Agronomy Research **16**(S1), 1017–1024, 2018
https://doi.org/10.15159/AR.18.019

Testing of ISM band at remotes for unlocking vehicles

J. Hart[1,*] and V. Hartová[2]

[1]Czech University of Life Sciences Prague, Faculty of Engineering, Department of Technological Equipment of Buildings, Kamýcká 129, CZ165 00 Prague, Czech Republic
[2]Czech University of Life Sciences Prague, Faculty of Engineering, Department of Vehicles and Ground Transport, Kamýcká 129, CZ165 00 Prague, Czech Republic
[*]Correspondence: janhart77@gmail.com

Abstract. Every modern car has a remote control for wireless unlocking. Wireless drivers for unlocking the vehicle using frequency in the ISM bands. ISM bands are unlicensed bands. They are usually used for industrial, medical and scientific purposes. The question is whether wireless transmission parameters are sufficient and do not violate defined range of ISM band. Another important aspect is the security of the wireless transmissions and any other signal interference. The problem of interference plays an important role in ensuring the quality and safety of wireless communications, especially when wireless networks can be found everywhere. The issues of remote control vehicles is very important due to the resulting security of a guarded vehicle. One of the major risks that may occur are data transmission that the signal is blocked by another signal and the end user does not notice. In this case, does not lock the vehicle nor ensuring its securing security system. Tests which were performed accurately determined the bandwidth of broadcast remote control for each vehicle. Vehicles for which the tests were conducted are standard vehicles used to frequent occurrence. These are the following types: Alfa Romeo, Hyundai, Mercedes, Škoda and Toyota. Subsequently, the analysis was performed of transmission compared with standard broadcast of jammers. All test drivers worked in the band ISM433. These tests clearly demonstrated that not every manufacturer strictly observes ranges of ISM band. This may affect traffic on surrounding licensed bands.

Key words: Remotes, vehicle, wireless transmission, interference, measuring.

INTRODUCTION

Currently, the issue of electromagnetic interference is growing steadily and much attention is focused on it from both scientists and the general public. Electromagnetic interference is increasing almost every day, and disseminators include seemingly risk-free parts of everyday life such as home appliances, machinery and devices, urban environments and high-voltage lines that supply electricity in both areas near and far away (hereinafter common electromagnetic interference). It has been shown that it also arises, for example, in the thermal treatment of materials. It is not possible to state that this is directly a natural disaster, but it does have a major impact on both the environment, and the functionality of various communication technologies (Mpitziopoulos et al., 2007; Commander et al., 2008; Altman et al., 2011; Bradna & Malaťák, 2016).

Electromagnetic interference is also increased with the boom in wireless technologies, which has led to a large increase in the use of wireless devices. Through their broadcasts, these devices gradually overload individual frequencies, which leads not only to transmission errors, but sometimes also to their disabling. Electromagnetic interference overloading of 433 MHz and 868 MHz frequencies, through which the wireless component of wireless transmissions with remotes for unlocking vehicles communicates, strongly affects their reliability, usability (Commander et al., 2008; Tahir & Shah, 2008; Pelechrinis et al., 2009; Hart & Hartová, 2014).

Although common electromagnetic interference for wireless transmission with remotes for unlocking vehicles is very risky, it is not the greatest risk. The greatest risks are becoming low-frequency jammers that are able to jam ongoing communication between a remotes and vehicles, thus disabling the alarm (Staff & Honey, 1999; Mpitziopoulos et al., 2007; Siddhabathula et al., 2012; Hartová & Hart, 2017).

Many research has shown that not every transmitter meets the ISM band. These bands are free of charge and are specified by the telecommunication authorities. It was therefore a question of whether wireless communications with remotes for unlocking vehicles meet the necessary requirements of telecommunication authorities. If these requirements were not met, it would have had a major impact on the production engineering of these remotes (Hart & Hartová, 2014; Hartová & Hart, 2017).

