An Introduction to Cybersecurity at Physical Layer: Obstacles at Radio Channel to Mitigate Hackers' Chance

Inigo Cuinas[1, 2]
[1]*Department of Signal Theory and Communications, University of Vigo, Rua Maxwell s/n, 36310 Vigo, Spain*
[2]*atlanTTic Research Center, University of Vigo, Rua Maxwell s/n, 36310 Vigo, Spain*
inhigo@uvigo.es

***Abstract*—Cybersecurity commonly focuses on higher layers of Open Systems Interconnection (OSI) model, as it is a discipline associated to Computer Science. However, physical layer is the front line of the defence of a system against external attacks, and Electrical Engineering, concretely Radiofrequency Engineering, can provide tools to reinforce radio networks also in terms of information security. This paper analyses different techniques related to site shielding. From hard traditional shielding, similar to Faraday cages, to different soft shielding solutions as vegetation fences and frequency selective surfaces (FSS), the variety of solutions is broad and would be useful in actual deployments. Finally, Building Information Modelling (BIM) appears as an interesting tool that could be incorporated along the design and construction of an office building to improve the electromagnetic behaviour, and subsequently the cybersecurity issues of the communication networks hosted by the building itself.**

***Index Terms*—Building materials; Cybersecurity; Frequency selective surface; Isolation; Radio systems.**

I. INTRODUCTION

All Electrical and Computer Science engineers used to draw on the traditional Open Systems Interconnection (OSI) model of seven layers to define a communications system and to explain how each specific development relates to the complete framework [1]. Then, we know that we can organize and describe a system within seven levels of abstraction: application, presentation, session, transport, network, data link, and physical (from more abstract to more tangible). In general, when we talk about cybersecurity, we think on the most advanced (or abstract) layers, as we commonly focus more on logic situations than on physical events. In fact, physical layer becomes "the ugly duckling" among the OSI levels for cybersecurity researchers, as they are more interested in the way hackers can access, alter, disturb, and even control those communication systems than on limiting these activities at physical level.

Further away, we can consider the physical layer as the forgotten layer in terms of cybersecurity. Many engineers could ask themselves about what they could do related to cables (or better radio links) in terms of cybersecurity. This kind of questions opens the door for the contribution of radio engineers in providing knowledge and tools to help in security information to communication systems.

More and more wireless communication systems are deployed providing a wide collection of services to interchange data that deserve a moment to think on information security and the chances of a hacker to obtain or modify this information. Obviously, if the hacker is not within the coverage of the radio system, it is not possible for him or her to access the information. Being connected to a system is the first step to attempt to disturb it, and a physical connection (cable or radio) is required to that accessing event. Then, proposals that allow something like controlling or limiting the radio coverage range of a wireless system would act as a defence against malicious accesses. This fact anticipates solutions that involve hard walls, vegetation fences, and frequency selective surfaces (FSSs), from those very primitive to the more sophisticated proposals. Thus, a variety of techniques to provide network coverage isolation would represent a first front line in defending a system against cyberattacks. Results from our experimental research are presented in this work combined with the effect on the cybersecurity application.

Different solutions for shielding the radio networks of wireless systems can be considered during the design of office buildings by introducing that information in Building Information Models (BIMs) as a way of providing physical layer cybersecurity from the own structure design. This proposal would lead to higher efficient buildings in terms of information security giving additional performance to the companies established within them.

With these premises, the following sections will cover the previously commented aspects. The second section devotes to site shielding as a security strategy. The third section describes the hard shielding solutions, and the fourth section

Manuscript received 12 May, 2020; accepted 18 August, 2020.

This work was developed in the framework of Erasmus+ LMPI under Grant No. 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP, being the underlying research funded by Spanish Ministry of Science Development and Innovation under Grant No. TEC2017-85529-C3-3-R, by the regional government Xunta de Galicia under Grant No. ED431C 2019/26, and by European Regional Development Fund (ERDF).

the soft shielding, with special emphasis on vegetation fences, and FSS. The fifth section introduces BIMs and gives some insight on their applicability to network deployment within new buildings. Finally, conclusions occupy the sixth section.

II. SITE SHIELDING AS A SECURITY STRATEGY

As inspired by the introduction, the underlying issue is not just security, but largely security. In fact, site shielding becomes a relevant topic in current wireless network deployment, independently of cybersecurity, but its interest grows when analysed in terms of security.

The rapid proliferation of wireless systems, if most of them are within the non-licensed band of the radio electric spectrum, could lead to a collapse of all of them due to the (in-band and adjacent bands) interferences among the networks installed inside the same building and many times inside the same floor or even in the same office. The problem is not an individual or specific mismatch, as wireless standards are prepared to solve connection falls, generally by retransmitting the same information. The actual problem is that most of the networks are sharing the same spectrum allocation: when interferences force a retransmission and many networks are retransmitting at the same time, the spectrum bands become overloaded and the transmission capacity collapses. In this case, site shielding or better physical shielding separating wireless networks would reduce the probability of such catastrophic events.

