Progress In Electromagnetics Research C, Vol. 70, 83–90, 2016

Development of a Cyber-Secured Zone with Directive Antennas and Noise Generation

Joshua Haney[1], Jinxi Chen[2], and Sungkyun Lim[1, *]

Abstract—A wireless cyber secure zone has been created by controlling RF propagation using directive antennas and noise generation to establish a functional boundary for a wireless network. Directive microstrip patch antennas were constructed in the 2.4-GHz ISM band, and a commercial router was used to generate a wireless network on a specified channel. The FM transmitters for noise generation were set to the same channel in the 2.4-GHz ISM band, and the directive microstrip patch antennas were arranged facing outward creating an inner cyber secure zone for the wireless network. Outside the cyber secure zone, the wireless network was undetectable.

1. INTRODUCTION

Cyber security is a growing concern with the continued integration of technology in everyday life. For home, business, and industry, wireless systems tend to have the greatest security threats, but their mobility and convenient wireless networks are highly desirable by end users. Due to the broad coverage area, an attacker just has to be in range of the wireless access point, and they would have the opportunity to capture personal or classified data [1–4]. For this reason, companies and government entities have been targeted and have lost critical information, so more cyber secure oriented wireless networks are required. [5, 6] use noise generation in a secure zone around the transmitter to protect from attackers. With multiple antennas beamforming is used to communicate with the receiver outside of the secure zone. That is as long as the attacker is in the secure zone they will not be able to sense the transmitted signal. This method is good for transmitting information securely, but is not reasonable for areas such as offices or building where there are many devices inside needing to communicate constantly. In this paper, by controlling direction of radiation patterns of noise-generating antennas in wireless network communication, the cyber-secured zone is achieved.

Directive antennas play a critical role in this cyber-secured communication systems design. Some directive antenna designs can have a large and bulky profile, and they may not be suitable for establishing an electrical boundary [7]. Directive antennas for consideration were the Yagi-Uda antenna, the microstrip patch antenna, and the helical antenna [8, 9]. A closely spaced Yagi antennas can also allow for a decreased physical size without losing gain and radiation characteristics [10]. Ultimately, the microstrip patch antenna in the 2.4-GHz ISM band was chosen due to low profile, ease of fabrication, slim profile, reasonable directional gain, wide beamwidth, and mass production with cheap price.

The proposed system design shows that there is a central area with wireless devices that can communicate and not have their wireless data be collected from outside of a determined boundary. Figure 1 shows a model overview with internal wireless devices and outward facing noise generation antennas. These noise generation antennas create an internal area without inserted noise, and an external area that injects noise on the same frequency that the internal system operates on. This

Received 21 October 2016, Accepted 9 December 2016, Scheduled 18 December 2016

* Corresponding author: Sungkyun Lim (sklim@georgiasouthern.edu).

[1] Department of Electrical Engineering, Georgia Southern University, Statesboro, GA 30460, USA. [2] TDK Corp. of America, Peachtree City, GA 30269, USA.

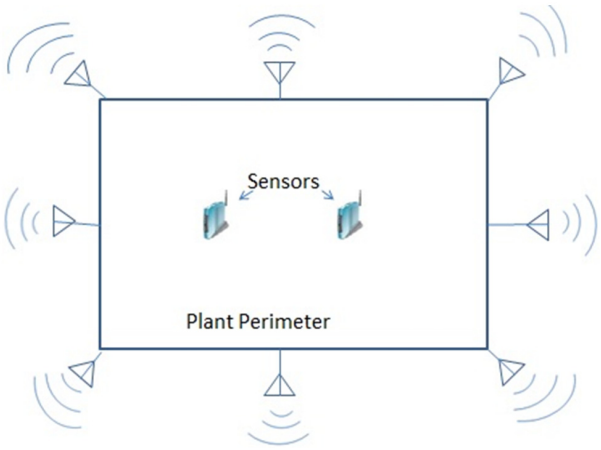


Figure 1. System model overview.

requires external attackers to do additional and excessive filtering, and it ultimately adds an additional barrier to access secure data. The noise generation system would provide another barrier for intruders, networks should still maintain high levels of digital security and cryptography [11].

With continued implementation of smart grid technology, this system would be economical and applicable on large and small scales for home area networks as well as larger business area networks to establish greater system integrity for each element being added to the grid [12, 13].

