http://dx.doi.org/10.14311/MAD.2013.06.01 ISSN 1805-7578

The use of Wireless Sensor Network for increasing airport security

Jakub Kraus
ATM Systems Laboratory,
Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University
Horská 3, Praha 2, 128 03, Czech Republic
e-mail: kraus@fd.cvut.cz

Petr Fajčík
Department of Air Transport,
Faculty of Transportation Sciences, Czech Technical University
Horská 3, Praha 2, 128 03, Czech Republic

Peter Vittek
Department of Air Transport,
Faculty of Transportation Sciences, Czech Technical University
Horská 3, Praha 2, 128 03, Czech Republic

Tomáš Duša
Department of Air Transport,
Faculty of Transportation Sciences, Czech Technical University
Horská 3, Praha 2, 128 03, Czech Republic

Abstract – **This article focuses on the use of wireless sensor networks for airport security, respectively using sensor networks as a replacement or add-on to existing security measures. The article describes the sensor network and its possible application to various airport objects and financial analysis of the perimeter security with wireless sensor network.**

Keywords – WSN, sensor network, security, airport

I. INTRODUCTION

Sufficient airport security is one of the primary requirements for airport operation. However, it is important to distinguish between large and small aviation. Large international airports serving commercial air transport are almost perfectly secured with the latest technical means and procedures which are constantly updated and modernized to minimize all possible threats.

At present, attention also hits the security of small airports used only for the purposes of general aviation. Even the small airport should meet certain safety requirements. The problem, however, is the fact that these airports, operated by aero clubs, do not have sufficient resources to provide at least minimal security. It is therefore necessary to look for new ways and means to achieve the desired security and at the same time to minimize costs as much as possible.

II. WIRELESS SENSOR NETWORK

These new technology can be a wireless sensor network. Wireless sensor networks (WSN) consist of a group of small devices that are deployed in a specific area and communicate with each other wirelessly in order to monitor or control. By monitoring is meant data gathering using sensors and sending the measured values to superior system for processing, analysis and evaluation.

Space for the use of wireless sensor networks is enormous. Their implementations are offered everywhere where is financially or otherwise disadvantageous to use metallic cables to supply or to transmit the data. WSN is relatively new technology, because the standards that define this kind of networks have been created in the last decade. Most wireless sensor network is therefore defined by the IEEE 802.15.4 standard that defines the physical radio transmission and link layer. It also defines the star and peer-to-peer (p2p) topology, but some upgrade that would use this standard and use it with WSN in practice was missed. There are several protocols over IEEE 802.15.4, but they are often too complex because of the device synchronization, switching radio channels and routing complexity. This gap was filled by Zigbee Alliance, which aims to create a standard that will be actually used in practice. Their product is the Zigbee standard, which introduced a general topology - mesh, making it the most appropriate standard for wireless sensor networks.

TABLE I. COMPONENTS OF WSN NODE

Sensor	ICs sensing physical or chemical quantities and transform it into a digital signal
Sensor board	a fundamental component to which are connected all the elements of a sensor network devices (sensors, power supply, antenna, radio module, ...)
Microprocessor	usually 8bit, working on low frequency and low voltage
Firmware	software developed for the microprocessor, which defines the behaviour of a network device
Antenna and radio module	to ensure “wireless” of wireless sensor networks
Power supply	source of energy, energy storage, voltage regulator

http://dx.doi.org/10.14311/MAD.2013.06.01 ISSN 1805-7578

The reasons for increasing the use of sensor networks:

- lower price compared with commonly used means,
- increasing availability of suitable devices which can be implemented,
- the possibility of setting up a network in areas where it is not possible to use conventional means for lack of energy supply,
- possibility of creating an ad hoc network – network modification "tailored" to the requirements.

Due to the current high prices it is advisable to use a minimum number of nodes. The ideal situation would be network witch covers the whole area of the airport. It would allow better monitoring of the intruder to determine the direction of its movement and estimate its speed. However, the cost of such network will be several times higher than the proposed network, in which sensors are installed only around the perimeter.