In parallel, the use of shielding techniques would improve the information security. As users of a wireless network are not physically connected to that network (i.e., there is no cable between each user and the network equipment), they can be linked from places out of system manager surveillance. In fact, they can access the network outside the company, and even outside the own building from a public area. The people accessing the wireless network can use its facilities for private purposes, and even for forbidden or malicious actions. From this point of view, network shielding is a security issue: limiting the coverage of the wireless network to areas controlled by the network owner would reduce the possible unauthorized or malicious access.

The site shielding arises as a technique to mitigate these problems, e.g., by limiting the radio coverage [2]–[5], or even blocking the radio waves from certain directions, the radio systems could be safeguarded against connection from transmitters out of their specific area, and in parallel, interference could be reduced. As a consequence, the number of wireless networks sharing the same physical area may increase maintaining the required quality standards, as well as their protection against unauthorized accesses grows.

Thus, site shielding can be interpreted as the installation of physical elements that limit the radio coverage as a barrier to attenuate signals from other networks and to defend the own wireless system form outer interferences or attacks. This could be a direct contradiction with the traditional impossibility to put fences to the sky, but under certain conditions, this could be possible. In fact, there are several options with hard installations commented in Section III and softer alternatives as those developed in Section IV.

Figures 1–3 depict the situation in a graphical mode. In the open space configuration (Fig. 1), the radio waves emitted from any Wi-Fi base point, represented in green on the house walls, travel freely around this transmitting point, creating a volume with radio coverage.

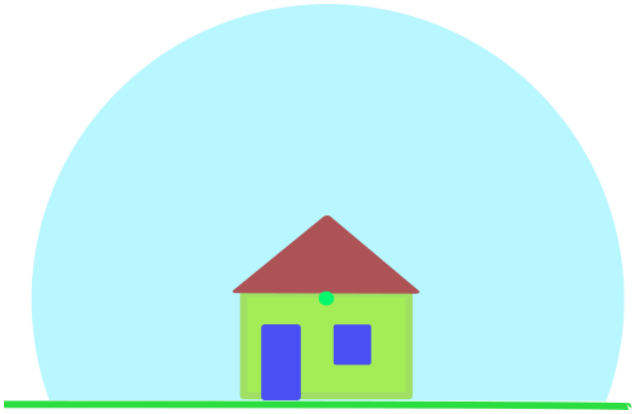

Fig. 1. Coverage around a domestic Wi-Fi access point.

When installing elements providing hard shielding (Fig. 2), these elements block the radio wave propagation, creating shadowed areas from which it is not possible to connect to the Wi-Fi system, as coverage does not reach them. On the other hand, soft shielding (Fig. 3) reduces, but does not block the radio propagation.

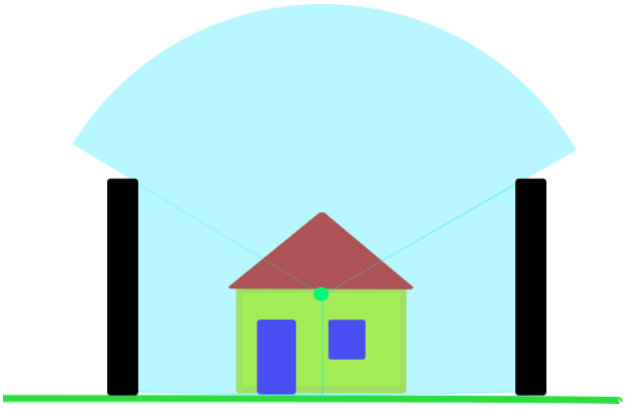

Fig. 2. Coverage around a domestic Wi-Fi access point with hard shielding elements.

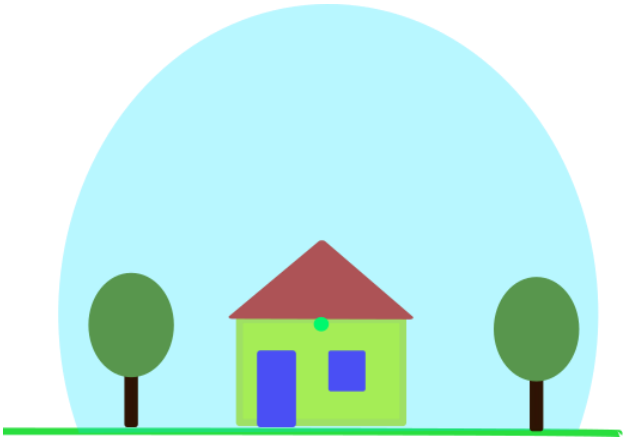

Fig. 3. Coverage around a domestic Wi-Fi access point with soft shielding elements.