2. MICROSTRIP PATCH ANTENNA DESIGN IN SIMULATION AND MEASUREMENT

To determine the dimensions of the antenna to be used in the system, a microstrip patch antenna was designed, and its dimensions were optimized using a Genetic Algorithm (GA) [14–16]. The dimensions of the antenna was optimized by the GA for maximizing realized gain in the zenith direction for the desired ISM band frequency range. The cost function is shown in (1).

$$\text{Cost function} = (10 - \text{Realized Gain})\,[\text{dB}] \tag{1}$$

The results of the GA yielded the dimensions shown in Figure 2(a), and then it was subsequently fabricated as shown in Figure 2(b).

Upon completion of the microstrip patch antenna simulation, the constructed microstrip patch was measured and compared to the simulated results. Figure 3 shows the S_{11} of the antenna in both

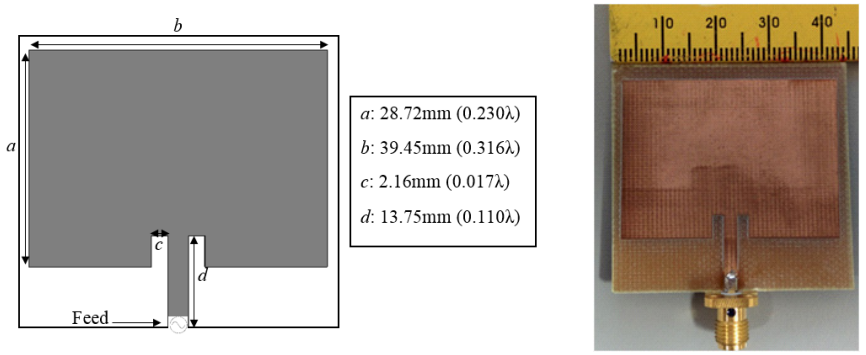


Figure 2. (a) Simulated microstrip patch design at 2.4 GHz, (b) fabricated 2.4 GHz microstrip patch antenna.

simulation and measurement. Although there is a slight frequency shift due to minor construction differences from the simulation, both −3-dB impedance bandwidths still cover the 2.4-GHz ISM band of 2.4 GHz to 2.4835 GHz [17]. −3-dB simulated impedance bandwidth is between 2.27 GHz and 2.52 GHz (10.6%), and −3-dB measured impedance bandwidth is between 2.30 GHz and 2.49 GHz (7.9%). Figure 4 shows the simulated and measured radiation patterns of the chosen microstrip patch geometry. In the E-plane the 3-dB simulated beamwidth is 98 degrees and the measured 3-dB beamwidth is 102 degrees. In the H-plane the 3-dB simulated beamwidth is 106 degrees and the measured 3-dB beamwidth is 82 degrees. Both the simulated and measured results agree fairly well. An operational beamwidth was also measured. The determination of operational beamwidth was done by placing the omnidirectional fixed gain and power antenna in close proximity of noise generation antenna. Then the receiver was maintained at a fixed arc in the direction of noise electromagnetic noise propagation. When the receiver detected a usable signal from the router, the angle was marked. With an operational beamwidth established, a linear distance can be calculated and applied to form an internal cyber secure zone. The measured operational beamwidth is 120 degrees. The maximum simulated realized gain is 3.6 dBi with a front to back ratio of 8.5 dB at 2.4 GHz. The maximum measured realized gain is 3.3 dBi with a front to back ratio of 11.2 dB at the same frequency.

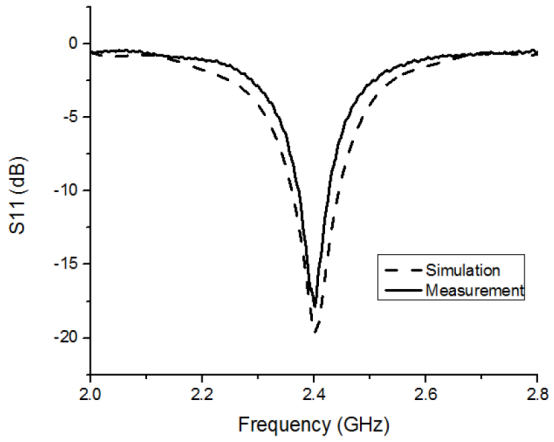


Figure 3. S_{11} of simulated and measured microstrip patch antenna.