The gateway is connected to the Base Station and it should by ideally located in the control tower, where it is possible after

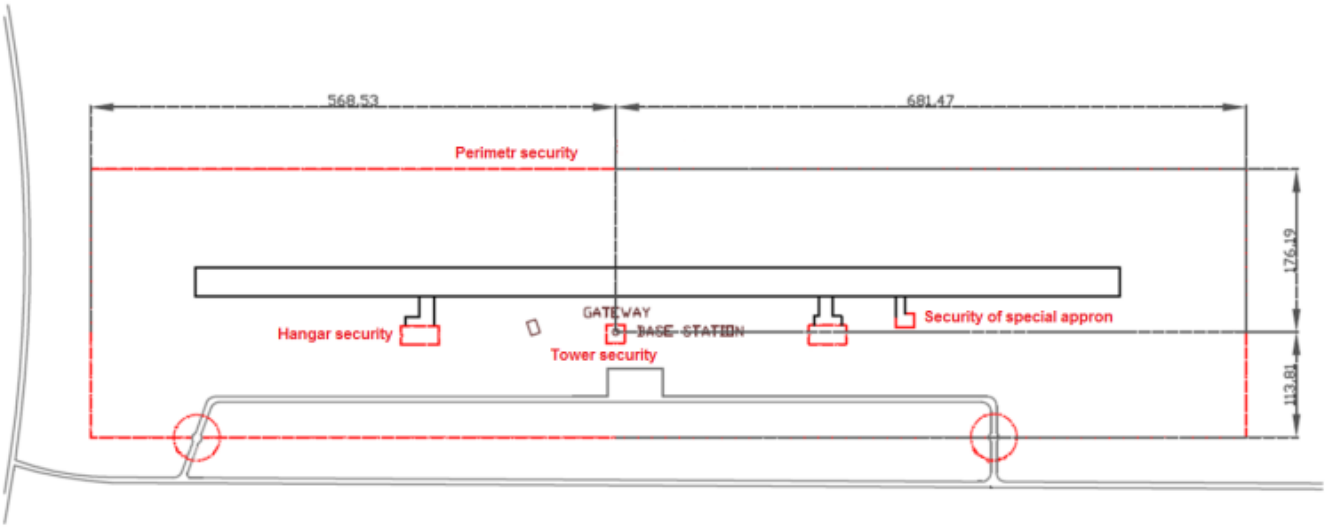

Figure 1. Model airport and necessary security measures

III. Airport Security with WSN

Figure 1 shows a model for airport security done by wireless sensor network. Thanks to analysis of possible scenarios for violation of the airport, it was chosen five areas for securing which are the hangars, stands used to check the aircraft, control tower, access points and perimeter.

A. *Design of suitable type of sensor networks*

After examining the possible types of technical equipment, topologies and standards used for wireless sensor networks, it has been selected star topology, based on the IEEE 802.15.4 standard. The proposed network at the airport has only the task of collecting data, to which has this standard sufficient capability.

IEEE 802.15.4 allows networking up to 64,516 devices. For small airport security models are sufficient several hundred of wireless nodes. All these nodes are network devices type RFD - devices with limited functionality (Reduced Function Device) that are connected to the PAN coordinator - Meshlium gate. This allows connection of nodes to a distance of 7000 m. Figure 1 shows that none of the nodes could exceed that distance. The fact that each of the nodes is in the range of gateway eliminates the need to implement network where nodes communicate with each other and transmit information from the farthest sensor to the gateway. It is therefore possible to select simple star topology for the proposed network.

detecting intruders immediately identify potential threats and act adequately against it. The output forms a personal computer with a graphical interface, representing the airport. Gate Meshlium and computer have to have sufficient capacity to store transferred data. In the case of detection the triggered sensor is identified, or the image data are displayed.