MATERIALS AND METHODS

Tests which were performed accurately determined the bandwidth of broadcast remote control for each vehicle. Vehicles for which the tests were conducted are standard vehicles used to frequent occurrence. These are the following types: Alfa Romeo, Hyundai, Mercedes, Škoda and Toyota.

SPECTRAN HF-6060 spectrum analyser (Fig. 1) was used, which investigated the strength of the broadcasting remotes for unlocking vehicles at frequencies of 433 MHz (ISM 433). ISM 433 is only standard for ITU 1 (EMEA), not for Asia and therefore the cars distributed in ITU1 area were selected. The manufacturer must adhere to the wireless transmission standards of countries where he distributes his products.

Figure 1. Spectrum analyser SPECTRAN HF-6060 with an antenna.

The ISM (industrial, scientific and medical) bands that were measure are bands for radio broadcasts, which are used, for example, in industry, and for health and scientific purposes. They are of course also used in the commercial sector, where we most often encounter them with RC models and intruder and hold-up alarm systems. They are unlicensed (free) bands, which means that they are allowed to operate without license fees if they use homologated (approved) devices. Although a commercial company may save money by using them, but their one big disadvantage is that these frequencies do not guarantee against interference (Cumming, 1994; Capel, 1999; Powell & Shim, 2012).

Within the measurement the following values were set on the SPECTRAN HF-6060 spectrum analyser:

- Sampletime – 50 ms
- Samples – 500
- Bandwidth – 1 MHz

For each car, two identical controls were tested in five cycles. For all charts, top line shows wireless transmission and lower default values for natural interference. In the following figures (Figs 2–5) are an evident intensity of the wireless transmission vehicles: Hyundai i30, Mercedes-Benz CLK, Alfa Romeo 159 and Toyota Verso in the scope of ISM 433.

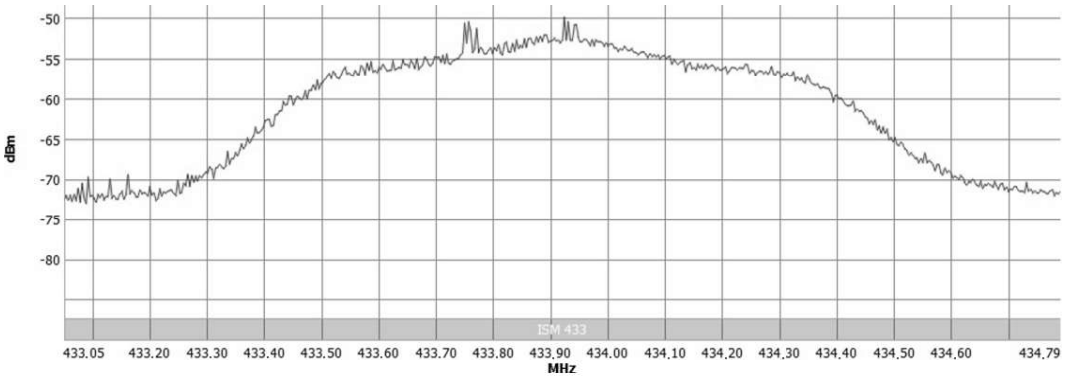

Figure 2. Transmission characteristics of Hyundai i30.

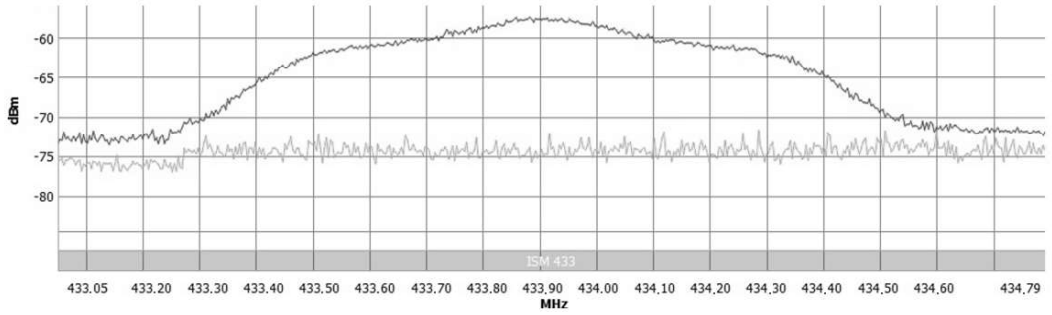

Figure 3. Transmission characteristics of Mercedes Benz CLK.