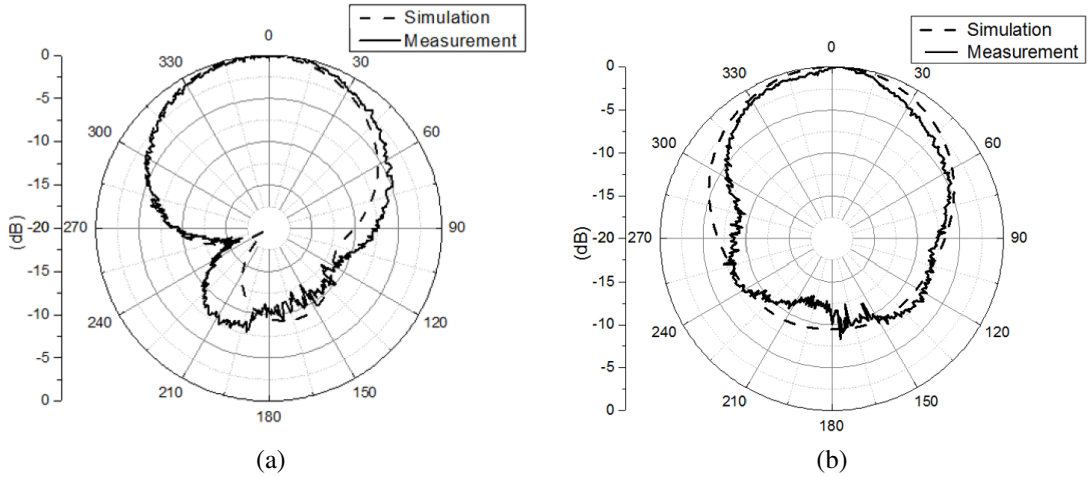
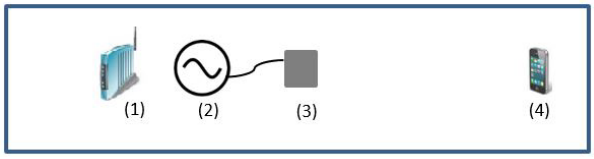


Figure 4. Simulated and measured radiation patterns in (a) E-plane, (b) H-plane.

3. EXPERIMENTAL SETUP AND RESULTS

A linear test was preliminarily performed using the FM transmitter [18] for generating noise signal, microstrip patch antenna, wireless router, and cell phone Wi-Fi analyzer. This linear test was performed in an empty hallway with the wireless router transmitting on channel 5 of the WLAN channels, and the noise signal generator also transmitting on channel 5. Channel 5 was chosen because it was seen that local Wi-Fi networks were not operating on this channel. This reduced any possible interference with other channels. Figures 5(a) and 6(a) show the diagram of the setup, 5(b) and 6(b) shows the physical locations for testing, and Figures 5(c) and 6(c) show the resultant graph of measured Wi-Fi routers in



Components/Icons:

(1) Wireless router

(2) Noise Signal Generator

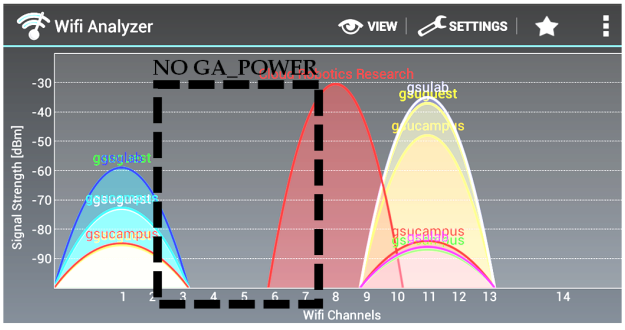
FM: Transmitter

(3) Microstrip Patch Antenna

(4) Cell Phone Wi-Fi Analyzer

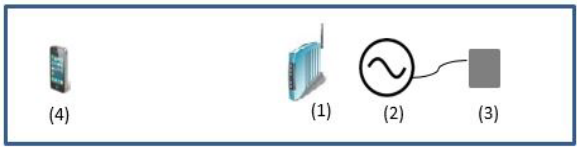
(a)

(b)



(c)

Figure 5. (a) Linear test conducted for proof of concept, (b) model of hallway, (c) wireless results.



