Intrusion Detection and Shielding Measurements using Signals of Opportunity

Rıdvan Aba[1]
[1]*University of Twente*
Enschede, The Netherlands
ridvan.aba@utwente.nl

Robert Vogt-Ardatjew[1]
[1]*University of Twente*
Enschede, The Netherlands

Frank Leferink[1,2]
[1]*University of Twente*
Enschede, The Netherlands
[2]*Thales, Nederland B.V.*
Hengelo, The Netherlands

***Abstract*—Shielding effectiveness measurements of big structures such as information security centers, safe rooms, and nuclear power plants can be challenging because they can be time-consuming, costly, and difficult to apply. Since the shielding effectiveness is a critical parameter for such structures, the measurements are needed to be repeated periodically, especially for TEMPEST shielded rooms. This study proposes an improvement to shielding effectiveness measurements utilizing signals of opportunity. In this technique, different from the classical measurement methods, the strengths of already-existing-signals in the given environment are used instead of purposely generating them with dedicated hardware. By taking the differences between the measurements performed inside and outside a cabinet, or a room, a quick estimation can be made for the shielding effectiveness. The technique can be applied to evaluate the deterioration of shielding or as a watchdog for intrusion detection. The paper concluded with a discussion of the pros and cons of the method.**

Keywords—shielding effectiveness, signals of opportunity, random-walk technique, TEMPEST

I. Introduction

Shielding effectiveness (SE) is the measure of the attenuation of an incident wave in terms of electric or magnetic field strength in a material [1]. The attenuation is a result of reflection, absorption, and multiple-reflection losses due to boundary mismatch [2]. SE is one of the major topics in the electromagnetic compatibility (EMC) world because it usually both increases immunity and reduces emissions. For this reason, SE is an important issue from household electronic devices to military equipment. It is also important for complete platforms like armored (shielded) vehicles, ships as well as buildings such as nuclear power plants, informatics centers, and TEMPEST shielded rooms.

A variety of different standards and measuring techniques for SE measurements depending on the intended use are available. A well-known measuring procedure is explained in IEEE Standard 299 [3] for shielded rooms. MIL-STD-188-125-1 is a widely used international standard for military applications [4]. An overview of shielding effectiveness measurement techniques is shown in [5]. Although the frequency range, dynamic range, applied power, and used antennas are different for each standard, the measurement technique is the same for all standardized SE measurements. While an electric or magnetic field is applied toward the material under the test, cabinet, or wall using a transmitter antenna, another receiver antenna measures the power from the opposite side. A representative SE measurement is given in Figure 1.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 955.816.

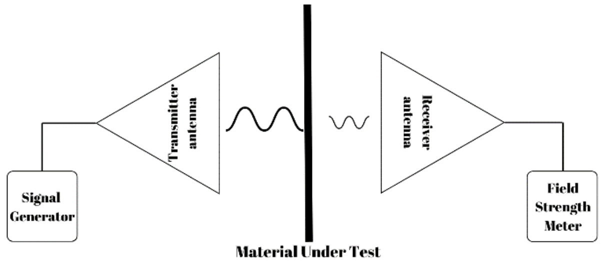

Fig. 1. Representative shielding effectiveness measurement

The traditional SE measurements can be time-consuming, costly, and difficult to apply, especially for big platforms such as safe rooms and buildings. The main reason is the necessity of synchronization between transmitter and receiver - both shall operate at the same frequency. The test may not be applicable to all necessary points because of the required antenna positions or the geometry. Also, the typically high transmitted power for SE measurements may be dangerous in some cases i.e. nuclear power plants. Therefore, alternative measurement methods are of interest. There exist some alternative and easier-to-apply methods for SE measurements for different materials and test sites. A new measurement technique was introduced in [6] where no amplifier is needed for achieving a large dynamic range due to the strong field intensity generated in the resonant cavities. For this technique, two vibrating intrinsic reverberation chambers (VIRCs) are used. An opening is left in the common wall of the two connected VIRCs, which is covered with the material under test. Another method is using the nested reverberation chamber technique [7]. In this method, a small reverberation chamber is located in the active volume of another big reverberation chamber. An opening in the small reverberation chamber is covered with the material under test. The receiver antenna is located in the small reverberation chamber while the transmitter is located in the big reverberation chamber but outside the small one. An SE measurement method using a hybrid nested reverberation chamber was introduced in [8]. In this method, instead of a small reverberation chamber a shielded box is located in the active volume of the reverberation chamber, and the SE measurement is performed. The above-mentioned measurement methods are suitable for small materials. These methods are not applicable to big structures, and already an overview was given in [5]. For this reason, an alternative measurement method was introduced in [9] for buildings. Instead of two antennas, only the receiver antenna is used for this method. The measurements are performed using the already-existing signals instead of applying a signal using a transmitter antenna. A few frequency bands are selected and the power is measured both inside and outside the building. The difference between the measured signal levels indicates SE of the building. A similar method was introduced in [10] for the nuclear power plants. A reference signal level is measured on the roof of the building. Performing the measurements inside the building and taking the difference between these two levels, the SE of the building is calculated.