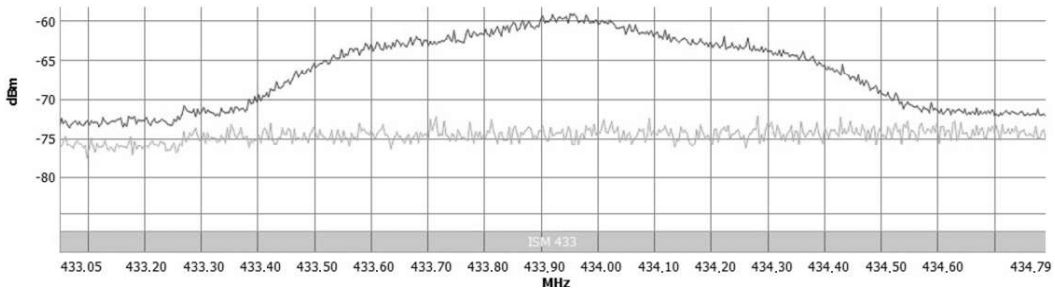

Figure 4. Transmission characteristics of Alfa Romeo 159.

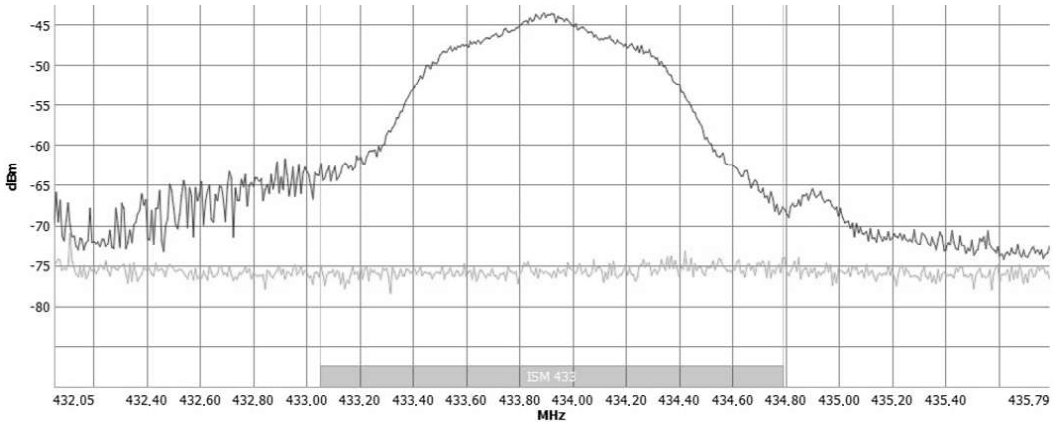

Figure 5. Transmission characteristics of Toyota Verso.

In the following figures (Figs 6–9) are an evident intensity of the wireless transmission vehicles: Škoda Fabia III, Škoda Octavia II, Škoda Superb II and Škoda Octavia III RS in the scope of ISM 433.