Components/Icons:

(1) Wireless router

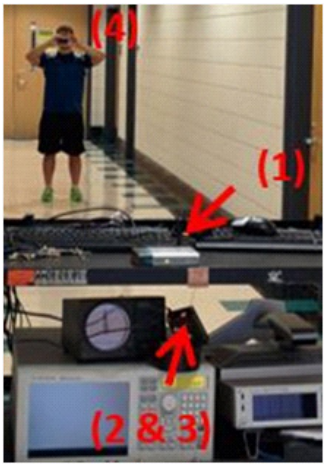
(2) Noise Signal Generator

FM: Transmitter

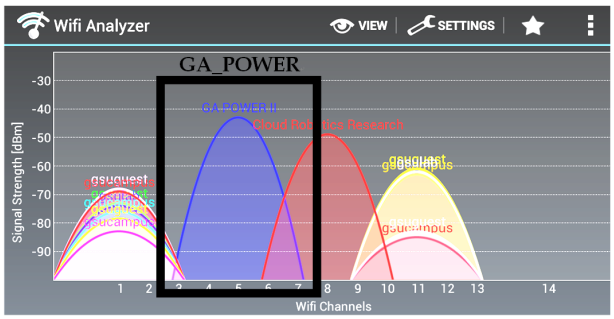
(3) Microstrip Patch Antenna

(4) Cell Phone Wi-Fi Analyzer

(a)



(b)



(c)

Figure 6. (a) Linear test conducted for proof of concept, (b) model of hallway, (c) wireless results.

the area. For the test, a router is projecting the named GA_POWER wireless network. The directive microstrip patch antenna is connected to the noise signal generator and is set up to point on the opposite side of the wireless router. In Figure 5, the noise signal generator is located between the wireless router and the cell phone Wi-Fi analyzer. As expected the GA_POWER wireless network cannot be seen in Figure 5(c) because of the generated noises. On the other hand, in Figure 6, the noise signal generator is no longer located between the wireless router and cell phone Wi-Fi analyzer. Now the GA_POWER wireless network can be easily seen in Figure 6(c) as well as being the strongest reading on the graph further giving sight to the strength of the security channel. Also note that the other networks in the area are still showing and accessible on both sides of the noise generator. Because it is on a channel unoccupied by other wireless networks, it will be easily protected without being detrimental to the performance of other local wireless networks.

Once the noise signal generator together with the directive microstrip patch antenna is shown to successfully eliminate the desired wireless network, an appropriate full scale test is performed as the next step. This takes setting up an established security perimeter using multiple antennas. In order to know the correct amount of microstrip patch antennas needed, the operational beamwidth was needed. This is the area where the microstrip patch antenna effectively eliminates the wireless networked being sensed. The test for this is modeled in Figure 7(a) and the measured operational beamwidth of 120 degrees was used for the design.

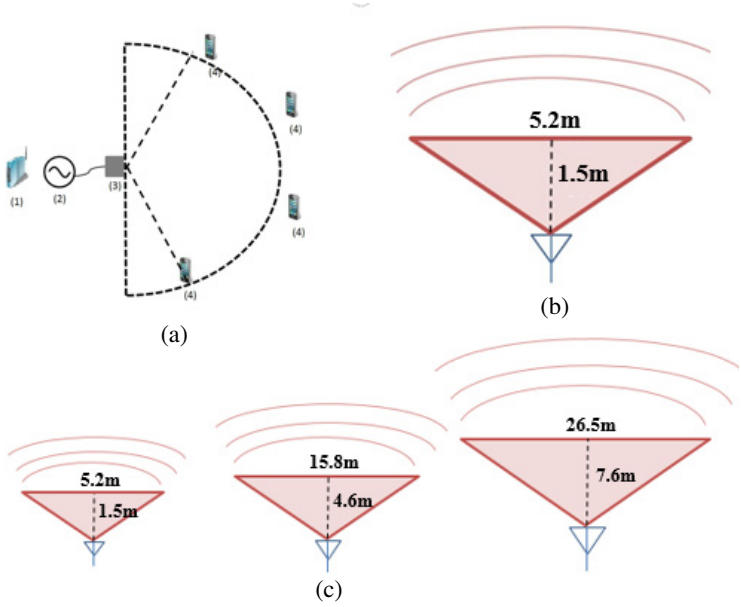


Figure 7. (a) Testing to determine the operational beamwidth of noise generation antenna. (b) The resulting 2D model of the direction and range of the antenna. (c) The 2D model shown to three different scales.

