Interdisciplinary Description of Complex Systems 17(1-A), 67-77, 2019

PROTECTED SPACES IN SMART CITIES AND THE IDENTIFICATION OF NEW RADIO SIGNALS IN THEIR ENVIRONMENT USING A COMPLEX MEASUREMENT METHOD

Gábor Bréda[1,] * and Péter János Varga[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Telecommunications Technology Institute
Budapest, Hungary

DOI: 10.7906/indecs.17.1.9
Regular article

Received: 6 November 2018.
Accepted: 31 December 2018.

ABSTRACT

This research focuses on the creation of a security boundary through the establishment of information security, more specifically by creating an environment that allows for information security for people-to-people communication. The relevance of the research is justified by the vulnerability of infocommunication tools and systems, as well as by the spread of increasingly cheaper information-gathering technologies. There was a need to create an environment where personal, communication between man and man could be realized so that its information content remains protected. Analysing the problem, there are a number of security solutions for information-technology devices, but the creation of a near-human analogue environment for information security is a frontier for the subject. In this approach, the direction of the research was determined by the task of developing an environment that excludes the online operation of infocommunication technologies that create an information security gap and how to identify the spatial position of radio-based communication devices in protected spaces that may be a source of information security. In connection with the continuous quality assurance of the protection, it is necessary to identify the radio signals in the environment of the protected room, which – in the majority of cases – is a built environment with buildings. We offer a new conceptual solution. We studied the operation of the information security breaches during the preliminary research phase by designing a protected space and, by virtue of their principal exclusion, we propose a schematic layout of a protected room, excluding many information security issues. The main purpose of the research is to present an environment that can create a safer person-to-person communication and to provide a novel possible conceptual solution for determining the location of the source of a radio signal.

KEYWORDS

protected room, information protection, protected meeting room, radio direction finding, inertial navigation

CLASSIFICATION

JEL: L63, L94, L96, L98

PACS: 84.40.Ua, 84.40.Xb

*Corresponding author, η: bredagabi@freemail.hu; - ;
H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION

The development of smart cities has greatly increased the use of wireless technologies. The close-range operation of a large number of radio devices involves the formation of interference and the problem of malfunctioning caused by disturbances. Faults in such malfunctions resulting from this kind of error can be a critical issue for the continued operation of smart cities, as basic infrastructures are built on these devices. Automation systems are everywhere, from positioning and communication functions in traffic through information infrastructure in business, to industrial wireless networks and smart homes [1]. As a result of the subject, a special problem emerges in terms of information security for smart cities. This problem is largely relevant to business and administrative infrastructure as the special physical security interface that could address the problem opposes smarting processes. In order to provide information security, an environment in which oral and visual information is secure is to be established [2]. One way to create security for word of mouth and the visually emerging information is to carry out the interaction between the walls of a protected conference room. The creation of such environment in a Smart environment is a special task because the entire verticality of the telecommunications acquis in the information society must be excluded from such an environment [3, 4]. The physical security of protected meeting rooms includes the need to ensure continuous testing and protection of the direct radio environment. By using a continuous monitoring system in the environment we are able to acquire a picture of the features of the radio ether and the presence of radio communication devices. In such environments, it is necessary to know the frequencies present and their sources and to detect new radio signals. The emergence of a new frequency may pose a security risk because the smart environment is fully covered by the arsenal of wireless telecommunications technologies. The source of the new signal that appears is to be identified in the same way as the source of possible disturbance for smart wireless systems. Protected premises relevant to the subject are in a densely-built environment following urbanization trends where the implementation of radio localization is difficult because of the delimiting walls of buildings and reflections. Researching the subject, the detection of interference of devices using standard wireless communication technology is a well-proven measurement system, but localizing disruptions is a difficult task. With the emergence of the problem, paralleling the complex security of the protected premises, the localization of a radio source may be a problem. This article first aims to provide an overview of the principle of the physical design of a protected conference room we deem appropriate and the principle of the protection of the radio protection, and then, later on, will continue to provide a solution to the problem of the exploration of the radiation source outlined above. The solution comes from the combined use of multiple technologies, which include conventional radio field measurements, inertial navigation, cloud-based data storage and data processing technology, and elements of computer visualization.

