algorithm went into standby mode, while the number of sensor events can reach a significant number. If the number of events grows, this would mean that the object is entered into a monitored zone, however, if the number of events remains small, it would mean that the sensor events causing random noise or other sources (wind, birds, etc.). Also, the activity of each sensor indicating the possible location of the object.

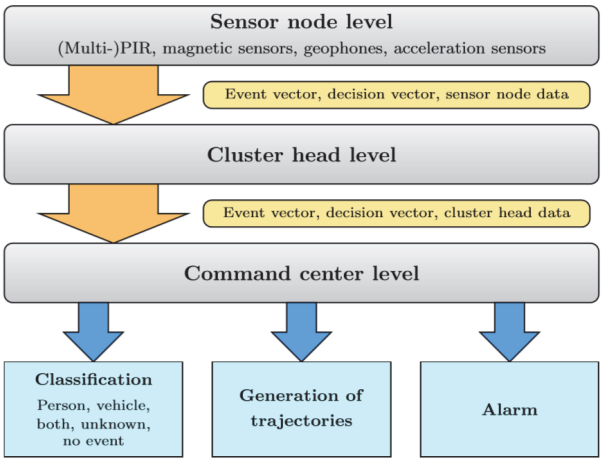

Fig. 3. Stream information in the algorithm for the detection, localization and classification [3]

The data which have reached the sensor node after a preprocessing are directly forwarded to the relevant cluster heads, where it is further processed. Each sensor node can suggest possible object position based on events from the sensor. The current position of an object determines the cluster head averaging position sensor events, having regard to the previous position of the object. After that, only the sensor events near the current position of the detected object are taken into account.

Data received in the command center are analyzed and based on them classification has been made for objects detected and localized in a monitored zone. Analyzing data from AMR and geophone sensors the command center classifies the type of object (face, a person who wears a metal object, auto or unknown)

C. Energy Supplies

Because of energy efficiency systems and limited access to energy, consumption within the sensor nodes must be strictly limited. The safety and reliability of the system should not be compromised. Regarding to this connection, we need to avoid reaching a sensor node failure due to lack of energy.

For these purposes, in the system is embedded early warning system, which periodically measured power level in battery cells and activates the alarm in the event of reaching critical values. The system measures the residual energy value, using the built-in model that calculates the energy consumption of consumed and remaining energy in the battery cells. The model calculates the remaining energy by measuring the time that the node and the associated sensors are conducted in the "awake" (work) and "sleep" (inactive node and sensors). In this way, it is possible to approximate the energy available depending on the capacity of power supply cells. The entire data about the level consumed and available energy is stored in the memory, in order to preserve the actual situation due to loss of power or reset the device.

IV. Implementation of the Proposed Solutions

Design specific wireless sensor network is related to a certain type of critical infrastructure. In the process of planning and design, it is necessary to estimate an adequate and cost-effective hardware. The possibility of choosing hardware is great, but when it is come to implementation should take care about low-cost hardware and low maintenance costs. Depending on the nature of the object that is stored (e.g., a bank, a mint, a security agency headquarters, the monastery, warehouse, prison, border, etc.) it is possible application of the fixed infrastructure with continuous power in a wireless sensor network. Use of multisensory nodes with greater sensitivity significantly increases the cost of the network, but it can be justified due to the importance of the object to be protected.

V. Conclusion

Everyday requests for the use of wireless sensor networks exceed capabilities of researchers and set in front of them quite a lot challenges with whom must be fought. Although wireless sensor networks are one of the fastest-growing fields of wireless networks, the hardware and software development is trying to keep up with the demands and needs of users. Institutions that take care of the protection of vital and critical infrastructure for society define the most complex requirements. This paper gives an overview of the achievements in the area of wireless sensor networks, with a focus on network architecture, its component parts, topology and protocols and algorithms that are used in making decisions. The use of wireless sensor networks using different types of sensors, may represent an efficient solution for protecting critical infrastructure.

References

[1] E. Jungert, N. Hallberg, and N. Wadströmer, „A System Design for Surveillance Systems Protecting Critical Infrastructures", *Journal of Visual Languages and Computing*, vol. 25, pp. 650-657, JSAN, 2014.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", *Comput. Netw.*, vol. 38, pp. 393-422, 2002.

[3] M. Niedermeier, X. He, H. Meer, C. Buschmann, K. Hartmann, B. Langmann, M. Koch, S. Fischer, and D. Pfisterer, "Critical Infrastructure Surveillance Using Secure Wireless Sensor Networks", *Journal of Sensor and Actuator Networks*, vol. 4, iss. 4, pp. 336-370, JSAN, 2015.

[4] G.B. Marković, and M.L. Dukić, „Wireless Sensor Networks, Part I: Basic Architecture, Features and Applications", *Telecommunications*, vol. 3, RATEL, 2008.

[5] G.B. Marković, and M.L. Dukić, „Wireless Sensor Networks, Part II: A Review of the Communication Architecture", *Telecommunications*, vol. 7, RATEL, 2008.

[6] A. Oračević, *Ad HOC Wireless Sensor Networks*", Faculty of Engineering, University of Bihać, 2013.