The SE measurements are performed regularly for many critical facilities and platforms. There is also a need for intrusion detection, e.g. watchdog system, or maybe just detection of a loss of SE, to check any deterioration, during the operation of the facility or platform. In this study, an improved version of the methods mentioned in [9] and [10] is used. Instead of taking the reference measurement on the roof of the building or putting the receiver antenna at a fixed-position during the measurements, the random-walk technique is utilized during the reference and SE measurements. The core idea of this study is to make a base for an alternative shielding effectiveness and intrusion detection in a time and cost-effective way. The novelty lies in the usage of the random-walk technique combined with the signals of opportunity to mimic multiple receivers using only one. The paper is organized as follows: in Section II, the details of the technique and the differences with the other techniques are discussed. In Section III, the measurement setup is explained. Results and discussion are given in Section IV, and Section V concludes the paper.

II. Measurement Technique

A. The Traditional Method

The traditional SE measurements are performed at specified distances, using certain antennas, and by dividing the material under test into subsections. Two exemplary SE measurement configurations are given in Figure 2 and Figure 3. These figures show two different measurement cases explained in IEEE 299 international standard [3]. The distances, measurement points, and polarization of the measuring antennas are specified and fixed. Considering the number of test frequencies, the number of antennas, and the dimensions of the building, the test period can take weeks. Also, some test points may not be tested properly because of the geometry of the structure under test.

B. Random-Walk and Signals of Opportunity Method

Considering the above-mentioned reasons, we propose to use signals of opportunity that already exist in the medium. The signals of opportunity method is not a new technique. It was already used for different purposes such as improving navigation accuracy [11], and mobile positioning in urban environments [12]. Signals of opportunity were already utilized in measuring the SE of big buildings. The method we propose in this study is an improved version of the methods explained in [9] and [10]. We combine the signals of opportunity and the random-walk measurement techniques. In this experiment, we use a lightweight real-time spectrum analyzer (RTSA) to apply the random-walk measurement technique to measure the maximum power levels both inside and outside the facility, building, platform, or even a single cabinet. Utilizing the ergodic theory, one can say that the average behavior of the signals measured by a moving measuring unit equals the average behavior of the signals measured by a big number of measuring units [13]. Considering this statement we can say that the implementation of random walk simulates the use of multiple software-defined radio (SDR) probes.

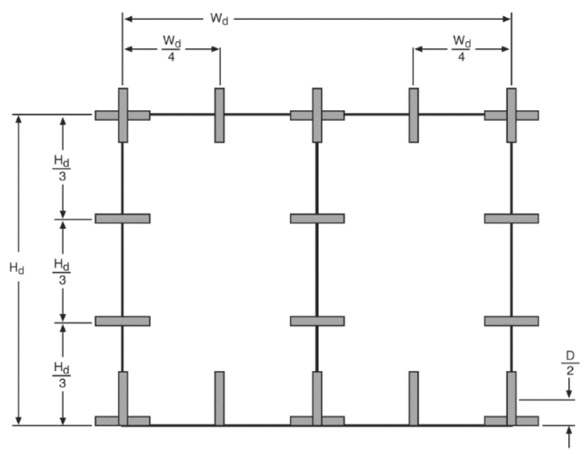

Fig. 2. Double entry panel door measurements [3]

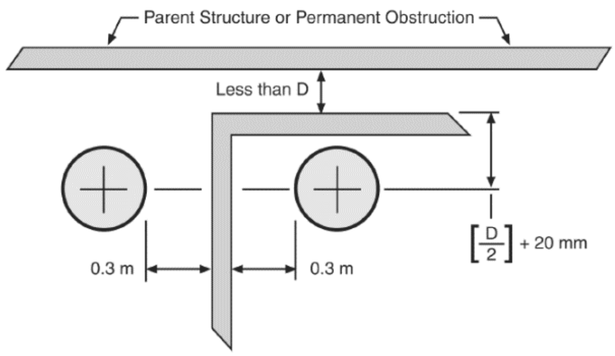

Fig. 3. Partially accessible corner seam measurements [3]