Data, that may either be open or undisclosed, is generated 24 hours a day in the information society of our time, as well as in smart cities. Data is usually stored on a data carrier or in an information-technology (IT) system to achieve the appropriate quality and capacity. You have to process data to turn it into information. The data processing and the storage of results are nowadays almost exclusively carried out on computing devices, which significantly increases the relevance of the creation of protection designs for the security of non-public data [5-9]. Data protection is dealt with by the legislator at a legislative level, and the protection of IT tools and networks, as the basic information sharing environment of the information society, is dealt with by development and research teams, as well as international and national organizations [10-16].

METHODOLOGY

In the initial phase of the research, general research methods were used. The review of the problem to be resolved, the examination the physical characteristics of human communication, and the examination of the emerging effects. Thereafter, a search for a conceptual solution to exclude problems that arise, and finally, a proposal was made for a conceptual design. During the research, the question of localizing radio signal sources in environments surrounded by buildings arose. Looking at the subject, it's difficulty became prominent. Analysing the problems that arise during the research, a novel conceptual solution can be proposed for the problem.

The expected outcomes at the end of the study:

- proposal for the design of a protected room,
- investigation of the possibilities of the localization of radio signal sources,
- proposal for the localization of radio signals in the vicinity of a protected room.

CONCEPTUAL DEFINITIONS

"Smart City: A smart or a 'more livable' city is a settlement that uses the technology options available (primarily information and communication technology) in an innovative way that promotes a better, more diversified and more sustainable urban environment. A city may be called 'smart' if sustainable economic development and a further increase of living standards is stimulated and driven by the investment in human capital, traditional (e.g. transport) and modern information and communication infrastructure – while treating natural resources wisely" [17].

According to literature [18]: "Information protection (or information security as defined by the NIST): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1. integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
2. confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
3. availability, which means ensuring timely and reliable access to and use of information."

Our conceptual definition of a protected room is as follows. From the point of view of the subject, we define a demarcated area as a protected area where sensitive, valuable data and information (at the right place, classified data, and information) are displayed in an acoustic and visual form. The intended objective is that the data and information that are produced in a protected room should be impossible for unauthorized parties to acquire. The aim is to create and maintain a uniform protection strength.

"Radio direction finding (DF) system: It is an antenna array and a receiver arranged in a combination to determine the azimuth angle of a distant emitter. All DF systems derive the emitter location by initially determining the angle-of-arrival (AOA). Classically, radio direction finding techniques have been based on multiple-antenna systems that employ multiple receivers" [19].

Radio monitoring: an inspection of the radio frequency environment that constantly monitors the characteristics of a radio spectrum in question. It is able to detect radio signals that appear in the examined range and it can indicate if there is a deviation from the reference value in the case of a signal.

"Inertial navigation is a self-contained navigation technique in which measurements provided by accelerometers and gyroscopes are used to track the position and orientation of an object relative to a known starting point, orientation and velocity" [20].

THE EMERGING BREACH IN INFORMATION SECURITY

To ensure that non-public information is displayed (be qualified or sensitive) more criteria must be met. The confidentiality, integrity, credibility, and availability of data, as well as the necessity and proportionality of the protection, and the principle requirement of knowledge [5, 8, 9] must not be violated [4, 21]. In order for data to be interpretable by a human being, one has to elaborate it and get to know it during a process [15]. The information should continue to comply with the data criteria. The processing of protected information usually takes place in a delimited system, as well as in an environment protected by engineering and the previously mentioned laws and organizations. Cognition and sharing in a human-human context require new physical and protective measures to achieve a level of defense consistency. Human cognizance is carried out with the help of sensory organs, especially hearing and vision. The display of information in a form that is directly understandable to man, and is happening in the processor, storage and transmission chains that are considered well protected, encompasses a new medium – the protection of which that cannot be ignored. This medium is the space in which the information is displayed acoustically and visually. Cognition requires interfaces. The physical phenomena appearing in voice-based transmission are either the vibrations of the voice generated by human communication or the sound of a speaker from an IT media player. During visual transmission, the physical phenomena are either the paper with the written information or the information content of the various monitors and projectors. There are several physical phenomena in the chain that need to be investigated from an information security point of view, and in the emergence of a theoretical information security breach resulting from their occurrence, security steps may be needed to be taken to block a possible channel [22]. If stored and transmitted information are provided with a high level of protection in IT and storage systems, then beside the protection of legal, theoretical and IT elements, the physical design of the environment compliant to information security also cannot be neglected, as data and information is displayed there in their purest, most human-close form. With regards to its notion, we call a protected room a demarcated area where the exchange of data and information on data carrier devices, and human-to-human communication can be realized in accordance with the criteria for classified information. During cognition and communication, primary and secondary physical phenomena are created that carry the information itself, thereby opening up the possibility of information leakage. A primary phenomenon is the sound, that makes uses the air pressure waves as a transmission channel to make the eardrum of nearby communicators and the surface of nearby objects vibrate. In the case of visual communication, photons of light are reflected by the written media and are directly emitted by the monitor or projector and travel through the air into the eyes of the participants. Secondary phenomena are magnetic fluxes that correlate with the appearance of information resulting from the operation of equipment used in communication, additional vibrations in the sound generated by the sound, and scattered beams during the reflection of light. In addition, further information security problems may be posed by telecommunication devices at the site of communication, the networks of which now offer almost complete geographical coverage [23]. Based on the data protection criteria and considering the possibilities of technology, it can be stated that in the case of human-to-human communication, and cognition of information with the help of a technology tool, the primary and secondary data generated at the site of the interaction can be intercepted in the absence of adequate protection and thereby the fulfillment of the data protection criteria could be at harm. Sensitive data and information must be processed and distributed to the right holders within the walls of a room, a protected area in which they are secure [24, 25]. The physical phenomena resulting from the various forms of communication and the contributing additional information must be in the plane of the bounding walls of the protected space [26-31].