III. HARD SHIELDING SOLUTIONS

When the objective is to block the radio wave

propagation isolating an area from external transmissions, and then eliminating the possibility of connections from outside, a first canonical solution is the use of classical Electromagnetic theory. It seems to be obvious that the construction of a Faraday cage enclosing the volume to be protected makes physically impossible to establish a radio connection between inside and outside extremes. This is absolutely safe, but extremely costly.

An easier alternative hard solution is the use of reinforced concrete walls, which provide so strong attenuations that establishing a radio link becomes almost impossible. However, the solution is not so aesthetic, and windows and doors turn out to be holes to the radio waves to come inside. Definitively, reinforced concrete walls or fences have strong impact, i.e., are very unfriendly and exceptionally expensive.

A less expensive option is the use of brick walls, which provides less, but perhaps enough attenuation to be proposed. Depending on the designer, the contractor, and even the local tradition, the size of the bricks, their design, and the materials they are made of can be different. In Southern European countries, the hollow bricks made by clay are very common, but dimensions vary in different countries, and also the organization of the transversal squared hollows: 1x3, 2x4 (e.g., Fig. 4), 3x4, and many other configurations.

Fig. 4. Example of 2x4 hollow clay brick.

A deep research done with wall samples made of different types of bricks and a variety of wall finishing (none, smooth painted plaster, and rough painted plaster) performed within an anechoic chamber gave us an idea of the performance of such a barrier for blocking radio waves. Figure 5 depicts the scheme of the measurement system within the anechoic chamber. This chamber was divided by a wall covered with absorbing pyramidal foam elements, with a centred open window placed just at the line of sight between transmitting and receiving antennas, to place the samples under test to check their attenuation properties.

As a result of the internal material hollow pattern and wall finishing, the brick wall samples presented a frequency selective behaviour, providing attenuations to waves transmitted across up to 60 dB at certain frequencies when using 20 cm thick bricks, and between 20 dB and 30 dB with 11 cm and 15 cm thick bricks, which are also considerable attenuations. However, at certain frequencies within the sub-6 GHz band, there are bands with attenuations below 10 dB. Besides, there are clear differences depending on the polarization of the incident wave. The geometry of the brick has a clear impact on the performance of the wall as a shielding method. Thus, wireless propagation through hollow clay brick walls should not be neglected in indoor radio planning stages, depending on the frequency used [6].

As a comparison, a concrete wall sample provided attenuations from 7 dB at 1 GHz to 30 dB at 10 GHz in a monotonically growing linear pattern due to its homogenous composition.

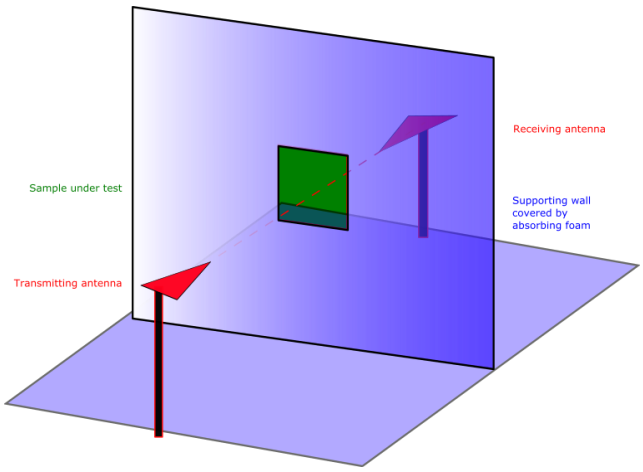

Fig. 5. Scheme of the measurement system.

IV. SOFT SHIELDING SOLUTIONS

Although soft shielding solutions provide less attenuation figures than hard versions, those are lighter, cheaper, and more aesthetic compared to the previously mentioned ones, and they could be good alternatives, depending on the specific need. In this section, we analyse two possibilities: the use of vegetation or the more controllable FSS.

A. Vegetation Fences

The proposal is the use of trees, organized in lines, as a barrier to attenuate signals from other networks [7] and to protect the own wireless system from outer interferences. Both inside plants and decorative trees can be used for this proposal: interior plants for cutting the line of sight between adjacent networks within the same floor of an office building and decorative trees to reduce the outdoor coverage of the wireless network around the own building, thus providing additional protection against hacker attacks or limiting the access to external users, which in both cases signifies an improvement in network security.

We developed a large measurement campaign in order to check the performance of vegetation fences as electromagnetic isolators. We centered the efforts in band used by wireless networks (2.4 GHz and 5.8 GHz) and in those of mobile systems (900 MHz, 1800 MHz, and 2100 MHz), gathering the attenuation induced by lines of small trees or bushes. Figure 6 shows the configuration of the basic measurement setup installed in open spaces. We organized the vegetation specimens in different fence configurations, allowing single and double lines and more or less density (by selecting different distances between adjacent specimens).