Using the Friis transmission formula, a scalable model can be designed. This is due to the relation of gains in the wireless networks and the noise transmission antennas [19, 20]. Friis transmission Equation (2), where P_R is the power available at the input of the receiving antenna, P_T is the output power of the transmitting antenna, G_T and G_R are the respective transmitting and receiving gains of the antenna, and R is the distance between the antennas. Assuming all the values in this equation remain constant, then the values in the Signal-to-Noise ratio equation (SNR) in Equation (3) should also remain constant. In equation (3) P_{signal} is the power of the signal being transmitted, while P_{noise} is the power of the noise, or in this case the noise being transmitted. By transmitting a higher noise power in relation to the transmitted power, it will become difficult for anyone to access the wireless

network.

$$P_R = \frac{P_T G_T G_R \lambda^2}{(4\pi R)^2} \tag{2}$$

$$\text{SNR} = \frac{P_{\text{signal}}}{P_{\text{noise}}} \tag{3}$$

For the model an arbitrary zenith distance of 5 feet was chosen, and a subsequent calculation of 17 feet (5.2 meters) was determined from the operational beamwidth as shown in Figure 7(b). This 2D model can be scaled based on known distances for the intended cyber secure zone access points as shown in Figure 7(c). This allows for a variability in setup making the design adaptable to different

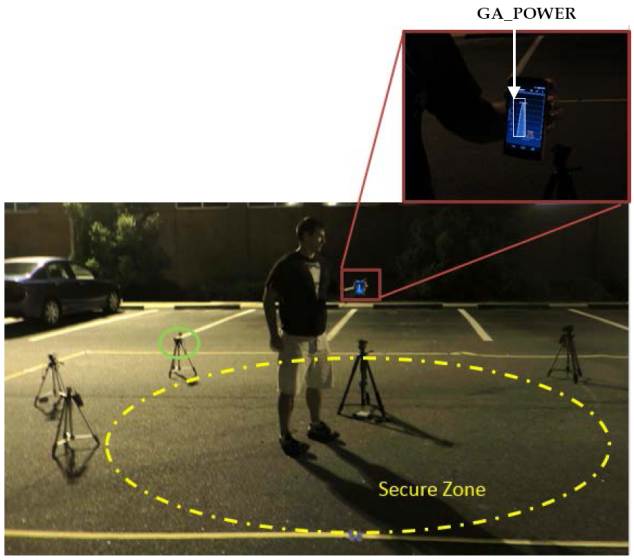


Figure 8. Wireless results inside the secure zone.

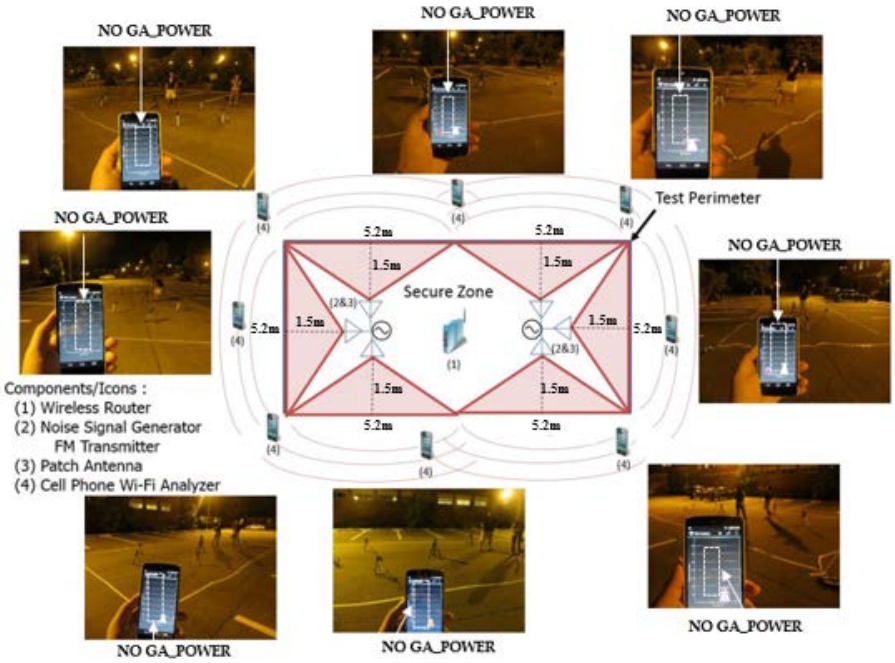


Figure 9. Wireless results outside the secure zone.

buildings and areas.