BASIC DIRECTIVES FOR ESTABLISHING PROTECTED POINTS

The establishment of the security organization of a protected room, or protected meeting room in our case, cannot be conceived without the use of defense resources. Resources, based on their type, can be live solutions and technical protection tools [32-34]. In this research, we focus on the development of physical and technical protection solutions. When establishing a protected room, placement is the first step. The location of such a room should, as an autonomous space, be positioned as an interior space of a building group, with a complete horizontal and vertical interconnection. The physical security of the protected room can be further enhanced when it is surrounded by a fully controlled space. The design proposal is the realization of a shell model, according to which a new autonomous space is created within the designated space, with the realization of special needs. This new partition wall should be made of a material that remains sufficiently firm, even in the case of long-term human presence. In terms of material, breakdown and restoration should not be possible without traces. The space between existing and formed spaces must be permeable from all directions due to the feasibility of subsequent checks. The inner side of the confining outer space has to be shielded in order to dampen the radio signals originating from within the inner space and to prevent access to the communication channels from the outside [35]. The ventilation of the inner room must be solved from the outside room so that the flow of fresh air indirectly arrives at the inner compartment's airspace to avoid contact with the direct outside space. In the space between the two rooms and in the engineering channels, noise has to be generated to prevent the transmission of sound vibrations from the interior room. The walling of the exterior enclosing room must be checked for the degree of acoustic attenuation of the sound that is coming from the interior room, and in the case of weak dampening, it must be sound attenuated [36-38]. The lighting of the meeting room should also be provided with light sources on the walling of the surrounding room, thus reducing the number of technical installations used in the protected room. Considering the furnishing of the meeting room, simplicity should be sought after. Furniture items should contain as little metal as possible, relying mainly on glass and transparent plexiglass furniture, if possible [39]. When designing the protection, the room complex must be secured with proper locking and access control system. When constructing the electronic property protection, it is recommended to create an autonomous camera surveillance system and electronic property protection that is separate from the central defense system. When discussing the comprehensive design of the complex security of protected premises, the monitoring of the radio environment of the room cannot be neglected [32]. In the vicinity of a protected room, it is necessary to know the characteristics of the radio spectrum and the origin of the frequencies found therein. Despite the shell model, an emerging radio signal may still carry a security risk and identify its origin is a must.

One possible information leakage channel in protected rooms is the security vulnerability that emerges due to radio signals. The solution to the problem is the operation of the radio monitoring system, which performs radio spectrum monitoring and analysis. If a new radio signal is displayed in the protected room or in its vicinity, the monitoring system shall generate an indication for the operator. The source of the sign to be displayed needs to be identified to reduce the security risk. Such a room can be seen in Figure 1.