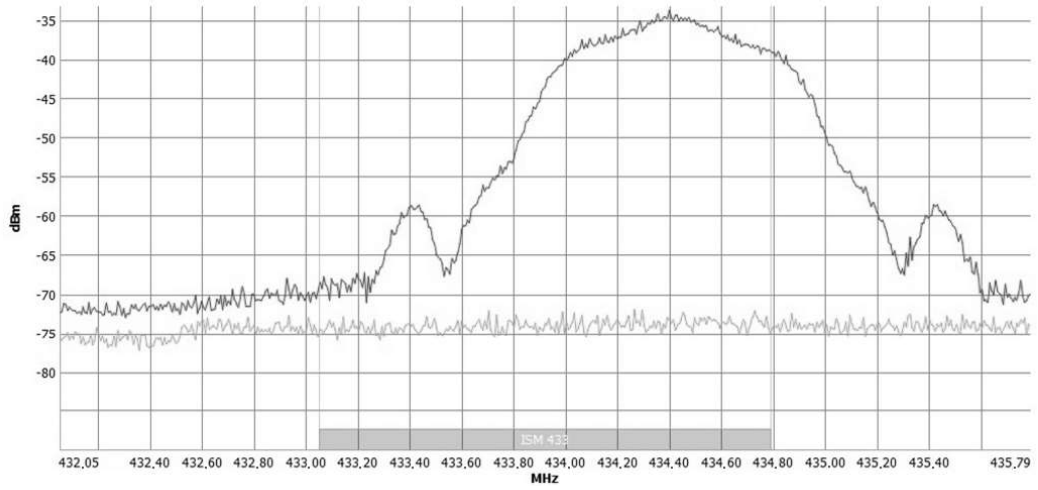

Figure 6. Transmission characteristics of Škoda Fabia III.

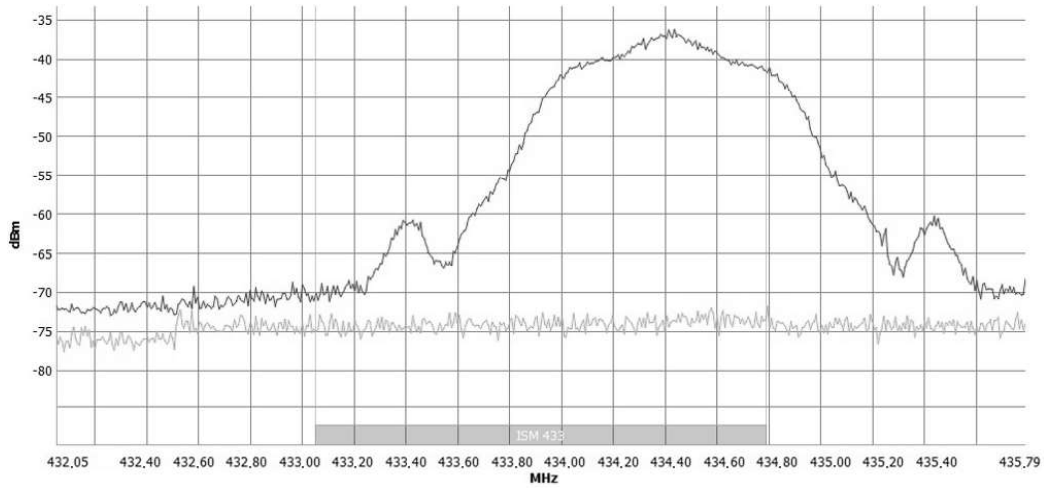

Figure 7. Transmission characteristics of Škoda Octavia II.