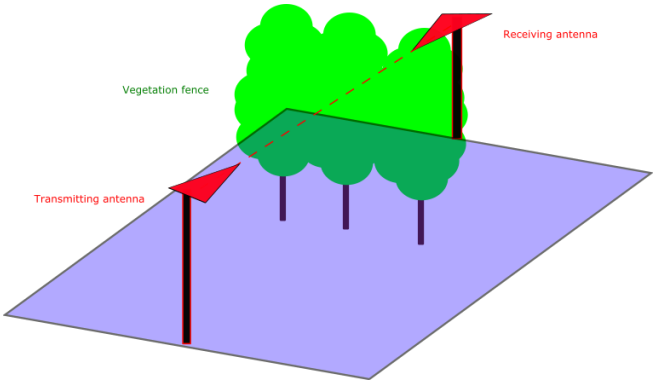

Fig. 6. Setup for measuring attenuation due to vegetation fences.

The measurements were done in narrowband conditions, with separate transmitter and receiver, and mounting the receiver on an automated linear positioner that moved parallel to the fence. We considered up to seven vegetal species, ten specimens from each, and specimens made all fences from the same species.

The selection of the indoor species is based on their popularity as decorative elements in buildings and indoor yards. They were *Heptapleurum arboricola gold capella* (commonly known as schefflera), *Dypsis lutescens* (areca palm) and *Ficus elastica* (ficus). On the other hand, outdoor species were chosen because of being typically used to make private fences in a short time or because of their massive foliage that favours electromagnetic shielding. The selection was: *Callistemon laevis* (callistemon or bottlebrush), *Camellia japonica* (camellia), *Juniperus communis hibernica* (Irish juniper), and *Thuja atrovirens* (white cedar). Figure 7 shows an example of double-line fence built up with ten specimens of *Camellia japonica*.

Fig. 7. Double fence made by *Camellia japonica* specimens.

Regarding wireless networks, we measured median attenuations up to 10.7 dB at 2.4 GHz with a double fence made of Irish juniper specimens and up to 21.2 dB at 5.8 GHz in similar configuration and species. Although these attenuation figures do not assure the complete isolation of the network, they represent important values considering the low aesthetic impact of the fences [8]–[10] compared to concrete walls.

The limitations on the applicability of this proposal reside on the variability of the induced attenuation due to the movement of the leaves that is translated into changes in the barrier configuration or the differences in humidity content of the plants during the measurement period, and what is more important, during the effective use as isolating fences.

However, what is interesting is that it is the improvement in isolation provided by these fences. Analysing the wireless standards, we can observe the reduction of the minimum free-interference distance in Table I, where we used the attenuation provided by the strongest vegetation fence, which was made of Irish juniper specimens. The interference mitigation is clearly possible using vegetation fences, as inferred from these results computed following the indications of 802.11 standard [11]. Thus, separating the coverage areas of two adjacent networks, the distance at which an element of one of the networks could be from an element of the other without interference is clearly reduced, improving the quality of service of both wireless networks.

TABLE I. REDUCTION OF MINIMUM FREE-INTERFERENCE DISTANCE WITH AND WITHOUT VEGETATION FENCE.

Modulation scheme	**Minimum distance (m)**	
	No fence	**Fence**
QPSK (Quadrature Phase Shift Keying)	2.95	0.8
16-QAM (Quadrature Amplitude Modulation)	6.6	1.79
64-QAM	13.65	3.69

When the objective is to protect against external attacks, the additional attenuation induced by the hurdle also reduces the physical distance at which a connection is possible, compared to the open situation. Thus, installing vegetation fences in the gardens around office buildings directly reduces the coverage of the wireless networks in the surroundings, and then the area from which an attack could be shouting is compacted. Consequently, the coverage extension could be closed to the allotment, not allowing the network access from public places, such as the street, so that uncontrolled accesses could be reduced compared to open coverage situation (line of sight from the wireless access points), as they must provide from a more reduced distance.

In that situation, some calculations could be made for determining the maximum distances at which a connection is possible. The sensitivity of network receivers could be used to compute the improvement provided by the fence in terms of protection against external attacks, considering some basic data from the 802.11 standard [11]:

– Maximum transmitting power: 20 dBm (2.4 GHz), 30 dBm (5.8 GHz);
– Typical transmitting power: 13 dBm;
– Sensitivity: -80 dBm (1 Mbit/s), -75 dBm (2 Mbit/s).

Using the data mentioned above, the coverage distances in free space conditions and when obstructed by a tree have been computed. Table II and Table III provide the results for the best case when using Irish junipers as unit elements within the vegetation fence.

In fact, these values are worst cases (in terms of radio propagation, the best cases), as the attenuation due to the building facade and walls, windows, doors, and other elements is not included in the computation. Distances with 5.8 GHz are perhaps assumable for the usage of vegetation fences.

TABLE II. MAXIMUM COVERAGE RANGE, ASSUMING MAXIMUM TRANSMITTING POWER.