This method is not a perfect way of measuring the SE because the utilized signals are expected to be inconsistent throughout both space and time due to the dynamics of the environment. Since we perform the SE measurements without applying any extra signal, it is critical to measure the maximum power levels (max hold) to maximize the dynamic range. One of the points to be underlined here is the signal levels are changing over time. If the antenna was measuring at a fixed position, due to the dynamic environment the possibility of missing the maximum signal level would increase. With the help of the random-walk technique, the possibility of missing the maximum signal is reduced, as well as the time dependence of the measurement. Another point to be considered is the power level measured inside the facility, building, or platform may be at a higher level than outside because of the resonances or other sources inside occupying the same, even narrow, frequency band. Therefore, the results obtained are not expected to be as precise as the standardized SE measurement results. It is nonetheless a good approach for big structures because of its time and cost-efficiency, and main purpose: to check if a facility, building, or platform deteriorates over time. Or for intrusion detection for a cabinet, facility, building, or platform. In these cases, there is more interest in the relative change of SE over time, rather than providing the perfect absolute SE value. Especially for the information security centers, TEMPEST shielded cabinets and shielded rooms where the SE value is critical and the measurements should be performed periodically. This method gives a chance to estimate the SE of the facility, building, or platform in a cost and time-effective way to check degradation or intrusion. A representative SE measurement using the signals of opportunity method is given in Figure 4.

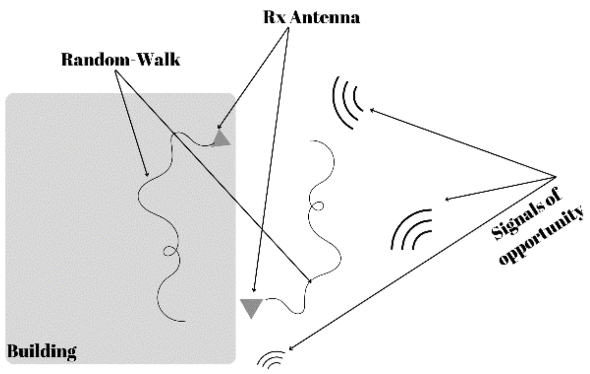

Fig. 4. SE measurements using signals of opportunity

Fig. 7. Outside measurements

III. Measurement Setup

We performed the measurements to estimate the SE of a wall of a building located on the University of Twente campus, Enschede, The Netherlands. For these measurements, we used only one antenna as a receiver, a lightweight RTSA to be able to utilize the random-walk and a laptop. The antenna is linearly polarized, broadband discone antenna. The measurements were carried out for 400 MHz – 3 GHz while the RTSA was in max-hold and data streaming mode. The sweep time was 140 ms. The measurement setup is given in Figure 5. The measurements were performed inside (Figure 6) and outside (Figure 7) the building during a random-walk, and the maximum power level is saved. The difference between the maximum power levels is the estimated SE. Different from the standardized method, the distance from the wall and the polarization of the antenna are randomly changed due to the random-walk. The measurements were taken for 5 minutes for each side.