METHODS FOR DETERMINING THE LOCATION OF A RADIO EMITTER

The continuous testing of the radio environment and the detection of the newly emerging frequencies can be done in several ways, but the framework of this study does not allow for it to be explicated. However, it is a tough task to identify the sources of radio signals around the protected areas of smart cities. The localization of a radio source is provided by the methods of radio direction measurement and positioning and their combinations. Listing the methods,

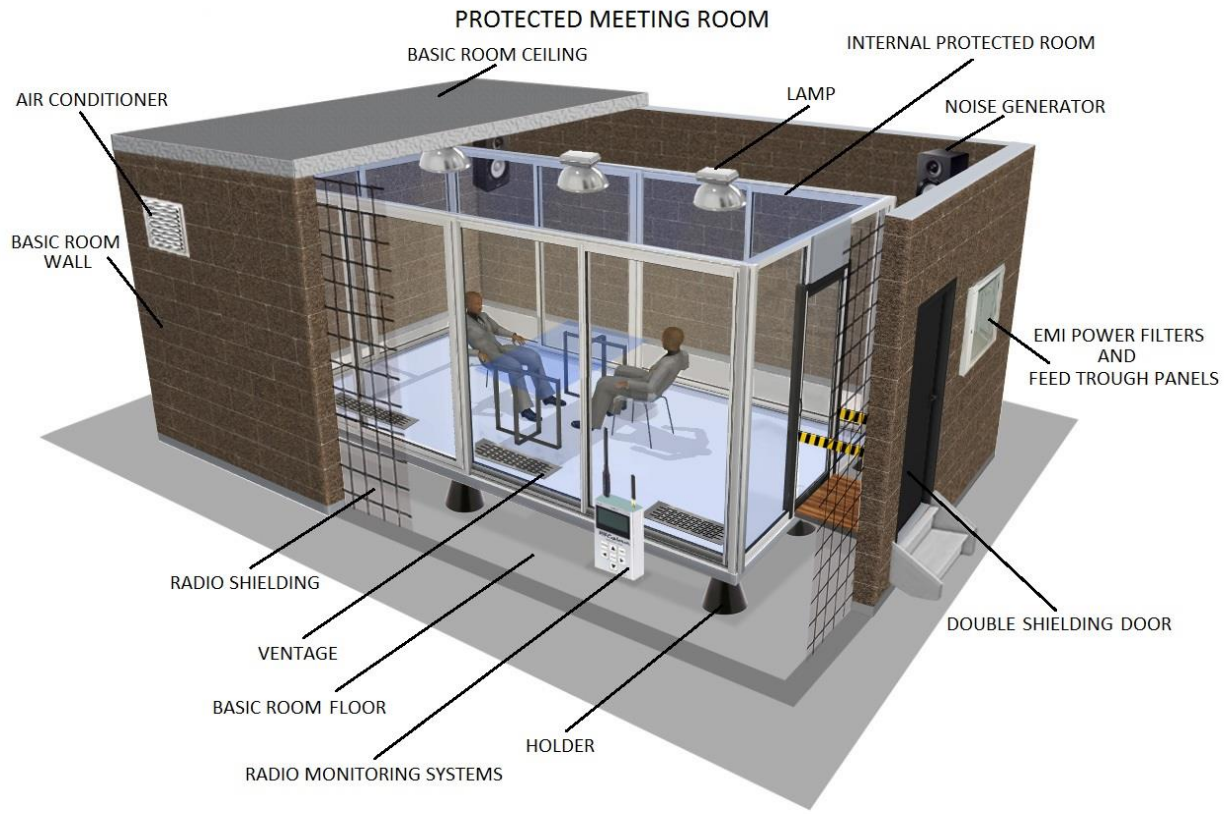

Figure 1. Possible design a protected room based on own idea.

the following options are available. The AOA is measured based on the angle of incidence of the signal. When an antenna is used as a directed spatial filter, the direction of the signal's radiation is measured from a plurality of spatial reference points by direction measurement,

and then the intersection point is calculated or represented to obtain the source position. It can be used with elevated efficacy in densely-built and internal spaces, due to shadowing and reflections [40]. Another solution could be the *Time Difference of Arrival*, the time difference between the arrival of signals, and the *Time of Arrival* measurement method, which is based on measuring the time the signals arrive. The method requires a simultaneous setting of at least three reception points. Because distances are small, high-precision timing and accurate time synchronization between the reception points are a necessity. It is effective when detecting impulse signals.