Frequency	Transmission rate	Maximum coverage distance	
		No fence	Fence
2.4 GHz	1 Mbit/s	1.98 km	580 m
	2 Mbit/s	1.12 km	326.4 m
5.8 GHz	1 Mbit/s	2.60 km	226.7 m
	2 Mbit/s	1.46 km	127.5 m

TABLE III. MAXIMUM COVERAGE RANGE, ASSUMING TYPICAL TRANSMITTING POWER.

Frequency	Transmission rate	Maximum coverage distance	
		No fence	Fence
2.4 GHz	1 Mbit/s	888.6 m	259.3 m
	2 Mbit/s	499.7 m	145.8 m
5.8 GHz	1 Mbit/s	367.7 m	32 m
	2 Mbit/s	206.8 m	18 m

As a conclusion, the use of hurdles made by trees or bushes can be useful for minimizing interference among wireless networks in high-traffic areas, but its usability against hacker attacks seems to be not so interesting, considering the distances computed. The species that make up the barrier must be everlasting and densely foliated, and the specimens must be tall enough to cut the line of sight between both radio link ends.

On the other hand, there are some intrinsic problems as the instability, the variability of the attenuation induced, the effect of wind moving the leaves, the seasonal variations (growing, deciduous species), the effect of humidity and temperature, etc.

B. Frequency Selective Surfaces

FSSs are generally passive circuits, but there are also active circuits that perform as filters in open space. Then, these surfaces select the frequency bands for which they are transparent and those for which they present an opaque behavior. This is why they are "frequency selective". There are several generic responses for a FSS: band stop, band pass, low pass or high pass (exactly as electronic filters). This allows the designer to tune the FSS to eliminate some specific bands or make some them be transparent to other bands, being then flexible to protect some areas against certain radio links (i.e., wireless networks) while allowing some other communications (i.e., mobile phones). This flexibility makes the FSSs as good solutions for fixed frequency-dependent shielding, as well as for other applications, such as radomes, filters in indoor environments (both angular and spatial), dichroic filters, and others.

The history of FSS began in 1956 with the publication of research on sheet arrays selecting which frequencies were allowed to be absorbed and which were forced to reflect [12]. From that time, several researchers worked on this issue, specially developed ten years ago. At the beginning, the application was mainly military due to the possibilities of using such a material for RADAR camouflaging elements. Then, the range of uses moved to other areas, and cybersecurity is now among the most popular.

Research on FSS developed when the improvement of new and high precision analytical methods and the growing computation capability of our numerical equipment allowed the use of software suites to solve large and complex electromagnetic problems. The availability of these solvers provided the researchers with tools to design and optimize multitude of models and to construct and test only those with the promising future. Thus, research moved from large military laboratories, valid for costly experimental research, to small university centers, where professors with good knowledge on Electromagnetics, but not able to use expensive equipment, are now allowed to develop FSS designs adapted to specific applications and to optimize their performance using large batteries of simulations.

The variety of designs is then enormous: research on this area is fashionable nowadays, and new articles are constantly appearing on this topic. Typically, the FSS consist in a unit cell design, which flat geometry determines the frequency tuning repeated in a periodic array configuration. These arrays could be two-dimensional (or better quasi-two dimensional, as thin sheets could present several layers) or three-dimensional. The mutual coupling among unit cells slightly modifies the exact tuning of the complete surface so that its design is usually made in two steps: it begins with the simulation and optimization of the unit cell, and once it is tuned, the simulation (or the experimental analysis) extends to a larger matrix of a number of organized copies of that unit cell. Figure 8 shows two examples of unit cell designs.

There is also a large variety of materials for constructing prototypes or commercial solutions based on FSS concepts. Typically, laboratory proof-of concept prototyping is based on printed circuit boards (PCBs). However, final usable realizations could be also built on textiles, electrically conductive ink, metallic 3D elements, or even fluids [13].

It is well known that a PCB consists of a dielectric laminated substrate covered by copper sheets from one or both sides, determining if it is single sided or double sided. Besides, there exist multi-layered boards with multiple dielectric substrates and multiple copper layers. They are the most popular for prototyping as it is easy to create the printed patterns by etching chemical procedures, which can be performed at any electronics workshop. Other alternatives require more complex or specific equipment.

As an example, Fig. 9 shows a 50x50 cm^2 prototype of a FSS design printed on PCB. Some researches go further and provide a collection of equations that relate dimensions to frequencies and even bandwidths in order to help other designers to create new versions of each proposal.

Electrically conductive ink (i.e., with metallic components) is also an explored alternative for prototyping FSS designs deposed over different substrates, such as glass, paper, different polyester materials or solid (3D printed) objects. The ink technique is opposite to PCB-based prototyping: ink technique is additive and PCB-based prototyping is based on subtractive methods. As silver nanoparticle ink is available in inkjet printable format, it is very popular among researchers focused on this kind of activity.