With the 2D model of the noise generating antenna in place, a 5.2 meter by 10.4 meter test area was established and marked. The wireless router was placed in the center of the intended secure zone, and the noise generation antennas were all placed facing outward as shown Figure 8. The receiving antenna and network detection scheme is used with a standard Wi-Fi antenna that is 802.11 a/b/g/n compliant and integrated into a cellular phone. In proximity to the wireless router, the network was clearly detectable and ready for use as shown in Figure 8. Figure 9 shows that the network that was previously detected inside the secure zone, is now masked due interference and change in the associated channel's SNR. It is also noted that other channels and networks are detectable and operationally unaffected outside of the specified channel for securing the internal wireless network.

4. CONCLUSIONS

A wireless secure zone was modeled by using antennas with noise signal generators, wireless router, and cell phone Wi-Fi analyzer around a central wireless network. Directive antennas were used for controlling the direction noise generation. A directive microstrip patch antenna was chosen for its slim profile, gain, wide beamwidth, and ease of construction. After modelling of the noise generation effective area, a full internal cyber secure zone can be created. This system will be potentially useful to enhance cyber security in wireless networks implemented in homes, offices, sensor networks, and buildings requiring secure communication such as power plants and government buildings.

ACKNOWLEDGMENT

This work was supported by Southern Company and Georgia Power.

REFERENCES

1. Eun-Kyu, L., M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, Vol. 50, No. 8, 46–52, 2012.
2. Erol-Katntarci, M. and H. T. Mouftah, "Energy efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 1, 179–197, 2015.
3. Hussain, S., M. J. Ikram, and N. Arshad, "A low cost implementation of home area networks for home energy management systems," *2014 IEEE Fourth Int. Conf. on Big Data and Cloud Computing*, 2014.
4. Kominos, N., E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges, and countermeasures," *Communications Surveys & Tutorials*, Vol. 16, No. 4, 2014.
5. Romero-Zurita, N., D. Mclernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, Vol. 8, No. 8, 1248–1257, 2014.
6. Khisti, A. and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, 3088–3104, 2010.
7. Balanis, C. A., *Antenna Theory: Analysis and Design*, 3rd Edition, John Wiley & Sons, New York, 2005.
8. Stutzman, W. L., *Antenna Theory and Design*, John Wiley & Sons, New Jersey, 1998.
9. Johnson, R. C., *Antenna Engineering Handbook*, McGraw-Hill, New York, 1993.
10. Lim, S. and H. Ling, "Design of a closely spaced, folded Yagi antenna," *IEEE Antenna Wireless Propag. Lett.*, 302–305, 2006.
11. Kartalopoulos, S. V., "A primer on cryptography in communications," *IEEE Commun. Mag.*, Vol. 44, No. 4, 146–151, 2006.
12. Vajjiravelu, S. and A. Punitha, "Survey on wireless technologies and security procedures," *Int. Conf. on Information Communication and Embedded Systems (ICICES)*, 2013.

13. Su, H., M. Qiu, and H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," *IEEE Commun. Mag.*, Vol. 50, No. 8, 62–68, 2012.
14. Rahmat-Sami, Y. and E. Michielssen, *Electromagnetic Optimization by Genetic Algorithms*, Wiley, New York, 1999.
15. Azaro, R., F. G. B. De Natale, M. Donelli, A. Massa, and E. Zeni, "Optimized design of a multifunction/multiband antenna for automotive rescue systems," *IEEE Trans. Antennas Propag.*, Vol. 54, No. 2, 392–400, 2006.
16. Donelli, M., I. Craddock, D. Gibbins, and M. Sarafianou, "A three-dimensional time domain microwave imaging method for breast cancer detection based on an evolutionary algorithm," *Progress In Electromagnetics Research M*, Vol. 18, 179–195, 2011.
17. http://www.ecfr.gov, "Electronic code of federal regulations".
18. http://support.radioshack.com/support_video/doc66/66337.pdf, "Room to Room Audio/Video Sender," RadioShack.
19. Chu, T. S., "An approximate generalization of the Friis transmission formula," *Proc. IEEE*, 296–297, 1965.
20. Hogg, D. C., "Fun with the Friis free-space transmission formula," *IEEE Antennas Propag. Mag.*, Vol. 35, No. 4, 33–35, 1993.