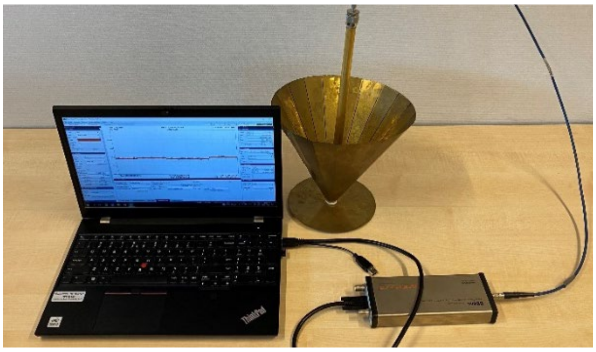

Fig. 5. Measurement setup

Fig. 6. Inside measurements

IV. Results & Discussion

The measurements were performed from 400 MHz to 3 GHz for both inside and outside. The measured power levels for inside and outside are given in Figure 8. Taking the difference between these measured power levels, the estimated SE results are given in Figure 9. At first glance, one could say that the SE is not continuous and therefore the results do not make sense. However, if we look at the measurement results performed inside and outside, we can see that the signals of opportunity are observed in certain bands, not in the whole spectrum. Another attractive result that can be seen from Figure 9 is that SE looks negative around 1750 MHz, which is not expected to happen. This is caused by the repeaters installed inside the building. The measurements were performed while normal life continued in the building, where there were some active EM signal sources such as WI-FI modules and telephones. However, the signal appears inside, it is invisible outside. We can conclude as the SE should be the absolute value of the calculated value because the source of the field could be inside or outside. The corrected SE results are given in Figure 10. According to the results, the maximum measured SE value is 35.4 dB at 935 MHz where it goes smaller values for other frequencies. Also, the dynamic range is small compared to standard SE measurements as expected. It is important to bear in mind the results are dependent on already existing signals. Also, the measurements were taken for a standard wall having big openings. For this reason, the results are satisfactory. Being critical, a question may arise, “can SE be measured if there are different EM sources inside and outside, and if there are EM

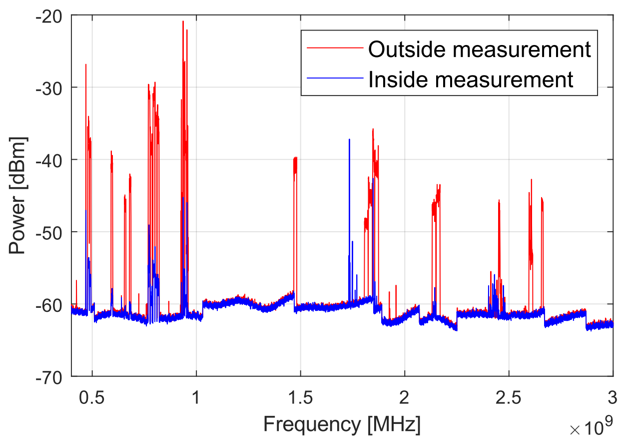

Fig. 8. Inside and outsude measurement results

emissions from these sources, at the same frequency, equal or very close levels?” In this case, the method we used would fail to measure the correct SE value. It should also be noted that if the measured signal level is low, the SE value cannot be measured correctly due to ambient noise. In such cases, the suggested here technique needs to be improved to isolate the signal coming from outside from the signals inside. Instead of measuring the total power in the given bandwidth, the power of a specific signal, e.g. in a specific Wi-Fi channel, should be compared by utilizing e.g. an SDR receiver instead of a spectrum analyzer.

V. CONCLUSION

This paper discusses a watchdog SE measurement method utilizing the already existing signals of opportunity. Also with the help of random-walk technique, the possible highest power level is measured. The strongest side of this method is performing the SE measurements without applying any extra signal. Only one antenna is used as a receiver for both inside and outside measurements. Also, a lightweight real-time spectrum analyzer and laptop are used to analyze the field. The random-walk represents the situation where several antennas and SDR receivers are being used, making use of the spatial ergodicity concept. Taking the difference between the power levels measured inside and outside, the SE value is estimated in a time and cost-effective way. This method is well-suited to check if a facility, building, platform, or even cabinet deteriorates over time, and for leakage and intrusion detection of secure rooms and TEMPEST shielded rooms.

To develop a full picture of SE and intrusion detection measurement utilizing signals of opportunity, additional study will be needed. The next step in our research is to use several SDR receivers which are tuned to known transmitters and record the received signal strength over time.