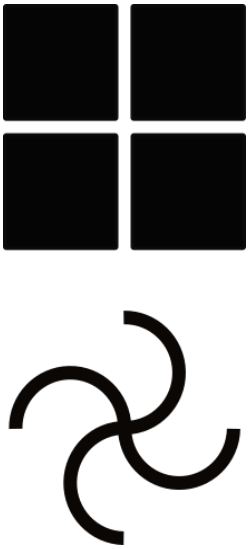

Fig. 8. Examples of unit cell designs for FSS.

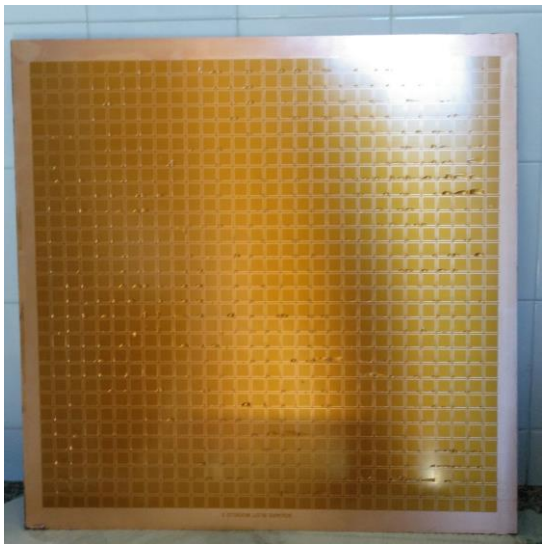

Fig. 9. Prototype of a FSS design.

Textile-conductive designs are another way of constructing FSS and they could be used as curtains, e.g., for cybersecurity applications. Considering that windows are the areas of the building facades that induce less attenuation to radio waves propagating across them, installing curtains like FSS could be a good and aesthetic solution.

The possible application of such a proposal is to cover the walls (or other perimeter elements) of a room to avoid radio waves of certain frequencies going out of the confined place or to avoid waves from outside coming inside. With adequate frequency tuning, it likely makes impossible to access the information carried by these radio waves from the places that are not controlled.

Measurement of prototypes is performed following a system as explained in Fig. 2 [13]–[18]. The basis is to gather the frequency response of the radio channel consisting on the transmitting and receiving antennas blocked by the FSS sample in the middle and to compare that with the response of the channel in line of sight conditions, without the FSS blocking the link, doing all of that within an anechoic chamber. Different techniques have been used to mitigate the diffraction on the PCB edges, being the most popular the use of an isolating wall covered by absorber foam, with a window in the centre to place the sample.

Depending on the design, attenuations of 20 dB or 30 dB, and up to 50 dB have been reached, which could be similar to brick walls and larger than vegetation fences, with the advantage of a deeper control on the frequency tuning and the stability of the figures. For example, designs like square loop provide 40 dB at 2.4 GHz [14], quarter ring - 45 dB at 2.4 GHz and 25 dB at 5.1 GHz [15], 3-D mechanically tunable square slot - 60 dB at 1.7 GHz and 40 dB at 3.5 GHz [16], and tunable square slot - 40 dB at 3 GHz [17].

The open possibilities of FSS incorporated to the building design are enormous, as they could be identified as future luxury elements in residential and office buildings as the elements that afford radio electric isolation comparable to those providing humidity isolation or thermal isolation.

V. BUILDING INFORMATION MODELS

BIMs are models to simulate the building performance from different points of view: constructive (as traditional work related to architecture), thermal, rain/humidity performance, sound/noise behaviour, and so on. BIM works as a layered model, in which each layer provides information about specific elements within the building: water, electricity, warming, air conditioning, thermal performance, and so on. The full building incorporates all these elements and information, but people working to create the building only need to obtain data from one or several layers, but probably never all the content. This simplifies the process of designing and constructing a house, as each specialist can work independently in his/her layer or layers, allowing multiple interactions during design and redesign processes and avoiding conflicts.

Adding electromagnetic performance as an additional layer of BIM would be an opportunity to incorporate radio electric isolation from the design. Thus, isolation would be considered as construction, instead of being an additional element incorporated when the user (a company or a family) detects detects the need of it. In fact, BIM is not a product, but a process to predict efficiently the assessment of different constructive performances. Its importance lays on the possibility of managing information and collaboration among teams associated with a constructive project (i.e., energy efficiency, acoustics performance) [19].

Looking forward towards the near future, the incorporation of electromagnetic attenuation and scattering characteristics from the various layers of building materials into BIM will be effective only when society changes. The first step will be when population reflects on the importance of keeping a control on the information we allow to radio transmit to the rest of the world and on the information we allow the rest of the world to provide to us. In fact, each building material could have its electromagnetic characteristics included within the BIM database, allowing the system to simulate the indoor radio coverage of a domestic Wi-Fi network, and thus to identify possible sources of malicious or non-desired accesses. Therefore, Cybersecurity at radio level would be included in the architectonic design of buildings.