However, although the methods for outdoor measurements are usually successfully applied, in the event of interference and multiple path signal propagation, they do not give a satisfactory result in every case. In densely built environments and in the interior of buildings, the main problem in the detection of radio signals is their reflection from objects and the scattering of these reflections. To determine the radio source within buildings, a better solution would be to determine signal strength decreases by using the Received Signal Strength (RSS) method. By knowing the damping of the medium, and by measuring the intensity of the incoming signal in different places, and then calculating the distance and attenuation, the source location can be determined by representing the intersection of the circles [19, 41-43]. The increase in damping value in open terrain for an isotropic antenna is proportional to the square of the distance between the transmitter and receiver. Between and within buildings, this value can only be modeled using complex formulas. Depending on the frequency and the built environment, several damping formulas can be written. The literature contains the Okumara-Hata model, which is contained in the expression (1) [44]:

$$PL = 69{,}55+26{,}16\cdot\log(f) - 13{,}82\cdot(h_t - h_r) - c(h_r) + [44{,}9 - 6{,}55\cdot\log(h_t - h_r)]\cdot\log(d), \quad (1)$$

where PL is propagation loss measured in dB, f frequency measured in Hz, d distance between transmitter and receiver measured in m, h_t and h_r transmit and receiving, respectielly, antenna height measured in m, and $c(h_r)$ correction factor, the value of which is as follows:

$$c(h_r) = -\begin{cases} 3{,}2\cdot\log^2(11{,}75\cdot h_r) - 4{,}97; & \text{in a large city,} \\ [1{,}1\cdot\log(f) - 0{,}7]\cdot h_r - [1{,}56\cdot\log(f)] - 1{,}8; & \text{in a small town,} \\ 2\cdot\log^2\dfrac{f}{28} + 5{,}4; & \text{in a suburban area,} \\ 3{,}2\cdot\log^2(f) - 18{,}33\cdot\log(f) + 40{,}94; & \text{in an open area.} \end{cases} \quad (2)$$

Furthermore, the International Telecommunication Union (ITU) prescribed formulas of which ITU-R P.1238-7 02/2012 has been optimized for frequencies above 900 MHz. The term is described in the following expression [45]:

$$L_{total} = 20\cdot\log(f) + N\cdot\log(d) + L_f(n) - 28, \quad (3)$$

where N is a distance power loss coefficient, d separation distance (measured in m) between the base station and portable terminal (with $d > 1$ m), L_f floor penetration loss factor measured in dB and n number of floors between base station and portable terminal ($n \geq 1$).

DETECTION OF RADIO SOURCE IN A DENSELY BUILT ENVIRONMENT WITH THE COMBINED USE OF COMPLEX TECHNOLOGIES

As you can see, attenuation is strongly dependent on the environment. Therefore, it is not easy to determine the location of a radio source, even when using the RSS method, furthermore, navigation within the buildings without a GPS signal is also a challenge. The conceptual layout presented can provide a novel solution to these difficulties. This solution can, in principle, achieve the best results with the simultaneous use of several already existing simple technologies. The implementation consists of a complex measuring unit and a data processing evaluation part. The measuring unit measures its own spatial position and the strength of the set radio signal on the spot. The data processing unit displays the recorded data on a graphical interface to the user. One possible solution to measuring accurate spatial location is inertial navigation. The principle of the operation of inertial navigation systems is based on the application of physical phenomena that occur when accelerated movement of bodies is examined in a standing right-angle coordinate system. Accelerometers are used to measure inertial navigation systems. Nowadays, small size *Inertial Measurement Unit* sensors are available that can be used and are accurate enough to accomplish this task. The sensors perform complex functions in terms of their operation by providing acceleration, rotation and magnetic field data through their output. The coordinates that are absolutely necessary for positioning are calculated from the second integral of the accelerometer timing signals [46-49], see Figure 2.

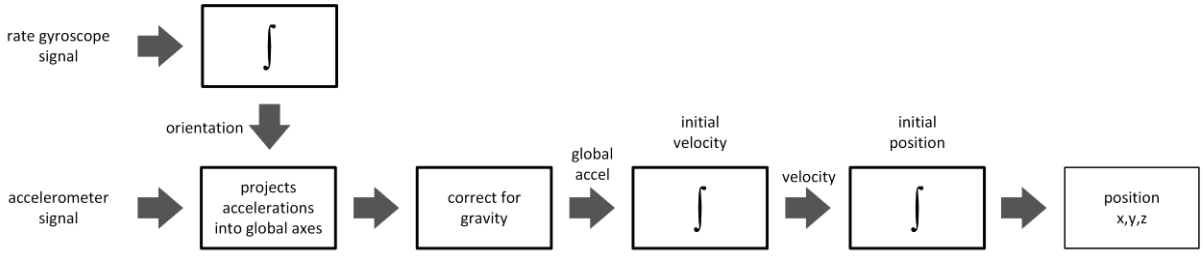

Figure 2. Gyroscope-based positioning [48].