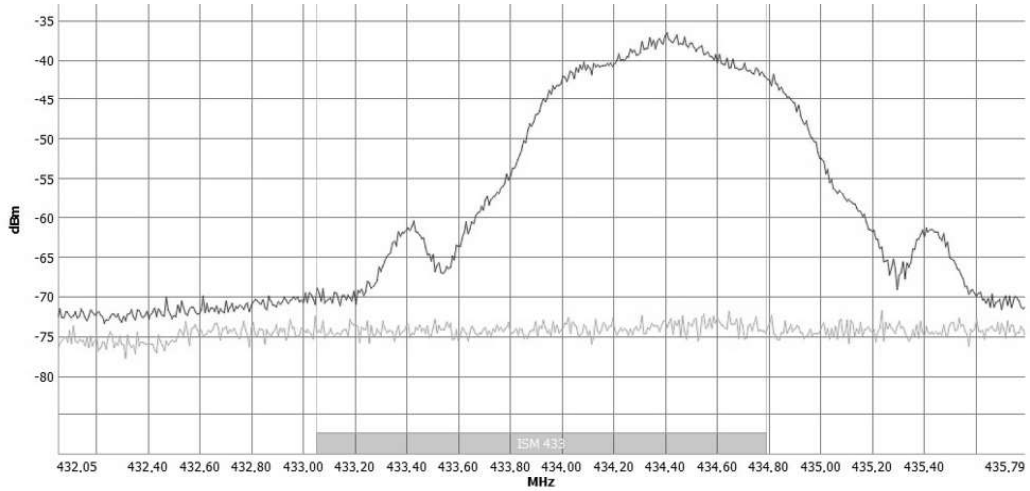

Figure 8. Transmission characteristics of Škoda Superb II.

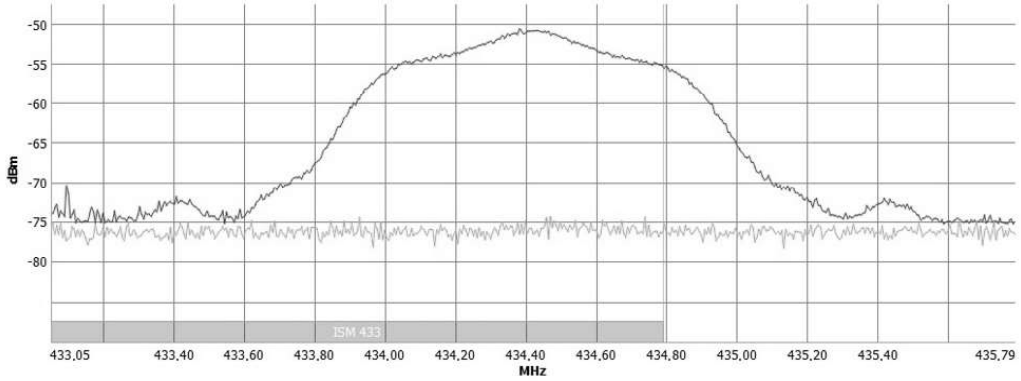

Figure 9. Transmission characteristics of Škoda Octavia III RS.

In the last figure (Fig. 10) is an evident intensity of the wireless transmission of vehicle Toyota Auris in the scope of ISM 433.

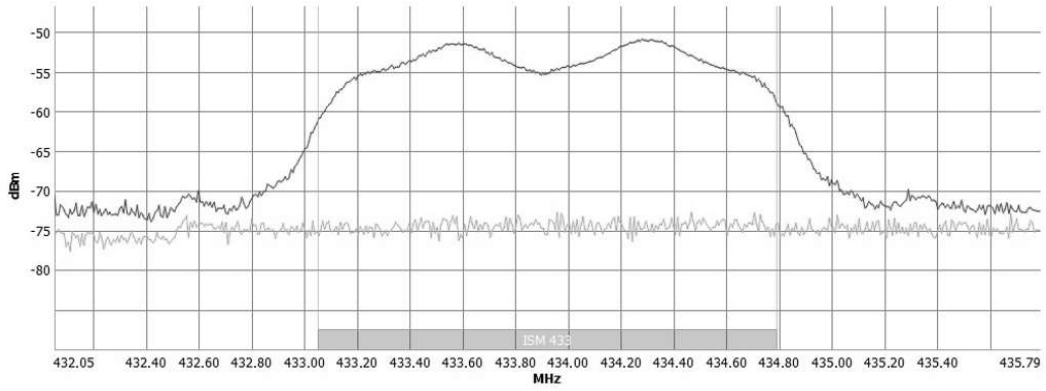

Figure 10. Transmission characteristics of Toyota Auris.