VI. CONCLUSIONS

This paper explains possible actions to mitigate, and also to eliminate the possibility to suffer a hacker attack by accessing our own radio network. The idea departs from the concept of site shielding, which consists of creating barriers that restrict the radio wave propagation to a limit that hackers cannot access the wireless network because the coverage of its access points is not enough to reach the malicious person location. This is why it is considered as a physical layer technique to reduce the effect of cybersecurity attacks. Thus, the analysis of the various options for hard and soft shielding of electromagnetic waves is the main topic of this paper.

A collection of results of different measurement campaigns is presented for both hard and soft shielding proposals: brick walls, vegetation fences, and FSS. Depending on the options, stronger attenuations or cheaper and more aesthetic solutions could be reached.

In general terms, hard shielding proposals provide deeper attenuation than softer ones. In fact, depending on the strategy, a total blockage of the radio waves being transmitted across the obstacle could be reached, as it is the case of using Faraday cages. However, this is an extreme solution for aesthetic and economic reasons.

The next step in protection with a bit less attenuation, but still hard impact, is the construction of concrete, or even reinforced concrete walls or fences. They induced extra attenuations without any kind of frequency selectivity: attenuation grows monotonically with the frequency, and it does not depend on the wave polarization. As an example, a 10 cm width concrete wall would provide attenuations from 5 dB at 500 MHz to 35 dB at 10 GHz in a continuous growing.

Less attenuation at cheaper cost and with possibilities that are more decorative become the characteristics of the softest among the hard shielding techniques, which is the building with brick walls. The attenuation provided by brick walls depends a lot on the design of the unit bricks (they could be solid or hollowed), the material they are made from, and the finishing applied on their surface (the own brick surface, a plaster covering, painting over the plaster, etc.). Besides, the hollow pattern determines a frequency dependent effect: the brick wall could be almost transparent (attenuations less than 3 dB) for some frequencies and strongly attenuating for other (up to 45 dB) as a consequence of the ratios between brick dimensions and electric wavelengths.

Moving to soft site shielding, another two options could be considered: vegetation fences and frequency selective surfaces. Both are more aesthetic and lighter than hard techniques, but their performance and cost are completely different.

We can use different vegetation species to create fences around gardens or to separate spaces within an office building inducing additional attenuation that improves the isolation of a wireless network. Depending on the species (very strong dependence) and on the wave polarization (vertical is more affected than horizontal), we measured additional losses of around 10 dB at 2.4 GHz and 21 dB at 5.8 GHz. These are valuable figures. However, a vegetation fence neither provides a constant attenuation at any point (as it depends on the configuration, density, etc. of each specimen on the fence) nor presents a constant of monotonically growing attenuation with frequency (as the water and other components' resonance frequencies have clear effects). Anyway, vegetal species must be selected considering the canopy density, the size and dimensions of the leaves, the movement of the wind induced in such leaves, the humidity capacity of the species, the seasonal variations, and giving priority to evergreen plants.

The other soft alternative is the addition of FSS design to the perimeter walls. FSSs are like filters in the open space, allowing the transmission of some frequencies with very low losses and blocking almost completely other bands. The variety of designs and implementation possibilities is very wide, providing an important range of applications and a good flexibility for designers when deciding the best option. Nowadays, it is a growing field among the scientific community for both cybersecurity applications and other areas of interest. The designers can manage several parameters and patterns to obtain attenuation exactly in the bands they need and the impact on the building is very low. Oppositely, the cost by area is higher than most of the previously commented solutions.

After analysing the behavior of those solutions against electromagnetic waves, we know that different materials interact on a different way to the radio waves, and we could obtain advantages on these responses using natural or artificial materials and/or designs to improve information security in terms of limiting possible accesses to our wireless networks.

The next step is the incorporation of that knowledge in the process of designing and constructing a building in a standard way. Thus, the proposal of adding new layers on BIM systems to consider the electromagnetic behavior of the different constructive elements and to predict the isolation characteristics of the building in terms of wireless communication systems and their protection against hacker attacks, should be the next step in architecture proposals. Then, cybersecurity at physical level would be included in a similar scale as thermal performance.

CONFLICTS OF INTEREST

The author declares that he has no conflicts of interest.

REFERENCES

[1] J. D. Day and H. Zimmermann, "The OSI reference model", *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334–1340, Dec. 1983. DOI: 10.1109/PROC.1983.12775.

[2] A. Devos, C. Vyncke, and A. Vander Vorst, "Simulation of the effect of site shielding on digital communication systems: From diffraction to global link performance", in *Proc. of 9th Int. Conf. Antennas Propag*., 1995, vol. 2, pp. 190–194. DOI: 10.1049/cp:19950412.

[3] C. J. Haslett and D. A. Jacklin, "Site shielding reduction due to transmission through buildings in a city centre environment", in *Proc. of 9th Int. Conf. Antennas Propag.*, 1995, vol. 2, pp. 37–41. DOI: 10.1049/cp:19950378.