At about the same time, the signal strength and bandwidth signal are determined with a software radio with surround antennas. We assign the values of the strength of the radio signal in the given space to the location data, previously calculated from point to point. The resulting data is transferred to a database. After the data processing, the radio field strength distribution of the area is examined based on a given frequency and is then shown graphically in three dimensions. Visualization can be carried out by matching the combination of various false color and thermal imaging methods with the blueprints and maps of the examined area. The implementation and evaluation of the measurement, in the case of a preconfigured system, does not require special expertise from the people performing the task. The layout principle is shown in Figure 3.

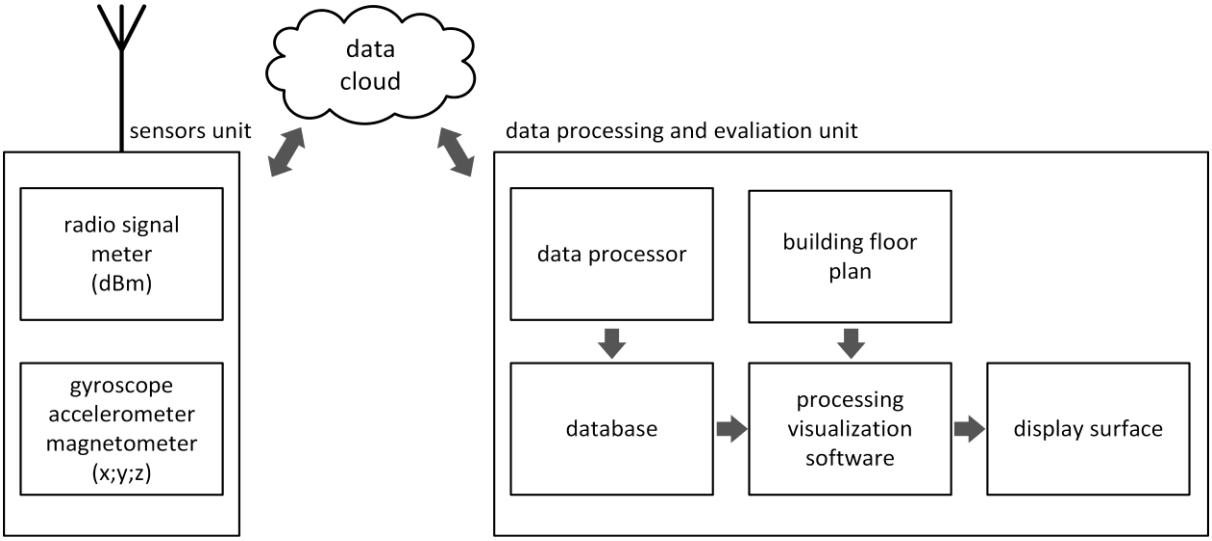

Figure 3. Location-based radio coverage meter layout.

The system consists of two separate units. By analyzing the layout, it becomes obvious that the evaluating display unit does not have to be on the measuring site and the measurementdata can be evaluated offline and online too. The small size of the radio measuring unit, that functions as a probe, allows for it to be easily integrated into a variety of autonomous robots (UAVs, UGVs) so that areas can be mapped quickly to detect the source of the given radio signal. In the following, the practical implementation of the measuring system is to be carried out in connection with the continuation and closure of the research so that we can conclude the feasibility of the theory based on the realistic measured data.

SUMMARY

The data security of human communication that goes on in smart cities carries the heightened risk of data breach, that is cumulatively present due to the opportunities offered by the different technologies. The physical design of protected rooms, which requires the creation of a separate room for the sake of information security is discussed in this article. The space around the protected premises, as a possible data transmission channel, requires the task of continuous control. New radio frequencies near protected areas may be the source of information security hazards, the source of which is to be identified. There are several possible solutions for measuring radio direction and determining transmitter location, however, it is difficult to implement these solutions in built environments, due to the attenuation and multi-path diffusion phenomena. By studying this problem, we would like to offer a novel conceptual solution to the task, which can provide a solution for discovering sources of radio signals in a built environment. The positioning, measuring and evaluation functions used in the measurement fit into the concept of simple implementation that is a typical to smart systems.

ACKNOWLEDGMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System", application number: GINOP-2.2.1-15-2017-00098.

REFERENCES

[1] Tokody, D. and Schuster, Gy.: *Driving Forces Behind Smart City Implementations – The Next Smart Revolution*.
Journal of Emerging Research and Solutions in ICT **1**(2), 1-16, 2016,

[2] Lazányi, K.: *The role of safety culture in supporting managerial decisions.*
Taylor Gazdálkodás- és szervezéstudományi folyóirat **1**, 143-150, 2016,

[3] Kuris, Z.: *New directions in complex information protection in relation to the protection of national classified information*.
Hadmérnök **5**(4), 2010,

[4] Lazányi, K.: *The safety culture.*
Taylor Gazdálkodás-és szervezéstudományi folyóirat **1**(2), 398-405, 2015,

[5] –: *2009 CLV. Act on the Protection of Classified Information.*
accessed 1st December 2017,

[6] *90/2010 (III. 26.) Government Decree on the operation of the National Security Supervisory Authority and the handling of classified information.*
accessed 1st December 2017,

[7] *92/2010. (III. 31.) Government Decree on detailed rules for industrial safety inspection and site security certification*.
accessed 1st December 2017,

[8] *161/2010. (V. 6.) Government Decree on detailed rules for the electronic security of classified information and the authorization and regulatory oversight of concealed activities.*
accessed 1st December 2017,

[9] *Act L of 2013 on Electronic Information Security of Public and Municipal Bodies.*
accessed 1st December 2017,

[10] GovCERT-Hungary.
http://www.cert-hungary.hu, accessed 1st December 2017,

[11] Marshall, D.A.; Sushil, J.J. and Podell, H.J.: *Information Security: An Integrated Collection of Essays*.
IEEE Computer Society Press Los Alamitos, 1995,

[12] *ISO/IEC 20000-1:2011 Information technology – Service management.*
https://www.iso.org/standard/51986.html, accessed 1st December 2017,

[13] 2011 CXII. *Act on the Right to Information Self-Determination and Freedom of Information*.
accessed 1st December 2017,

[14] ISO: I*SO/IEC_27000-series, Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
https://www.iso.org/standard/73906.html, accessed 1st December 2017,

[15] Ackoff, R.L.: *From Data to Wisdom.*
Journal of Applied Systems Analysis **16**, 3-9, 1989,

[16] IBM Global Business Services Executive Report: *Smarter cityes for smarter groeth; How cities can optimize their systems for the talent-based economy.*
IBM Global Business service, Executive report, IBM Institute for Business Value, 2010,
http://www.zurich.ibm.com/pdf/isl/infoportal/IBV_SC3_report_GBE03348USEN.pdf, accessed 1st December 2017,

