Realization of Cyber-Security for IEEE 802.15-Based Wireless Sensors by Controlling the Propagation of RF Signals

Joseph P. Meador, Jinxi Chen, Yen Le*, and Sungkyun Lim
Department of Electrical Engineering
Georgia Southern University
Statesboro, GA 30460, U.S.A.

Due to the versatility and increased use of wireless systems, the need to secure these systems increases as well. Security of wireless systems is critical for governments, companies and homes that are transmitting private or classified data. To protect this data, encryption schemes have been employed to prevent or delay a system intruder from accessing the data. Recently, IEEE 802.15-based technologies, in particular ZigBee, have become targets of the hacking community. Traditional Wi-Fi hacking software has been adapted to sniff ZigBee packet data.

In this paper, more secure implementation for IEEE 802.15-based wireless sensor technologies is provided. Since security cannot be enhanced in currently available products without completely rewriting the security protocol, an approach to secure the wireless system by controlling the propagation of RF signals with noise generators is suggested. Using the noise generators with directive antennas and then placing them on the perimeter of a building, a wireless system can be secured if these outward facing antennas generate noise at a higher relative power level than the internal wireless router. Model overview of wireless security system using outward facing directive antennas on the boundary of a wireless network is shown in Fig. 1. A microstrip patch antenna with directive characteristics was simulated and shown to have a 3-dB beamwidth of 98° which can then be modeled and allowed to be placed strategically for a given wireless network's geometry. The patch antenna and system is designed using the 2.4-GHz IEEE 802.15 band and is tested with equipment that is designed for operating in the part of the RF spectrum. The results of the wireless system show that the secured wireless system is completely invisible to any individual outside of the secured area.

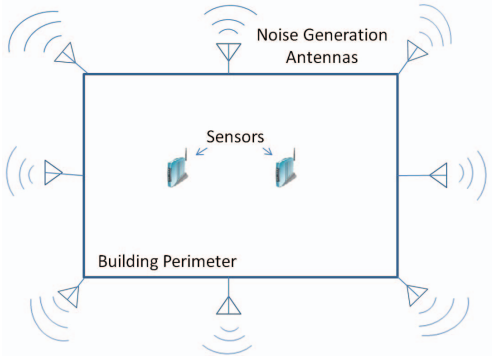

Fig. 1. System Model Overview