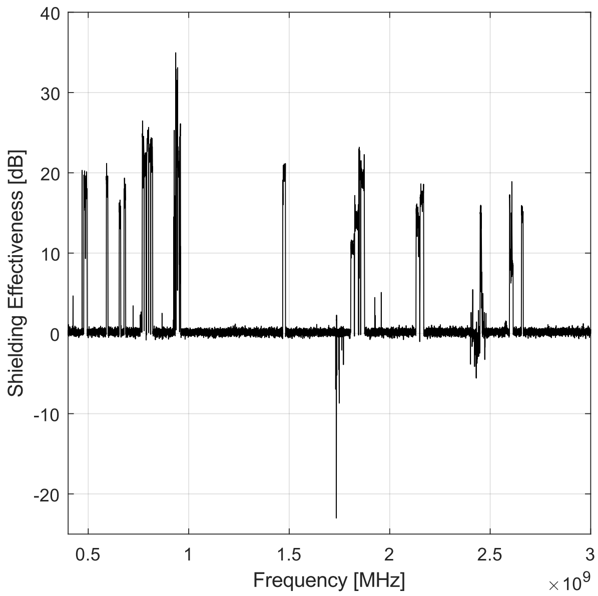

Fig. 9. Estimated shielding effectiveness values

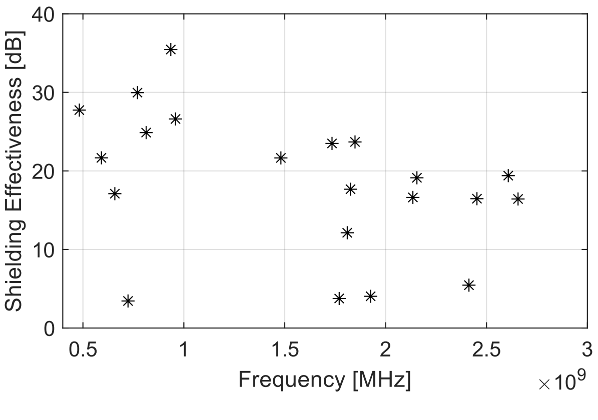

Fig. 10. Corrected shielding effectiveness values

REFERENCES

[1] R. B. Keller, *Design for Electromagnetic Compatibility-In a Nutshell: Theory and Practice*. Springer Nature, 2023.

[2] S. A. Schelkunoff, *Electromagnetic Waves*. D. van Nostrand Company, Inc., 1943, pp. *303–312*.

[3] "IEEE Draft Standard Method for Measuring the Shielding Effectiveness of Enclosures and Boxes Having All Dimensions between 0.1 m and 2 m," in IEEE P299.1/D6, July 2013 , vol., no., pp.1-101, 10 July 2013.

[4] MIL-STD-188-125-1, High-altitude electromagnetic pulse (HEMP) protection for ground-based C41 facilities performing critical, timeurgent missions, part 1 fixed facilities, App.A, Shielding effectiveness (SE) test procedures, 2005.

[5] H. Bergsma, C. Clemens and F. Leferink, "Shielding Effectiveness of Cabinets using IEEE 299 and IEEE 299.1 and Effect of Loading," 2022 International Symposium on Electromagnetic Compatibility – EMC Europe, Gothenburg, Sweden, 2022, pp. 59-63, doi: 10.1109/EMCEurope51680.2022.9901235.

[6] S. van de Beek, R. Vogt-Ardatjew, H. Schipper and F. Leferink, "Vibrating Intrinsic Reverberation Chambers for shielding effectiveness measurements," International Symposium on Electromagnetic Compatibility - EMC EUROPE, Rome, Italy, 2012, pp. 1-6, doi: 10.1109/EMCEurope.2012.6396655.

[7] M. O. Hatfield, "Shielding effectiveness measurements using mode-stirred chambers: a comparison of two approaches," in IEEE Transactions on Electromagnetic Compatibility, vol. 30, no. 3, pp. 229-238, Aug. 1988, doi: 10.1109/15.3301.

[8] H. E. Ozdemir et al., "A Novel Hybrid Nested Reverberation Chamber Measurement Technique for Shielding Effectiveness of Conductive Fabrics," 2022 International Symposium on Electromagnetic Compatibility – EMC Europe, Gothenburg, Sweden, 2022, pp. 201-205, doi: 10.1109/EMCEurope51680.2022.9901027.

[9] E. B. Savage, J. L. Gilbert, W. A. Radasky and M. J. Madrid, "An alternative EM shielding effectiveness measurement method for buildings," 2010 Asia-Pacific International Symposium on Electromagnetic Compatibility, Beijing, China, 2010, pp. 138-141, doi: 10.1109/APEMC.2010.5475830.

[10] H. Kim, K. Lee and H. Lim, "Simple Measurement Methods of Shielding Effectiveness in Nuclear Power Plants," 2018 International Symposium on Antennas and Propagation (ISAP), Busan, Korea (South), 2018, pp. 1-2.

[11] E. Kim and Y. Shin, "Analysis of the Signals of Opportunity and Cooperative Based Positioning for UAS Navigation in Deep Urban Area," 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 2019, pp. 1-8, doi: 10.1109/ICNSURV.2019.8735152.

[12] C. Yang and A. Soloviev, "Mobile Positioning with Signals of Opportunity in Urban and Urban Canyon Environments," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 1043-1059, doi: 10.1109/PLANS46316.2020.9109876.

[13] M. Brin and G. Stuck, *Introduction to Dynamical Systems*. Cambridge University Press, 2002.