[17] Lados, M.: *Cities for Smarter Growth*.
IBM Institute for Business, 2011,

[18] Lord, N.: *Information Protection vs. Information Assurance: Differentiating Between Two Critical IT Functions*.
Digital Guardian, 2016,
[19] Nisar, A.: *Radio Direction Finding: Theory and Practices.*
https://www.researchgate.net/profile/Nisar_Ahmed10/publication/289779492_Radio_Direction_Finding_Theory_and_Practices/links/569e752508ae21a56424b5a2/Radio-Direction-Finding-Theory-and-Practices.pdf, accessed 1st December 2017,
[20] Woodman, O. J.: *An introduction to inertial navigation*.
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf, accessed 1st December 2017,
[21] Kuris, Z.: *Approaching Complex Information Security Implementation Options*.
Hadmérnök **4**(2), 311-318, 2009,
[22] Tokody, D. and Mezei, I.J.: *Creating smart, sustainable and safe cities*.
2017 IEEE 15th International Symposium on Intelligent Systems and Informatics, 14-16 Sept. 2017. IEEE, Subotica, 2017,
[23] Ványa, L.: *Modernizing electronic warfare assets, systems and management in the face of new challenges, in particular electronic countermeasures.*
[24] Haig, Zs.: *Complex Interpretation of Information Security, Robotage 6.*
http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf, accessed 1st December 2017,
[25] Kerti, A.: *Examination of the technical subsystem of the management and information system with special regard to quality assurance and transmission security.*
Miklós Zrínyi University of National Defense, 2010,
[26] Muha, L.: *Protecting critical information infrastructures of the Republic of Hungary.*
Miklós Zrínyi University of National Defense, 2007,
[27] Haig, Zs.: *Information-based threats to the information society.*
Hadtudomány **17**(3), 2007,
[28] Rajnai, Z. and Fregan, B.: *Critical Infrastructure Protection.*
Proceedings of the XXI. International Scientific Conference of Young Engineers, pp.349-352, 2016,
[29] Vadász, P.: *Competitive intelligence as a branch of economic intelligence.*
Hadmérnök **9**(2), 343-357, 2014,
[30] Varga, P.J.: *The critical infrastructure and critical information infrastructure.*
Hadmérnök **3**(2), 149-156, 2008,
[31] Keszthelyi, A.: *Information security, basic technical knowledge.*
Vállalkozásfejlesztés a XXI. században, pp.303-340, 2012,
[32] Berek, L.: *Security systems.*
Nemzeti Közszolgálati Egyetem, Budapest, 2014,
[33] Berek, L.; Berek, T. and Berek, L.: *Person and property security textbook.*
Óbudai Egyetem, Budapest, 2016,
[34] Boros, B. et al.: *Law enforcement, property protection.*
BME, Budapest, 1997,
[35] –: *Information on the tasks of the National Security Supervisory Authority and on the qualification of electromagnetic radiation protection on the Internet*.
http://www.nbf.hu/tempestmer.html, accessed 1st December 2017,
[36] Töltési, I.: *Monitoring protection in business 1*.
Detektor plus folyóirat, pp.32-33, 2006,
[37] Töltési, I.: *Monitoring protection in business 2*.
Detektor plus folyóirat, pp.58-59, 2006,
[38] Töltési, I.: *Monitoring protection in business 3.*
Detektor plus folyóirat, pp.47-49, 2006,
[39] Vaszari, Á.: *Business Intelligence for Multinational Companies and Small and Medium Enterprises.*
Budapest Technical College, Budapest, 2007,
[40] Karl, R.: *Antenna book.*
Műszaki Könyvkiadó, Budapest, 1977,

[41] Németh, Zs.: *Locating on wireless networks*.
BME, Budapest, 2009,
[42] –: GOP 1.1.1-11-2011-0048 *Examination of localization methods, protocols and their applicability.*
http://www.corvex.hu/files/3214/2668/9380/R14AB_Lokalizacios_modszerek_protokollok_es_alkalmazhatosaguk.pdf, accessed 1st December 2017,
[43] Paul, D.: *An Introduction to Radio Direction Finding Methodologies.*
https://wireless.vt.edu/symposiumarchives/2015_slides/document.pdf, accessed 1st December 2017,
[44] Takács, Gy.: *Positioning with mobile phone and mobile network.*
Híradástechnika **63**(8), 20-27, 2008,
[45] International Telecommunication Union: *Recommendation ITU-R P-1238-7: Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz.*
https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1238-7-201202-S!!PDF-E.pdf, accessed 1st December 2017,
[46] Kornél, Gy.; Varga, P.J. and Illési, Zs.: *WLAN heat mapping in hybrid network.*
In: Novitzká, V.; Korečko, Š. and Szakál, A., eds.: *Proceedings of the 2017 IEEE 14th International Scientific Conference on Informatics*. IEEE, Poprad, pp.94-97, 2017,
http://dx.doi.org/10.1109/INFORMATICS.2017.8327228,
[47] Smalling, K.M. and Eure, K.W.: *A Short Tutorial on Inertial Navigation System and Global Positioning System Integration*.
https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150018921.pdf, accessed 1st December 2017,
[48] Woodman O.J.: *An introduction to inertial navigation.*
Technical Report UCAM-CL-TR-696, University of Cambridge, 2007,
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf, accessed 1st December 2017,
[49] Cveticanin, L.; Mester, Gy. and Biro, I.: *Parameter Influence on the Harmonically Excited Duffing Oscillator.*
Acta Polytechnica Hungarica **11**(5), 145-160, 2014.