B. *Areas for securing*

The primary activity was the choice, against what will be the WSN used, i.e. which sensor types should be used. Given the diversity of the areas from the perimeter to the control tower, following sensors were chosen:

- Presence (PIR - passive infrared)
- Magnetic field (MG)
- Ammonia (NH_3)
- Carbon Monoxide (CO)
- Carbon Dioxide (CO_2)
- Nitrogen Dioxide (NO_2)
- Oil-based fuels (CH_4, C_4H_{10}, CH_3CH_2OH, H_2)
- Hall Effect

To utilize the aforementioned sensors they have to be mounted on a sensor board, therefore it is necessary to use:

- Events sensor board
- Gases sensor board

And also:

- Radiation sensor board

http://dx.doi.org/10.14311/MAD.2013.06.01 ISSN 1805-7578

- Video Camera sensor board

All these basic elements can secure perimeter (PIR, MG, cameras), access points and stands (NH_3, radiation), entrances to buildings and movement in them (doors, PIR, cameras) as well as detection of a fire or spill fuels (CO, CO_2, NO_2, oil-based fumes).

To complete the sensor place is needed only a radio module and power supply. Li-Ion rechargeable battery is the best choice for power supply and each sensory panel gets its radio module with antenna.

Given these requirements for a reasonable level of security for a small airport, products from Libelium company, which specializes in sensor networks was selected for costs calculations.

IV. Cost Analysis of WSN for Securing Airport Perimeter

A. *Option 1 – using only PIR and magnetic field sensors*

This option calculates with security measures done by motion sensors and magnetic field sensors. The number of nodes is governed by a range of motion sensor, which is 12 m. The need to cover the entire perimeter requires overlap of coverage of adjacent sensors. In the disposition of the sensors shown in Figure 2 is the distance between adjacent sensors 14 m. For perimeter security, which is 3080 m, are therefore required 220 motion sensors. In order to maintain the lowest costs, the sensors are placed only around the airport perimeter.

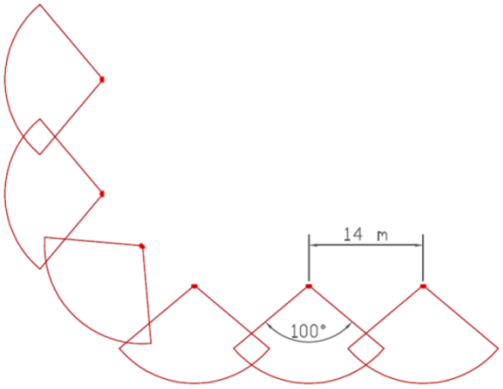

Figure 2. Layout of sensors – option 1

Table II. Calculation of Option 1

Part	Price (CZK/pc)	Quantity	Overall (CZK)
Sensor Board WEVENTS	1 875	220	412 500
Motion sensor EKMB1203111	438	220	96 360
Magnetic field sensor KMZ51	26	220	5 720
Radio module Waspmote	3 750	220	825 000
Battery	750	220	165 000
Σ			1 504 580

B. *Option 2 –using PIRand magnetic field sensors supplemented with camera sensors*

The second variant also uses motion and magnetic sensors, but also uses camera sensors. One-fifth of all nodes securing the perimeter are cameras. Specifically, it is implemented 176 motion and magnetic sensors and 44 camera and motion sensors for perimeter security. This means that for every seventy meters is placed one camera. This will increase the amount of information that will be available for the operator in the event of detection while the increase in price is small. Of course, the number of camera nodes could be chosen as needed, but it is necessary to take account of their relatively higher price.

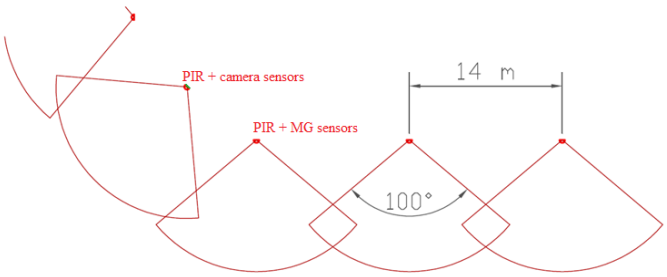

Figure 3. Layout of sensors – option 2

Table III. Calculation of Option 2

Part	Price (CZK/pcs)	Quantity	Overall (CZK)
Sensor Board WEVENTS	1 875	176	330 000
Motion sensor EKMB1203111	438	220	96 360
Magnetic field sensor KMZ51	26	176	4 576
Video camera sensor board WCAM-ST	4 225	44	185 900
3G + GPS	6 125	44	269 500
Radio module Waspmote	3 750	176	660 000
Battery	750	220	165 000
Σ			1 711 336