[4] S. A. Bokhari, M. Keer, and F. E. Gardiol, "Site shielding of earthstation antennas", *IEEE Antennas Propag. Mag*., vol. 37, no. 1, pp. 7–24, Feb. 1995. DOI: 10.1109/74.370577.

[5] A. V. Alejos, M. G. Sánchez, and I. Cuiñas, "Measurement and analysis of propagation mechanisms at 40 GHz: Viability of site shielding forced by obstacles", *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3369–3380, Nov. 2008. DOI: 10.1109/TVT.2008.920052.

[6] D. Ferreira, I. Cuiñas, R. F. S. Caldeirinha, and T. R. Fernandes, "Hollow clay brick wall propagation analysis and modified brick design for enhanced WiFi coverage", *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 1, pp. 331–339, Jan. 2018. DOI: 10.1109/TAP.2017.2772028.

[7] I. Cuiñas, A. V. Alejos, and M. G. Sánchez, "Vegetal barriers for minimizing electromagnetic pollution at cellular phone bands", *Electronics Letters*, vol. 41, no. 6, pp. 340–341, Mar. 2005. DOI: 10.1049/el:20058001.

[8] P. Gómez, I. Cuiñas, A. V. Alejos, M. G. Sánchez, and J. A. Gay-Fernández, "Analysis of the performance of vegetation barriers to reduce electromagnetic pollution", *IET Microwaves, Antennas and Propagation*, vol. 5, no. 6, pp. 651–663, Apr. 2011. DOI: 10.1049/iet-map.2010.0158.

[9] P. Gómez, I. Cuiñas, A. V. Alejos, M. G. Sánchez, and R. F. S. Caldeirinha, "Shrub-blown time variability in attenuation and scattering at cellular frequencies", *IET Microwaves, Antennas and Propagation*, vol. 4, no. 4, pp. 526–542, Apr. 2010. DOI: 10.1049/iet-map.2009.0116.

[10] I. Cuiñas, P. Gómez, A. V. Alejos, and M. G. Sánchez, "Reducing electromagnetic pollution by shrub lines supported by lattice structures", *Electronics Letters*, vol. 45, no. 13, pp. 664–666, Jun. 2009. DOI: 10.1049/el.2009.0948.

[11] *IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE 802.11-2016, Dec. 2016.

[12] G. V. Trentini, "Partially reflecting sheet arrays", *IRE Trans. Antennas Propag.*, vol. 4, no. 4, pp. 666–671, 1956. DOI: 10.1109/TAP.1956.1144455.

[13] D. Ferreira, R. F. S. Caldeirinha, I. Cuiñas, and T. R. Fernandes, "A review of manufacturing materials and production methods for frequency-selective structures", *IEEE Antennas and Propagation Magazine*, vol. 60, no. 6, pp. 110–119, Dec. 2018. DOI: 10.1109/MAP.2018.2870583.

[14] D. Ferreira, R. F. S. Caldeirinha, I. Cuiñas, and T. R. Fernandes, "Square loop and slot frequency selective surfaces study for equivalent circuit model optimization", *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 9, pp. 3947–3955, Sep. 2015. DOI: 10.1109/TAP.2015.2444420.

[15] D. Ferreira, R. F. S. Caldeirinha, I. Cuiñas, and T. R. Fernandes, "Dual-band single-layer quarter ring frequency selective surface for Wi-Fi applications", *IET Microwaves, Antennas and Propagation*, vol. 10, no. 4, pp. 435–441, 2016. DOI: 10.1049/iet-map.2015.0641.

[16] D. Ferreira, R. F. S. Caldeirinha, I. Cuiñas, and T. R. Fernandes, "3D mechanically tunable square slot FSS", *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 1, pp. 242–250, 2017. DOI: 10.1109/TAP.2016.2631131.

[17] D. Ferreira, R. F. S. Caldeirinha, I. Cuiñas, and T. R. Fernandes, "Tunable square slot FSS equivalent circuit modelling and optimisation", *IET Microwaves, Antennas and Propagation*, vol. 11, no. 5, pp. 737–742, 2017. DOI: 10.1049/iet-map.2016.0540.

[18] D. Ferreira, I. Cuiñas, R. F. S. Caldeirinha, and T. R. Fernandes, "Multi-semicircle based single- and dual-band narrowband frequency selective surfaces", *IEEE Antennas and Propagation Magazine*, vol. 61, no. 2, pp. 32–39, Apr. 2019. DOI: 10.1109/MAP.2019.2895661.

[19] R. F. S. Caldeirinha, T. R. Fernandes, I. Cuiñas, and H. Rodrigues, "A framework for the inclusion of RF transparency parameters into BIM databases", in *Proc. of Microwaves and Optoelectronics Conference, IMOC 2019*, Aveiro, Portugal, 2019.