RESULTS AND DISCUSSION

From the measured results of wireless transmissions using the remote control to unlock the vehicle based on best provided wireless transmissions shown in Figs 2, 5 and 10 respectively.

They have the power in their broadcasts and do not depart from prescribed ISM band. At the same time wireless transmissions in the results in Fig. 10 and implemented in parallel in two bands, thereby reducing the likelihood jamming. Wireless transmissions in Figs 3 and 4 while also do not interfere outside ISM bands, but their broadcasts is weaker over the previous variants. It may give rise to a situation that, due to natural electromagnetic interference is not successfully transmitted. The remaining transmissions, shown in Figs 6–9, although they have great power, but failed to comply with specified range of transmission for the ISM band, so should officially not used at all. A comparison of different wireless transmissions can be seen in Fig. 11, based on the above parameters. This figure shows the percentage of transmission quality for each measured vehicle.

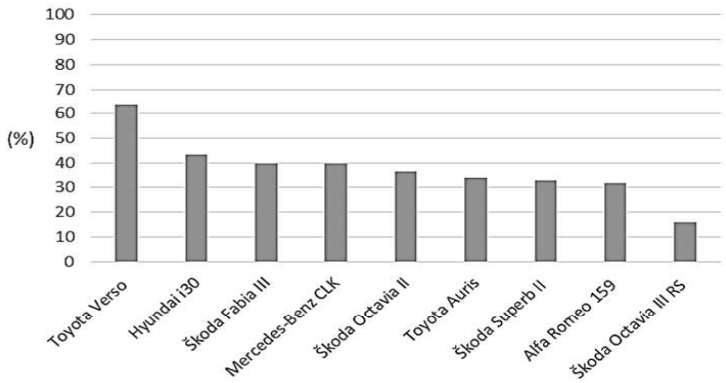

Figure 11. Evaluation of individual criteria through a multi-criteria scoring options.

Since the first public demonstration of radio and radio communication in 1893 by Nikola Tesla, people have been trying to find a way to communicate with each other without such communication being interfered with. One of the biggest booms in this research began during the Vietnam War, as described by the author of the article 'The Progress of Tactical Radios from Legacy Systems to Cognitive Radios.' (Elmasry, 2013). Many years of research have passed since this historic turning point, but this also includes jamming devices as described in the article 'Responsive Communications Jamming Against Radio-Controlled Improvised Explosive Devices' (Mietzner et al., 2012), where the author focused mainly on protective jammers used to protect against 'radio-controlled improvised explosive devices (RCIEDs)'.

According to recent research and gradual overloading of ISM bands, it is necessary to further develop the possibilities of unlicensed bands, as described in the article 'Complex radio frequency (RF) communications with virtual pulses' (Maina et al., 2008), which describes the use of virtual pulses for communication. It also includes protection against interference. It is also advisable to constantly explore other options, thanks to which new wireless sensor networks could develop, as described by the authors in the article 'UWB wireless sensor networks: UWEN – A practical example' (Opperman et al., 2004), where they favour the use of Impulse-radio-based UWB technology for WSN development.

CONCLUSIONS

Wireless transmissions with remotes for unlocing vehicles are very susceptible to interference – both interference caused by the environment, and interference caused by a targeted jammer.

The measured values clearly show that not every wireless transmissions with remotes for unlocing vehicles has effective intensity against band interference. In order to ensure the vehicle system, guarded vahicle and property, it is important that the band interference control is flawless.

It is important to have an overview of the reliability and functionality of each wireless transmissions. When using wireless transmissions, it is also important for remotes to have bidirectional communication, which increases the system's chances to detect band interference, and also allows the transmission to be switched to a free zone. The only problem would then be if the perpetrator used a smart jammer with detection of used frequencies.