To each variant is necessary to add additional costs of gateway and computer for data processing. It is also appropriate to include spare batteries for replacement and recharging.

Table IV. Calculation of Additional Costs

Part	Price (CZK/pcs)	Quantity	Overall (CZK)
Gateway Meshlium	16 875	1	16 875
Base station – PC	20 000	1	20 000
Spare batteries	750	20	15 000
Σ			41 875

C. Option 3 – conventional security with fencing

The traditional way to prevent the entry of an intruder into the airport is fence. After comparing different types of fencing it was chosen type of mesh Bastille, which is often used exactly in securing airports and is used for example at airports Čáslav, Náměšť nad Oslavou, Pardubice and also around ANS of the Czech Republic in Jeneč. This is a plastic-coated wire mesh with a wire diameter 3 mm, mesh size 76 x 38 mm. Fencing height could be 150 and 200 cm. Suitable pillars for this type of fence, and also very often used at airports, are Univers columns with a diameter of 48 mm. One pillar is every 2.2 meters. Every tenth column is reinforced with two struts. With a length of 3080 m of perimeter is therefore needed mesh 3080 m long, 1400 pillars and 140 struts. Columns in the corners also need two struts, bringing the number of struts to 148 units.

It is important to note that the actual fencing can be easily overcome, whether climbing over, digging under or cutting. If the fence is not accompanied by other security features, such as sensors detecting an attempt to climb over or damaged fence, airport personnel is not informed in any way about the entry of intruder to the perimeter.

Means to increase the effectiveness of the fence are for example concrete blocks under the fence or pillars extensions with barbed and razor wire. The disadvantage, however, is a big increase in price.

TABLE V. CALCULATION OF BASIC OPTION 3

	Price for 1pcs, 1m (CZK)	Quantity (pcs, m)	Overall (CZK)
Fence Bastila 200 cm	356	3 080	1 096 480
Pillar Univers 200 cm,	330	1 400	462 000
Struts Univers	618	148	91 464
Σ			1 649 944

TABLE VI. CALCULATION OF EXTENDED OPTION 3

	Price for 1pcs (CZK)	Quantity (pcs)	Overall (CZK)
Pillar extension Univers	652	148	96 496
Barbed wire 250 m	2452	12,32	30 208
Concreate block under fence 2980 mm	605	1033,5	624 965
Σ			751 669

V. CONCLUSION

In this article, we have shown that modern technology such as wireless sensor networks, can replace the original solution. And area of airport security is very suitable for wireless sensor network (WSN). WSN are in fact able to act actively - provide real time data.

Economic analysis of securing the perimeter, where we compared the two options of wireless sensor networks and conventional security measure - fence - showed as more economical to use a wireless sensor network, despite the relatively higher prices of WSN components. However, in the future with the development of WSN, this situation will be even more inclined to use modern technology.

II. ACKNOWLEDGEMENTS

This paper was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS12/165/OHK2/2T/16.

REFERENCES

[1] Callaway, Edgar H, Jr: Wireless Sensor Networks: Architectures and Protocols.

[2] Wireless sensor network (WSN) [online]. [cit. 2013-08-08]. Available at <http://embedsoftdev.com/embedded/wireless-sensor-network-wsn/>

[3] Events board technical guide.pdf [online]. [cit. 2013-08-08]. Available at <http://www.libelium.com/development/waspmote/documentation/events-board-technical-guide/>

[4] Libelium. Libelium. [online]. Available at: <http://www.libelium.com/>