Vehicles Škoda Fabia III, Škoda Octavia II, Škoda Superb II and Škoda Octavia III RS detected overlapping outside ISM bands. It is therefore recommended that the wireless technology of these vehicles be changed. It is recommended that this change be made due to a weak signal even for vehicles Mercedes Benz CLK and Alfa Romeo 159, even though their transmission is within the ISM bandwidth.

All of the measured data are also important for manufacturers of vehicle systems as feedback on their products. In the future, there will be efforts to expand similar tests to other I&HAS manufacturers, as the reliability of these systems is very important, and it will be necessary to check them after deficiencies in the tested systems are ascertained.

ACKNOWLEDGEMENTS. It is a project supported by the CULS IGA TF 'The University Internal Grant Agency' (Analysis of the risks associated with the transmission of large data and data from sensor networks through wireless transmission in ISM bands).

REFERENCES

Altman, E., Avrachenkov, K. & Garnaev, A. 2011. Jamming in wireless networks under uncertainty. *Mobile Networks & Applications* **16**, 246–254.

Bradna, J. & Malaťák, J. 2016. Flue gases thermal emission concentration during waste biomass combustion in small combustion device with manual fuel supply. *Research in Agricultural Engineering* 1–7.

Capel, V. 1999. *Security Systems & Intruder Alarms*. Elsevier Science, 301 pp.

Commander, C.V., Pardalos, P.M., Ryabchenko, V., Shylo, O., Uryasev, S. & Zrazhevsky, G. 2008. Jamming communication networks under complete uncertainty. *Optimization Letters* **2**, 53–70.

Elmasry, G.F. 2013. The Progress of Tactical Radios from Legacy Systems to Cognitive Radios. *IEEE Communications Magazine* 51, 50–56.

Hart, J. & Hartová, V. 2014. The risks of data transmissions in intrusion and hold-up alarm systems and solutions thereto. In: *3rd International Conference on Applied Materials and Electronics Engineering*, pp. 570–574.

Hartová, V. & Hart, J. 2017. Livestock monitoring system using bluetooth technology. In: *Agronomy Research* **15**(3), 707–712.

Maina, J.Y., Mickle, M.H., Lovell, M.R. & Schaefer, L.A. 2008. Complex radio frequency (RF) communications with virtual pulses. *Computers & Electrical Engineering* **34**, 423–437.

Mietzner, J., Nickel, P., Meusling, A., Loos, P. & Bauch, G. 2012. Responsive Communications Jamming Against Radio-Controlled Improvised Explosive Devices. *IEEE Communications Magazine* **50**, 38–46.

Mpitziopoulos, A., Gavalas, D., Pantziou, G. & Konstantopoulos, C. 2007. Defending wireless sensor networks from jamming attacks. *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications* **1–9**, 81–85.

Oppermann, I., Stoica, L., Rabbachin, A., Shelby, Z. & Haapola, J. 2004. UWB wireless sensor networks: UWEN – A practical example. *IEEE Communications Magazine* **42**, S27–S32.

Pelechrinis, K., Koutsopoulos, I., Broustis, I. & Krishnamurthy, S.V. 2009. Lightweight Jammer Localization in Wireless Networks: System Design and Implementation. *IEEE Global Telecommunications Conference* **1–8**, 1301–1306.

Powell, S. & Shim, J.P. 2012. Wireless Technology: Applications, Management, and Security. Springer-Verlag, New York, 276 pp.

Siddhabathula, K., Dong, Q., Liu, D.G. & Wright, M. 2012. Fast Jamming Detection in Sensor Networks. *IEEE International Conference on Communications (ICC)*, pp. 934–938.

Staff, H. & Honey, G. 1999. Electronic Security Systems Pocket Book. Elsevier Science, 226 pp.

Tahir, H. & Shah, S.A.A. 2008. Wireless Sensor Networks – A Security Perspective. In: *INMIC: 2008 International Multitopic Conference*, pp. 189–193.